# 约74970个

# Windows : User management

Microsoft Windows 'Account Operators' Group User List

Microsoft Windows 'Administrators' Group User List

Microsoft Windows 'Backup Operators' Group User List

Microsoft Windows 'Domain Administrators' Group User List

Microsoft Windows 'Print Operators' Group User List

Microsoft Windows 'Replicator' Group User List

Microsoft Windows 'Server Operators' Group User List

Microsoft Windows - Local Users Information : Automatically Disabled Accounts

Microsoft Windows - Local Users Information : Can't Change Password

Microsoft Windows - Local Users Information : Disabled Accounts

Microsoft Windows - Local Users Information : Never Changed Passwords

Microsoft Windows - Local Users Information : Passwords Never Expire

Microsoft Windows - Local Users Information : User Has Never Logged In

Microsoft Windows - Users Information : Automatically Disabled Accounts

Microsoft Windows - Users Information : Can't Change Password

Microsoft Windows - Users Information : Disabled Accounts

Microsoft Windows - Users Information : Never Changed Password

Microsoft Windows - Users Information : Passwords Never Expire

Microsoft Windows - Users Information : User Has Never Logged In

Microsoft Windows Domain User Information

Microsoft Windows Guest Account Belongs to a Group

Microsoft Windows Local User Information

Microsoft Windows SAM user enumeration

Microsoft Windows SMB : Obtains the Password Policy

Microsoft Windows User Aliases List

Microsoft Windows User Groups List

SMB Use Domain SID to Enumerate Users

SMB Use Host SID to Enumerate Local Users

SMB Use Host SID to Enumerate Local Users Without Credentials

# Windows : Microsoft Bulletins

ADV180002: Microsoft SQL Server January 2018 Security Update (Meltdown) (Spectre)

Intel Microcode Updates for Windows 10 / Windows Server 2016 / Windows Server 2019 (May 2019) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB3211308: Security Update for Hyper-V in Windows Server 2008 (April 2017)

KB3217841: Security Update for the Hyper-V Denial of Service Vulnerability (April 2017)

KB4014793: Microsoft Wordpad Remote Code Execution vulnerability (April 2017)

KB4015067: Security Update for the Scripting Engine Memory Corruption Vulnerability (April 2017)

KB4015068: Security Update for the LDAP Elevation of Privilege Vulnerability (April 2017)

KB4015195: Security Update for the Win32k Information Disclosure Vulnerability (April 2017)

KB4015217: Windows 10 1607 April 2017 Cumulative Update

KB4015219: Windows 10 Version 1511 April 2017 Cumulative Update

KB4015221: Windows 10 Version 1507 April 2017 Cumulative Update

KB4015380: Security Update for the ATMFD.dll Information Disclosure Vulnerability (April 2017)

KB4015383: Security Updates for the libjpeg Information Disclosure Vulnerability (April 2017)

KB4015583: Windows 10 Version 1703 April 2017 Cumulative Update

KB4016871: Windows 10 Version 1703 May 2017 Cumulative Update

KB4018483: Security update for Adobe Flash Player (April 2017)

KB4018588: Security Update for Microsoft Exchange Server

KB4019472: Windows 10 Version 1607 and Windows Server 2016 May 2017 Cumulative Update

KB4019473: Windows 10 Version 1511 May 2017 Cumulative Update

KB4019474: Windows 10 Version 1507 May 2017 Cumulative Update

KB4020535: Security Update for the Scripting Engine Memory Corruption Vulnerability (May 2017)

KB4020821: Security update for Adobe Flash Player (May 2017)

KB4022714: Windows 10 Version 1511 June 2017 Cumulative Update

KB4022715: Windows 10 Version 1607 and Windows Server 2016 June 2017 (CVE-2017-8529)

KB4022715: Windows 10 Version 1607 and Windows Server 2016 June 2017 Cumulative Update

KB4022725: Windows 10 Version 1703 June 2017 Cumulative Update

KB4022727: Windows 10 Version 1507 June 2017 Cumulative Update

KB4022730: Security update for Adobe Flash Player (June 2017)

KB4025338: Windows 10 July 2017 Cumulative Update

KB4025339: Windows 10 Version 1607 and Windows Server 2016 July 2017 Cumulative Update

KB4025342: Windows 10 Version 1703 July 2017 Cumulative Update

KB4025344: Windows 10 Version 1511 July 2017 Cumulative Update

KB4025376: Security update for Adobe Flash Player (July 2017)

KB4034658: Windows 10 Version 1607 and Windows Server 2016 August 2017 Cumulative Update

KB4034660: Windows 10 Version 1511 August 2017 Cumulative Update

KB4034662: Security update for Adobe Flash Player (August 2017)

KB4034668: Windows 10 August 2017 Cumulative Update

KB4034674: Windows 10 Version 1703 August 2017 Cumulative Update

KB4036996: Security Update for SQL Server (August 2017)

KB4038781: Windows 10 September 2017 Cumulative Update

KB4038782: Windows 10 Version 1607 and Windows Server 2016 September 2017 Cumulative Update

KB4038783: Windows 10 Version 1511 September 2017 Cumulative Update

KB4038788: Windows 10 Version 1703 September 2017 Cumulative Update

KB4038806: Security update for Adobe Flash Player (September 2017)

KB4041676: Windows 10 Version 1703 October 2017 Cumulative Update (KRACK)

KB4041689: Windows 10 Version 1511 October 2017 Cumulative Update (KRACK)

KB4041691: Windows 10 Version 1607 and Windows Server 2016 October 2017 Cumulative Update (KRACK)

KB4042895: Windows 10 October 2017 Cumulative Update (KRACK)

KB4048951: Security update for Adobe Flash Player (November 2017)

KB4048952: Windows 10 Version 1511 November 2017 Cumulative Update

KB4048953: Windows 10 Version 1607 and Windows Server 2016 November 2017 Cumulative Update

KB4048954: Windows 10 Version 1703 November 2017 Cumulative Update

KB4048955: Windows 10 Version 1709 and Windows Server Version 1709 November 2017 Cumulative Update

KB4048956: Windows 10 LTSB November 2017 Cumulative Update

KB4049179: Security update for Adobe Flash Player (October 2017)

KB4053577: Security update for Adobe Flash Player (December 2017)

KB4053578: Windows 10 Version 1511 December 2017 Security Update

KB4053579: Windows 10 Version 1607 and Windows Server 2016 December 2017 Security Update

KB4053580: Windows 10 Version 1703 December 2017 Security Update

KB4053581: Windows 10 December 2017 Security Update

KB4054517: Windows 10 Version 1709 and Windows Server Version 1709 December 2017 Security Update

KB4056887: Security update for Adobe Flash Player (January 2018)

KB4056888: Windows 10 Version 1511 January 2018 Security Update (Meltdown)(Spectre)

KB4056890: Windows 10 Version 1607 and Windows Server 2016 January 2018 Security Update (Meltdown)(Spectre)

KB4056891: Windows 10 Version 1703 January 2018 Security Update (Meltdown)(Spectre)

KB4056892: Windows 10 Version 1709 and Windows Server Version 1709 January 2018 Security Update (Meltdown)(Spectre)

KB4056893: Windows 10 LTSB January 2018 Security Update (Meltdown)(Spectre)

KB4056897: Windows 7 and Windows Server 2008 R2 January 2018 Security Update (Meltdown)(Spectre)

KB4056898: Windows 8.1 and Windows Server 2012 R2 January 2018 Security Update (Meltdown)(Spectre)

KB4056899: Windows Server 2012 January 2018 Security Update

KB4074587: Windows 7 and Windows Server 2008 R2 February 2018 Security Update

KB4074588: Windows 10 Version 1709 and Windows Server Version 1709 February 2018 Security Update

KB4074589: Windows Server 2012 February 2018 Security Update

KB4074590: Windows 10 Version 1607 and Windows Server 2016 February 2018 Security Update (Meltdown)(Spectre)

KB4074591: Windows 10 Version 1511 February 2018 Security Update (Meltdown)(Spectre)

KB4074592: Windows 10 Version 1703 February 2018 Security Update (Meltdown)(Spectre)

KB4074595: Security update for Adobe Flash Player (February 2018)

KB4074596: Windows 10 February 2018 Security Update (Meltdown)(Spectre)

KB4074597: Windows 8.1 and Windows Server 2012 R2 February 2018 Security Update

KB4088776: Windows 10 Version 1709 and Windows Server Version 1709 March 2018 Security Update

KB4088779: Windows 10 Version 1511 March 2018 Security Update

KB4088782: Windows 10 Version 1703 March 2018 Security Update

KB4088785: Security update for Adobe Flash Player (March 2018)

KB4088786: Windows 10 March 2018 Security Update

KB4088787: Windows 10 Version 1607 and Windows Server 2016 March 2018 Security Update

KB4088878: Windows 7 and Windows Server 2008 R2 March 2018 Security Update (Meltdown)(Spectre)

KB4088879: Windows 8.1 and Windows Server 2012 R2 March 2018 Security Update (Meltdown)(Spectre)

KB4088880: Windows Server 2012 March 2018 Security Update (Meltdown)(Spectre)

KB4093107: Windows 10 Version 1703 April 2018 Security Update

KB4093108: Windows 7 and Windows Server 2008 R2 April 2018 Security Update

KB4093109: Windows 10 Version 1511 April 2018 Security Update

KB4093110: Security update for Adobe Flash Player (April 2018)

KB4093111: Windows 10 April 2018 Security Update

KB4093112: Windows 10 Version 1709 and Windows Server Version 1709 April 2018 Security Update (Meltdown)(Spectre)

KB4093115: Windows 8.1 and Windows Server 2012 R2 April 2018 Security Update

KB4093119: Windows 10 Version 1607 and Windows Server 2016 April 2018 Security Update

KB4093122: Windows Server 2012 April 2018 Security Update

KB4100480: Windows Kernel Elevation of Privilege Vulnerability

KB4103712: Windows 7 and Windows Server 2008 R2 May 2018 Security Update

KB4103715: Windows 8.1 and Windows Server 2012 R2 May 2018 Security Update

KB4103716: Windows 10 May 2018 Security Update

KB4103721: Windows 10 Version 1803 and Windows Server Version 1803 May 2018 Security Update

KB4103723: Windows 10 Version 1607 and Windows Server 2016 May 2018 Security Update

KB4103726: Windows Server 2012 May 2018 Security Update

KB4103727: Windows 10 Version 1709 and Windows Server Version 1709 May 2018 Security Update

KB4103729: Security update for Adobe Flash Player (May 2018)

KB4103731: Windows 10 Version 1703 May 2018 Security Update

KB4284819: Windows 10 Version 1709 and Windows Server Version 1709 June 2018 Security Update

KB4284835: Windows 10 Version 1803 and Windows Server Version 1803 June 2018 Security Update

KB4284846: Windows Server 2012 June 2018 Security Update

KB4284860: Windows 10 June 2018 Security Update

KB4284867: Windows 7 and Windows Server 2008 R2 June 2018 Security Update

KB4284874: Windows 10 Version 1703 June 2018 Security Update

KB4284878: Windows 8.1 and Windows Server 2012 R2 June 2018 Security Update

KB4284880: Windows 10 Version 1607 and Windows Server 2016 June 2018 Security Update

KB4287903: Security update for Adobe Flash Player (June 2018)

KB4338814: Windows 10 Version 1607 and Windows Server 2016 July 2018 Security Update

KB4338819: Windows 10 Version 1803 and Windows Server Version 1803 July 2018 Security Update

KB4338820: Windows Server 2012 July 2018 Security Update

KB4338823: Windows 7 and Windows Server 2008 R2 July 2018 Security Update

KB4338824: Windows 8.1 and Windows Server 2012 R2 July 2018 Security Update

KB4338825: Windows 10 Version 1709 and Windows Server Version 1709 July 2018 Security Update

KB4338826: Windows 10 Version 1703 July 2018 Security Update

KB4338829: Windows 10 July 2018 Security Update

KB4338832: Security update for Adobe Flash Player (July 2018)

KB4343885: Windows 10 Version 1703 August 2018 Security Update (Foreshadow)

KB4343887: Windows 10 Version 1607 and Windows Server 2016 August 2018 Security Update (Foreshadow)

KB4343888: Windows 8.1 and Windows Server 2012 R2 August 2018 Security Update (Foreshadow)

KB4343892: Windows 10 August 2018 Security Update (Foreshadow)

KB4343896: Windows Server 2012 August 2018 Security Update (Foreshadow)

KB4343897: Windows 10 Version 1709 And Windows Server Version 1709 August 2018 Security Update (Foreshadow)

KB4343899: Windows 7 and Windows Server 2008 R2 August 2018 Security Update (Foreshadow)

KB4343902: Security update for Adobe Flash Player (August 2018)

KB4343909: Windows 10 Version 1803 and Windows Server Version 1803 August 2018 Security Update (Foreshadow)

KB4457128: Windows 10 Version 1803 and Windows Server Version 1803 September 2018 Security Update

KB4457131: Windows 10 Version 1607 and Windows Server 2016 September 2018 Security Update

KB4457132: Windows 10 September 2018 Security Update

KB4457138: Windows 10 Version 1703 September 2018 Security Update

KB4457140: Windows Server 2012 September 2018 Security Update

KB4457142: Windows 10 Version 1709 and Windows Server Version 1709 September 2018 Security Update

KB4457143: Windows 8.1 and Windows Server 2012 R2 September 2018 Security Update

KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update

KB4457146: Security update for Adobe Flash Player (September 2018)

KB4457984: Windows Server 2008 September 2018 Security Update

KB4462915: Windows 7 and Windows Server 2008 R2 October 2018 Security Update

KB4462917: Windows 10 Version 1607 and Windows Server 2016 October 2018 Security Update

KB4462918: Windows 10 Version 1709 and Windows Server Version 1709 October 2018 Security Update

KB4462919: Windows 10 Version 1803 and Windows Server Version 1803 October 2018 Security Update

KB4462922: Windows 10 October 2018 Security Update

KB4462931: Windows Server 2012 October 2018 Security Update

KB4462937: Windows 10 Version 1703 October 2018 Security Update

KB4462941: Windows 8.1 and Windows Server 2012 R2 October 2018 Security Update

KB4463104: Windows Server 2008 October 2018 Security Update

KB4464330: Windows 10 Version 1809 and Windows Server 2019 October 2018 Security Update

KB4465659 BitLocker Security Feature Bypass Vulnerability

KB4465660 BitLocker Security Feature Bypass Vulnerability

KB4465661 BitLocker Security Feature Bypass Vulnerability

KB4465663 BitLocker Security Feature Bypass Vulnerability

KB4465664 BitLocker Security Feature Bypass Vulnerability

KB4467106: Windows 7 and Windows Server 2008 R2 November 2018 Security Update

KB4467678: Windows Server 2012 November 2018 Security Update

KB4467680: Windows 10 November 2018 Security Update

KB4467686: Windows 10 Version 1709 and Windows Server Version 1709 November 2018 Security Update

KB4467691: Windows 10 Version 1607 and Windows Server 2016 November 2018 Security Update

KB4467694: Security update for Adobe Flash Player (November 2018)

KB4467696: Windows 10 Version 1703 November 2018 Security Update

KB4467700: Windows Server 2008 November 2018 Security Update

KB4467702: Windows 10 Version 1803 and Windows Server Version 1803 November 2018 Security Update

KB4467703: Windows 8.1 and Windows Server 2012 R2 November 2018 Security Update

KB4467708: Windows 10 Version 1809 and Windows Server 2019 November 2018 Security Update

KB4471319: Windows Server 2008 December 2018 Security Update

KB4471321: Windows 10 Version 1607 and Windows Server 2016 December 2018 Security Update

KB4471322: Windows 8.1 and Windows Server 2012 R2 December 2018 Security Update

KB4471323: Windows 10 December 2018 Security Update

KB4471324: Windows 10 Version 1803 and Windows Server Version 1803 December 2018 Security Update

KB4471326: Windows Server 2012 December 2018 Security Update

KB4471327: Windows 10 Version 1703 December 2018 Security Update

KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update

KB4471329: Windows 10 Version 1709 and Windows Server Version 1709 December 2018 Security Update

KB4471331: Security update for Adobe Flash Player (December 2018)

KB4471332: Windows 10 Version 1809 and Windows Server 2019 December 2018 Security Update

KB4477029: Security update for Adobe Flash Player (November 2018)

KB4480116: Windows 10 Version 1809 and Windows Server 2019 January 2019 Security Update

KB4480957: Windows Server 2008 January 2019 Security Update

KB4480960: Windows 7 and Windows Server 2008 R2 January 2019 Security Update

KB4480961: Windows 10 Version 1607 and Windows Server 2016 January 2019 Security Update

KB4480962: Windows 10 January 2019 Security Update

KB4480964: Windows 8.1 and Windows Server 2012 R2 January 2019 Security Update

KB4480966: Windows 10 Version 1803 and Windows Server Version 1803 January 2019 Security Update

KB4480972: Windows Server 2012 January 2019 Security Update

KB4480973: Windows 10 Version 1703 January 2019 Security Update

KB4480978: Windows 10 Version 1709 and Windows Server Version 1709 January 2019 Security Update

KB4483228: Windows 10 December 2018 OOB Security Update

KB4483229: Windows 10 Version 1607 and Windows Server 2016 December 2018 OOB Security Update

KB4483230: Windows 10 Version 1703 December 2018 OOB Security Update

KB4483232: Windows 10 Version 1709 and Windows Server Version 1709 December 2018 OOB Security Update

KB4483234: Windows 10 Version 1803 and Windows Server Version 1803 December 2018 OOB Security Update

KB4483235: Windows 10 Version 1809 and Windows Server 2019 December 2018 OOB Security Update

KB4486564: Windows 7 and Windows Server 2008 R2 February 2019 Security Update

KB4486993: Windows Server 2012 February 2019 Security Update

KB4486996: Windows 10 Version 1709 and Windows Server Version 1709 February 2019 Security Update

KB4487017: Windows 10 Version 1803 and Windows Server Version 1803 February 2019 Security Update

KB4487018: Windows 10 February 2019 Security Update

KB4487019: Windows Server 2008 February 2019 Security Update

KB4487020: Windows 10 Version 1703 February 2019 Security Update

KB4487026: Windows 10 Version 1607 and Windows Server 2016 February 2019 Security Update

KB4487028: Windows 8.1 and Windows Server 2012 R2 February 2019 Security Update

KB4487038: Security update for Adobe Flash Player (February 2019)

KB4487044: Windows 10 Version 1809 and Windows Server 2019 February 2019 Security Update

KB4489868: Windows 10 Version 1803 and Windows Server Version 1803 March 2019 Security Update

KB4489871: Windows 10 Version 1703 March 2019 Security Update

KB4489872: Windows 10 March 2019 Security Update

KB4489876: Windows Server 2008 March 2019 Security Update

KB4489882: Windows 10 Version 1607 and Windows Server 2016 March 2019 Security Update

KB4489883: Windows 8.1 and Windows Server 2012 R2 March 2019 Security Update

KB4489884: Windows Server 2012 March 2019 Security Update

KB4489885: Windows 7 and Windows Server 2008 R2 March 2019 Security Update

KB4489886: Windows 10 Version 1709 and Windows Server Version 1709 March 2019 Security Update

KB4489899: Windows 10 Version 1809 and Windows Server 2019 March 2019 Security Update

KB4493441: Windows 10 Version 1709 and Windows Server Version 1709 April 2019 Security Update

KB4493448: Windows 7 and Windows Server 2008 R2 April 2019 Security Update

KB4493450: Windows Server 2012 April 2019 Security Update

KB4493458: Windows Server 2008 April 2019 Security Update

KB4493464: Windows 10 Version 1803 and Windows Server Version 1803 April 2019 Security Update

KB4493467: Windows 8.1 and Windows Server 2012 R2 April 2019 Security Update

KB4493470: Windows 10 Version 1607 and Windows Server 2016 April 2019 Security Update

KB4493474: Windows 10 Version 1703 April 2019 Security Update

KB4493475: Windows 10 April 2019 Security Update

KB4493478: Security update for Adobe Flash Player (April 2019)

KB4493509: Windows 10 Version 1809 and Windows Server 2019 April 2019 Security Update

KB4494440: Windows 10 Version 1607 and Windows Server 2016 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4494441: Windows 10 Version 1809 and Windows Server 2019 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4497932: Security update for Adobe Flash Player (May 2019)

KB4499154: Windows 10 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4499158: Windows Server 2012 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4499165: Windows 8.1 and Windows Server 2012 R2 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4499167: Windows 10 Version 1803 and Windows Server Version 1803 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4499175: Windows 7 and Windows Server 2008 R2 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (BlueKeep)

KB4499179: Windows 10 Version 1709 and Windows Server Version 1709 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4499180: Windows Server 2008 and Windows Vista SP2 May 2019 Security Update (BlueKeep)

KB4499181: Windows 10 Version 1703 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

KB4503263: Windows Server 2012 June 2019 Security Update

KB4503267: Windows 10 Version 1607 and Windows Server 2016 June 2019 Security Update

KB4503269: Windows 7 and Windows Server 2008 R2 June 2019 Security Update

KB4503279: Windows 10 Version 1703 June 2019 Security Update

KB4503284: Windows 10 Version 1709 June 2019 Security Update

KB4503286: Windows 10 Version 1803 June 2019 Security Update

KB4503287: Windows Server 2008 June 2019 Security Update

KB4503290: Windows 8.1 and Windows Server 2012 R2 June 2019 Security Update

KB4503291: Windows 10 June 2019 Security Update

KB4503293: Windows 10 Version 1903 June 2019 Security Update

KB4503308: Security update for Adobe Flash Player (June 2019)

KB4503327: Windows 10 Version 1809 and Windows Server 2019 June 2019 Security Update

KB4507435: Windows 10 Version 1803 July 2019 Security Update (SWAPGS)

KB4507450: Windows 10 Version 1703 July 2019 Security Update (SWAPGS)

KB4507453: Windows 10 Version 1903 July 2019 Security Update (SWAPGS)

KB4507455: Windows 10 Version 1709 July 2019 Security Update (SWAPGS)

KB4507456: Windows 7 and Windows Server 2008 R2 July 2019 Security Update (SWAPGS)

KB4507457: Windows 8.1 and Windows Server 2012 R2 July 2019 Security Update (SWAPGS)

KB4507458: Windows 10 July 2019 Security Update (SWAPGS)

KB4507460: Windows 10 Version 1607 and Windows Server 2016 July 2019 Security Update (SWAPGS)

KB4507461: Windows Server 2008 July 2019 Security Update (SWAPGS)

KB4507464: Windows Server 2012 July 2019 Security Update (SWAPGS)

KB4507469: Windows 10 Version 1809 and Windows Server 2019 July 2019 Security Update (SWAPGS)

KB4511553: Windows 10 Version 1809 and Windows Server 2019 August 2019 Security Update

KB4512482: Windows Server 2012 August 2019 Security Update

KB4512486: Windows 7 and Windows Server 2008 R2 August 2019 Security Update

KB4512489: Windows 8.1 and Windows Server 2012 R2 August 2019 Security Update

KB4512491: Windows Server 2008 August 2019 Security Update

KB4512497: Windows 10 August 2019 Security Update

KB4512501: Windows 10 Version 1803 August 2019 Security Update

KB4512507: Windows 10 Version 1703 August 2019 Security Update

KB4512508: Windows 10 Version 1903 August 2019 Security Update

KB4512516: Windows 10 Version 1709 August 2019 Security Update

KB4512517: Windows 10 Version 1607 and Windows Server 2016 August 2019 Security Update

KB4512578: Windows 10 Version 1809 and Windows Server 2019 September 2019 Security Update

KB4515384: Windows 10 Version 1903 September 2019 Security Update

KB4516033: Windows 7 and Windows Server 2008 R2 September 2019 Security Update

KB4516044: Windows 10 Version 1607 and Windows Server 2016 September 2019 Security Update

KB4516051: Windows Server 2008 September 2019 Security Update

KB4516058: Windows 10 Version 1803 September 2019 Security Update

KB4516062: Windows Server 2012 September 2019 Security Update

KB4516064: Windows 8.1 and Windows Server 2012 R2 September 2019 Security Update

KB4516066: Windows 10 Version 1709 September 2019 Security Update

KB4516068: Windows 10 Version 1703 September 2019 Security Update

KB4516070: Windows 10 September 2019 Security Update

KB4516115: Security update for Adobe Flash Player (September 2019)

KB4517389: Windows 10 Version 1903 October 2019 Security Update

KB4519338: Windows 10 Version 1809 and Windows Server 2019 October 2019 Security Update

KB4519985: Windows Server 2012 October 2019 Security Update

KB4519990: Windows 8.1 and Windows Server 2012 R2 October 2019 Security Update

KB4519998: Windows 10 Version 1607 and Windows Server 2016 October 2019 Security Update

KB4520003: Windows 7 and Windows Server 2008 R2 October 2019 Security Update

KB4520004: Windows 10 Version 1709 October 2019 Security Update

KB4520008: Windows 10 Version 1803 October 2019 Security Update

KB4520009: Windows Server 2008 October 2019 Security Update

KB4520010: Windows 10 Version 1703 October 2019 Security Update

KB4520011: Windows 10 October 2019 Security Update

KB4523205: Windows 10 Version 1809 and Windows Server 2019 November 2019 Security Update

KB4524570: Windows 10 Version 1903 and Windows 10 Version 1909 November 2019 Security Update

KB4525232: Windows 10 November 2019 Security Update

KB4525233: Windows 7 and Windows Server 2008 R2 November 2019 Security Update

KB4525236: Windows 10 Version 1607 and Windows Server 2016 November 2019 Security Update

KB4525237: Windows 10 Version 1803 November 2019 Security Update

KB4525239: Windows Server 2008 November 2019 Security Update

KB4525241: Windows 10 Version 1709 November 2019 Security Update

KB4525250: Windows 8.1 and Windows Server 2012 R2 November 2019 Security Update

KB4525253: Windows Server 2012 November 2019 Security Update

KB4528760: Windows 10 Version 1903 and Windows 10 Version 1909 January 2020 Security Update

KB4530681: Windows 10 December 2019 Security Update

KB4530684: Windows 10 Version 1903 and Windows 10 Version 1909 December 2019 Security Update

KB4530689: Windows 10 Version 1607 and Windows Server 2016 December 2019 Security Update

KB4530692: Windows 7 and Windows Server 2008 R2 December 2019 Security Update

KB4530698: Windows Server 2012 December 2019 Security Update

KB4530714: Windows 10 Version 1709 December 2019 Security Update

KB4530715: Windows 10 Version 1809 and Windows Server 2019 December 2019 Security Update

KB4530717: Windows 10 Version 1803 December 2019 Security Update

KB4530719: Windows Server 2008 December 2019 Security Update

KB4530730: Windows 8.1 and Windows Server 2012 R2 December 2019 Security Update

KB4532691: Windows 10 Version 1809 and Windows Server 2019 February 2020 Security Update

KB4532693: Windows 10 Version 1903 and Windows 10 Version 1909 February 2020 Security Update

KB4534271: Windows 10 Version 1607 and Windows Server 2016 January 2020 Security Update

KB4534273: Windows 10 Version 1809 and Windows Server 2019 January 2020 Security Update

KB4534276: Windows 10 Version 1709 January 2020 Security Update

KB4534288: Windows Server 2012 January 2020 Security Update

KB4534293: Windows 10 Version 1803 January 2020 Security Update

KB4534306: Windows 10 January 2020 Security Update

KB4534309: Windows 8.1 and Windows Server 2012 R2 January 2020 Security Update

KB4534312: Windows Server 2008 January 2020 Security Update

KB4534314: Windows 7 and Windows Server 2008 R2 January 2020 Security Update

KB4537759: Security update for Adobe Flash Player (February 2020)

KB4537762: Windows 10 Version 1803 February 2020 Security Update

KB4537764: Windows 10 Version 1607 and Windows Server 2016 February 2020 Security Update

KB4537776: Windows 10 February 2020 Security Update

KB4537789: Windows 10 Version 1709 February 2020 Security Update

KB4537794: Windows Server 2012 February 2020 Security Update

KB4537803: Windows 8.1 and Windows Server 2012 R2 February 2020 Security Update

KB4537813: Windows 7 and Windows Server 2008 R2 February 2020 Security Update

KB4537822: Windows Server 2008 February 2020 Security Update

KB4538461: Windows 10 Version 1809 and Windows Server 2019 March 2020 Security Update

KB4540670: Windows 10 Version 1607 and Windows Server 2016 March 2020 Security Update

KB4540673: Windows 10 Version 1903 and Windows 10 Version 1909 March 2020 Security Update

KB4540681: Windows 10 Version 1709 March 2020 Security Update

KB4540689: Windows 10 Version 1803 March 2020 Security Update

KB4540693: Windows 10 March 2020 Security Update

KB4540694: Windows Server 2012 March 2020 Security Update

KB4541500: Windows 7 and Windows Server 2008 R2 March 2020 Security Update

KB4541504: Windows Server 2008 March 2020 Security Update

KB4541505: Windows 8.1 and Windows Server 2012 R2 March 2020 Security Update

KB4549949: Windows 10 Version 1809 and Windows Server 2019 April 2020 Security Update

KB4549951: Windows 10 Version 1903 and Windows 10 Version 1909 April 2020 Security Update

KB4550922: Windows 10 Version 1803 April 2020 Security Update

KB4550927: Windows 10 Version 1709 April 2020 Security Update

KB4550929: Windows 10 Version 1607 and Windows Server 2016 April 2020 Security Update

KB4550930: Windows 10 April 2020 Security Update

KB4550957: Windows Server 2008 April 2020 Security Update

KB4550965: Windows 7 and Windows Server 2008 R2 April 2020 Security Update

KB4550970: Windows 8.1 and Windows Server 2012 R2 April 2020 Security Update

KB4550971: Windows Server 2012 April 2020 Security Update

KB4551762: Windows 10 Version 1903 and Windows 10 Version 1909 OOB Security Update (ADV200005)(CVE-2020-0796)

Microsoft ASP.NET Core Privilege Escalation (March 2018)

Microsoft Patch Bulletin Feasibility Check

Microsoft Project RCE Vulnerability (April 2020)

Microsoft Security Advisory 4025685: Guidance for older platforms (XP / 2003) (EXPLODINGCAN)

Microsoft Security Advisory 4025685: Windows Vista (June 2017)

Microsoft Security Advisory 4500331: Guidance for older platforms (XP / 2003) (BlueKeep)

Microsoft Windows Summary of Missing Patches

MS KB3057154: Update to harden use of DES encryption (3057154)

MS00-029: NT IP Fragment Reassembly Patch Not Applied (jolt2) (259728)

MS00-035: MS SQL7.0 Service Pack may leave passwords on system (263968)

MS00-036: NT ResetBrowser frame & HostAnnouncement flood patch (262694)

MS00-047: NetBIOS Name Server Protocol Spoofing patch (269239)

MS00-052: Relative Shell Path patch (269049)

MS00-053: Service Control Manager Named Pipe Impersonation patch (269523)

MS00-062: Local Security Policy Corruption (269609)

MS00-065: Still Image Service Privilege Escalation patch (272736)

MS00-066: Malformed RPC Packet patch (272303)

MS00-067: Telnet Client NTLM Authentication Vulnerability (272743)

MS00-070: LPC and LPC Ports Vulnerabilities patch (266433)

MS00-086: Webserver file request parsing (277873)

MS00-089: Domain Account Lockout Vulnerability (274372)

MS00-091: Incomplete TCP/IP Packet Vulnerability (199346)

MS01-003: Winsock2ProtocolCatalogMutex Mutex Local DoS (279336)

MS01-008: NTLMSSP Local Privilege Escalation (280119)

MS01-009: Malformed PPTP Packet Stream Remote DoS (283001)

MS01-011 / MS01-036: LDAP over SSL Arbitrary User Password Modification (287397 / 299687)

MS01-025: Index Server Multiple Vulnerabilities (294472 / 296185)

MS01-046: IrDA Driver Malformed Packet Remote DoS (252795)

MS01-048: RPC Endpoint Mapper Malformed Request DoS (305399)

MS01-059: Unchecked Buffer in Universal Plug and Play can Lead to System Compromise (315000)

MS02-001: Trusted Domain SID Remote Privilege Escalation (311401)

MS02-003: WinReg Remote Registry Key Manipulation (316056)

MS02-005: MSIE 5.01 5.5 6.0 Cumulative Patch (890923)

MS02-006: Malformed SNMP Management Request Remote Overflow (314147)

MS02-008: XML Core Services patch (318203)

MS02-009: IE VBScript Handling patch (318089)

MS02-012: Malformed Data Transfer Request can Cause Windows SMTP Service to Fail (313450)

MS02-013: Cumulative VM Update (300845)

MS02-014: Unchecked buffer in Windows Shell (313829)

MS02-016: Opening Group Policy Files (318089)

MS02-017: MUP overlong request kernel overflow Patch (311967)

MS02-018: Cumulative Patch for Internet Information Services (327696)

MS02-021: Word Mail Reply Arbitrary Script Execution (321804)

MS02-024: Windows Debugger flaw can Lead to Elevated Privileges (320206)

MS02-025: Exchange 2000 Exhaust CPU Resources (320436)

MS02-026: ASP.NET Worker Process StateServer Mode Remote Overflow (322289)

MS02-029: Windows RAS Local Overflow (318138)

MS02-030: Unchecked Buffer in SQLXML (321911)

MS02-031: Cumulative patches for Excel and Word for Windows (324458)

MS02-035: MS SQL Installation may leave passwords on system (263968)

MS02-040 / MS03-033: Unchecked buffer in MDAC Function (326573 / 823718)

MS02-042: Flaw in Network Connection Manager Could Enable Privilege Elevation (326886)

MS02-045: Unchecked buffer in Network Share Provider (326830)

MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (323172)

MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing (328145)

MS02-051: Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure (324380)

MS02-052: Flaw in Microsoft VM Could Allow Code Execution (810030)

MS02-054: Unchecked Buffer in File Decompression Functions Could Lead to Code Execution (329048)

MS02-055: Unchecked Buffer in Windows Help Facility Could Enable Code Execution (323255)

MS02-060: Flaw in WinXP Help center could enable file deletion (328940)

MS02-063: Unchecked Buffer in PPTP Implementation Could Enable DOS Attacks (329834)

MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified (329170)

MS02-071: WM\_TIMER Message Handler Privilege Elevation (328310)

MS02-072: Unchecked Buffer in XP Shell Could Enable System Compromise (329390)

MS03-001: Unchecked buffer in Locate Service (810833)

MS03-005: Unchecked Buffer in XP Redirector (810577)

MS03-007: Unchecked Buffer in ntdll.dll (815021)

MS03-008: Flaw in Windows Script Engine (814078)

MS03-009: Microsoft ISA Server DNS - Denial Of Service (331065)

MS03-010: Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks (331953)

MS03-011: Flaw in Microsoft VM (816093)

MS03-012: Microsoft ISA Server Winsock Proxy DoS (331066)

MS03-013: Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges (811493)

MS03-017: Windows Media Player Skin Download Overflow (817787)

MS03-018: Cumulative Patch for Internet Information Services (11114)

MS03-021: Windows Media Player Library Access (819639)

MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution (823559)

MS03-024: SMB Request Handler Buffer Overflow (817606)

MS03-025: Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation (822679)

MS03-026 / MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (823980 / 824146)

MS03-027: Buffer overrun in Windows Shell (821557)

MS03-029: Flaw in Windows Function may allow DoS (823803)

MS03-030: DirectX MIDI Overflow (819696)

MS03-031: Cumulative Patch for MS SQL Server (815495)

MS03-034: NetBIOS Name Service Reply Information Leakage (824105) (credentialed check)

MS03-035: Word Macros may run automatically (827653)

MS03-037: Visual Basic for Application Overflow (822715)

MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)

MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control (826232)

MS03-043: Buffer Overrun in Messenger Service (828035)

MS03-044: Buffer Overrun in Windows Help (825119)

MS03-045: Buffer Overrun in the ListBox and in the ComboBox (824141)

MS03-049: Buffer Overflow in the Workstation Service (828749)

MS03-050: Word and/or Excel may allow arbitrary code to run (831527)

MS04-001: Vulnerability in Microsoft ISA Server 2000 H.323 Filter(816458)

MS04-002: Exchange Privilege Escalation (832759)

MS04-003: MDAC Buffer Overflow (832483)

MS04-006: WINS Server Remote Overflow (830352)

MS04-007: ASN.1 parsing vulnerability (828028)

MS04-008: Windows Media Services Remote Denial of Service (832359)

MS04-009: Vulnerability in Outlook could allow code execution (828040)

MS04-010: MSN Messenger Information Disclosure (838512)

MS04-011: Microsoft Hotfix (credentialed check) (835732)

MS04-012: Microsoft Hotfix (credentialed check) (828741)

MS04-013: Cumulative Update for Outlook Express (837009)

MS04-014: Microsoft Hotfix (credentialed check) (837001)

MS04-015: Microsoft Help Center Remote Code Execution (840374)

MS04-016: Vulnerability in DirectPlay Could Allow Denial of Service (839643)

MS04-018: Cumulative Security Update for Outlook Express (823353)

MS04-019: Utility Manager Could Allow Code Execution (842526)

MS04-020: Vulnerability in POSIX could allow code execution (841872)

MS04-021: IIS Redirection Vulnerability (credentialed check) (841373)

MS04-022: Task Scheduler Vulnerability (841873)

MS04-023: Vulnerability in HTML Help Could Allow Code Execution (840315)

MS04-024: Buffer overrun in Windows Shell (839645)

MS04-026: Vulnerability in Exchange Server 5.5 Outlook Web Access XSS (842436)

MS04-027: Vulnerability in WordPerfect Converter (884933)

MS04-028: Buffer Overrun in JPEG Processing (833987)

MS04-029: Vulnerability in RPC Runtime Library Could Allow Information Disclosure and Denial of Service (873350)

MS04-030: WebDAV XML Message Handler Denial of Service (824151)

MS04-031: Vulnerability in NetDDE Could Allow Code Execution (841533)

MS04-032: Security Update for Microsoft Windows (840987)

MS04-033: Microsoft Excel Code Execution (886836)

MS04-034: Vulnerability in zipped folders may allow code execution (873376)

MS04-035: Vulnerability in SMTP Could Allow Remote Code Execution (885881)

MS04-037: Vulnerability in Windows Shell (841356)

MS04-039: ISA Server 2000 and Proxy Server 2.0 Internet Content Spoofing (888258)

MS04-040: Cumulative Security Update for Internet Explorer (889293)

MS04-041: Vulnerabilities in WordPad (885836)

MS04-042: Windows NT Multiple DHCP Vulnerabilities (885249)

MS04-043: Vulnerabilities in HyperTerminal (873339)

MS04-044: Vulnerabilities in Windows Kernel and LSASS (885835)

MS04-045: WINS Code Execution (870763)

MS05-001: HTML Help Code Execution (890175)

MS05-002: Cursor and Icon Format Handling Code Execution (891711)

MS05-003: Indexing Service Code Execution (871250)

MS05-004: ASP.NET Path Validation Vulnerability (887219)

MS05-005: Vulnerability in Microsoft Office XP could allow Remote Code Execution (873352)

MS05-007: Vulnerability in Windows Could Allow Information Disclosure (888302)

MS05-008: Vulnerability in Windows Shell (890047)

MS05-009: Vulnerability in PNG Processing Could Allow Remote Code Execution (890261)

MS05-010: Vulnerability in the License Logging Service (885834)

MS05-011: Vulnerability in SMB may allow remote code execution (885250)

MS05-012: Vulnerability in OLE and COM Could Allow Code Execution (873333)

MS05-013: Vulnerability in the DHTML Editing Component may allow code execution (891781)

MS05-015: Vulnerability in the Hyperlink Object Library may allow code execution (888113)

MS05-016: Vulnerability in Windows Shell (893086)

MS05-017: Vulnerability in MSMQ Could Allow Code Execution (892944)

MS05-018: Vulnerabilities in Windows Kernel (890859)

MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066)

MS05-021: Vulnerability in SMTP Could Allow Remote Code Execution (894549)

MS05-022: Vulnerability in MSN Messenger Could Lead to Remote Code Execution (896597)

MS05-023: Vulnerability in Word May Lead to Code Execution (890169)

MS05-024: Vulnerability in Web View Could Allow Code Execution (894320)

MS05-025: Cumulative Security Update for Internet Explorer (883939)

MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution (896358)

MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422)

MS05-028: Vulnerability in Web Client Service Could Allow Remote Code Execution (896426)

MS05-029: Vulnerability in Exchange Server 5.5 Outlook Web Access XSS (895179)

MS05-030: Vulnerability in Outlook Express Could Allow Remote Code Execution (897715)

MS05-031: Vulnerability in Step-by-Step Interactive Training (898458)

MS05-032: Vulnerability in Microsoft Agent Could Allow Spoofing (890046)

MS05-033: Vulnerability in Telnet Client Could Allow Information Disclosure (896428)

MS05-034: Cumulative Update for ISA Server 2000 (899753)

MS05-035: Vulnerability in Word May Lead to Code Execution (903672)

MS05-036: Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)

MS05-037: Vulnerability in JView Profiler Could Allow Code Execution (903235)

MS05-038: Cumulative Security Update for Internet Explorer (896727)

MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)

MS05-040: Vulnerability in Telephony Service Could Allow Remote Code Execution (893756)

MS05-041: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (899591)

MS05-042: Vulnerability in Kerberos Could Allow Denial of Service, Information Disclosure and Spoofing (899587)

MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (896423)

MS05-044: Vulnerability in the Windows FTP Client Could Allow File Transfer Location Tampering (905495)

MS05-045: Vulnerability in Network Connection Manager Could Allow Denial of Service (905414)

MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)

MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (905749)

MS05-048: Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (907245)

MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)

MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution (904706)

MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)

MS05-052: Cumulative Security Update for Internet Explorer (896688)

MS05-053: Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424)

MS05-054: Cumulative Security Update for Internet Explorer (905915)

MS05-055: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (908523)

MS06-001: Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (912919)

MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution (908519)

MS06-003: Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Could Allow Remote Code Execution (902412)

MS06-004: Cumulative Security Update for Internet Explorer (910620)

MS06-005: Vulnerability in Windows Media Player Could Allow Remote Code Execution (911565)

MS06-006: Vulnerability in Windows Media Player Plug-in Could Allow Remote Code Execution (911564)

MS06-007: Vulnerability in TCP/IP Could Allow Denial of Service (913446)

MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution (911927)

MS06-009: Vulnerability in Korean Input Method Could Allow Elevation of Privilege (901190)

MS06-010: Vulnerability in PowerPoint 2000 Could Allow Information Disclosure (889167)

MS06-011: Permissive Windows Services DACLs Could Allow Elevation of Privilege (914798)

MS06-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (905413)

MS06-013: Cumulative Security Update for Internet Explorer (912812)

MS06-014: Vulnerability in MDAC Could Allow Code Execution (911562)

MS06-015: Vulnerabilities in Windows Explorer Could Allow Remote Code Execution (908531)

MS06-016: Vulnerability in Outlook Express Could Allow Remote Code Execution (911567)

MS06-017: FrontPage fpadmdll.dll Multiple Parameter XSS (917627)

MS06-018: Vulnerability in MSDTC Could Allow Denial of Service (913580)

MS06-019: Vulnerability in Microsoft Exchange Could Allow Remote Code Execution (916803)

MS06-021: Cumulative Security Update for Internet Explorer (916281)

MS06-022: Vulnerability in ART Image Rendering Could Allow Remote Code Execution (918439)

MS06-023: Vulnerability in Microsoft JScript Could Allow Remote Code Execution (917344)

MS06-024: Vulnerability in Windows Media Player Could Allow Remote Code Execution (917734)

MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280)

MS06-027: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (917336)

MS06-028: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (916768)

MS06-029: Vulnerability in Microsoft Exchange Server Running Outlook Web Access Could Allow Script Injection (912442)

MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege (914389)

MS06-031: Vulnerability in RPC Mutual Authentication Could Allow Spoofing (917736)

MS06-032: Vulnerability in TCP/IP Could Allow Remote Code Execution (917953)

MS06-033: Vulnerabilities in ASP.NET could allow information disclosure (917283)

MS06-034: Vulnerability in Microsoft IIS using ASP Could Allow Remote Code Execution (917537)

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159)

MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution (914388)

MS06-037: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (917285)

MS06-038: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (917284)

MS06-039: Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (915384)

MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883)

MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution (920683)

MS06-042: Cumulative Security Update for Internet Explorer (918899)

MS06-043: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (920214)

MS06-044: Vulnerability in Microsoft Management Console Could Allow Remote Code Execution (917008)

MS06-045: Vulnerability in Windows Explorer Could Allow Remote Code Execution (921398)

MS06-046: Vulnerability in HTML Help Could Allow Remote Code Execution (922616)

MS06-047: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (921645)

MS06-048: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (922968)

MS06-049: Vulnerability in Windows Kernel Could Result in Elevation of Privilege (920958)

MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution (920670)

MS06-051: Vulnerability in Windows Kernel Could Result in Remote Code Execution (917422)

MS06-052: Vulnerability in Pragmatic General Multicast (PGM) Could Allow Remote Code Execution (919007)

MS06-053: Vulnerability in Indexing Service Could Allow XSS (920685)

MS06-054: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (910729)

MS06-055: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (925486)

MS06-056: Vulnerabilities in ASP.NET could allow information disclosure (922770)

MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution (923191)

MS06-058: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (924163)

MS06-059: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (924164)

MS06-060: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (924554)

MS06-061: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (924191)

MS06-062: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (922581)

MS06-063: Vulnerability in Server Service Could Allow Denial of Service (923414)

MS06-064: Vulnerability in TCP/IP IPv6 Could Allow Denial of Service (922819)

MS06-065: Vulnerability in Windows Object Packager Could Allow Remote Execution (924496)

MS06-066: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (923980)

MS06-067: Cumulative Security Update for Internet Explorer (922760)

MS06-068: Vulnerability in Microsoft Agent Could Remote Code Execution (920213)

MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution (924270)

MS06-071: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (928088)

MS06-072: Cumulative Security Update for Internet Explorer (925454)

MS06-073: Vulnerability in Visual Studio 2005 Could Allow Remote Code Execution (925674)

MS06-074: Vulnerability in SNMP Could Allow Remote Code Execution (926247)

MS06-075: Vulnerability in Windows Could Allow Elevation of Privilege (926255)

MS06-076: Cumulative Security Update for Outlook Express (923694)

MS06-077: Vulnerability in Remote Installation Service Could Allow Remote Code Execution (926121)

MS06-078: Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689/925398)

MS07-002: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (927198)

MS07-003: Vulnerabilities in Microsoft Outlook Could Allow Remote Code Execution (925938)

MS07-004: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)

MS07-005: Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (923723)

MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)

MS07-007: Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802)

MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)

MS07-009: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779)

MS07-010: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution (932135)

MS07-011: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)

MS07-012: Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)

MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)

MS07-014: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (929434)

MS07-015: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (932554)

MS07-016: Cumulative Security Update for Internet Explorer (928090)

MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (925902)

MS07-018: Vulnerabilities in Microsoft Content Management Server Could Allow Remote Code Execution (925939)

MS07-019: Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261)

MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)

MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)

MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)

MS07-023: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (934233)

MS07-024: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (934232)

MS07-025: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (934873)

MS07-026: Vulnerability in Microsoft Exchange Could Allow Remote Code Execution (931832)

MS07-027: Cumulative Security Update for Internet Explorer (931768)

MS07-028: Vulnerability in CAPICOM Could Allow Remote Code Execution (931906)

MS07-029: Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (935966)

MS07-030: Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (927051)

MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840)

MS07-032: Vulnerability in Windows Vista Could Allow Information Disclosure (931213)

MS07-033: Cumulative Security Update for Internet Explorer (933566)

MS07-034: Cumulative Security Update for Outlook Express and Windows Mail (929123)

MS07-035: Vulnerability in Win 32 API Could Allow Remote Code Execution (935839)

MS07-036: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (936542)

MS07-037: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (936548)

MS07-038: Vulnerability in Windows Vista Firewall Could Allow Information Disclosure (935807)

MS07-039: Microsoft Windows Active Directory LDAP Service Remote Code Execution (926122)

MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)

MS07-041: Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373)

MS07-042: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227)

MS07-043: Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)

MS07-044: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (940965)

MS07-045: Cumulative Security Update for Internet Explorer (937143)

MS07-046: Vulnerability in GDI Could Allow Remote Code Execution (938829)

MS07-047: Vulnerability in Windows Media Player Could Allow Remote Code Execution (936782)

MS07-048: Vulnerabilities in Windows Gadgets Could Allow Remote Code Execution (938123)

MS07-049: Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (937986)

MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (938127)

MS07-051: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)

MS07-052: Vulnerability in Crystal Reports for Visual Studio Could Allow Remote Code Execution (941522)

MS07-053: Vulnerability in Windows Services for UNIX Could Allow Elevation of Privilege (939778)

MS07-054: Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution (942099)

MS07-055: Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution (923810)

MS07-056: Cumulative Security Update for Outlook Express and Windows Mail (941202)

MS07-057: Cumulative Security Update for Internet Explorer (939653)

MS07-058: Vulnerability in RPC Could Allow Denial of Service (933729)

MS07-059: Vulnerability in Windows SharePoint Could Result in Elevation of Privilege (942017)

MS07-060: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (942695)

MS07-061: Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460)

MS07-062: Vulnerability in DNS Could Allow Spoofing (941672)

MS07-063: Vulnerability in SMBv2 Could Allow Remote Code Execution (942624)

MS07-064: Vulnerabilities in DirectX Could Allow Remote Code Execution (941568)

MS07-065: Vulnerability in Message Queuing Could Allow Remote Code Execution (937894)

MS07-066: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (943078)

MS07-067: Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege (944653)

MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 / 944275)

MS07-069: Cumulative Security Update for Internet Explorer (942615)

MS08-001: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644)

MS08-002: Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485)

MS08-003: Vulnerability in Active Directory Could Allow Denial of Service (946538)

MS08-004: Vulnerability in Windows TCP/IP Could Allow Denial of Service (946456)

MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)

MS08-006: Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830)

MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)

MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)

MS08-009: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (947077)

MS08-010: Cumulative Security Update for Internet Explorer (944533)

MS08-011: Vulnerabilities in Microsoft Works File Converter Could Allow Remote Code Execution (947081)

MS08-012: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (947085)

MS08-013: Vulnerability in Microsoft Office Could Allow Remote Code Execution (947108)

MS08-014: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (949029)

MS08-015: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (949031)

MS08-016: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (949030)

MS08-017: Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (933103)

MS08-018: Vulnerability in Microsoft Project Could Allow Remote Code Execution (950183)

MS08-019: Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (949032)

MS08-020: Vulnerability in DNS Client Could Allow Spoofing (945553)

MS08-021: Vulnerabilities in GDI Could Allow Remote Code Execution (948590)

MS08-022: Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution (944338)

MS08-023: Security Update of ActiveX Kill Bits (948881)

MS08-024: Cumulative Security Update for Internet Explorer (947864)

MS08-025: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)

MS08-026: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (951207)

MS08-027: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (951208)

MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)

MS08-029: Vulnerabilities in Microsoft Malware Protection Engine Could Allow Denial of Service (952044)

MS08-030: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (951376)

MS08-031: Cumulative Security Update for Internet Explorer (950759)

MS08-032: Cumulative Security Update of ActiveX Kill Bits (950760)

MS08-033: Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)

MS08-034: Vulnerability in WINS Could Allow Elevation of Privilege (948745)

MS08-035: Vulnerability in Active Directory Could Allow Denial of Service (953235)

MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762)

MS08-037: Vulnerabilities in DNS Could Allow Spoofing (953230)

MS08-038: Vulnerability in Windows Explorer Could Allow Remote Code Execution (950582)

MS08-039: Vulnerabilities in Outlook Web Access for Exchange Server Could Allow Elevation of Privilege (953747)

MS08-040: Vulnerabilities in Microsoft SQL Server Could Allow Elevation of Privilege (941203)

MS08-041: Vulnerability in the ActiveX Control for the Snapshot Viewer for Microsoft Access Could Allow Remote Code Execution (955617)

MS08-042: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (955048)

MS08-043: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (954066)

MS08-044: Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (924090)

MS08-045: Cumulative Security Update for Internet Explorer (953838)

MS08-046: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)

MS08-047: Vulnerability in IPsec Policy Processing Could Allow Information Disclosure (953733)

MS08-048: Security Update for Outlook Express and Windows Mail (951066)

MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution (950974)

MS08-050: Vulnerability in Windows Messenger Could Allow Information Disclosure (955702)

MS08-051: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (949785)

MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593)

MS08-053: Vulnerability in Windows Media Encoder 9 Could Allow Remote Code Execution (954156)

MS08-054: Vulnerability in Windows Media Player Could Allow Remote Code Execution (954154)

MS08-055: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (955047)

MS08-056: Microsoft Office CDO Protocol (cdo:) Content-Disposition: Attachment Header XSS (957699)

MS08-057: Microsoft Excel Multiple Method Remote Code Execution (956416)

MS08-058: Microsoft Internet Explorer Multiple Vulnerabilities (956390)

MS08-059: Microsoft Host Integration Server (HIS) SNA RPC Request Remote Overflow (956695)

MS08-060: Microsoft Windows Active Directory LDAP(S) Request Handling Remote Overflow (957280)

MS08-061: Microsoft Windows Kernel Multiple Privilege Elevation (954211)

MS08-062: Microsoft IIS IPP Service Unspecified Remote Overflow (953155)

MS08-063: Microsoft Windows SMB File Name Handling Remote Underflow (957095)

MS08-064: Microsoft Windows Virtual Address Descriptors (VAD) Local Privilege Escalation (956841)

MS08-065: Microsoft Windows Message Queuing Service RPC Request Handling Remote Code Execution (951071)

MS08-066: Microsoft Windows Ancillary Function Driver (afd.sys) Local Privilege Escalation (956803)

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644) (ECLIPSEDWING)

MS08-068: Vulnerability in SMB Could Allow Remote Code Execution (957097)

MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218)

MS08-070: Vulnerabilities in Visual Basic 6.0 ActiveX Controls Could Allow Remote Code Execution (932349)

MS08-071: Vulnerabilities in GDI+ Could Allow Remote Code Execution (956802)

MS08-072: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (957173)

MS08-073: Microsoft Internet Explorer Multiple Vulnerabilities (958215)

MS08-074: Microsoft Excel Multiple Method Remote Code Execution (959070)

MS08-075: Vulnerabilities in Windows Search Could Allow Remote Code Execution (959349)

MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)

MS08-077: Vulnerability in Microsoft Office SharePoint Server Could Cause Elevation of Privilege (957175)

MS08-078: Microsoft Internet Explorer Security Update (960714)

MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (958687)

MS09-002: Cumulative Security Update for Internet Explorer (961260)

MS09-003: Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (959239)

MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)

MS09-005: Vulnerabilities in Microsoft Office Visio Could Allow Remote Code Execution (957634)

MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)

MS09-007: Vulnerability in SChannel Could Allow Spoofing (960225)

MS09-008: Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)

MS09-009: Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)

MS09-010: Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)

MS09-011: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373)

MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)

MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)

MS09-014: Cumulative Security Update for Internet Explorer (963027)

MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)

MS09-016: Vulnerabilities in Microsoft ISA Server and Forefront Threat Management Gateway Could Cause Denial of Service (961759)

MS09-017: Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)

MS09-018: Vulnerabilities in Active Directory Could Allow Remote Code Execution (971055)

MS09-019: Cumulative Security Update for Internet Explorer (969897)

MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)

MS09-021: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)

MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)

MS09-023: Vulnerability in Windows Search Could Allow Information Disclosure (963093)

MS09-024: Vulnerability in Microsoft Works Converters Could Allow Remote Code Execution (957632)

MS09-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)

MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege (970238)

MS09-027: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514)

MS09-028: Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)

MS09-029: Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)

MS09-030: Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (969516)

MS09-031: Vulnerability in Microsoft ISA Server 2006 Could Cause Elevation of Privilege (970953)

MS09-032: Cumulative Security Update of ActiveX Kill Bits (973346)

MS09-033: Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (969856)

MS09-034: Cumulative Security Update for Internet Explorer (972260)

MS09-035: Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706)

MS09-036: Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service (970957)

MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)

MS09-038: Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)

MS09-039: Vulnerabilities in WINS Could Allow Remote Code Execution (969883)

MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032)

MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657)

MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution (960859)

MS09-043: Vulnerabilities in Microsoft Office Web Components Control Could Allow Remote Code Execution (973472)

MS09-043: Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638)

MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927)

MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961)

MS09-046: Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)

MS09-047: Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812)

MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)

MS09-049: Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution (970710)

MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517) (EDUCATEDSCHOLAR)

MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682)

MS09-052: Vulnerability in Windows Media Player Could Allow Remote Code Execution (974112)

MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)

MS09-054: Cumulative Security Update for Internet Explorer (974455)

MS09-055: Cumulative Security Update of ActiveX Kill Bits (973525)

MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)

MS09-057: Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)

MS09-058: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486)

MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467)

MS09-060: Vulnerabilities in Microsoft Active Template Library (ATL) ActiveX Controls for Microsoft Office Could Allow Remote Code Execution (973965)

MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution (974378)

MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)

MS09-063: Vulnerability in Web Services on Devices API Could Allow Remote Code Execution (973565)

MS09-064: Vulnerability in the License Logging Service (974783)

MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)

MS09-066: Vulnerability in Active Directory Could Allow Denial of Service (973309)

MS09-067: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)

MS09-068: Vulnerability in Microsoft Office Word Could Allow Remote Code Execution (976307)

MS09-069: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)

MS09-070: Vulnerabilities in Active Directory Federation Services Could Allow Remote Code Execution (971726)

MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)

MS09-072: Cumulative Security Update for Internet Explorer (976325)

MS09-073: Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution (975539)

MS09-074: Vulnerability in Microsoft Office Project Could Allow Remote Code Execution (967183)

MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)

MS10-002: Cumulative Security Update for Internet Explorer (978207)

MS10-003: Vulnerability in Microsoft Office (MSO.DLL) Could Allow Remote Code Execution (978214)

MS10-004: Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)

MS10-005: Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706)

MS10-006: Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)

MS10-007: Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)

MS10-008: Cumulative Security Update of ActiveX Kill Bits (978262)

MS10-009: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)

MS10-010: Vulnerability in Windows Server 2008 Hyper-V Could Allow Denial of Service (977894)

MS10-011: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)

MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468)

MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)

MS10-014: Vulnerability in Kerberos Could Allow Denial of Service (977290)

MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)

MS10-016: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)

MS10-017: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)

MS10-018: Cumulative Security Update for Internet Explorer (980182)

MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution (981210)

MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)

MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)

MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)

MS10-023: Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)

MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)

MS10-025: Vulnerability in Microsoft Windows Media Services Could Allow Remote Code Execution (980858)

MS10-026: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)

MS10-027: Vulnerability in Windows Media Player Could Allow Remote Code Execution (979402)

MS10-028: Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (980094)

MS10-029: Vulnerability in Windows ISATAP Component Could Allow Spoofing (978338)

MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)

MS10-031: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)

MS10-032: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)

MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)

MS10-034: Cumulative Security Update of ActiveX Kill Bits (980195)

MS10-035: Cumulative Security Update for Internet Explorer (982381)

MS10-036: Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)

MS10-037: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)

MS10-038: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)

MS10-039: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2028554)

MS10-040: Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)

MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343)

MS10-042: Vulnerability in Help and Support Center Could Allow Remote Code Execution (2229593)

MS10-043: Vulnerability in Canonical Display Driver Could Allow Remote Code Execution (2032276)

MS10-044: Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335)

MS10-045: Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212)

MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198) (EASYHOOKUP)

MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)

MS10-048: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)

MS10-049: Vulnerabilities in SChannel could allow Remote Code Execution (980436)

MS10-050: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (981997)

MS10-051: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)

MS10-052: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)

MS10-053: Cumulative Security Update for Internet Explorer (2183461)

MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)

MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)

MS10-056: Vulnerability in Microsoft Office Word Could Allow Remote Code Execution (2269638)

MS10-057: Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution (2269707)

MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)

MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799)

MS10-060: Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)

MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) (EMERALDTHREAD)

MS10-062: Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (975558)

MS10-063: Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2320113)

MS10-064: Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212)

MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)

MS10-066: Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (982802)

MS10-067: Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2259922)

MS10-068: Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539)

MS10-069: Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2121546)

MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)

MS10-071: Cumulative Security Update for Internet Explorer (2360131)

MS10-072: Vulnerabilities in SafeHTML Could Allow Information Disclosure (2412048)

MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)

MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)

MS10-075: Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679)

MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)

MS10-077: Vulnerability in .NET Framework Could Allow Remote Code Execution (2160841)

MS10-078: Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege (2279986)

MS10-079: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)

MS10-080: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)

MS10-081: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)

MS10-082: Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)

MS10-083: Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)

MS10-084: Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2360937)

MS10-085: Vulnerability in SChannel Could Allow Denial of Service (2207566)

MS10-086: Vulnerability in Windows Shared Cluster Disks Could Allow Tampering (2294255)

MS10-087: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)

MS10-088: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2293386)

MS10-089: Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Elevation of Privilege (2316074)

MS10-090: Cumulative Security Update for Internet Explorer (2416400)

MS10-091: Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199)

MS10-092: Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)

MS10-093: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (2424434)

MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution (2447961)

MS10-095: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)

MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)

MS10-097: Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)

MS10-098: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)

MS10-099: Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege (2440591)

MS10-100: Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)

MS10-101: Vulnerability in Windows Netlogon Service Could Allow Denial of Service (2207559)

MS10-102: Vulnerability in Hyper-V Could Allow Denial of Service (2345316)

MS10-103: Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)

MS10-104: Vulnerability in Microsoft SharePoint Could Allow Remote Code Execution (2455005)

MS10-105: Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)

MS10-106: Vulnerability in Microsoft Exchange Server Could Allow Denial of Service (2407132)

MS11-001: Vulnerability in Windows Backup Manager Could Allow Remote Code Execution (2478935)

MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)

MS11-003: Cumulative Security Update for Internet Explorer (2482017)

MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)

MS11-005: Vulnerability in Active Directory Could Allow Denial of Service (2478953)

MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)

MS11-007: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)

MS11-008: Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2451879)

MS11-009: Vulnerability in JScript and VBScript Scripting Engine Could Allow Information Disclosure (2475792)

MS11-010: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2476687)

MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)

MS11-012: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)

MS11-013: Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)

MS11-014: Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege (2478960)

MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)

MS11-016: Vulnerability in Microsoft Groove Could Allow Remote Code Execution (2494047)

MS11-017: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (2508062)

MS11-018: Cumulative Security Update for Internet Explorer (2497640)

MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)

MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)

MS11-021: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2489279)

MS11-022: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2489283)

MS11-023: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2489293)

MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)

MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)

MS11-026: Vulnerability in MHTML Could Allow Information Disclosure (2503658)

MS11-027: Cumulative Security Update of ActiveX Kill Bits (2508272)

MS11-028: Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015)

MS11-029: Vulnerability in GDI+ Could Allow Remote Code Execution (2489979)

MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)

MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666)

MS11-032: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618)

MS11-033: Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2485663)

MS11-034: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)

MS11-035: Vulnerability in WINS Could Allow Remote Code Execution (2524426)

MS11-036: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2545814)

MS11-037: Vulnerability in MHTML Could Allow Information Disclosure (2544893)

MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490)

MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)

MS11-040: Vulnerability in Threat Management Gateway Firewall Client Could Allow Remote Code Execution (2520426)

MS11-041: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)

MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512)

MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution (2536276)

MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)

MS11-045: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2537146)

MS11-046: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665)

MS11-047: Vulnerability in Hyper-V Could Allow Denial of Service (2525835)

MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275)

MS11-049: Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893)

MS11-050: Cumulative Security Update for Internet Explorer (2530548)

MS11-051: Vulnerability in Active Directory Certificate Services Web Enrollment Could Allow Elevation of Privilege (2518295)

MS11-052: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521)

MS11-053: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (2566220)

MS11-054: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)

MS11-055: Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2560847)

MS11-056: Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)

MS11-057: Critical Cumulative Security Update for Internet Explorer (2559049)

MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485)

MS11-059: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2560656)

MS11-060: Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2560978)

MS11-061: Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250)

MS11-062: Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454)

MS11-063: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)

MS11-064: Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)

MS11-065: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (2570222)

MS11-066: Vulnerability in Microsoft Chart Control Could Allow Information Disclosure (2567943)

MS11-067: Vulnerability in Microsoft Report Viewer Could Allow Information Disclosure (2578230)

MS11-068: Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)

MS11-069: Vulnerability in .NET Framework Could Allow Information Disclosure (2567951)

MS11-070: Vulnerability in WINS Could Allow Elevation of Privilege (2571621)

MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)

MS11-072: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2587505)

MS11-073: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2587634)

MS11-074: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)

MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)

MS11-076: Vulnerability in Windows Media Center Could Allow Remote Code Execution (2604926)

MS11-077: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)

MS11-078: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)

MS11-079: Vulnerabilities in Microsoft Forefront Unified Access Gateway Could Cause Remote Code Execution (2544641)

MS11-080: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2592799)

MS11-081: Critical Cumulative Security Update for Internet Explorer (2586448)

MS11-082: Vulnerabilities in Host Integration Server Could Allow Denial of Service (2607670)

MS11-083: Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)

MS11-084: Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)

MS11-085: Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)

MS11-086: Vulnerability in Active Directory Could Allow Elevation of Privilege (2630837)

MS11-087: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)

MS11-088: Vulnerability in Microsoft Office IME (Chinese) Could Allow Elevation of Privilege (2652016)

MS11-089: Vulnerability in Microsoft Office Could Allow Remote Code Execution (2590602)

MS11-090: Cumulative Security Update of ActiveX Kill Bits (2618451)

MS11-091: Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2607702)

MS11-092: Vulnerability in Windows Media Could Allow Remote Code Execution (2648048)

MS11-093: Vulnerability in OLE Could Allow Remote Code Execution (2624667)

MS11-094: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2639142)

MS11-095: Vulnerability in Active Directory Could Allow Remote Code Execution (2640045)

MS11-096: Vulnerability in Microsoft Excel Could Allow Remote Code Execution (2640241)

MS11-097: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712)

MS11-098: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171)

MS11-099: Cumulative Security Update for Internet Explorer (2618444)

MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)

MS12-001: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)

MS12-002: Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)

MS12-003: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524)

MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)

MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)

MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)

MS12-007: Vulnerability in AntiXSS Library Could Allow Information Disclosure (2607664)

MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)

MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)

MS12-010: Cumulative Security Update for Internet Explorer (2647516)

MS12-011 : Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841)

MS12-012: Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)

MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)

MS12-014: Vulnerability in Indeo Codec Could Allow Remote Code Execution (2661637)

MS12-015: Vulnerabilities in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2663510)

MS12-016: Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)

MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170)

MS12-018: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)

MS12-019: Vulnerability in DirectWrite Could Allow Denial of Service (2665364)

MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)

MS12-021: Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019)

MS12-022: Vulnerability in Expression Design Could Allow Remote Code Execution (2651018)

MS12-023: Cumulative Security Update for Internet Explorer (2675157)

MS12-024: Vulnerability in Windows Could Allow Remote Code Execution (2653956)

MS12-025: Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)

MS12-026: Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Information Disclosure (2663860)

MS12-027: Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258)

MS12-028: Vulnerability in Microsoft Office Could Allow Remote Code Execution (2639185)

MS12-029: Vulnerability in Microsoft Word Could Allow Remote Code Execution (2680352)

MS12-030: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2663830)

MS12-031: Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2597981)

MS12-032: Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338)

MS12-033: Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege (2690533)

MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)

MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)

MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)

MS12-037: Cumulative Security Update for Internet Explorer (2699988)

MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)

MS12-039: Vulnerabilities in Lync Could Allow Remote Code Execution (2707956)

MS12-040: Vulnerability in Microsoft Dynamics AX Enterprise Portal Could Allow Elevation of Privilege (2709100)

MS12-040: Vulnerability in Microsoft Dynamics AX Enterprise Portal Could Allow Elevation of Privilege (MSSQL check)

MS12-041: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)

MS12-042: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)

MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)

MS12-044: Cumulative Security Update for Internet Explorer (2719177)

MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)

MS12-046: Vulnerability in Visual Basic for Applications Could Allow Remote Code Execution (2707960)

MS12-047: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)

MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)

MS12-049: Vulnerability in TLS Could Allow Information Disclosure (2655992)

MS12-050: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2695502)

MS12-052: Cumulative Security Update for Internet Explorer (2722913)

MS12-053: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2723135)

MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)

MS12-055: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)

MS12-056: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2706045)

MS12-057: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2731879)

MS12-058: Vulnerabilities in Microsoft Exchange Server WebReady Document Viewing Could Allow Remote Code Execution (2740358)

MS12-059: Buffer Overflow in Microsoft Visio and Visio Viewer Could Allow Remote Code Execution (2733918)

MS12-060: Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573)

MS12-061: Vulnerability in Visual Studio Team Foundation Server Could Allow Elevation of Privilege (2719584)

MS12-062: Vulnerability in System Center Configuration Manager Could Allow Elevation of Privilege (2741528)

MS12-063: Cumulative Security Update for Internet Explorer (2744842)

MS12-064: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2742319)

MS12-065: Vulnerability in Microsoft Works Could Allow Remote Code Execution (2754670)

MS12-066: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)

MS12-067: Vulnerabilities in FAST Search Server 2010 for SharePoint Parsing Could Allow Remote Code Execution (2742321)

MS12-068: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197)

MS12-069: Vulnerability in Kerberos Could Allow Denial of Service (2743555)

MS12-070: Vulnerability in SQL Server Could Allow Elevation of Privilege (2754849)

MS12-071: Cumulative Security Update for Internet Explorer (2761451)

MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution (2727528)

MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure (2733829)

MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2745030)

MS12-075: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)

MS12-076: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2720184)

MS12-077: Cumulative Security Update for Internet Explorer (2761465)

MS12-078: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)

MS12-079: Vulnerability in Microsoft Word Could Allow Remote Code Execution (2780642)

MS12-080: Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2784126)

MS12-081: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)

MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution (2770660)

MS12-083: Vulnerability in IP-HTTPS Component Could Allow Security Feature Bypass (2765809)

MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)

MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)

MS13-003: Vulnerabilities in System Center Operations Manager Could Allow Elevation of Privilege (2748552)

MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324)

MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)

MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220)

MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service (2769327)

MS13-008: Security Update for Internet Explorer (2799329)

MS13-009: Security Update for Internet Explorer (2792100)

MS13-010: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2797052)

MS13-011: Vulnerability in Media Decompression Could Allow Remote Code Execution (2780091)

MS13-012: Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2809279)

MS13-013: Vulnerabilities in FAST Search Server 2010 for SharePoint Parsing Could Allow Remote Code Execution (2784242)

MS13-014: Vulnerability in NFS Server Could Allow Denial of Service (2790978)

MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2800277)

MS13-016: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778344)

MS13-017: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2799494)

MS13-018: Vulnerability in TCP/IP Could Allow Denial of Service (2790655)

MS13-019: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)

MS13-020: Vulnerability in OLE Automation Could Allow Remote Code Execution (2802968)

MS13-021: Security Update for Internet Explorer (2809289)

MS13-022: Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (2814124)

MS13-023: Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2801261)

MS13-024: Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176)

MS13-025: Vulnerability in Microsoft OneNote Could Allow Information Disclosure (2816264)

MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)

MS13-028: Security Update for Internet Explorer (2817183)

MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2828223)

MS13-030: Vulnerability in SharePoint Could Allow Information Disclosure (2827663)

MS13-031: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2813170)

MS13-032: Vulnerability in Active Directory Could Lead to Denial of Service (2830914)

MS13-033: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2820917)

MS13-034: Vulnerability in Microsoft Antimalware Client Could Allow Elevation of Privilege (2823482)

MS13-035: Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)

MS13-036: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2829996)

MS13-037: Cumulative Security Update for Internet Explorer (2829530)

MS13-038: Security Update for Internet Explorer (2847204)

MS13-039: Vulnerability in HTTP.sys Could Allow Denial of Service (2829254)

MS13-040: Vulnerabilities in .NET Framework Could Allow Spoofing (2836440)

MS13-041: Vulnerability in Lync Could Allow Remote Code Execution (2834695)

MS13-042: Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2830397)

MS13-043: Vulnerability in Microsoft Word Could Allow Remote Code Execution (2830399)

MS13-044: Vulnerability in Microsoft Visio Could Allow Information Disclosure (2834692)

MS13-045: Vulnerability in Windows Essentials Could Allow Information Disclosure (2813707)

MS13-046: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2840221)

MS13-047: Cumulative Security Update for Internet Explorer (2838727)

MS13-048: Vulnerability in Windows Kernel Could Allow Information Disclosure (2839229)

MS13-049: Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (2845690)

MS13-050: Vulnerability in Windows Print Spooler Components Could Allow Elevation of Privilege (2839894)

MS13-051: Vulnerability in Microsoft Office Could Allow Remote Code Execution (2839571)

MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)

MS13-053: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (2850851)

MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)

MS13-055: Cumulative Security Update for Internet Explorer (2846071)

MS13-056: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2845187)

MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (2847883)

MS13-058: Vulnerability in Windows Defender Could Allow Elevation of Privilege (2847927)

MS13-059: Cumulative Security Update for Internet Explorer (2862772)

MS13-060: Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2850869)

MS13-061: Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2876063)

MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)

MS13-063: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2859537)

MS13-064: Vulnerability in Windows NAT Driver Could Allow Denial of Service (2849568)

MS13-065: Vulnerability in ICMPv6 Could Allow Denial of Service (2868623)

MS13-066: Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (2873872)

MS13-067: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)

MS13-068: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2756473)

MS13-069: Cumulative Security Update for Internet Explorer (2870699)

MS13-070: Vulnerability in OLE Could Allow Remote Code Execution (2876217)

MS13-071: Vulnerability in Windows Theme File Could Allow Remote Code Execution (2864063)

MS13-072: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2845537)

MS13-073: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2858300))

MS13-074: Vulnerabilities in Microsoft Access Could Allow Remote Code Execution (2848637)

MS13-075: Vulnerability in Microsoft Office IME (Chinese) Could Allow Elevation of Privilege (2878687)

MS13-076: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2876315)

MS13-077: Vulnerability in Windows Service Control Manager Could Allow Elevation of Privilege (2872339)

MS13-078: Vulnerability in FrontPage Could Allow Information Disclosure (2825621)

MS13-079: Vulnerability in Active Directory Could Allow Denial of Service (2853587)

MS13-080: Cumulative Security Update for Internet Explorer (2879017)

MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)

MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2878890)

MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)

MS13-084: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2885089)

MS13-085: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080)

MS13-086: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2885084)

MS13-087: Vulnerability in Silverlight Could Allow Information Disclosure (2890788)

MS13-088: Cumulative Security Update for Internet Explorer (2888505)

MS13-089: Critical Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)

MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986)

MS13-091: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2885093)

MS13-092: Vulnerability in Hyper-V Could Allow Elevation of Privilege (2893986)

MS13-093: Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)

MS13-094: Vulnerability in Microsoft Outlook Could Allow Information Disclosure (2894514)

MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service (2868626)

MS13-096: Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (2908005)

MS13-097: Cumulative Security Update for Internet Explorer (2898785)

MS13-098: Vulnerability in Windows Could Allow Remote Code Execution (2893294)

MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution (2909158)

MS13-100: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2904244)

MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430)

MS13-102: Vulnerability in LRPC Client Could Allow Elevation of Privilege (2898715)

MS13-103: Vulnerability in ASP.NET SignalR Could Allow Elevation of Privilege (2905244)

MS13-104: Vulnerability in Microsoft Office Could Allow Information Disclosure (2909976)

MS13-105: Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (2915705)

MS13-106: Vulnerability in a Microsoft Office Shared Component Could Allow Security Feature Bypass (2905238)

MS14-001: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2916605)

MS14-002: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2914368)

MS14-003: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2913602)

MS14-004: Vulnerability in Microsoft Dynamics AX Could Allow Denial of Service (2880826)

MS14-005: Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2916036)

MS14-006: Vulnerability in ICMPv6 Could Allow Denial of Service (2904659)

MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution (2912390)

MS14-008: Vulnerability in Microsoft Forefront Protection for Exchange Could Allow Remote Code Execution (2927022)

MS14-009: Vulnerabilities in .NET Framework Could Allow Privilege Escalation (2916607)

MS14-010: Cumulative Security Update for Internet Explorer (2909921)

MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (2928390)

MS14-012: Cumulative Security Update for Internet Explorer (2925418)

MS14-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2929961)

MS14-014: Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)

MS14-015: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2930275)

MS14-016: Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass (2934418)

MS14-017: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2949660)

MS14-018: Cumulative Security Update for Internet Explorer (2950467)

MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2922229)

MS14-020: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (2950145)

MS14-021: Security Update for Internet Explorer (2965111)

MS14-022: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2952166)

MS14-023: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2961037)

MS14-024: Vulnerability in a Microsoft Common Control Could Allow Security Feature Bypass (2961033)

MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege (2962486)

MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)

MS14-027: Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege (2962488)

MS14-028: Vulnerabilities in iSCSI Could Allow Denial of Service (2962485)

MS14-029: Security Update for Internet Explorer (2962482)

MS14-030: Vulnerability in Remote Desktop Could Allow Tampering (2969259)

MS14-031: Vulnerability in TCP Protocol Could Allow Denial of Service (2962478)

MS14-032: Vulnerability in Microsoft Lync Server Could Allow Information Disclosure (2969258)

MS14-033: Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2966061)

MS14-034: Vulnerability in Microsoft Word Could Allow Remote Code Execution (2969261)

MS14-035: Cumulative Security Update for Internet Explorer (2969262)

MS14-036: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (2967487)

MS14-037: Cumulative Security Update for Internet Explorer (2975687)

MS14-038: Vulnerability in Windows Journal Could Allow Remote Code Execution (2975689)

MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege (2975685)

MS14-040: Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (2975684)

MS14-041: Vulnerability in Microsoft DirectShow Could Allow Elevation of Privilege (2975681)

MS14-042: Vulnerability in Microsoft Service Bus Could Allow Denial of Service (2972621)

MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution (2978742)

MS14-044: Vulnerability in SQL Server Could Allow Elevation of Privilege (2984340)

MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2984615)

MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass (2984625)

MS14-047: Vulnerability in LRPC Could Allow Security Feature Bypass (2978668)

MS14-048: Vulnerability in OneNote Could Allow Remote Code Execution (2977201)

MS14-049: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (2962490)

MS14-050: Vulnerability in Microsoft SharePoint Server Could Allow Elevation of Privilege (2977202)

MS14-051: Cumulative Security Update for Internet Explorer (2976627)

MS14-052: Cumulative Security Update for Internet Explorer (2977629)

MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service (2990931)

MS14-054: Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (2988948)

MS14-055: Vulnerability in Microsoft Lync Server Could Allow Denial of Service (2990928)

MS14-056: Cumulative Security Update for Internet Explorer (2987107)

MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)

MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)

MS14-059: Vulnerability in ASP.NET MVC Could Allow Security Feature Bypass (2990942)

MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)

MS14-061: Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

MS14-062: Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254)

MS14-063: Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege (2998579)

MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)

MS14-065: Cumulative Security Update for Internet Explorer (3003057)

MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)

MS14-067: Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)

MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780) (ESKIMOROLL)

MS14-069: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3009710)

MS14-070: Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)

MS14-071: Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)

MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)

MS14-073: Vulnerability in Microsoft SharePoint Foundation Could Allow Elevation of Privilege (3000431)

MS14-074: Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass (3003743)

MS14-075: Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3009712)

MS14-076: Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass (2982998)

MS14-077: Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (3003381)

MS14-078: Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)

MS14-079: Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (3002885)

MS14-080: Cumulative Security Update for Internet Explorer (3008923)

MS14-081: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3017301)

MS14-082: Vulnerability in Microsoft Office Could Allow Remote Code Execution (3017349)

MS14-083: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (3017347)

MS14-084: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3016711)

MS14-085: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3013126)

MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266)

MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (3020393)

MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (3021674)

MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege (3025421)

MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (3022777)

MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (3004365)

MS15-007: Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (3014029)

MS15-008: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3019215)

MS15-009: Security Update for Internet Explorer (3034682)

MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)

MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)

MS15-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3032328)

MS15-013: Vulnerability in Microsoft Office Could Allow Security Feature Bypass (3033857)

MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass (3004361)

MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (3031432)

MS15-016: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3029944)

MS15-017: Vulnerability in Virtual Machine Manager Could Allow Elevation of Privilege (3035898)

MS15-018: Cumulative Security Update for Internet Explorer (3032359)

MS15-019: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3040297)

MS15-020: Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (3041836) (EASYHOOKUP)

MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (3032323)

MS15-022: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3038999)

MS15-023: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (3034344)

MS15-024: Vulnerability in PNG Processing Could Allow Information Disclosure (3035132)

MS15-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)

MS15-026: Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3040856)

MS15-027: Vulnerability in NETLOGON Could Allow Spoofing (3002657)

MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (3030377)

MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (3035126)

MS15-030: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (3039976)

MS15-031: Vulnerability in Schannel Could Allow Security Feature Bypass (3046049) (FREAK)

MS15-032: Cumulative Security Update for Internet Explorer (3038314)

MS15-033: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)

MS15-035: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)

MS15-036: Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (3052044)

MS15-037: Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (3046269)

MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)

MS15-039: Vulnerability in XML Core Services Could Allow Security Feature Bypass (3046482)

MS15-040: Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (3045711)

MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure (3048010)

MS15-042: Vulnerability in Windows Hyper-V Could Allow Denial of Service (3047234)

MS15-043: Cumulative Security Update for Internet Explorer (3049563)

MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)

MS15-045: Vulnerability in Windows Journal Could Allow Remote Code Execution (3046002)

MS15-046: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3057181)

MS15-047: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (3058083)

MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3057134)

MS15-049: Vulnerability in Silverlight Could Allow Elevation of Privilege (3058985)

MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege (3055642)

MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191)

MS15-052: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514)

MS15-053: Vulnerabilities in JScript and VBScript Scripting Engines Could Allow Security Feature Bypass (3057263)

MS15-054: Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service (3051768)

MS15-055: Vulnerability in Schannel Could Allow Information Disclosure (3061518)

MS15-056: Cumulative Security Update for Internet Explorer (3058515)

MS15-057: Vulnerability in Windows Media Player Could Allow Remote Code Execution (3033890)

MS15-058: Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718)

MS15-059: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3064949)

MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (3059317)

MS15-061: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057839)

MS15-062: Vulnerability in Active Directory Federation Services Could Allow Elevation of Privilege (3062577)

MS15-063: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (3063858)

MS15-064: Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3062157)

MS15-065: Cumulative Security Update for Internet Explorer (3076321)

MS15-066: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3072604)

MS15-067: Vulnerability in RDP Could Allow Remote Code Execution (3073094)

MS15-068: Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution (3072000)

MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)

MS15-070: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)

MS15-071: Vulnerability in NETLOGON Could Allow Elevation of Privilege (3068457)

MS15-072: Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (3069392)

MS15-073: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3070102)

MS15-074: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (3072630)

MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege (3072633)

MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (3067505)

MS15-077: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (3077657)

MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904)

MS15-079: Cumulative Security Update for Internet Explorer (3082442)

MS15-080 : Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)

MS15-081: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)

MS15-082: Vulnerability in RDP Could Allow Remote Code Execution (3080348)

MS15-083: Vulnerability in Server Message Block Could Allow Remote Code Execution (3073921)

MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure (3080129)

MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege (3082487)

MS15-086: Vulnerability in System Center Operations Manager Could Allow Elevation of Privilege (3075158)

MS15-087: Vulnerability in UDDI Services Could Allow Elevation of Privilege (3082459)

MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)

MS15-089: Vulnerability in WebDAV Could Allow Information Disclosure (3076949)

MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3060716)

MS15-091: Cumulative Security Update for Microsoft Edge (3084525)

MS15-092: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3086251)

MS15-093: Security Update for Internet Explorer (3088903)

MS15-094: Cumulative Security Update for Internet Explorer (3089548)

MS15-095: Cumulative Security Update for Microsoft Edge (3089665)

MS15-096: Vulnerability in Active Directory Service Could Allow Denial of Service (3072595)

MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)

MS15-098: Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)

MS15-099: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)

MS15-100: Vulnerability in Windows Media Center Could Allow Remote Code Execution (3087918)

MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)

MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657)

MS15-103: Vulnerabilities in Microsoft Exchange Server Could Allow Information Disclosure (3089250)

MS15-104: Vulnerabilities in Skype for Business Server and Lync Server Could Allow Elevation of Privilege (3089952)

MS15-105: Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass (3091287)

MS15-106: Cumulative Security Update for Internet Explorer (3096441)

MS15-107: Cumulative Security Update for Microsoft Edge (3096448)

MS15-108: Security Update for JScript and VBScript to Address Remote Code Execution (3089659)

MS15-109: Security Update for Windows Shell to Address Remote Code Execution (3096443)

MS15-110: Security Updates for Microsoft Office to Address Remote Code Execution (3089440)

MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege (3096447)

MS15-112: Cumulative Security Update for Internet Explorer (3104517)

MS15-113: Cumulative Security Update for Microsoft Edge (3104519)

MS15-114: Security Update for Windows Journal to Address Remote Code Execution (3100213)

MS15-115: Security Update for Microsoft Windows to Address Remote Code Execution (3105864)

MS15-116: Security Update for Microsoft Office to Address Remote Code Execution (3104540)

MS15-117: Security Update for NDIS to Address Elevation of Privilege (3101722)

MS15-118: Security Update for .NET Framework to Address Elevation of Privilege (3104507)

MS15-119: Security Update for Winsock to Address Elevation of Privilege (3104521)

MS15-120: Security Update for IPSec to Address Denial of Service (3102939)

MS15-121: Security Update for Schannel to Address Spoofing (3081320)

MS15-122: Security Update for Kerberos to Address Security Feature Bypass (3105256)

MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)

MS15-124: Cumulative Security Update for Internet Explorer (3116180)

MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (3125869)

MS15-125: Cumulative Security Update for Microsoft Edge (3116184)

MS15-126: Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3116178)

MS15-127: Security Update for Microsoft Windows DNS to Address Remote Code Execution (3100465)

MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)

MS15-129: Security Update for Silverlight to Address Remote Code Execution (3106614)

MS15-130: Security Update for Microsoft Uniscribe to Address Remote Code Execution (3108670)

MS15-131: Security Update for Microsoft Office to Address Remote Code Execution (3116111)

MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (3116162)

MS15-133: Security Update for Windows PGM to Address Elevation of Privilege (3116130)

MS15-134: Security Update for Windows Media Center to Address Remote Code Execution (3108669)

MS15-135: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3119075)

MS16-001: Cumulative Security Update for Internet Explorer (3124903)

MS16-002: Cumulative Security Update for Microsoft Edge (3124904)

MS16-003: Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3125540)

MS16-004: Security Update for Microsoft Office to Address Remote Code Execution (3124585)

MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)

MS16-006: Security Update for Silverlight to Address Remote Code Execution (3126036)

MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (3124901)

MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege (3124605)

MS16-009: Cumulative Security Update for Internet Explorer (3134220)

MS16-010: Security Update in Microsoft Exchange Server to Address Spoofing (3124557)

MS16-011: Cumulative Security Update for Microsoft Edge (3134225)

MS16-012: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)

MS16-013: Security Update for Windows Journal to Address Remote Code Execution (3134811)

MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228)

MS16-015: Security Update for Microsoft Office to Address Remote Code Execution (3134226)

MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041)

MS16-017: Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)

MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)

MS16-019: Security Update for .NET Framework to Address Denial of Service (3137893)

MS16-020: Security Update for Active Directory Federation Services to Address Denial of Service (3134222)

MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (3133043)

MS16-022: Security Update for Adobe Flash Player (3135782)

MS16-023: Cumulative Security Update for Internet Explorer (3142015)

MS16-024: Cumulative Security Update for Microsoft Edge (3142019)

MS16-025: Security Update for Windows Library Loading to Address Remote Code Execution (3140709)

MS16-026: Security Update for Graphic Fonts to Address Remote Code Execution (3143148)

MS16-027: Security Update for Windows Media to Address Remote Code Execution (3143146)

MS16-028: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3143081)

MS16-029: Security Update for Microsoft Office to Address Remote Code Execution (3141806)

MS16-030: Security Update for Windows OLE to Address Remote Code Execution (3143136)

MS16-031: Security Update for Microsoft Windows to Address Elevation of Privilege (3140410)

MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege (3143141)

MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (3143142)

MS16-034: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3143145)

MS16-035: Security Update for .NET Framework to Address Security Feature Bypass (3141780)

MS16-036: Security Update for Adobe Flash Player (3144756)

MS16-037: Cumulative Security Update for Internet Explorer (3148531)

MS16-038: Cumulative Security Update for Microsoft Edge (3148532)

MS16-039: Security Update for Microsoft Graphics Component (3148522)

MS16-040: Security Update for Microsoft XML Core Services (3148541)

MS16-041: Security Update for .NET Framework (3148789)

MS16-042: Security Update for Microsoft Office (3148775)

MS16-044: Security Update for Windows OLE (3146706)

MS16-045: Security Update for Windows Hyper-V (3143118)

MS16-046: Security Update for Secondary Logon (3148538)

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock)

MS16-048: Security Update for CSRSS (3148528)

MS16-049: Security Update for HTTP.sys (3148795)

MS16-050: Security Update for Adobe Flash Player (3154132)

MS16-051: Cumulative Security Update for Internet Explorer (3155533)

MS16-052: Cumulative Security Update for Microsoft Edge (3155538)

MS16-053: Cumulative Security Update for JScript and VBScript (3156764)

MS16-054: Security Update for Microsoft Office (3155544)

MS16-055: Security Update for Microsoft Graphics Component (3156754)

MS16-056: Security Update for Windows Journal (3156761)

MS16-057: Security Update for Windows Shell (3156987)

MS16-058: Security Update for Windows IIS (3141083)

MS16-059: Security Update for Windows Media Center (3150220)

MS16-060: Security Update for Windows Kernel (3154846)

MS16-061: Security Update for Microsoft RPC (3155520)

MS16-062: Security Update for Windows Kernel-Mode Drivers (3158222)

MS16-063: Cumulative Security Update for Internet Explorer (3163649)

MS16-064: Security Update for Adobe Flash Player (3163207)

MS16-065: Security Update for .NET Framework (3156757)

MS16-066: Security Update for Virtual Secure Mode (3155451)

MS16-067: Security Update for Volume Manager Driver (3155784)

MS16-068: Cumulative Security Update for Microsoft Edge (3163656)

MS16-069: Cumulative Security Update for JScript and VBScript (3163640)

MS16-070: Security Update for Microsoft Office (3163610)

MS16-071: Security Update for Microsoft Windows DNS Server (3164065)

MS16-072: Security Update for Group Policy (3163622)

MS16-073: Security Update for Windows Kernel-Mode Drivers (3164028)

MS16-074: Security Update for Microsoft Graphics Component (3164036)

MS16-075: Security Update for Windows SMB Server (3164038)

MS16-076: Security Update for Netlogon (3167691)

MS16-077: Security Update for WPAD (3165191)

MS16-078: Security Update for Windows Diagnostic Hub (3165479)

MS16-079: Security Update for Microsoft Exchange Server (3160339)

MS16-080: Security Update for Microsoft Windows PDF (3164302)

MS16-081: Security Update for Active Directory (3160352)

MS16-082: Security Update for Microsoft Windows Search Component (3165270)

MS16-083: Security Update for Adobe Flash Player (3167685)

MS16-084: Cumulative Security Update for Internet Explorer (3169991)

MS16-085: Cumulative Security Update for Microsoft Edge (3169999)

MS16-086: Cumulative Security Update for JScript and VBScript (3169996)

MS16-087: Security Update for Windows Print Spooler (3170005)

MS16-088: Security Update for Microsoft Office (3170008)

MS16-089: Security Update for Windows Secure Kernel Mode (3170050)

MS16-090: Security Update for Windows Kernel-Mode Drivers (3171481)

MS16-091: Security Update for .NET Framework (3170048)

MS16-092: Security Update for Windows Kernel (3171910)

MS16-093: Security Update for Adobe Flash Player (3174060)

MS16-094: Security Update for Secure Boot (3177404)

MS16-095: Cumulative Security Update for Internet Explorer (3177356)

MS16-096: Cumulative Security Update for Microsoft Edge (3177358)

MS16-097: Security Update for Microsoft Graphics Component (3177393)

MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466)

MS16-099: Security Update for Microsoft Office (3177451)

MS16-100: Security Update for Secure Boot (3179577)

MS16-101: Security Update for Windows Authentication Methods (3178465)

MS16-102: Security Update for Microsoft Windows PDF Library (3182248)

MS16-103: Security Update for ActiveSyncProvider (3182332)

MS16-104: Cumulative Security Update for Internet Explorer (3183038)

MS16-105: Cumulative Security Update for Microsoft Edge (3183043)

MS16-106: Security Update for Microsoft Graphics Component (3185848)

MS16-107: Security Update for Microsoft Office (3185852)

MS16-108: Security Update for Microsoft Exchange Server (3185883)

MS16-109: Security Update for Silverlight (3182373)

MS16-110: Security Update for Microsoft Windows (3178467)

MS16-111: Security Update for Windows Kernel (3186973)

MS16-112: Security Update for Windows Lock Screen (3178469)

MS16-113: Security Update for Windows Secure Kernel Mode (3185876)

MS16-114: Security Update for Windows SMBv1 Server (3185879)

MS16-115: Security Update for Microsoft Windows PDF Library (3188733)

MS16-116: Security Update in OLE Automation for VBScript Scripting Engine (3188724)

MS16-117: Security Update for Adobe Flash Player (3188128)

MS16-118: Cumulative Security Update for Internet Explorer (3192887)

MS16-119: Cumulative Security Update for Microsoft Edge (3192890)

MS16-120: Security Update for Microsoft Graphics Component (3192884)

MS16-121: Security Update for Microsoft Office (3194063)

MS16-122: Security Update for Microsoft Video Control (3195360)

MS16-123: Security Update for Windows Kernel-Mode Drivers (3192892)

MS16-124: Security Update for Windows Registry (3193227)

MS16-125: Security Update for Windows Diagnostic Hub (3193229)

MS16-126: Security Update for Microsoft Internet Messaging API (3196067)

MS16-127: Security Update for Adobe Flash Player (3194343)

MS16-128: Security Update for Adobe Flash Player (3201860)

MS16-129: Cumulative Security Update for Microsoft Edge (3199057)

MS16-130: Security Update for Microsoft Windows (3199172)

MS16-131: Security Update for Microsoft Video Control (3199151)

MS16-132: Security Update for Microsoft Graphics Component (3199120)

MS16-133: Security Update for Microsoft Office (3199168)

MS16-134: Security Update for Common Log File System Driver (3193706)

MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135)

MS16-136: Security Update for SQL Server (3199641)

MS16-137: Security Update for Windows Authentication Methods (3199173)

MS16-138: Security Update for Microsoft Virtual Hard Disk Driver (3199647)

MS16-139: Security Update for Windows Kernel (3199720)

MS16-140: Security Update for Boot Manager (3193479)

MS16-141: Security Update for Adobe Flash Player (3202790)

MS16-142: Cumulative Security Update for Internet Explorer (3198467)

MS16-144: Cumulative Security Update for Internet Explorer (3204059)

MS16-145: Cumulative Security Update for Microsoft Edge (3204062)

MS16-146: Security Update for Microsoft Graphics Component (3204066)

MS16-147: Security Update for Microsoft Uniscribe (3204063)

MS16-148: Security Update for Microsoft Office (3204068)

MS16-149: Security Update for Microsoft Windows (3205655)

MS16-150: Security Update for Secure Kernel Mode (3205642)

MS16-151: Security Update for Windows Kernel-Mode Drivers (3205651)

MS16-152: Security Update for Windows Kernel (3199709)

MS16-153: Security Update for Common Log File System Driver (3207328)

MS16-154: Security Update for Adobe Flash Player (3209498)

MS16-155: Security Update for .NET Framework (3205640)

MS17-001: Security Update for Microsoft Edge (3214288)

MS17-002: Security Update for Microsoft Office (3214291)

MS17-003: Security Update for Adobe Flash Player (3214628)

MS17-004: Security Update for Local Security Authority Subsystem Service (3216771)

MS17-005: Security Update for Adobe Flash Player (4010250)

MS17-006: Cumulative Security Update for Internet Explorer (4013073)

MS17-007: Cumulative Security Update for Microsoft Edge (4013071)

MS17-008: Security Update for Windows Hyper-V (4013082)

MS17-009: Security Update for Microsoft Windows PDF Library (4010319)

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya)

MS17-011: Security Update for Microsoft Uniscribe (4013076)

MS17-012: Security Update for Microsoft Windows (4013078)

MS17-013: Security Update for Microsoft Graphics Component (4013075)

MS17-014: Security Update for Microsoft Office (4013241)

MS17-015: Security Update for Microsoft Exchange Server (4013242)

MS17-016: Security Update for Windows IIS (4013074)

MS17-017: Security Update for Windows Kernel (4013081)

MS17-018: Security Update for Windows Kernel-Mode Drivers (4013083)

MS17-019: Security Update for Active Directory Federation Services (4010320)

MS17-020: Security Update for Windows DVD Maker (3208223)

MS17-021: Security Update for Windows DirectShow (4010318)

MS17-022: Security Update for Microsoft XML Core Services (4010321)

MS17-023: Security Update for Adobe Flash Player (4014329)

Security and Quality Rollup for .NET Framework (April 2017)

Security and Quality Rollup for .NET Framework (January 2018)

Security and Quality Rollup for .NET Framework (May 2017)

Security and Quality Rollup for .NET Framework (Sep 2017)

Security Update for Exchange (September 2018)

Security Update for Internet Explorer (CVE-2019-1367)

Security Update for Live Meeting 2007 / Lync 2010 and 2013 / Skype for Business 2016 (June 2017)

Security Update for Microsoft Office Excel Products (September 2017)

Security Update for Microsoft Office Online Server and Office Web Apps (October 2017)

Security Update for Microsoft Office Online Server and Office Web Apps (September 2017)

Security Update for Microsoft Office Online Server and SharePoint Server 2010 Office Web Apps (July 2017)

Security Update for Microsoft Office Products (April 2017) (Petya)

Security Update for Microsoft Office Products (July 2017)

Security Update for Microsoft Office Products (June 2017)

Security Update for Microsoft Office Products (May 2017)

Security Update for Microsoft Office Web Apps Server / Office Online Server (June 2017)

Security Update for Microsoft Office Word Viewer (October 2017)

Security Update for Microsoft SharePoint Server (January 2018)

Security Update for Microsoft SharePoint Server (June 2017)

Security Update for Microsoft SharePoint Server 2010 (August 2017)

Security Update for Microsoft SharePoint Server 2016 (December 2017)

Security Update for Microsoft SharePoint Server and Project Server (July 2017)

Security Updates for Azure DevOps Server (June 2019)

Security Updates for Exchange (April 2019)

Security Updates for Exchange (August 2018)

Security Updates for Exchange (December 2017)

Security Updates for Exchange (December 2018)

Security Updates for Exchange (February 2019)

Security Updates for Exchange (February 2020)

Security Updates for Exchange (January 2019)

Security Updates for Exchange (July 2019)

Security Updates for Exchange (June 2019)

Security Updates for Exchange (March 2018)

Security Updates for Exchange (March 2020)

Security Updates for Exchange (May 2018)

Security Updates for Exchange (November 2019)

Security Updates for Exchange (October 2018)

Security Updates for Exchange (September 2017)

Security Updates for Exchange (September 2019)

Security Updates for Internet Explorer (April 2017)

Security Updates for Internet Explorer (April 2018)

Security Updates for Internet Explorer (April 2019)

Security Updates for Internet Explorer (April 2020)

Security Updates for Internet Explorer (August 2017)

Security Updates for Internet Explorer (August 2018)

Security Updates for Internet Explorer (August 2019)

Security Updates for Internet Explorer (December 2017)

Security Updates for Internet Explorer (December 2018 OOB)

Security Updates for Internet Explorer (December 2018)

Security Updates for Internet Explorer (December 2019)

Security Updates for Internet Explorer (February 2018)

Security Updates for Internet Explorer (February 2019)

Security Updates for Internet Explorer (February 2020)

Security Updates for Internet Explorer (January 2018)

Security Updates for Internet Explorer (January 2019)

Security Updates for Internet Explorer (January 2020)

Security Updates for Internet Explorer (July 2017)

Security Updates for Internet Explorer (July 2018)

Security Updates for Internet Explorer (July 2019)

Security Updates for Internet Explorer (June 2017)

Security Updates for Internet Explorer (June 2018)

Security Updates for Internet Explorer (June 2019)

Security Updates for Internet Explorer (March 2018)

Security Updates for Internet Explorer (March 2019)

Security Updates for Internet Explorer (March 2020)

Security Updates for Internet Explorer (May 2017)

Security Updates for Internet Explorer (May 2018)

Security Updates for Internet Explorer (May 2019)

Security Updates for Internet Explorer (November 2017)

Security Updates for Internet Explorer (November 2018)

Security Updates for Internet Explorer (November 2019)

Security Updates for Internet Explorer (October 2017)

Security Updates for Internet Explorer (October 2018)

Security Updates for Internet Explorer (October 2019)

Security Updates for Internet Explorer (September 2017)

Security Updates for Internet Explorer (September 2018)

Security Updates for Internet Explorer (September 2019)

Security Updates for Microsoft .NET core and ASP.NET (Bypass) (July 2018)

Security Updates for Microsoft .NET core and ASP.NET (DoS) (July 2018)

Security Updates for Microsoft .NET core and ASP.NET Core (DoS) (September 2018)

Security Updates for Microsoft .NET Framework (August 2018)

Security Updates for Microsoft .NET Framework (December 2018)

Security Updates for Microsoft .NET Framework (February 2019)

Security Updates for Microsoft .NET Framework (January 2019)

Security Updates for Microsoft .NET Framework (January 2020)

Security Updates for Microsoft .NET Framework (July 2018) (deprecated)

Security Updates for Microsoft .NET Framework (July 2019)

Security Updates for Microsoft .NET Framework (May 2018)

Security Updates for Microsoft .NET Framework (May 2019)

Security Updates for Microsoft .NET Framework (September 2018)

Security Updates for Microsoft .NET Framework (September 2019)

Security Updates for Microsoft Access Products (April 2020)

Security Updates for Microsoft Access Products (July 2018)

Security Updates for Microsoft Access Products (March 2018)

Security Updates for Microsoft Business Productivity Server (April 2020)

Security Updates for Microsoft Dynamics 365 (on-premises) (April 2020)

Security Updates for Microsoft Dynamics 365 (on-premises) (October 2019)

Security Updates for Microsoft Excel Products (April 2018)

Security Updates for Microsoft Excel Products (April 2019)

Security Updates for Microsoft Excel Products (April 2020)

Security Updates for Microsoft Excel Products (August 2018)

Security Updates for Microsoft Excel Products (December 2018)

Security Updates for Microsoft Excel Products (December 2019)

Security Updates for Microsoft Excel Products (February 2018)

Security Updates for Microsoft Excel Products (February 2019)

Security Updates for Microsoft Excel Products (February 2020)

Security Updates for Microsoft Excel Products (January 2018)

Security Updates for Microsoft Excel Products (January 2020)

Security Updates for Microsoft Excel Products (July 2019)

Security Updates for Microsoft Excel Products (June 2018)

Security Updates for Microsoft Excel Products (March 2018)

Security Updates for Microsoft Excel Products (May 2018)

Security Updates for Microsoft Excel Products (November 2017)

Security Updates for Microsoft Excel Products (November 2018)

Security Updates for Microsoft Excel Products (November 2019)

Security Updates for Microsoft Excel Products (October 2018)

Security Updates for Microsoft Excel Products (October 2019)

Security Updates for Microsoft Excel Products (September 2018)

Security Updates for Microsoft Excel Products (September 2019)

Security Updates for Microsoft Lync Server 2013 (September 2019)

Security Updates for Microsoft Lync Server and Skype for Business Server (June 2019)

Security Updates for Microsoft Office Compatibility Pack SP3 (October 2017)

Security Updates for Microsoft Office Compatibility Pack SP3 (September 2017)

Security Updates for Microsoft Office Compatibility Products (April 2018)

Security Updates for Microsoft Office Compatibility Products (December 2018)

Security Updates for Microsoft Office Compatibility Products (June 2018)

Security Updates for Microsoft Office Compatibility Products (March 2018)

Security Updates for Microsoft Office Compatibility Products (May 2018)

Security Updates for Microsoft Office Compatibility Products (November 2018)

Security Updates for Microsoft Office Compatibility Products (September 2018)

Security Updates for Microsoft Office Compatibility SP3 (January 2018)

Security Updates for Microsoft Office Compatibility SP3 (November 2017)

Security Updates for Microsoft Office Online Server (February 2020)

Security Updates for Microsoft Office Online Server (January 2020)

Security Updates for Microsoft Office Online Server (November 2019)

Security Updates for Microsoft Office Online Server (October 2019)

Security Updates for Microsoft Office Online Server and Microsoft Office Web Apps (December 2018)

Security Updates for Microsoft Office Online Server and Microsoft Office Web Apps (January 2018)

Security Updates for Microsoft Office Online Server and Microsoft Office Web Apps (June 2018)

Security Updates for Microsoft Office Online Server and Microsoft Office Web Apps (March 2018)

Security Updates for Microsoft Office Online Server Apps (May 2019)

Security Updates for Microsoft Office Products (April 2018)

Security Updates for Microsoft Office Products (April 2019)

Security Updates for Microsoft Office Products (April 2020)

Security Updates for Microsoft Office Products (August 2018)

Security Updates for Microsoft Office Products (August 2019)

Security Updates for Microsoft Office Products (December 2017)

Security Updates for Microsoft Office Products (December 2018)

Security Updates for Microsoft Office Products (December 2019)

Security Updates for Microsoft Office Products (February 2018)

Security Updates for Microsoft Office Products (February 2019)

Security Updates for Microsoft Office Products (February 2020)

Security Updates for Microsoft Office Products (January 2018)

Security Updates for Microsoft Office Products (January 2019)

Security Updates for Microsoft Office Products (January 2020)

Security Updates for Microsoft Office Products (July 2018)

Security Updates for Microsoft Office Products (July 2019)

Security Updates for Microsoft Office Products (June 2018)

Security Updates for Microsoft Office Products (June 2019)

Security Updates for Microsoft Office Products (March 2018)

Security Updates for Microsoft Office Products (March 2019)

Security Updates for Microsoft Office Products (March 2020)

Security Updates for Microsoft Office Products (May 2018)

Security Updates for Microsoft Office Products (May 2019)

Security Updates for Microsoft Office Products (November 2017)

Security Updates for Microsoft Office Products (November 2018)

Security Updates for Microsoft Office Products (November 2019)

Security Updates for Microsoft Office Products (October 2017)

Security Updates for Microsoft Office Products (October 2018)

Security Updates for Microsoft Office Products (October 2019)

Security Updates for Microsoft Office Products (September 2017)

Security Updates for Microsoft Office Products (September 2018)

Security Updates for Microsoft Office Products (September 2019)

Security Updates for Microsoft Office Viewer Products (April 2018)

Security Updates for Microsoft Office Viewer Products (December 2018)

Security Updates for Microsoft Office Viewer Products (January 2018)

Security Updates for Microsoft Office Viewer Products (January 2019)

Security Updates for Microsoft Office Viewer Products (June 2018)

Security Updates for Microsoft Office Viewer Products (November 2017)

Security Updates for Microsoft Office Viewer Products (November 2018)

Security Updates for Microsoft Office Viewer Products (September 2018)

Security Updates for Microsoft Office Viewer Products / Office Compatibility Products (August 2018)

Security Updates for Microsoft Office Viewer Products / Office Compatibility Products (July 2018)

Security Updates for Microsoft Office Viewer Products / Office Compatibility Products (October 2018)

Security Updates for Microsoft Office Viewers (September 2017)

Security Updates for Microsoft Office Viewers And Compatibility Products (February 2019)

Security Updates for Microsoft Office Web Apps (April 2018)

Security Updates for Microsoft Office Web Apps (April 2020)

Security Updates for Microsoft Office Web Apps (August 2018)

Security Updates for Microsoft Office Web Apps (August 2019)

Security Updates for Microsoft Office Web Apps (January 2019)

Security Updates for Microsoft Office Web Apps (March 2020)

Security Updates for Microsoft Office Web Apps (May 2018)

Security Updates for Microsoft Office Web Apps (November 2017)

Security Updates for Microsoft Office Web Apps (November 2018)

Security Updates for Microsoft Office Web Apps (October 2018)

Security Updates for Microsoft Office Web Apps / Office Online Server (June 2019)

Security Updates for Microsoft PowerPoint Products (April 2020)

Security Updates for Microsoft Powerpoint Products (August 2018)

Security Updates for Microsoft PowerPoint Products (December 2018)

Security Updates for Microsoft PowerPoint Products (December 2019)

Security Updates for Microsoft PowerPoint Products (October 2018)

Security Updates for Microsoft Powerpoint Products (September 2017)

Security Updates for Microsoft Project (September 2019)

Security Updates for Microsoft Project Server (June 2019)

Security Updates for Microsoft Project Server (November 2018)

Security Updates for Microsoft Publisher Products (April 2020)

Security Updates for Microsoft Publisher Products (June 2018)

Security Updates for Microsoft Publisher Products (September 2017)

Security Updates for Microsoft SharePoint Server (April 2018)

Security Updates for Microsoft SharePoint Server (April 2019)

Security Updates for Microsoft SharePoint Server (April 2020)

Security Updates for Microsoft Sharepoint Server (August 2018)

Security Updates for Microsoft SharePoint Server (August 2019)

Security Updates for Microsoft Sharepoint Server (December 2018)

Security Updates for Microsoft Sharepoint Server (February 2019)

Security Updates for Microsoft SharePoint Server (February 2020)

Security Updates for Microsoft Sharepoint Server (January 2019)

Security Updates for Microsoft Sharepoint Server (July 2018)

Security Updates for Microsoft SharePoint Server (July 2019)

Security Updates for Microsoft Sharepoint Server (June 2018)

Security Updates for Microsoft SharePoint Server (June 2019)

Security Updates for Microsoft Sharepoint Server (March 2019)

Security Updates for Microsoft SharePoint Server (March 2020)

Security Updates for Microsoft SharePoint Server (May 2019)

Security Updates for Microsoft SharePoint Server (November 2018)

Security Updates for Microsoft SharePoint Server (November 2019)

Security Updates for Microsoft SharePoint Server (Oct 2019)

Security Updates for Microsoft Sharepoint Server (October 2017)

Security Updates for Microsoft SharePoint Server (October 2018)

Security Updates for Microsoft Sharepoint Server (September 2017)

Security Updates for Microsoft SharePoint Server (September 2018)

Security Updates for Microsoft SharePoint Server (September 2019)

Security Updates for Microsoft SharePoint Server and Microsoft Project Server (February 2018)

Security Updates for Microsoft SharePoint Server and Microsoft Project Server (March 2018)

Security Updates for Microsoft SharePoint Server and Microsoft Project Server (May 2018)

Security Updates for Microsoft SharePoint Server and Microsoft Project Server (November 2017)

Security Updates for Microsoft Skype for Business (December 2019)

Security Updates for Microsoft Skype for Business and Microsoft Lync (January 2019 OOB)

Security Updates for Microsoft Skype for Business and Microsoft Lync (July 2018)

Security Updates for Microsoft Skype for Business and Microsoft Lync (July 2019)

Security Updates for Microsoft Skype for Business and Microsoft Lync (November 2018)

Security Updates for Microsoft Skype for Business and Microsoft Lync (October 2017)

Security Updates for Microsoft Skype for Business and Microsoft Lync and Microsoft Live Meeting (September 2017)

Security Updates for Microsoft SQL Server (February 2020)

Security Updates for Microsoft SQL Server (July 2019)

Security Updates for Microsoft SQL Server (May 2019)

Security Updates for Microsoft SQL Server 2016 and 2017 x64 (August 2018)

Security Updates for Microsoft Team Foundation Server (February 2019)

Security Updates for Microsoft Team Foundation Server (January 2019)

Security Updates for Microsoft Team Foundation Server (March 2019)

Security Updates for Microsoft Team Foundation Server (March 2020)

Security Updates for Microsoft Team Foundation Server (November 2018)

Security Updates for Microsoft Team Foundation Server / Azure DevOps Server (April 2019)

Security Updates for Microsoft Team Foundation Server / Azure DevOps Server (May 2019)

Security Updates for Microsoft Team Foundation Server and Azure DevOps Server (July 2019)

Security Updates for Microsoft Team Foundation Server and Azure DevOps Server (September 2019)

Security Updates for Microsoft Visio Products (April 2020)

Security Updates for Microsoft Visual Studio Products (April 2018)

Security Updates for Microsoft Visual Studio Products (April 2020)

Security Updates for Microsoft Visual Studio Products (Aug 2018)

Security Updates for Microsoft Visual Studio Products (August 2019)

Security Updates for Microsoft Visual Studio Products (December 2018)

Security Updates for Microsoft Visual Studio Products (December 2019)

Security Updates for Microsoft Visual Studio Products (February 2019)

Security Updates for Microsoft Visual Studio Products (January 2019)

Security Updates for Microsoft Visual Studio Products (July 2018)

Security Updates for Microsoft Visual Studio Products (July 2019)

Security Updates for Microsoft Visual Studio Products (March 2019)

Security Updates for Microsoft Visual Studio Products (March 2020)

Security Updates for Microsoft Visual Studio Products (May 2019)

Security Updates for Microsoft Visual Studio Products (November 2019)

Security Updates for Microsoft Visual Studio Products (September 2019)

Security Updates for Microsoft Word Products (April 2018)

Security Updates for Microsoft Word Products (April 2020)

Security Updates for Microsoft Word Products (August 2019)

Security Updates for Microsoft Word Products (December 2017)

Security Updates for Microsoft Word Products (December 2019)

Security Updates for Microsoft Word Products (January 2018)

Security Updates for Microsoft Word Products (January 2019)

Security Updates for Microsoft Word Products (July 2018)

Security Updates for Microsoft Word Products (June 2019)

Security Updates for Microsoft Word Products (March 2018)

Security Updates for Microsoft Word Products (March 2020)

Security Updates for Microsoft Word Products (May 2018)

Security Updates for Microsoft Word Products (May 2019)

Security Updates for Microsoft Word Products (November 2017)

Security Updates for Microsoft Word Products (November 2018)

Security Updates for Microsoft Word Products (October 2018)

Security Updates for Microsoft Word Products (September 2018)

Security Updates for Microsoft Word Viewer (February 2018)

Security Updates for Outlook (April 2020)

Security Updates for Outlook (August 2018)

Security Updates for Outlook (August 2019)

Security Updates for Outlook (December 2018)

Security Updates for Outlook (February 2018)

Security Updates for Outlook (February 2020)

Security Updates for Outlook (January 2018)

Security Updates for Outlook (January 2019)

Security Updates for Outlook (July 2017)

Security Updates for Outlook (July 2019)

Security Updates for Outlook (June 2018)

Security Updates for Outlook (November 2018)

Security Updates for Outlook (October 2017)

Security Updates for Outlook (October 2018)

Security Updates for Outlook (September 2017)

Security Updates for Windows 10 / Windows Server 2016 (August 2018) (Spectre) (Meltdown) (Foreshadow)

Security Updates for Windows 10 / Windows Server 2016 (January 2019) (Spectre)

Security Updates for Windows 10 / Windows Server 2016 (September 2018) (Spectre)

Security Updates for Windows 10 / Windows Server 2016 / Windows Server 2019 (March 2019) (Spectre) (Meltdown) (Foreshadow)

Security Updates for Windows 10 / Windows Server 2019 (February 2019) (Spectre) (Meltdown) (Foreshadow)

Security Updates for Windows Server 2008 (April 2018)

Security Updates for Windows Server 2008 (August 2018) (Foreshadow)

Security Updates for Windows Server 2008 (February 2018)

Security Updates for Windows Server 2008 (July 2018)

Security Updates for Windows Server 2008 (June 2018)

Security Updates for Windows Server 2008 (March 2018)

Security Updates for Windows Server 2008 (May 2018)

Skype for Business and Lync Spoofing Vulnerability

Windows 10, Server 2016 and Server 2019 September 2019 Security Update (CVE-2019-1367)

Windows 2008 August 2017 Multiple Security Updates

Windows 2008 December 2017 Multiple Security Updates

Windows 2008 January 3 2018 Multiple Security Updates

Windows 2008 July 2017 Multiple Security Updates

Windows 2008 June 2017 Multiple Security Updates

Windows 2008 May 2017 Multiple Security Updates

Windows 2008 November 2017 Multiple Security Updates

Windows 2008 October 2017 Multiple Security Updates (KRACK)

Windows 2008 September 2017 Multiple Security Updates

Windows 7 and Windows 2008 R2 April 2017 Security Updates (Petya)

Windows 7 and Windows Server 2008 R2 August 2017 Security Updates

Windows 7 and Windows Server 2008 R2 December 2017 Security Updates

Windows 7 and Windows Server 2008 R2 July 2017 Security Updates

Windows 7 and Windows Server 2008 R2 June 2017 Security Updates

Windows 7 and Windows Server 2008 R2 May 2017 Security Updates

Windows 7 and Windows Server 2008 R2 November 2017 Security Updates

Windows 7 and Windows Server 2008 R2 October 2017 Security Updates (KRACK)

Windows 7 and Windows Server 2008 R2 September 2017 Security Updates

Windows 8 June 2017 Security Updates

Windows 8.1 and Server 2012 R2 KB4345424 Update

Windows 8.1 and Windows Server 2012 R2 April 2017 Security Updates

Windows 8.1 and Windows Server 2012 R2 August 2017 Security Updates

Windows 8.1 and Windows Server 2012 R2 December 2017 Security Updates

Windows 8.1 and Windows Server 2012 R2 July 2017 Security Updates

Windows 8.1 and Windows Server 2012 R2 June 2017 Security Updates

Windows 8.1 and Windows Server 2012 R2 May 2017 Security Updates

Windows 8.1 and Windows Server 2012 R2 November 2017 Security Updates

Windows 8.1 and Windows Server 2012 R2 October 2017 Security Updates (KRACK)

Windows 8.1 and Windows Server 2012 R2 September 2017 Security Updates

Windows Server 2012 April 2017 Security Updates (Petya)

Windows Server 2012 August 2017 Security Updates

Windows Server 2012 December 2017 Security Updates

Windows Server 2012 July 2017 Security Updates

Windows Server 2012 June 2017 Security Updates

Windows Server 2012 May 2017 Security Updates

Windows Server 2012 November 2017 Security Updates

Windows Server 2012 October 2017 Security Updates (KRACK)

Windows Server 2012 September 2017 Security Updates

# Windows

TeamViewer Insecure Directory Permissions Privilege Escalation

2X ApplicationServer TuxSystem ActiveX ExportSettings() Method Arbitrary File Overwrite

2X Client TuxClientSystem ActiveX InstallClient() Method Arbitrary MSI Package Installation

3CTftpSvc Long Transport Mode Remote Overflow

3D-FTP Multiple Directory Traversal Vulnerabilities

3DGreetings Player ActiveX Multiple Buffer Overflows

3ivx MPEG-4 < 5.0.2 Buffer Overflow

7-Zip < 16.00 Multiple Vulnerabilities

7-Zip < 16.03 NULL Pointer Dereference DoS

7-Zip < 18.00 Multiple Vulnerabilities

7-Zip < 18.05 Memory Corruption Arbitrary Code Execution

7-Zip < 4.57 Archive Handling Unspecified Issue

7-Zip ARJ File Handling Overflow

7-Zip Installed

7-Zip Recent Files

Absolute Software Computrace LoJack for Laptops Detection

ACDSee Pro < 5.2 Multiple Memory Corruption Vulnerabilities

Acer AcerCtrls.APlunch ActiveX Arbitrary Command Execution

Acer LunchApp.APlunch ActiveX Arbitrary Command Execution

Active Directory - Enumerate Computer Objects

Active Directory - Enumerate Directory Trusts

Active Directory - Enumerate Group Memberships

Active Directory - Enumerate User Account Policy

Active Directory - Enumerate Users and Groups

activePDF Server < 3.8.6 Packet Handling Remote Overflow

activePDF Server < 3.8.6 Packet Handling Remote Overflow (credentialed check)

Acunetix Web Vulnerability Scanner 4 < 4.0.20060717 Denial of Service

Acunetix Web Vulnerability Scanner Detection

Adobe Acrobat 11.0.4 Crafted PDF File Handling JavaScript Scheme URI Execution (APSB13-25)

Adobe Acrobat 9.x / 10.x Multiple Vulnerabilities (APSB11-08)

Adobe Acrobat 9.x / 10.x Unspecified Memory Corruption (APSB11-06)

Adobe Acrobat 9.x < 9.4.1 Multiple Vulnerabilities (APSB10-28)

Adobe Acrobat < 10.0.1 / 9.4.2 / 8.2.5 Multiple Vulnerabilities (APSB11-03)

Adobe Acrobat < 10.1 / 9.4.5 / 8.3 Multiple Vulnerabilities (APSB11-16)

Adobe Acrobat < 10.1.1 / 9.4.6 / 8.3.1 Multiple Vulnerabilities (APSB11-21, APSB11-24)

Adobe Acrobat < 10.1.10 / 11.0.07 Multiple Vulnerabilities (APSB14-15)

Adobe Acrobat < 10.1.11 / 11.0.08 Sandbox Bypass (APSB14-19)

Adobe Acrobat < 10.1.12 / 11.0.09 Multiple Vulnerabilities (APSB14-20)

Adobe Acrobat < 10.1.13 / 11.0.10 Multiple Vulnerabilities (APSB14-28)

Adobe Acrobat < 10.1.14 / 11.0.11 Multiple Vulnerabilities (APSB15-10)

Adobe Acrobat < 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-15)

Adobe Acrobat < 10.1.2 / 9.5 Multiple Vulnerabilities (APSB12-01)

Adobe Acrobat < 10.1.3 / 9.5.1 Multiple Vulnerabilities (APSB12-08)

Adobe Acrobat < 10.1.4 / 9.5.2 Multiple Vulnerabilities (APSB12-16)

Adobe Acrobat < 10.1.9 / 11.0.6 Multiple Vulnerabilities (APSB14-01)

Adobe Acrobat < 11.0.1 / 10.1.5 / 9.5.3 Multiple Vulnerabilities (APSB13-02)

Adobe Acrobat < 11.0.14 / 15.006.30119 / 15.010.20056 Multiple Vulnerabilities (APSB16-02)

Adobe Acrobat < 11.0.15 / 15.006.30121 / 15.010.20060 Multiple Vulnerabilities (APSB16-09)

Adobe Acrobat < 11.0.16 / 15.006.30172 / 15.016.20039 Multiple Vulnerabilities (APSB16-14)

Adobe Acrobat < 11.0.17 / 15.006.30198 / 15.017.20050 Multiple Vulnerabilities (APSB16-26)

Adobe Acrobat < 11.0.18 / 15.006.30243 / 15.020.20039 Multiple Vulnerabilities (APSB16-33)

Adobe Acrobat < 11.0.19 / 15.006.30279 / 15.023.20053 Multiple Vulnerabilities (APSB17-01)

Adobe Acrobat < 11.0.2 / 10.1.6 / 9.5.4 Multiple Vulnerabilities (APSB13-07)

Adobe Acrobat < 11.0.20 / 2015.006.30306 / 2017.009.20044 Multiple Vulnerabilities (APSB17-11)

Adobe Acrobat < 11.0.21 / 2015.006.30355 / 2017.011.30066 / 2017.012.20098 Multiple Vulnerabilities (APSB17-24)

Adobe Acrobat < 11.0.23 / 2015.006.30392 / 2017.011.30068 / 2018.009.20044 Multiple Vulnerabilities (APSB17-36)

Adobe Acrobat < 11.0.3 / 10.1.7 / 9.5.5 Multiple Vulnerabilities (APSB13-15)

Adobe Acrobat < 11.0.4 / 10.1.8 Multiple Vulnerabilities (APSB13-22)

Adobe Acrobat < 15.006.30434 / 17.011.30096 / 18.011.20055 Multiple Vulnerabilities (APSB18-21)

Adobe Acrobat < 2015.006.30413 / 2017.011.30078 / 2018.011.20035 Multiple Vulnerabilities (APSB18-02)

Adobe Acrobat < 2015.006.30418 / 2017.011.30080 / 2018.011.20040 Multiple Vulnerabilities (APSB18-09)

Adobe Acrobat < 2019.010.20091 / 2017.011.30120 / 2015.006.30475 Multiple Vulnerabilities (APSB19-07)

Adobe Acrobat < 6.0.5 PDF Distillation Overflow

Adobe Acrobat < 6.0.6 / 7.0.9 Multiple Vulnerabilities

Adobe Acrobat < 7.1.0 / 8.1.2 Unspecified JavaScript Method Handling Arbitrary Code Execution

Adobe Acrobat < 8.1.1 Crafted PDF File Arbitrary Code Execution

Adobe Acrobat < 8.1.2 / 7.1.0 Multiple Vulnerabilities

Adobe Acrobat < 8.1.3 Multiple Vulnerabilities

Adobe Acrobat < 9.1 / 8.1.4 / 7.1.1 Multiple Vulnerabilities

Adobe Acrobat < 9.1.1 / 8.1.5 / 7.1.2 getAnnots() JavaScript Method PDF Handling Memory Corruption (APSB09-06)

Adobe Acrobat < 9.1.2 / 8.1.6 / 7.1.3 Multiple Vulnerabilities

Adobe Acrobat < 9.1.3 Flash Handling Unspecified Arbitrary Code Execution

Adobe Acrobat < 9.2 / 8.1.7 / 7.1.4 Multiple Vulnerabilities (APSB09-15)

Adobe Acrobat < 9.3 / 8.2 Multiple Vulnerabilities (APSB10-02)

Adobe Acrobat < 9.3.1 / 8.2.1 Multiple Vulnerabilities (APSB10-07)

Adobe Acrobat < 9.3.2 / 8.2.2 Multiple Vulnerabilities (APSB10-09)

Adobe Acrobat < 9.3.3 / 8.2.3 Multiple Vulnerabilities (APSB10-15)

Adobe Acrobat < 9.3.4 / 8.2.4 Multiple Vulnerabilities (APSB10-17)

Adobe Acrobat < 9.4 / 8.2.5 Multiple Vulnerabilities (APSB10-21)

Adobe Acrobat < 9.4.7 Multiple Memory Corruption Vulnerabilities (APSB11-30)

Adobe Acrobat <= 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-24)

Adobe Acrobat <= 15.006.30434 / 17.011.30096 / 18.011.20055 Multiple Vulnerabilities (APSB18-29)

Adobe Acrobat <= 15.006.30448 / 17.011.30099 / 18.011.20058 Multiple Vulnerabilities (APSB18-34)

Adobe Acrobat <= 15.006.30452 / 17.011.30102 / 18.011.20063 Multiple Vulnerabilities (APSB18-30)

Adobe Acrobat <= 15.006.30456 / 17.011.30105 / 19.008.20080 NTLM SSO Hash Theft (APSB18-40)

Adobe Acrobat <= 15.006.30457 / 17.011.30106 / 19.008.20081 Multiple Vulnerabilities (APSB18-41)

Adobe Acrobat <= 2015.006.30461 / 2017.011.30110 / 2019.010.20064 Multiple Vulnerabilities (APSB19-02)

Adobe Acrobat <= 2015.006.30475 / 2017.011.30120 / 2019.010.20091 Vulnerability (APSB19-13)

Adobe Acrobat <= 2015.006.30482 / 2017.011.30127 / 2019.010.20098 Multiple Vulnerabilities (APSB19-17)

Adobe Acrobat <= 2015.006.30495 / 2017.011.30140 / 2019.010.20100 Multiple Vulnerabilities (APSB19-18)

Adobe Acrobat <= 2015.006.30498 / 2017.011.30143 / 2019.012.20035 Multiple Vulnerabilities (APSB19-41)

Adobe Acrobat <= 2015.006.30503 / 2017.011.30148 / 2019.012.20040 Multiple Vulnerabilities (APSB19-49)

Adobe Acrobat <= 2015.006.30505 / 2017.011.30152 / 2019.021.20056 Multiple Vulnerabilities (APSB19-55)

Adobe Acrobat <= 2015.006.30508 / 2017.011.30156 / 2019.021.20061 Multiple Vulnerabilities (APSB20-05)

Adobe Acrobat <= 2015.006.30510 / 2017.011.30158 / 2020.006.20034 Multiple Vulnerabilities (APSB20-13)

Adobe Acrobat Detection

Adobe Acrobat Help Page XSS

Adobe Acrobat Unsupported Version Detection

Adobe After Effects <= 16.1.2 Arbitrary Code Execution (APSB20-09)

Adobe After Effects <= 17.0.1 Information Disclosure (APSB20-21)

Adobe After Effects Installed

Adobe AIR 3.x <= 3.1.0.4880 Multiple Memory Corruption Vulnerabilities (APSB12-07)

Adobe AIR 3.x <= 3.2.0.2070 Multiple Vulnerabilities (APSB12-14)

Adobe AIR 3.x <= 3.3.0.3670 Multiple Vulnerabilities (APSB12-19)

Adobe AIR 3.x <= 3.4.0.2540 Multiple Vulnerabilities (APSB12-22)

Adobe AIR 3.x <= 3.4.0.2710 Multiple Vulnerabilities (APSB12-24)

Adobe AIR 3.x <= 3.5.0.1060 Buffer Overflow (APSB13-05)

Adobe AIR 3.x <= 3.5.0.600 Multiple Vulnerabilities (APSB12-27)

Adobe AIR 3.x <= 3.5.0.880 Buffer Overflow (APSB13-01)

Adobe AIR 3.x <= 3.6.0.597 Buffer Overflow (APSB13-09)

Adobe AIR 3.x <= 3.6.0.6090 Multiple Vulnerabilities (APSB13-11)

Adobe AIR < 1.5 Multiple Vulnerabilities (APSB08-23)

Adobe AIR < 1.5.2 Multiple Vulnerabilities (APSB09-10)

Adobe AIR < 1.5.3 Multiple Vulnerabilities (APSB09-19)

Adobe AIR < 1.5.3.9130 Multiple Vulnerabilities (APSB10-06)

Adobe AIR < 2.0.2.12610 Multiple Vulnerabilities (ASPB10-14)

Adobe AIR < 2.0.3 Multiple Vulnerabilities (APSB10-16)

Adobe AIR < 2.5.1 Multiple Vulnerabilities (APSB10-26)

Adobe AIR < 2.6 Unspecified Memory Corruption (APSB11-05)

Adobe AIR < 2.6.0.19140 ActionScript Predefined Class Prototype Addition Remote Code Execution (APSB11-07)

Adobe AIR < 2.7.1 Multiple Vulnerabilities (APSB11-21)

Adobe AIR <= 15.0.0.293 Multiple Vulnerabilities (APSB14-24)

Adobe AIR <= 15.0.0.356 Multiple Vulnerabilities (APSB15-01)

Adobe AIR <= 17.0.0.124 Multiple Vulnerabilities (APSB15-05)

Adobe AIR <= 17.0.0.144 Multiple Vulnerabilities (APSB15-06)

Adobe AIR <= 17.0.0.144 Multiple Vulnerabilities (APSB15-09)

Adobe AIR <= 17.0.0.172 Multiple Vulnerabilities (APSB15-11)

Adobe AIR <= 18.0.0.144 Multiple Vulnerabilities (APSB15-16)

Adobe AIR <= 18.0.0.180 Multiple Vulnerabilities (APSB15-19)

Adobe AIR <= 18.0.0.199 Multiple Vulnerabilities (APSB15-23)

Adobe AIR <= 19.0.0.190 Multiple Vulnerabilities (APSB15-25)

Adobe AIR <= 19.0.0.213 Multiple Vulnerabilities (APSB15-28)

Adobe AIR <= 19.0.0.241 Multiple Vulnerabilities (APSB15-32)

Adobe AIR <= 20.0.0.204 Multiple Vulnerabilities (APSB16-01)

Adobe AIR <= 20.0.0.233 Multiple Vulnerabilities (APSB16-04)

Adobe AIR <= 20.0.0.260 Multiple Vulnerabilities (APSB16-08)

Adobe AIR <= 21.0.0.198 Multiple Vulnerabilities (APSB16-15)

Adobe AIR <= 22.0.0.153 Android Applications Runtime Analytics MitM (APSB16-31)

Adobe AIR <= 3.0 Multiple Vulnerabilities (APSB11-28)

Adobe AIR <= 3.7.0.1530 Multiple Vulnerabilities (APSB13-14)

Adobe AIR <= 3.7.0.1860 Memory Corruption (APSB13-16)

Adobe AIR <= 3.7.0.2090 Multiple Vulnerabilities (APSB13-17)

Adobe AIR <= 3.8.0.870 Memory Corruptions (APSB13-21)

Adobe AIR <= 3.9.0.1030 Memory Corruptions (APSB13-26)

Adobe AIR <= AIR 13.0.0.111 Multiple Vulnerabilities (APSB14-16)

Adobe AIR <= AIR 13.0.0.83 Multiple Vulnerabilities (APSB14-14)

Adobe AIR <= AIR 14.0.0.110 Multiple Vulnerabilities (APSB14-18)

Adobe AIR <= AIR 14.0.0.178 Multiple Vulnerabilities (APSB14-21)

Adobe AIR <= AIR 15.0.0.249 Multiple Vulnerabilities (APSB14-22)

Adobe AIR <= AIR 3.9.0.1210 Multiple Vulnerabilities (APSB13-28)

Adobe AIR <= AIR 3.9.0.1380 Multiple Vulnerabilities (APSB14-02)

Adobe AIR <= AIR 4.0.0.1628 Multiple Vulnerabilities (APSB14-09)

Adobe AIR Detection

Adobe AIR Unsupported Version Detection

Adobe Audition < CS5.5 Multiple SES Session File Processing Overflows (APSB11-10)

Adobe Audition Installed

Adobe Bridge CC 9.0.3 Multiple Vulnerabilities (APSB19-04) (Windows)

Adobe Bridge CC < 6.2 Multiple Memory Corruption Vulnerabilities (APSB16-03)

Adobe Bridge Installed

Adobe Camera Raw Plug-In Multiple Vulnerabilities

Adobe ColdFusion 2016.x < 2016u12 / 2018.x < 2018u5 Multiple Vulnerabilities (APSB19-47)

Adobe ColdFusion 10 on IIS Unspecified DoS (APSB12-25) (credentialed check)

Adobe ColdFusion 10 WebSockets CFC Public Method Invocation (APSB13-19) (credentialed check)

Adobe ColdFusion 10.x < 10u23 / 11.x < 11u12 / 2016.x < 2016u4 Multiple Vulnerabilities (APSB17-14)

Adobe ColdFusion 11.x < 11u13 / 2016.x < 2016u5 Multiple Vulnerabilities (APSB17-30)

Adobe ColdFusion 11.x < 11u14 / 2016.x < 2016u6 Multiple Vulnerabilities (APSB18-14)

Adobe ColdFusion 11.x < 11u15 / 2016.x < 2016u7 / 2018.x < 2018u1 Multiple Vulnerabilities (APSB18-33)

Adobe ColdFusion 2016.x < 2016u14 / 2018.x < 2018u8 Multiple Vulnerabilities (APSB20-16)

Adobe ColdFusion 2016.x < 2016u15 / 2018.x < 2018u9 Multiple Vulnerabilities (APSB20-18)

Adobe ColdFusion 9/9.0.1/9.0.2 On JRun DoS (APSB13-19) (credentialed check)

Adobe ColdFusion < 11.x < 11u16 / 2016.x < 2016u8 / 2018.x < 2018u2 Multiple Vulnerabilities (APSB19-10)

Adobe ColdFusion < 11.x < 11u18 / 2016.x < 2016u10 / 2018.x < 2018u3 Vulnerability (APSB19-14)

Adobe ColdFusion < 11.x < 11u19 / 2016.x < 2016u11 / 2018.x < 2018u4 Multiple Vulnerabilities (APSB19-27)

Adobe ColdFusion < 2018.x < 2018u7 Vulnerability (APSB19-58)

Adobe ColdFusion BlazeDS XXE (APSB15-21) (credentialed check)

Adobe ColdFusion Hash Collision DoS (APSB12-06) (credentialed check)

Adobe ColdFusion HTTP Response Splitting (APSB12-15) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB11-04) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB11-14) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB13-03) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB13-10) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB13-27) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB14-23) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB15-29) (credentialed check)

Adobe ColdFusion Multiple Vulnerabilities (APSB16-16) (credentialed check)

Adobe ColdFusion Unspecified DoS (APSB12-21) (credentialed check)

Adobe ColdFusion Unspecified DoS (APSB14-29) (credentialed check)

Adobe ColdFusion Unspecified Reflected XSS (APSB16-22)

Adobe ColdFusion Unspecified Sandbox Bypass (APSB12-26) (credentialed check)

Adobe ColdFusion Unspecified XSS (APSB15-07) (credentialed check)

Adobe ColdFusion Unsupported Version Detection (credentialed check)

Adobe ColdFusion XML External Entity (XXE) Injection Information Disclosure (APSB16-30)

Adobe ColdFusion XSS Vulnerabilities (APSB11-29) (credentialed check)

Adobe Configurator Installed

Adobe Contribute Installed

Adobe Contribute Publishing Server Administrator Password Local Disclosure

Adobe Creative Cloud <= 3.5.1.209 Arbitrary File Read/Write Vulnerability

Adobe Creative Cloud Desktop < 3.7.0.272 Multiple Vulnerabilities (APSB16-21)

Adobe Creative Cloud Desktop < 3.8.0.310 Unquoted Search Path Local Privilege Escalation (APSB16-34)

Adobe Creative Cloud Desktop < 4.0.0.185 Multiple Vulnerabilities (APSB17-13)

Adobe Creative Cloud Desktop < 4.5.0.331 Multiple Vulnerabilities (APSB18-12)

Adobe Creative Cloud Desktop < 4.6.1 Privilege Escalation Vulnerability (APSB18-32)

Adobe Creative Cloud Desktop < 5.1.0.407 Arbitrary File Deletion Vulnerability (APSB20-11)

Adobe Creative Cloud Desktop <= 4.5.0.324 Privilege Escalation Vulnerability (APSB18-20)

Adobe Creative Cloud Desktop <= 4.6.1.393 Multiple Vulnerabilities (APSB19-39)

Adobe Creative Cloud Desktop <= 4.7.0.400 Privilege Escalation Vulnerability (APSB19-11)

Adobe Creative Cloud Installed

Adobe Digital Editions 2.0.0 'rmsdk\_wrapper.dll' Memory Corruption (APSB13-20)

Adobe Digital Editions 2.0.1 Memory Corruption (APSB14-03)

Adobe Digital Editions < 4.0.1 Information Disclosure (APSB14-25)

Adobe Digital Editions < 4.5.1 RCE (APSB16-06)

Adobe Digital Editions < 4.5.10 Out-Of-Bounds Read Vulnerability (APSB19-04)

Adobe Digital Editions < 4.5.10.186048 Heap Overflow Vulnerability (APSB19-16)

Adobe Digital Editions < 4.5.11 Multiple Vulnerabilities (APSB20-07)

Adobe Digital Editions < 4.5.2 Multiple Vulnerabilities (APSB16-28)

Adobe Digital Editions < 4.5.3 Multiple Information Disclosure Vulnerabilities (APSB16-45)

Adobe Digital Editions < 4.5.4 Multiple Vulnerabilities (APSB17-05)

Adobe Digital Editions < 4.5.5 Multiple Vulnerabilities (APSB17-20)

Adobe Digital Editions < 4.5.6 Multiple Vulnerabilities (APSB17-27)

Adobe Digital Editions < 4.5.7 Multiple Vulnerabilities (APSB17-39)

Adobe Digital Editions < 4.5.8 Multiple Vulnerabilities (APSB18-13)

Adobe Digital Editions < 4.5.9 Multiple Vulnerabilities (APSB18-27)

Adobe Digital Editions <= 4.5.11.187212 Information Disclosure (APSB20-23)

Adobe Digital Editions Installed

Adobe Download Manager < 2.2 AOM File Handling Section Name Overflow

Adobe Download Manager Arbitrary File Download (APSB10-08)

Adobe Dreamweaver < 18.1 OS Command Injection Vulnerability

Adobe Dreamweaver < 19.1 Information Disclosure Vulnerability (APSB19-21)

Adobe Dreamweaver <= 18.0 / <= 19.0 DLL Hijacking Privilege Escaalation Vulnerability (APSB19-40)

Adobe Dreamweaver Installed

Adobe Drive Installed

Adobe Encore Installed

Adobe Extension Manager Installed

Adobe Flash Player <= 17.0.0.134 Multiple Vulnerabilities (APSB15-06)

Adobe Flash Player <= 17.0.0.169 Multiple Vulnerabilities (APSB15-09)

Adobe Flash Player <= 17.0.0.188 Multiple Vulnerabilities (APSB15-11)

Adobe Flash Player <= 18.0.0.161 RCE (APSB15-14)

Adobe Flash Player <= 18.0.0.194 Multiple Vulnerabilities (APSB15-16)

Adobe Flash Player <= 18.0.0.203 Multiple RCE Vulnerabilities (APSB15-18)

Adobe Flash Player <= 18.0.0.209 Multiple Vulnerabilities (APSB15-19)

Adobe Flash Player <= 18.0.0.232 Multiple Vulnerabilities (APSB15-23)

Adobe Flash Player <= 19.0.0.185 Multiple Vulnerabilities (APSB15-25)

Adobe Flash Player <= 19.0.0.207 Vulnerability (APSB15-27)

Adobe Flash Player <= 19.0.0.226 Multiple Vulnerabilities (APSB15-28)

Adobe Flash Player <= 19.0.0.245 Multiple Vulnerabilities (APSB15-32)

Adobe Flash Player <= 20.0.0.235 Multiple Vulnerabilities (APSB16-01)

Adobe Flash Player <= 20.0.0.286 Multiple Vulnerabilities (APSB16-04)

Adobe Flash Player <= 20.0.0.306 Multiple Vulnerabilities (APSB16-08)

Adobe Flash Player <= 21.0.0.197 Multiple Vulnerabilities (APSB16-10)

Adobe Flash Player <= 21.0.0.226 Multiple Vulnerabilities (APSB16-15)

Adobe Flash Player <= 21.0.0.242 Multiple Vulnerabilities (APSB16-18)

Adobe Flash Player <= 22.0.0.192 Multiple Vulnerabilities (APSB16-25)

Adobe Flash Player <= 22.0.0.211 Multiple Vulnerabilities (APSB16-29)

Adobe Flash Player <= 23.0.0.162 Multiple Vulnerabilities (APSB16-32)

Adobe Flash Player <= 23.0.0.185 Arbitrary Code Execution (APSB16-36)

Adobe Flash Player <= 23.0.0.205 Multiple Vulnerabilities (APSB16-37)

Adobe Flash Player <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)

Adobe Flash Player <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)

Adobe Flash Player <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)

Adobe Flash Player <= 24.0.0.221 Multiple Vulnerabilities (APSB17-07)

Adobe Flash Player <= 25.0.0.127 Multiple Vulnerabilities (APSB17-10)

Adobe Flash Player <= 25.0.0.148 Multiple Vulnerabilities (APSB17-15)

Adobe Flash Player <= 25.0.0.171 Multiple Vulnerabilities (APSB17-17)

Adobe Flash Player <= 26.0.0.131 Multiple Vulnerabilities (APSB17-21)

Adobe Flash Player <= 26.0.0.137 Multiple Vulnerabilities (APSB17-23)

Adobe Flash Player <= 26.0.0.151 Multiple Vulnerabilities (APSB17-28)

Adobe Flash Player <= 27.0.0.159 Type Confusion Vulnerability (APSB17-32)

Adobe Flash Player <= 27.0.0.183 (APSB17-33)

Adobe Flash Player <= 27.0.0.187 (APSB17-42)

Adobe Flash Player <= 28.0.0.126 (APSB18-01)

Adobe Flash Player <= 28.0.0.137 Use-after-free Remote Code Execution (APSA18-01) (APSB18-03)

Adobe Flash Player <= 28.0.0.161 (APSB18-05)

Adobe Flash Player <= 29.0.0.113 (APSB18-08)

Adobe Flash Player <= 29.0.0.140 (APSB18-16)

Adobe Flash Player <= 29.0.0.171 (APSB18-19)

Adobe Flash Player <= 30.0.0.113 (APSB18-24)

Adobe Flash Player <= 30.0.0.134 (APSB18-25)

Adobe Flash Player <= 30.0.0.154 (APSB18-31)

Adobe Flash Player <= 31.0.0.122 (APSB18-39)

Adobe Flash Player <= 31.0.0.148 (APSB18-44)

Adobe Flash Player <= 31.0.0.153 (APSB18-42)

Adobe Flash Player <= 32.0.0.114 (APSB19-06)

Adobe Flash Player <= 32.0.0.156 (APSB19-19)

Adobe Flash Player <= 32.0.0.171 (APSB19-26)

Adobe Flash Player <= 32.0.0.192 (APSB19-30)

Adobe Flash Player <= 32.0.0.238 (APSB19-46)

Adobe Flash Player <= 32.0.0.321 (APSB20-06)

Adobe Flash Player Unsupported Version Detection

Adobe Flash Professional <= 11.5.1.349 JPG Object Dimension Memory Allocation FLA File Handling Remote Overflow (APSB12-12)

Adobe Flash Professional Detection

Adobe FrameMaker < 15.0.5 Multiple Vulnerabilities (APSB20-04)

Adobe FrameMaker <= 14.0.0.361 (2017 Release) Privilege Escalation (APSB18-37)

Adobe FrameMaker Installed

Adobe Illustrator CC < 24.0.2 Multiple Vulnerabilites (APSB20-03)

Adobe Illustrator CS5 / CS5.5 Multiple Memory Corruption Vulnerabilities (APSB12-10)

Adobe Illustrator CS6 Stack Overflow (APSB14-11)

Adobe Illustrator Detection

Adobe Illustrator Multiple Vulnerabilities (APSB10-01)

Adobe Illustrator Path Subversion Arbitrary DLL Injection Code Execution (APSB10-29)

Adobe InDesign < 13.1.1 / 14.x < 14.0.2 Arbitrary Code Execution Vulnerability (APSB19-23)

Adobe InDesign CC < 13.1 Multiple Vulnerabilities (APSB18-11)

Adobe InDesign CC Installed

Adobe JRun 4.0 Multiple Vulnerabilities (APSB09-12)

Adobe JRun Detection

Adobe Media Encoder Installed

Adobe Media Encoder Installed (Windows)

Adobe PageMaker 7.0.1 / 7.0.2 Multiple Vulnerabilities (APSA08-10)

Adobe PageMaker Detection

Adobe PDF Plug-In < 8.0 / 7.0.9 / 6.0.6 Multiple Vulnerabilities (APSB07-01)

Adobe Photoshop 21.x <= 21.1.1 / CC 20.x <= 20.0.8 Multiple Vulnerabilities (APSB20-14)

Adobe Photoshop < CS5 / CS5.1 Multiple Arbitrary Code Execution Vulnerabilities (APSB12-11)

Adobe Photoshop CC 17.x < 17.0.2 / 18.x < 18.1 Multiple Vulnerabilities (APSB17-12)

Adobe Photoshop CC 18.x < 18.1.2 Multiple Vulnerabilities (APSB17-12)

Adobe Photoshop CC 18.x < 18.1.4 / 19.x < 19.1.4 Remote Code Execution Vulnerability (APSB18-17)

Adobe Photoshop CC 18.x < 18.1.6 / 19.x < 19.1.6 Multiple Vulnerabilities (APSB18-28)

Adobe Photoshop CC 19.x < 19.1.7 Information Disclosure Vulnerability (APSB18-43)

Adobe Photoshop CC 19.x <= 19.1.7 / 20.x <= 20.0.2 Vulnerability (APSB19-15)

Adobe Photoshop CC 19.x <= 19.1.8 / 20.x <= 20.0.5 Vulnerability (APSB19-44)

Adobe Photoshop CC 20.x <= 20.0.7 / 21.x <= 21.0.1 Multiple Vulnerabilities (APSB19-56)

Adobe Photoshop CC < 15.2.4 / 16.1.2 Multiple Memory Corruption Vulnerabilities (APSB16-03)

Adobe Photoshop CC Multiple Vulnerabilities (APSB15-12)

Adobe Photoshop CS5 < 12.0.2 (APSB10-30)

Adobe Photoshop CS5 < 12.0.4 Multiple Unspecified Vulnerabilities

Adobe Photoshop CS5 GIF File Memory Corruption (APSB11-22)

Adobe Photoshop CS6 Multiple Buffer Overflow Vulnerabilities (APSB12-20)

Adobe Photoshop Detection

Adobe Photoshop Elements Active File Monitor Service Privilege Escalation (APSB09-17)

Adobe Photoshop Unsupported Version Detection

Adobe Prelude CC < 8.1.1 Arbitrary Code Execution (APSB19-35)

Adobe Prelude Installed

Adobe Premiere Pro CC < 13.1.3 Remote Code Execution (APSB19-33)

Adobe Premiere Pro Installed

Adobe Presenter Installed

Adobe Reader 11.0.4 Crafted PDF File Handling JavaScript Scheme URI Execution (APSB13-25)

Adobe Reader 9.x / 10.x Multiple Vulnerabilities (APSB11-08)

Adobe Reader 9.x / 10.x Unspecified Memory Corruption (APSB11-06)

Adobe Reader < 10.0.1 / 9.4.2 / 8.2.6 Multiple Vulnerabilities (APSB11-03)

Adobe Reader < 10.1 / 9.4.5 / 8.3 Multiple Vulnerabilities (APSB11-16)

Adobe Reader < 10.1.1 / 9.4.6 / 8.3.1 Multiple Vulnerabilities (APSB11-21, APSB11-24)

Adobe Reader < 10.1.10 / 11.0.07 Multiple Vulnerabilities (APSB14-15)

Adobe Reader < 10.1.11 / 11.0.08 Sandbox Bypass (APSB14-19)

Adobe Reader < 10.1.12 / 11.0.09 Multiple Vulnerabilities (APSB14-20)

Adobe Reader < 10.1.13 / 11.0.10 Multiple Vulnerabilities (APSB14-28)

Adobe Reader < 10.1.14 / 11.0.11 Multiple Vulnerabilities (APSB15-10)

Adobe Reader < 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-15)

Adobe Reader < 10.1.2 / 9.5 Multiple Vulnerabilities (APSB12-01)

Adobe Reader < 10.1.3 / 9.5.1 Multiple Vulnerabilities (APSB12-08)

Adobe Reader < 10.1.4 / 9.5.2 Multiple Vulnerabilities (APSB12-16)

Adobe Reader < 10.1.9 / 11.0.6 Multiple Vulnerabilities (APSB14-01)

Adobe Reader < 11.0.1 / 10.1.5 / 9.5.3 Multiple Vulnerabilities (APSB13-02)

Adobe Reader < 11.0.14 / 15.006.30119 / 15.010.20056 Multiple Vulnerabilities (APSB16-02)

Adobe Reader < 11.0.15 / 15.006.30121 / 15.010.20060 Multiple Vulnerabilities (APSB16-09)

Adobe Reader < 11.0.16 / 15.006.30172 / 15.016.20039 Multiple Vulnerabilities (APSB16-14)

Adobe Reader < 11.0.17 / 15.006.30198 / 15.017.20050 Multiple Vulnerabilities (APSB16-26)

Adobe Reader < 11.0.18 / 15.006.30243 / 15.020.20039 Multiple Vulnerabilities (APSB16-33)

Adobe Reader < 11.0.19 / 15.006.30279 / 15.023.20053 Multiple Vulnerabilities (APSB17-01)

Adobe Reader < 11.0.2 / 10.1.6 / 9.5.4 Multiple Vulnerabilities (APSB13-07)

Adobe Reader < 11.0.20 / 2015.006.30306 / 2017.009.20044 Multiple Vulnerabilities (APSB17-11)

Adobe Reader < 11.0.21 / 2015.006.30355 / 2017.011.30066 / 2017.012.20098 Multiple Vulnerabilities (APSB17-24)

Adobe Reader < 11.0.23 / 2015.006.30392 / 2017.011.30068 / 2018.009.20044 Multiple Vulnerabilities (APSB17-36)

Adobe Reader < 11.0.3 / 10.1.7 / 9.5.5 Multiple Vulnerabilities (APSB13-15)

Adobe Reader < 11.0.4 / 10.1.8 Multiple Vulnerabilities (APSB13-22)

Adobe Reader < 2019.010.20091 / 2017.011.30120 / 2015.006.30475 Multiple Vulnerabilities (APSB19-07)

Adobe Reader < 6.0.6 / 7.0.9 Multiple Vulnerabilities

Adobe Reader < 7.0.8 Multiple Unspecified Vulnerabilities

Adobe Reader < 7.1.0 / 8.1.2 Multiple Vulnerabilities

Adobe Reader < 7.1.0 / 8.1.2 SU1 Unspecified JavaScript Method Handling Arbitrary Code Execution

Adobe Reader < 8.0 AcroPDF ActiveX Control Multiple Vulnerabilities

Adobe Reader < 8.1.1 Crafted PDF File Arbitrary Code Execution

Adobe Reader < 8.1.3 / 9.0 Multiple Vulnerabilities

Adobe Reader < 9.1 / 8.1.4 / 7.1.1 Multiple Vulnerabilities

Adobe Reader < 9.1.2 / 8.1.6 / 7.1.3 Multiple Vulnerabilities

Adobe Reader < 9.1.3 Flash Handling Unspecified Arbitrary Code Execution (APSB09-10)

Adobe Reader < 9.2 / 8.1.7 / 7.1.4 Multiple Vulnerabilities (APSB09-15)

Adobe Reader < 9.3 / 8.2 Multiple Vulnerabilities (APSB10-02)

Adobe Reader < 9.3.1 / 8.2.1 Multiple Vulnerabilities (APSB10-07)

Adobe Reader < 9.3.2 / 8.2.2 Multiple Vulnerabilities (APSB10-09)

Adobe Reader < 9.3.3 / 8.2.3 Multiple Vulnerabilities (APSB10-15)

Adobe Reader < 9.3.4 / 8.2.4 Multiple Vulnerabilities (APSB10-17)

Adobe Reader < 9.4 / 8.2.5 Multiple Vulnerabilities (APSB10-21)

Adobe Reader < 9.4.1 Multiple Vulnerabilities (APSB10-28)

Adobe Reader < 9.4.7 Multiple Memory Corruption Vulnerabilities (APSB11-30)

Adobe Reader <= 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-24)

Adobe Reader <= 15.006.30456 / 17.011.30105 / 19.008.20080 NTLM SSO Hash Theft (APSB18-40)

Adobe Reader <= 15.006.30457 / 17.011.30106 / 19.008.20081 Multiple Vulnerabilities (APSB18-41)

Adobe Reader <= 2015.006.30394 / 2017.011.30070 / 2018.009.20050 Multiple Vulnerabilities (APSB18-02)

Adobe Reader <= 2015.006.30417 / 2017.011.30079 / 2018.011.20038 Multiple Vulnerabilities (APSB18-09)

Adobe Reader <= 2015.006.30418 / 2017.011.30080 / 2018.011.20040 Multiple Vulnerabilities (APSB18-21)

Adobe Reader <= 2015.006.30434 / 2017.011.30096 / 2018.011.20055 Multiple Vulnerabilities (APSB18-29)

Adobe Reader <= 2015.006.30448 / 2017.011.30099 / 2018.011.20058 Multiple Vulnerabilities (APSB18-34)

Adobe Reader <= 2015.006.30452 / 2017.011.30102 / 2018.011.20063 Multiple Vulnerabilities (APSB18-30)

Adobe Reader <= 2015.006.30461 / 2017.011.30110 / 2019.010.20064 Multiple Vulnerabilities (APSB19-02)

Adobe Reader <= 2015.006.30475 / 2017.011.30120 / 2019.010.20091 Vulnerability (APSB19-13)

Adobe Reader <= 2015.006.30482 / 2017.011.30127 / 2019.010.20098 Multiple Vulnerabilities (APSB19-17)

Adobe Reader <= 2015.006.30493 / 2017.011.30138 / 2019.010.20099 Multiple Vulnerabilities (APSB19-18)

Adobe Reader <= 2015.006.30498 / 2017.011.30143 / 2019.012.20035 Multiple Vulnerabilities (APSB19-41)

Adobe Reader <= 2015.006.30503 / 2017.011.30148 / 2019.012.20040 Multiple Vulnerabilities (APSB19-49)

Adobe Reader <= 2015.006.30505 / 2017.011.30152 / 2019.021.20056 Multiple Vulnerabilities (APSB19-55)

Adobe Reader <= 2015.006.30508 / 2019.021.20061 Multiple Vulnerabilities (APSB20-05)

Adobe Reader <= 2015.006.30510 / 2017.011.30158 / 2020.006.20034 Multiple Vulnerabilities (APSB20-13)

Adobe Reader Detection

Adobe Reader Enabled in Browser (Google Chrome)

Adobe Reader Enabled in Browser (Internet Explorer)

Adobe Reader Enabled in Browser (Mozilla Firefox)

Adobe Reader Enabled in Browser (Opera)

Adobe Reader getAnnots() JavaScript Method PDF Handling Memory Corruption (APSB09-06)

Adobe Reader Unsupported Version Detection

Adobe Recent Files

Adobe RoboHelp / RoboHelp Server DOM-based XSS (APSB11-23)

Adobe RoboHelp 10 Unspecified Memory Corruption (APSB13-024)

Adobe RoboHelp FlashHelp Unspecified XSS (APSB11-09) (credentialed check)

Adobe RoboHelp for Word Unspecified XSS (APSB12-04) (credentialed check)

Adobe RoboHelp Installed

Adobe RoboHelp Multiple Vulnerabilities (APSB17-25)

Adobe RoboHelp Server Installed

Adobe RoboHelp Server Unspecified SQLi (APSB16-12)

Adobe RoboHelp Unspecified XSS (APSB16-46)

Adobe Shockwave Player <= 12.1.8.158 Multiple RCE Vulnerabilities (APSB15-17)

Adobe Shockwave Player <= 12.1.9.160 Multiple RCE (APSB15-22)

Adobe Shockwave Player <= 12.2.0.162 RCE (APSB15-26)

Adobe Shockwave Player <= 12.2.7.197 DLL Hijacking (APSB17-08)

Adobe Shockwave Player <= 12.2.8.198 Memory Corruption RCE (APSB17-18)

Adobe Shockwave Player <= 12.2.9.199 Memory Corruption RCE (APSB17-40)

Adobe Shockwave Player <= 12.3.4.204 Multiple memory corruption vulnerabilities (APSB19-20) (Windows)

Adobe Software Signed By Revoked Certificate (APSA12-01)

Adobe SpeedGrade Installed

Adobe SVG Viewer Circle Transform Remote Code Execution

Adtrustmedia PrivDog < 3.0.105.0 Security Bypass Vulnerability

AgileBits 1Password 6.3.3 Multiple Vulnerabilities

AgileBits 1Password Installed (Windows)

AIM Buddy Icon Overflow Vulnerability

AIM Smiley Icon Location Remote Denial Of Service

Akamai Download Manager ActiveX Control < 2.2.1.0 Multiple Vulnerabilities

Akamai Download Manager ActiveX Control < 2.2.3.5 Remote Code Execution

Akamai Download Manager ActiveX Control < 2.2.3.6 Arbitrary File Download

Akamai Download Manager ActiveX Control < 2.2.4.8 Buffer Overflow

Akamai Red Swoosh < 3333 referer Header Cross-Site Request Forgery

Allround Automations PL/SQL Developer < 11.0.6.1776 HTTP Insecure Update RCE

Allround Automations PL/SQL Developer Installed

Alt-N MDaemon < 11.0.1 Multiple Remote DoS

Alt-N MDaemon < 13.0.4 Multiple Vulnerabilities

Alt-N MDaemon Detection

Altiris AClient < 6.8.380 Local Vulnerabilities

Altiris AClient < 6.9.164 Multiple Local Vulnerabilities

Altiris Altiris.AeXNSPkgDL.1 ActiveX Control DownloadAndInstall() Method Arbitrary Code Execution

Altiris ConsoleUtilities 'BrowseAndSaveFile()' ActiveX Control Buffer Overflow

Altiris ConsoleUtilities ActiveX RunCmd Method Overflow

Altiris Deployment Solution < 6.9.176 Multiple Vulnerabilities

Altiris Deployment Solution Aclient Process (aclient.exe) Log File Viewer Local Privilege Escalation

Altiris Deployment Solution Agent < 6.9.176 Multiple Local Vulnerabilities

Altiris Deployment Solution Agent < 6.9.355 Local Privilege Escalation (SYM08-019)

Altiris Deployment Solution Server < 6.9 SP4 DBManager DoS (SYM10-007)

Altiris Deployment Solution Server < 6.9.355 Password Disclosure (SYM08-020)

Altiris Deployment Solution Server < 6.9.430 Multiple Vulnerabilities (SYM09-011)

Altiris Deployment Solution Server DB Manager Unauthenticated Command Execution

Altiris Notification Server Agent GUI Local Privilege Escalation (KB 39159)

Altiris Notification Server Agent Local Privilege Escalation Vulnerabilities

Altiris Notification Server Static Encryption Key (KB46763)

Amazon Web Services EC2 Instance Metadata Enumeration (Windows)

Antivirus Software Check

Anzio Web Print Object (WePO) ActiveX mainurl Parameter Buffer Overflow

AOL AIM 'sipXtapi.dll' Multiple Buffer Overflow Vulnerabilities

AOL dnUpdater ActiveX dnu.exe Init() Method Remote Code Execution

AOL Instant Messenger (AIM) Software Detection

AOL Instant Messenger (AIM) Software Detection (credentialed check)

AOL Radio AmpX ActiveX Control Buffer Overflow Vulnerabilities

AOL You've Got Pictures ActiveX Control (YGPPicFinder.DLL) Overflow

Apache JMeter < 4.0 Insecure RMI Registry Binding

Apache JMeter < 5.1 Unauthenticated Remote Code Execution Vulnerability

Apache JMeter Detection

Apache OpenOffice < 3.4.0 Multiple Memory Corruption Vulnerabilities

Apache OpenOffice < 3.4.1 Multiple Heap-Based Buffer Overflows

Apache OpenOffice < 4.0 Multiple Memory Corruption Vulnerabilities

Apache OpenOffice < 4.1.1 Multiple Vulnerabilities

Apache OpenOffice < 4.1.2 Multiple Vulnerabilities

Apache OpenOffice < 4.1.3 Multiple Vulnerabilities

Apache OpenOffice < 4.1.4 Multiple Vulnerabilities

Apache OpenOffice < 4.1.6 Virtual Table Arithmetic Overflow

Apache POI < 3.17 Multiple DoS Vulnerabilities

Apache POI Detection

Apache Struts 2.0.0 < 2.3.16.1 Multiple Vulnerabilities (credentialed check) (Deprecated)

Apache Struts Detection

Apache Subversion 1.0.x - 1.7.17 / 1.8.x < 1.8.10 Multiple Vulnerabilities

Apache Subversion 1.10.x < 1.10.4 / 1.11.x < 1.11.1 mod\_dav\_svn DoS

Apache Subversion 1.3.x - 1.7.14 / 1.8.x < 1.8.8 'mod\_dav\_svn' DoS

Apache Subversion 1.4.x - 1.7.12 / 1.8.x < 1.8.3 Multiple Symlink File Overwrite Vulnerabilities

Apache Subversion 1.4.x - 1.7.13 / 1.8.x < 1.8.5 Multiple DoS

Apache Subversion 1.6.x / 1.7.x / 1.8.x < 1.6.23 / 1.7.11 / 1.8.1 Multiple Vulnerabilities

Apache Subversion 1.8.x < 1.8.2 Multiple Vulnerabilities

Apache Subversion < 1.6.21 / 1.7.x < 1.7.9 Multiple DoS

Apache Subversion < 1.6.23 / 1.7.x < 1.7.10 Multiple Remote DoS

Apache Subversion < 1.6.4 'libsvn\_delta' Library Binary Delta svndiff Stream Parsing Multiple Overflows

Apache Subversion < 1.9.11 / 1.10.x < 1.10.5 / 1.11.x / 1.12.x < 1.12.1 Multiple Vulnerabilities

Apache Subversion Client Unsupported Version Detection

Apache Subversion Server Unsupported Version Detection

Apple Boot Camp Support Software < 5.1 AppleMNT.sys Driver PE Header Memory Corruption

Apple iCloud 7.x < 7.13 / 10.x < 10.6 Multiple Vulnerabilities

Apple iCloud < 7.12 Multiple Vulnerabilities

Apple iTunes < 10.0 Multiple (credentialed check)

Apple iTunes < 10.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 10.2.2 Multiple (credentialed check)

Apple iTunes < 10.5 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 10.5.1 Update Authenticity Verification Weakness (credentialed check)

Apple iTunes < 10.6 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 10.6.3 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 10.7 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 11.0.3 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 11.1 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 11.1.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 11.1.4 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 11.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.0.1 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.10.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.10.3 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.10.4 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.10.5 Multiple Vulnerabilities (credentialed check) (HT211105)

Apple iTunes < 12.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.3 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.3.1 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.3.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.4 DLL Injection Arbitrary Code Execution (credentialed check)

Apple iTunes < 12.4.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.5.1 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.5.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.5.4 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.5.5 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.6 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.6.1 WebKit Memory Corruption RCE (credentialed check)

Apple iTunes < 12.6.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.7 WebKit Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.7.1 WebKit Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.7.2 WebKit Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.7.3 WebKit Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.7.4 WebKit Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.7.5 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.8 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.9 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.9.1 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.9.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.9.3 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 12.9.6 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 7.4 Malformed Music File Heap Overflow (credentialed check)

Apple iTunes < 8.0 Integer Buffer Overflow (credentialed check)

Apple iTunes < 8.1 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 8.2 itms: URI Handling Overflow (credentialed check)

Apple iTunes < 9.0.1 PLS File Buffer Overflow (credentialed check)

Apple iTunes < 9.1 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 9.2 Multiple Vulnerabilities (credentialed check)

Apple iTunes < 9.2.1 'itpc:' Buffer Overflow (credentialed check)

Apple iTunes AAC File Parsing Integer Overflow (credentialed check)

Apple iTunes for Windows < 12.9.5 Multiple Vulnerabilities (credentialed check)

Apple iTunes For Windows iTunesHelper.exe Path Subversion Local Privilege Escalation (credentialed check)

Apple iTunes Mobile iOS Device Backup Enumeration (Windows)

Apple iTunes Version Detection (credentialed check)

Apple QuickTime < 7.7.7 Multiple Vulnerabilities (Windows)

Apple QuickTime < 7.7.8 Multiple Arbitrary Code Vulnerabilities (Windows)

Apple QuickTime < 7.7.9 Multiple RCE (Windows)

Apple QuickTime MPEG-2 Playback Component Code Execution

Apple QuickTime Unsupported on Windows

Apple Software Update Insecure Transport

Apple Software Update Installed

Application Compatibility Cache

Artifex Ghostscript .rsdparams Operator Handling Type Confusion RCE

Artifex Ghostscript < 9.25 PostScript Code Execution Vulnerability

Artifex Ghostscript < 9.26 PostScript Multiple Vulnerabilities

Artifex Ghostscript < 9.27 PostScript Security Bypass Vulnerability

Artifex Ghostscript < 9.50 Multiple Vulnerabilities

Artifex Ghostscript Installed

Artifex Ghostscript Multiple Vulnerabilities

Artifex Ghostscript PostScript Handling Buffer Overflow DoS

Artweaver 3.x < 3.1.5 JPG File Handling Stack-based Buffer Overflow

Artweaver 3.x < 3.1.6 AWD File Buffer Overflow

Artweaver Detection

Ask.com Toolbar AskJeevesToolBar.SettingsPlugin.1 ActiveX (askBar.dll) ShortFormat Property Arbitrary Code Execution

ASP.NET Core Denial of Service Vulnerability (April 2019)

ASP.NET Core Denial of Service Vulnerability (January 2019)

ATI Catalyst Dynamic Driver (atidsmxx.sys) Local Privilege Escalation

Atlassian JIRA Installed (Windows)

Atlassian JIRA Service Desk Path Traversal Vulnerability (2019-09-18)

Atlassian SourceTree 0.5.1.0 < 2.4.7.0 Multiple Vulnerabilities

Atlassian SourceTree 0.5.1.0 < 2.6.9 Remote Code Execution Vulnerabilities

Atlassian SourceTree 0.5a < 3.0.17 Multiple remote code execution vulnerabilities

Atlassian SourceTree 0.5a < 3.1.3 Remote Code Execution vulnerability

Attachmate Reflection for Secure IT Windows Server < 7.0 SP1 Multiple Unspecified Vulnerabilities

Attachmate Reflection for Secure IT Windows Server Installed

Attachmate Reflection Heartbeat Information Disclosure (Heartbleed)

Attachmate Reflection Secure IT Windows Client Information Disclosure (Heartbleed)

Attachmate Reflection X Heartbeat Information Disclosure (Heartbleed)

AUREATE Software Detection

Aurigma Image Uploader ActiveX Control < 4.5.70 Multiple Buffer Overflows

Authentec UPEK Protector Suite Weak Password Storage

Autodesk AutoCAD < 2014 Multiple Vulnerabilities

Autodesk AutoCAD Detection

Autodesk AutoCAD DWG Buffer Overflow

Autodesk Design Review < 2013 Hotfix 2 Multiple RCE

Autodesk Design Review < 2013 Hotfix 3 Multiple RCE

Autodesk Design Review AdView.AdViewer ActiveX Control RCE

Autodesk Design Review Installed

Autodesk DWG TrueView Buffer Overflow

Autodesk DWG TrueView Detection

Autodesk IDrop ActiveX Control Heap Corruption

AutoDesk LiveUpdate ActiveX Control ApplyPatch Method Execution

Autodesk SketchBook Pro < 6.2.5 / SketchBook Copic Edition < 2.0.2 Heap Buffer Overflow

Autodesk SketchBook Pro < 6.2.6 Multiple Overflow Vulnerabilities

Autodesk SketchBook Pro Detection

Autodesk VRED Detection

Autodesk VRED Pro 2014 < SR1 SP8 Remote Code Execution

Autonomy KeyView Filter Module Multiple Memory Corruption Vulnerabilities (Lotus Notes)

Avast Antivirus Detection and Status

Avast Antivirus Path Traversal Vulnerability

avast! Antivirus Server Edition Password Setting Weakness

avast! CAB / SIS File Handling Buffer Overflow

avast! Professional Edition < 4.8.1356 Multiple Vulnerabilities

avast! Professional Edition < 5.0.418 Local Privilege Escalation

avast! Server Edition LHA Archive Extended-header Field Processing Overflow

Avaya WinPDM < 3.8.5 Multiple Vulnerabilities

AVG 'ScriptHelperApi' ActiveX Remote Code Execution

AVG Anti-virus avg7core.sys 0x5348E004 IOCTL Local Privilege Escalation

AVG Anti-Virus Crafted UPX File Handling Divide-by-zero Remote DoS

AVG Internet Security Detection

Avira AntiVir File Handling Vulnerabilities

Avira AntiVir PDF Scan Evasion

Avira AntiVir RAR/CAB/ZIP/LH Scan Evasion

Avira AntiVir Zip Scan Evasion

Avira Desktop for Windows ACE Archive Handling Buffer Overflow

AXIS Camera Control (aka CamImage) AxisCamControl.ocx ActiveX SaveBMP Method Overflow

AxisCamControl ActiveX Control Buffer Overflow

AxWebRemoveCtrl ActiveX Control Arbitrary Code Execution

BagMRU Folder History

BargainBuddy Software Detection

BetterInternet Software Detection

Beyond Compare Detection

Beyond Compare Zip File Buffer Overflow

BFTelnet Username Handling Remote Overflow DoS

Big-IP Edge Gateway Client for Windows Detection

BIOS Info (SMB)

BIOS Info (WMI)

BitDefender Antivirus Detection and Status

BitDefender CAB Scan Evasion

BitDefender Client Log Creation Functionality Format String

BitDefender Online Anti-Virus Scanner ActiveX OScan8.ocx / OScan8.ocx InitX Method Arbitrary Code Execution

BitDefender PDF Scan Evasion

Bitsmith Personal Knowbase Detection

Bitsmith Software Personal Knowbase knowbase.exe FileOpen Dialogue Local Overflow

Bitvise SSH Client 6.x / 7.x < 7.41 Denial of Service (DoS) Vulnerability

Bitvise SSH Client Installed

Bitvise SSH Server < 7.41 Multiple Vulnerabilities

Bitvise SSH Server Installed

BitZipper 2013 < 2013 Update 1 Memory Corruption Vulnerability

BitZipper Installed

BlackBerry Desktop Manager Intellisync ActiveX Control Arbitrary Remote Code Execution

BlackBerry Desktop Software < 6.0 B47 Path Subversion Arbitrary DLL Injection Code Execution

BlackBerry Desktop Software < 6.0.1 Database Backup File Password Brute Force Weakness

BlackBerry Enterprise Server / Attachment Service PDF Distiller Buffer Overflow (KB24547)

BlackBerry Enterprise Server / Attachment Service PDF Distiller Buffer Overflow (KB24761)

BlackBerry Enterprise Server / Attachment Service PDF Distiller Buffer Overflow (KB25382)

BlackBerry Enterprise Server / Attachment Service PDF Distiller Unspecified Vulnerabilities (KB19860)

BlackBerry Enterprise Server / Enterprise Service / Enterprise Server Express Information Disclosure (KB35647)

BlackBerry Enterprise Server / Enterprise Service / Enterprise Server Express Information Disclosure (KB36175)

BlackBerry Enterprise Server / Unite! PDF Distiller Component Vulnerabilities (KB17118 / KB17119)

BlackBerry Enterprise Server Administration API Unspecified Remote Vulnerability (KB27258)

BlackBerry Enterprise Server Attachment Service Unspecified Vulnerabilities (KB18327)

BlackBerry Enterprise Server PNG and TIFF Image Processing Vulnerabilities (KB27244)

BlackBerry Enterprise Server SSL/TLS EXPORT\_RSA Ciphers Downgrade MitM (KB36811) (FREAK)

BlackBerry Enterprise Server TIFF Image Processing Vulnerabilities (KB33425)

BlackBerry Enterprise Server Unsupported Version

BlackBerry Enterprise Server Web Desktop Manager XSS (KB26296)

BlackBerry Enterprise Service 10 / BlackBerry Enterprise Server / BlackBerry Unite! Detection

BlackBerry Enterprise Service Information Disclosure (KB35882) (Heartbleed)

BlackBerry Enterprise Service Multiple Vulnerabilities (BSRT-2016-001)

BlackBerry Enterprise Service Remote Code Execution (KB35139)

BlackBerry Link < 1.2.3.53 Codec Demux Arbitrary Code Execution

BlackBerry Link Detection

BlackBerry Link Multiple Vulnerabilities

BlackBerry Multiple Products PDF Distiller Component PDF Processing Arbitrary Code Execution

BlackMoon FTP Server blackmoon.mdb Plaintext Password Disclosure

Blue Coat Authentication and Authorization Agent (BCAAA) Installed

Blue Coat Authentication and Authorization Agent Remote Overflow

Blue Coat ProxyClient < 3.3.3.3 / 3.4.x < 3.4.4.10 Certificate Validation MitM

Blue Coat ProxyClient Installed

Blue Coat Unified Agent < 4.1.3.151952 Certificate Validation MitM

Blue Coat Unified Agent < 4.6.2 Configuration File Manipulation Detection Failure

Blue Coat Unified Agent Installed

Blueberry FlashBack SDK 'BB FlashBack Recorder.dll' Remote Code Execution

Bonjour < 1.0.5 Multiple Vulnerabilities (APPLE-SA-2009-09-09)

BONZI BUDDY Software Detection

BrightStor Hierarchical Storage Manager < r11.6 Multiple Remote Vulnerabilities

Brilliant Digital Software Detection

Broadcom Wireless Driver (BCMWL5.SYS) Probe Response SSID Overflow

CA Antivirus Engine Multiple Scan Evasion

CA ARCserve Backup Agent Installed

CA ARCserve Backup for Laptops and Desktops Server and CA Desktop Management Suite Multiple Remote Vulnerabilities

CA ARCserve Backup for Laptops and Desktops Server, CA Protection Suite, and CA Desktop Management Suite Integer Underflow

CA ARCserve Backup Multiple Vulnerabilities (CA20121018) (credentialed check)

CA ARCserve Backup Network Service Network Request Parsing Remote DoS

CA ARCserve Backup Server Installed (credentialed check)

CA BrightStor ARCserve Backup Agent Credential Disclosure

CA BrightStor ARCserve Backup Agent for Windows Long String Overflow

CA BrightStor ARCserve Backup DBASVR for Windows Multiple Remote Buffer Overflows

CA BrightStor ARCserve Backup Discovery Service Overflow

CA BrightStor ARCserve Backup for Laptops & Desktops Server Multiple Vulnerabilities (QO83833)

CA BrightStor ARCserve Backup for Windows Multiple Remote Buffer Overflows (QO81201)

CA BrightStor ARCserve Backup ListCtrl ActiveX (ListCtrl.ocx) AddColumn() Method Overflow

CA BrightStor ARCserve Backup Multiple Remote Vulnerabilities (QO91094)

CA BrightStor ARCserve Backup Multiple Vulnerabilities (QO84983)

CA BrightStor ARCserve Backup Multiple Vulnerabilities (QO87569)

CA BrightStor ARCserve Backup Multiple Vulnerabilities (QO92996)

CA BrightStor ARCserve Backup RPC Interface (asdbapi.dll) Traversal Arbitrary Command Execution

CA BrightStor ARCserve Backup Tape Engine and Portmapper Multiple Vulnerabilities (QO86255)

CA BrightStor ARCserve Backup Tape Engine Multiple Remote Overflows (QO84983)

CA BrightStor ARCserve Backup Universal Agent Remote Overflow (QO66526)

CA DM Deployment Common Component Multiple DoS

CA eTrust Antivirus WebScan ActiveX Control Vulnerabilities

CA eTrust Intrusion Detection CPImportKey Function Overflow DoS

CA eTrust Intrusion Detection System Key Exchange Remote DoS

CA Gateway Security Detection

CA Gateway Security Malformed HTTP Packet Remote Code Execution

CA HIPS Kmxfw.sys Driver Multiple Remote Vulnerabilities

CA Host-Based Intrusion Prevention System Client kmxIds.sys DoS (CA20090818)

CA Host-Based Intrusion Prevention System Server Log Data XSS

CA iTechnology iGateway Service Content-Length Buffer Overflow

CA License Service Multiple Vulnerabilities

CA Multiple Products gui\_cm\_ctrls.ocx ActiveX Control Arbitrary Code Execution

CA Multiple Products InoCore.dll File Mapping Manipulation Local Overflow

CA Multiple Products inoweb Console Server Authentication Remote Overflow

CA Secure Content Manager HTTP Gateway Service FTP Vulnerabilities

CA Unified Infrastructure Management (UIM) Detection

CA Vet Scan Engine < 11.9.1 Library Remote Heap Overflow

Camtasia Studio Pre-generated SWF File csPreloader Parameter Unspecified Arbitrary Code Execution

CesarFTP settings.ini Authentication Credential Plaintext Disclosure

Check Point Endpoint Security Remote Access Client Installed

Check Point Remote Access Client Insecure Library Loading

Check Point SSL Network Extender ActiveX Control Remote Code Execution

Check Point ZoneAlarm Detection and Status

Chrome Browser Extension Enumeration

Cisco AnyConnect Portforwarder ActiveX Control Initialization Parameter Parsing Buffer Overflow

Cisco AnyConnect Secure Mobility Client 2.x / 3.x < 3.0(629) ATL Buffer Overflow

Cisco AnyConnect Secure Mobility Client 2.x / 3.x < 3.1(3103) Host Scan Multiple Vulnerabilities

Cisco AnyConnect Secure Mobility Client 2.x / 3.x < 3.1(5170) Multiple OpenSSL Vulnerabilities

Cisco AnyConnect Secure Mobility Client 2.x < 3.1.13015.0 / 4.x < 4.2.1035.0 Arbitrary File Manipulation

Cisco AnyConnect Secure Mobility Client 3.0 < 3.0 MR8 Multiple Vulnerabilities

Cisco AnyConnect Secure Mobility Client 3.1 < 3.1(495) MiTM

Cisco AnyConnect Secure Mobility Client 3.1.x < 4.3.4019.0 / 4.4.x < 4.4.225.0 Privilege Escalation

Cisco AnyConnect Secure Mobility Client 3.x < 3.1.10010.0 / 4.x < 4.1.4011.0 Arbitrary File Write

Cisco AnyConnect Secure Mobility Client 3.x < 3.1.11004.0 / 4.x < 4.1.6020.0 Privilege Escalation

Cisco AnyConnect Secure Mobility Client 4.0.x < 4.3.05017 / 4.4.x < 4.4.00243 SBL Module Privilege Escalation

Cisco AnyConnect Secure Mobility Client 4.2.x < 4.2.5015.0 / 4.3.x < 4.3.2039.0 Privilege Escalation Vulnerability

Cisco AnyConnect Secure Mobility Client < 2.3.254 Multiple Vulnerabilities

Cisco AnyConnect Secure Mobility Client < 3.1(5187) (POODLE)

Cisco AnyConnect Secure Mobility Client < 3.1(6068) XSS

Cisco AnyConnect Secure Mobility Client < 3.1(7021) / <= 4.0(48) Multiple Vulnerabilities (FREAK)

Cisco AnyConnect Secure Mobility Client < 3.1.10010.0 / 4.0.x < 4.0.4013.0 / 4.1.x < 4.1.4011.0 IPC File Write Vulnerability

Cisco AnyConnect Secure Mobility Client < 3.1.10010.0 / 4.0.x < 4.0.4014.0 / 4.1.x < 4.1.4011.0 Code Execution Vulnerability

Cisco AnyConnect Secure Mobility Client < 3.1.13015.0 / 4.2.x < 4.2.1035.0 Multiple OpenSSL Vulnerabilities

Cisco AnyConnect Secure Mobility Client < 3.1.8009.0 / 4.0.x < 4.0.2052.0 / 4.1.x < 4.1.28.0 Multiple Vulnerabilities

Cisco AnyConnect Secure Mobility Client < 4.4.02034 Local Privilege Escalation

Cisco AnyConnect Secure Mobility Client < 4.6.01098 Certificate Bypass Vulnerability

Cisco AnyConnect Secure Mobility Client Detection

Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability

Cisco AnyConnect Secure Mobility Client VPN Downgrade

Cisco AnyConnect Secure Mobility Client VPN Downloader RCE (cisco-sa-20120620-ac)

Cisco IP Communicator Certificate Trust List Manipulation

Cisco IP Communicator Installed

Cisco Jabber for Windows 8.x / 9.x / 10.x / 11.0.x / 11.1.x XMPP Connection MitM STARTTLS Downgrade (cisco-sa-20151224-jab)

Cisco Jabber for Windows 9.x < 9.2(2) 'Send Screen Capture' File Write

Cisco Jabber for Windows Detection

Cisco Linksys PlayerPT ActiveX Control SetSource() Multiple Overflows

Cisco Linksys PlayerPT ActiveX SetSource() Method base64string Argument Parsing Remote Overflow

Cisco Prime Data Center Network Manager Installed (Windows)

Cisco Secure Access Control Server for Windows Remote Code Execution

Cisco Secure ACS for Windows Installed

Cisco Security Agent Detection

Cisco Security Agent for Microsoft Windows Crafted SMB Packet Remote Overflow

Cisco Security Manager 4.9.x < 4.9(0.397) / 4.10.x < 4.10(0.189) OpenSSL ASN.1 Signature Handling DoS

Cisco TelePresence Management Suite Cross-Site Scripting Vulnerability

Cisco TelePresence Management Suite Cross-Site Scripting Vulnerability (cisco-sa-20190206-tms-xss)

Cisco Telepresence Management Suite Installed (Windows)

Cisco TelePresence Management Suite Simple Object Access Protocol Vulnerability

Cisco Telepresence Management Suite Web Detection

Cisco Unity Detection

Cisco Unity Remote Administration Authentication Bypass (cisco-sa-20081008-unity)

Cisco VPN Client 5.x < 5.0.07.0440 Untrusted Search Path DLL Privilege Escalation

Cisco VPN Client 5.x <= 5.0.07.0440 vpnclient.ini Privilege Escalation

Cisco VPN Client cvpnd.exe Privilege Escalation

Cisco VPN Client Dialer Local Privilege Escalation

Cisco VPN Client on Windows Dial-up Networking Dialog Local Privilege Escalation

Cisco VPN Client on Windows Service Control Manager DoS

Cisco VPN Client Unsupported

Cisco VPN Client Version Detection

Cisco WAAS Mobile Server < 3.5.5 Remote Code Execution

Cisco WAAS Mobile Server Detection

Cisco WebEx Advanced Recording Format RCE (cisco-sa-20180502-war)

Cisco WebEx ARF Player Buffer Overflow (cisco-sa-20120627-webex)

Cisco WebEx ARF Player Multiple Vulnerabilities (cisco-sa-20140507-webex)

Cisco WebEx ARF/WRF Player Installed

Cisco WebEx Extension for Chrome < 1.0.12 'atgpcext' Library GPC Sanitization RCE (cisco-sa-20170717-webex)

Cisco WebEx Extension for Chrome RCE (cisco-sa-20170124-webex)

Cisco WebEx Extension for Firefox < 1.0.12 'atgpcext' Library GPC Sanitization RCE (cisco-sa-20170717-webex)

Cisco WebEx for Firefox RCE (cisco-sa-20170124-webex)

Cisco WebEx for Internet Explorer RCE (cisco-sa-20170124-webex)

Cisco Webex Meetings Installed (Windows)

Cisco Webex Network Recording Player and Cisco Webex Player (cisco-sa-20191106-webex-player)

Cisco Webex Network Recording Player and Cisco Webex Player Multiple Vulnerabilities (cisco-sa-20200304-webex-player

Cisco WebEx Network Recording Player ARF File RCE (cisco-sa-20170621-wnrp)

Cisco WebEx One-Click Detection

Cisco WebEx One-Click Password Disclosure

Cisco Webex Teams for Windows Adaptive Cards Denial of Service (cisco-sa-webex-cards-dos-FWzNcXPq)

Cisco Webex Teams for Windows DLL Hijacking Vulnerability (cisco-sa-20191120-webex-teams-dll)

Cisco Webex Teams Installed (Windows)

Cisco WebEx WRF Player Multiple Buffer Overflows (cisco-sa-20120404-webex)

Cisco WebEx WRF Player Multiple Buffer Overflows (cisco-sa-20120627-webex)

Cisco WebEx WRF Player Multiple Buffer Overflows (cisco-sa-20121010-webex)

Cisco WebEx WRF Player Multiple Vulnerabilities (cisco-sa-20140507-webex)

Cisco WebEx WRF Player Multiple Vulnerabilities (cisco-sa-20171129-webex-players)

Cisco Wireless Control System Installed (Windows)

CiscoWorks Common Services Arbitrary Code Execution (cisco-sa-20101027-cs)

CiscoWorks Common Services Home Page Component Unspecified Shell Command Execution

CiscoWorks Common Services Installed

CiscoWorks Internetwork Performance Monitor CORBA GIOP Overflow

Citrix Access Gateway Plug-in for Windows ActiveX Control Multiple Vulnerabilities (CTX129902)

Citrix Access Gateway Plug-in for Windows ActiveX Control StartEPA() Method HTTP Response Header Parsing Overflows (CTX134303)

Citrix EdgeSight for Load Testing < 3.8.1 Remote Code Execution

Citrix EdgeSight for Load Testing Detection

Citrix EdgeSight Load Tester Buffer Overflow

Citrix ICA Client Multiple Remote Code Execution Vulnerabilities

Citrix License Server Licensing Management Console Unspecified Issue

Citrix Licensing Server Administration Components Multiple Vulnerabilities

Citrix Licensing Service Detection (credentialed check)

Citrix Online Plug-in Installed

Citrix Password Manager Agent Secondary Credentials Information Disclosure

Citrix Password Manager Service Stored Secondary Credentials Disclosure

Citrix Presentation Server 4.5 ActiveSync Feature Code Execution

Citrix Presentation Server 4.5 Code Execution

Citrix Presentation Server 4.5 Multiple Vulnerabilities

Citrix Presentation Server Client Unspecified Remote Code Execution

Citrix Presentation Server Clients Program Neighborhood Agent (PNAgent) Content Redirection Remote DoS

Citrix Provisioning Services 7.x < 7.12 Multiple Vulnerabilities (CTX219580)

Citrix Provisioning Services Detection

Citrix Provisioning Services SoapServer RCE (CTX133039)

Citrix Provisioning Services StreamProcess.exe 0x40020010 Packet Handling RCE

Citrix Provisioning Services StreamProcess.exe Remote Code Execution (CTX130846)

Citrix Provisioning Services Unsupported Version Detection

Citrix Receiver / Online Plug-in Remote Code Execution (CTX134681)

Citrix Receiver Installed

Citrix Secure Gateway Installed

Citrix Secure Gateway Unspecified DoS

Citrix Secure Gateway Unspecified Remote Code Execution

Citrix Studio Installed

Citrix Web Interface 4.6 / 5.0 / 5.0.1 Unspecified XSS

Citrix Web Interface 5.x < 5.4 Unspecified XSS

Citrix Workspace App Installed (Windows)

Citrix XenApp Online Plug-in / Receiver Crafted Certificate MitM Spoofing Weakness

Citrix XenApp Unspecified Remote DoS (CTX133159) (credentialed check)

Citrix XenApp XML Service Interface Crafted Packet Parsing Remote Code Execution (CTX135066)

Citrix XenApp/XenDesktop Multiple Code Execution Vulnerabilities (credentialed check)

Citrix XenDesktop 4.x / 5.x / 7.x Unauthorized Access (CTX139591)

Citrix XenDesktop BrokerAccessPolicyRule Policy Rule Remote Security Bypass

Citrix XenDesktop Virtual Desktop Agent USB Redirection Propagation Handling Access Restriction Bypass (CTX135813)

Citrix XenServer Tools Detection

Citrix XenServer Windows Guest Tools Remote DoS

ColdFusion Extended Support Version Detection (credentialed check)

ColdFusion Installed on Microsoft Windows (credentialed check)

COM+ Internet Services (CIS) Server Detection

Command Antivirus odapi.dll ActiveX Control Multiple Overflows

CommuniGate Pro POP Service Empty Inbox Remote DoS

CommuniGate Pro Server < 5.0.7 LDAP BER Decoding Multiple Vulnerabilities

CommuniGate Pro Server < 5.0.8 LDAP Module Field Handling Remote DoS

Commvault 11 < 11 SP7 Multiple Vulnerabilities

Commvault Installed (Windows)

Comodo Antivirus / Internet Security Installed

Comodo Antivirus / Internet Security Multiple Vulnerabilities

Comodo Internet Security < 3.9 RAR Archive Scan Evasion

Comodo Internet Security < 5.10 kernel ImageBase Executable Handling Remote DoS

Compression Plus CP5DLL32.DLL ZOO Archive Header Processing Overflow RCE

Computer Associates Anti-Virus Engine arclib.dll < 8.1.4.0 Multiple Flaws

Computer Associates ARCserve Backup LDBserver Remote Code Execution Vulnerability

Computer Associates XOsoft Multiple Flaws (CA20100406) (credentialed check)

Computer Manufacturer Information (WMI)

Computrace Detection

Conexant Audio Driver MicTray.exe / MicTray64.exe Keylogger

Core FTP < 2.2 build 1769 Multiple Buffer Overflows

Core FTP < 2.2 build 1785 CWD Command Buffer Overflow

Core FTP Filename Processing Boundary Error FTP List Command Response Parsing Remote Overflow

Corel ActiveCGM Browser ActiveX (acqm.dll) Multiple Overflows

Creative Software AutoUpdate Engine ActiveX (CTSUEng.ocx) Unspecified Overflow

CredSSP Remote Code Execution Vulnerability March 2018 Security Update

CRYPTO-Server installvariables.properties LDAP Credential Local Disclosure

Csound getnum() getnum Function Multiple Buffer Overflows

Csound util/lpci\_main.c main() Function Multiple Buffer Overflows

CSS Web Installer CSSWEBLib.Installer ActiveX InstallProduct1 Method Overflow

CuteFTP < 5.0.2.0 Multiple Vulnerabilities

CuteFTP Professional FTP Command Response Remote Overflow

Cygwin < 1.5.24 cygwin1.dll Crafted Filename Handling Overflow

CylancePROTECT 2.0.x < 2.0.1480 SSL Validation (Cy2008-002)

CylancePROTECT Detection

D-Link DCS-5605 Network Surveillance DcsCliCtrl.dll ActiveX Control SelectDirectory() Method Buffer Overflow

DameWare Mini Remote Control Authentication Credentials Persistence Weakness

DameWare Mini Remote Control Pre-Authentication Remote Overflow

DameWare Mini Remote Control Pre-Authentication Username Remote Overflow

DameWare Mini Remote Control Server Unspecified Local Privilege Escalation

DameWare NT Utilities Authentication Credentials Persistence Weakness

DameWare Remote Support < 9 Hotfix 2 / 10 Hotfix 2 DWExporter.exe Buffer Overflow

DameWare Remote Support Detection

Data Dynamics ActiveBar ActiveX Controls Code Execution

Data Execution Prevention (DEP) is Disabled

DCE Services Enumeration

Dell DellSystemLite.Scanner ActiveX Control Multiple Vulnerabilities

Dell eDellRoot / DSDTestProvider Root CA Certificates Installed

Dell SupportAssist Installed (Windows)

Dell Webcam CrazyTalk ActiveX Remote Overflow

DESlock+ < 3.2.7 Multiple Local Vulnerabilities

Detect Managed Software Install Location (Windows)

Deterministic Network Extender 'dne2000.sys' Local Privilege Escalation

DHCP Server Detection (Windows)

Direct3D Recent Program

DiskPulse Server Default Credentials

DivX Web Player < 1.4.3.4 Stream Format Chunk Buffer Overflow

DjVu Browser Plug-in < 6.1.1 Multiple Buffer Overflows

Docker for Windows Installed

Docker for Windows stable < 18.06.0-ce-win70 / edge < 18.06.0-ce-rc3-win68 Remote Privilege Escalation Vulnerability

Dr.Web File Name Handling Overflow

Dr.Web scanMail Function Unspecified Overflow

Drag And Zip File Name Handling Overflow

Dragon Telnet Server Login Name Handling Remote Overflow DoS

DriveLock DriveLock.exe HTTP Request Processing Remote Overflow

Dropbox Software Detection

DSSAGENT Software Detection

DynaZip < 5.0.0.8 / 6.0.0.5 Zip Archive Handling Multiple Overflows

EasyMail Objects IMAP4 Component Connect Method Remote Overflow

EasyMail SMTP Object ActiveX Control Multiple Buffer Overflows

EDraw Office Viewer ActiveX (EDraw.OfficeViewer) FtpDownloadFile Method Overflow

EDraw Office Viewer ActiveX (officeviewer.ocx) HttpDownloadFileToTempDir Method Overflow

eEye Retina Network Security Scanner Detection

eEye Retina Wireless Scanner (Standalone) Detection

eEye Retina Wireless Scanner .rws Handling Buffer Overflow

eIQnetworks Enterprise Security Analyzer EnterpriseSecurityAnalyzer.exe LICMGR\_ADDLICENSE Command Remote Overflow

eIQnetworks Enterprise Security Analyzer License Manager < 2.5.9 Multiple Remote Overflows

eIQnetworks Enterprise Security Analyzer Monitoring.exe Multiple Command Overflow

eIQnetworks Enterprise Security Analyzer Syslog Server Multiple Remote Overflows

EMC AutoStart ftAgent Multiple Remote Code Execution Vulnerabilities

EMC Data Protection Advisor Installed

EMC Documentum Content Server Detection

EMC Documentum Content Server Information Disclosure (ESA-2014-026)

EMC Documentum Content Server Information Disclosure (ESA-2015-131)

EMC Documentum Content Server Insecure Direct Object Reference (ESA-2014-156)

EMC Documentum Content Server Multiple Privilege Escalation Vulnerabilities (ESA-2014-091)

EMC Documentum Content Server Multiple Vulnerabilities (ESA-2014-046)

EMC Documentum Content Server Multiple Vulnerabilities (ESA-2014-064)

EMC Documentum Content Server Multiple Vulnerabilities (ESA-2014-079)

EMC Documentum Content Server Multiple Vulnerabilities (ESA-2015-131)

EMC Documentum eRoom Indexing Server Hummingbird Client Connector Buffer Overflow

EMC NetWorker 8.2.1.x < 8.2.2.6 / 9.0.x < 9.0.0.6 RCE

EMC NetWorker 8.x < 8.0.2.3 Management Console Information Disclosure

EMC NetWorker < 8.0.4.4 / 8.1.x < 8.1.3.6 / 8.2.x < 8.2.2.2 / 9.0.x < 9.0.0.2 RPC Authentication DoS

EMC NetWorker < 8.2.4.11 / 9.x < 9.1.1.6 / 9.2.x < 9.2.1.1

EMC NetWorker < 8.2.4.9 / 9.x < 9.1.1.3 / 9.2.x < 9.2.0.4

EMC NetWorker Installed

EMC NetWorker Module for MEDITECH 3.0 Build 87 - 90 Local Information Disclosure

EMC NetWorker Module for Microsoft Applications 2.2.1 / 2.3.x < 2.3 build 122 / 2.4.x < 2.4 build 375 Multiple Vulnerabilities

EMC NetWorker nsr\_render\_log Local Privilege Escalation

EMC NetWorker nsrpush Process Local Privilege Escalation

EMC NetWorker Server 9.x < 9.1.1.9 / 9.2.x < 9.2.1.4 / 18.1.0.1

EMC RSA Access Manager Detection (Windows)

EMC RSA Access Manager Information Disclosure (ESA-2014-029)

Enumerate Local Group Memberships

Enumerate Users via WMI

ePolicy Orchestrator SiteManager ActiveX Control Multiple Buffer Overflows

ER Mapper NCSView ActiveX Multiple Buffer Overflows

eScan < 9.0.718.1 MicroWorld Agent service (MWAGENT.EXE) Command Decryption Overflow

Eserv Non-Terminated Connection Saturation DoS

ESET Antivirus CAB Scan Evasion

ESXi Detection via VMWare Tools CMD execution

Eudora WorldMail Mail Management Server (MAILMA.exe) Remote Overflow

Evernote < 5.8.1 ActiveX Control Arbitrary File Overwrite

Evernote Detection (Windows)

Explorer Search History

eZ/eZphotoshare Connection Saturation Remote DoS

F-PROT Antivirus Engine < 4.4.4 Multiple File Handling DoS Vulnerabilities

F-Secure Anti-Virus Detection and Status

F-Secure Anti-Virus for Windows system32 Directory Crafted File Detection Bypass

F-Secure Archive Handling RCE (FSC-2008-2)

F-Secure Key Detection

F-Secure Key Plaintext Information Disclosure

F-Secure Multiple Products Web Console Pre-authentication Overflow RCE

F-Secure Products Archive Files Scan Evasion (2010-1)

F-Secure Products ZIP/RAR File Scan Evasion (FSC-2009-1)

F-Secure RPM Parsing Integer Overflow RCE (FSC-2008-3)

F-Secure ZIP/RAR Archive Handling Overflow Multiple RCE

F5 Networks BIG-IP Edge Client: session ID vulnerability (K06635145)

Facebook Photo Uploader ActiveX Control < 4.5.57.1 Multiple Buffer Overflows

FeedDemon < 2.0.0.25 Atom Feed Active Script Code Execution

Ffdshow < rev2347\_20081123 Remote Buffer Overflow

FileZilla Client < 3.7.2 SFTP Integer Overflow

FileZilla Client < 3.7.3 Multiple Vulnerabilities

FileZilla Client Installed

FileZilla FTP Client < 2.2.30a Multiple Buffer Overflow Vulnerabilities

FileZilla FTP Client < 2.2.32 Multiple Format Strings

FileZilla FTP Client Unspecified Overflow

FileZilla FTP Server < 0.9.22 Wildcard Handling Remote DoS

FileZilla FTP Server MLSD Command Overflow

FileZilla Server < 0.9.31 Denial of Service

FileZilla Server < 0.9.44 OpenSSL Heartbeat Information Disclosure (Heartbleed)

Firebird SQL Server Installed

Firebird SQL Server Remote Denial of Service (CVE-2014-9323)

Firefox 10.0.x < 10.0.3 Multiple Vulnerabilities

Firefox 10.0.x < 10.0.4 Multiple Vulnerabilities

Firefox 10.0.x < 10.0.5 Multiple Vulnerabilities

Firefox 10.0.x < 10.0.6 Multiple Vulnerabilities

Firefox 10.0.x < 10.0.7 Multiple Vulnerabilities

Firefox 10.0.x < 10.0.8 Multiple Vulnerabilities

Firefox 10.x < 10.0.1 Memory Corruption

Firefox 10.x < 10.0.10 Multiple Vulnerabilities

Firefox 10.x < 10.0.11 Multiple Vulnerabilities

Firefox 10.x < 10.0.12 Multiple Vulnerabilities

Firefox 10.x < 10.0.2 'png\_decompress\_chunk' Integer Overflow

Firefox 10.x < 10.0.9 Multiple Vulnerabilities

Firefox 3.0.x < 3.0.2 Multiple Vulnerabilities

Firefox 3.0.x < 3.0.4 Multiple Vulnerabilities

Firefox 3.0.x < 3.0.5 Multiple Vulnerabilities

Firefox 3.0.x < 3.0.6 Multiple Vulnerabilities

Firefox 3.0.x < 3.0.7 Multiple Vulnerabilities

Firefox 3.5 < 3.5.17 Multiple Vulnerabilities

Firefox 3.5 < 3.5.6 Multiple Vulnerabilities

Firefox 3.5 < 3.5.8 Multiple Vulnerabilities

Firefox 3.5.x < 3.5.1 Multiple Vulnerabilities

Firefox 3.5.x < 3.5.2 Multiple Vulnerabilities

Firefox 3.5.x < 3.5.3 Multiple Vulnerabilities

Firefox 3.5.x < 3.5.4 Multiple Vulnerabilities

Firefox 3.6 < 3.6.11 Multiple Vulnerabilities

Firefox 3.6 < 3.6.12 Buffer Overflow

Firefox 3.6 < 3.6.13 Multiple Vulnerabilities

Firefox 3.6 < 3.6.14 Multiple Vulnerabilities

Firefox 3.6 < 3.6.16 Invalid HTTP Certificates

Firefox 3.6 < 3.6.17 Multiple Vulnerabilities

Firefox 3.6 < 3.6.18 Multiple Vulnerabilities

Firefox 3.6 < 3.6.20 Multiple Vulnerabilities

Firefox 3.6 < 3.6.3 Remote Code Execution

Firefox 3.6 < 3.6.4 Multiple Vulnerabilities

Firefox 3.6 < 3.6.7 Multiple Vulnerabilities

Firefox 3.6 < 3.6.9 Multiple Vulnerabilities

Firefox 3.6.7 Remote Code Execution

Firefox 3.6.x < 3.6.2 Multiple Vulnerabilities

Firefox 3.6.x < 3.6.21 Out-of-Date CA List

Firefox 3.6.x < 3.6.22 Untrusted CA

Firefox 3.6.x < 3.6.23 Multiple Vulnerabilities

Firefox 3.6.x < 3.6.24 Multiple Vulnerabilities

Firefox 3.6.x < 3.6.26 Multiple Vulnerabilities

Firefox 3.6.x < 3.6.27 'png\_decompress\_chunk' Integer Overflow

Firefox 3.6.x < 3.6.28 Multiple Vulnerabilities

Firefox 3.x < 3.0.1 Multiple Vulnerabilities

Firefox 4 Multiple Vulnerabilities

Firefox 4.0 < 4.0.1 Multiple Vulnerabilities

Firefox < 0.10.1 Download Directory Arbitrary File Deletion

Firefox < 0.9.3 Null Character MIME Type Spoofing Arbitrary Code Execution

Firefox < 1.0 Multiple Spoofing Vulnerabilities

Firefox < 1.0.0 Multiple Vulnerabilities

Firefox < 1.0.1 Multiple Vulnerabilities

Firefox < 1.0.2 Multiple Vulnerabilities

Firefox < 1.0.3 Multiple Vulnerabilities

Firefox < 1.0.4 Multiple Vulnerabilities

Firefox < 1.0.6 Multiple Vulnerabilities

Firefox < 1.0.7 Multiple Vulnerabilities

Firefox < 1.0.8 Multiple Vulnerabilities

Firefox < 1.5.0.1 Multiple Vulnerabilities

Firefox < 1.5.0.10 / 2.0.0.2 Multiple Vulnerabilities

Firefox < 1.5.0.11 / 2.0.0.3 Multiple Vulnerabilities

Firefox < 1.5.0.12 / 2.0.0.4 Multiple Vulnerabilities

Firefox < 1.5.0.2 Multiple Vulnerabilities

Firefox < 1.5.0.3 iframe.contentWindow.focus() Overflow

Firefox < 1.5.0.4 Multiple Vulnerabilities

Firefox < 1.5.0.5 Multiple Vulnerabilities

Firefox < 1.5.0.7 Multiple Vulnerabilities

Firefox < 1.5.0.8 Multiple Vulnerabilities

Firefox < 1.5.0.9 / 2.0.0.1 Multiple Vulnerabilities

Firefox < 10.0 Multiple Vulnerabilities

Firefox < 12.0 Multiple Vulnerabilities

Firefox < 13.0 Multiple Vulnerabilities

Firefox < 14.0 Multiple Vulnerabilities

Firefox < 15.0 Multiple Vulnerabilities

Firefox < 16.0 Multiple Vulnerabilities

Firefox < 16.0.1 Multiple Vulnerabilities

Firefox < 16.0.2 Multiple Vulnerabilities

Firefox < 17.0 Multiple Vulnerabilities

Firefox < 18.0 Multiple Vulnerabilities

Firefox < 19.0 Multiple Vulnerabilities

Firefox < 19.0.2 nsHTMLEditor Use-After-Free

Firefox < 2.0.0.10 Multiple Vulnerabilities

Firefox < 2.0.0.12 Multiple Vulnerabilities

Firefox < 2.0.0.13 Multiple Vulnerabilities

Firefox < 2.0.0.14 Javascript Garbage Collector DoS

Firefox < 2.0.0.15 Multiple Vulnerabilities

Firefox < 2.0.0.16 / 3.0.1 Multiple Vulnerabilities

Firefox < 2.0.0.17 Multiple Vulnerabilities

Firefox < 2.0.0.18 Multiple Vulnerabilities

Firefox < 2.0.0.19 / 3.0.5 Multiple Vulnerabilities

Firefox < 2.0.0.20 Cross Domain Data Theft

Firefox < 2.0.0.5 Multiple Vulnerabilities

Firefox < 2.0.0.6 Multiple Vulnerabilities

Firefox < 2.0.0.7 Apple QuickTime Plug-In .qtl File qtnext Field Cross-context Scripting

Firefox < 2.0.0.8 Multiple Vulnerabilities

Firefox < 20 Multiple Vulnerabilities

Firefox < 21.0 Multiple Vulnerabilities

Firefox < 22.0 Multiple Vulnerabilities

Firefox < 23.0 Multiple Vulnerabilities

Firefox < 24.0 Multiple Vulnerabilities

Firefox < 25.0 Multiple Vulnerabilities

Firefox < 25.0.1 NSS and NSPR Multiple Vulnerabilities

Firefox < 26.0 Multiple Vulnerabilities

Firefox < 27.0 Multiple Vulnerabilities

Firefox < 28.0 Multiple Vulnerabilities

Firefox < 29.0 Multiple Vulnerabilities

Firefox < 3.0.10 Multiple Vulnerabilities

Firefox < 3.0.11 Multiple Vulnerabilities

Firefox < 3.0.12 Multiple Vulnerabilities

Firefox < 3.0.13 Multiple Vulnerabilities

Firefox < 3.0.14 Multiple Vulnerabilities

Firefox < 3.0.15 Multiple Vulnerabilities

Firefox < 3.0.16 Multiple Vulnerabilities

Firefox < 3.0.18 Multiple Vulnerabilities

Firefox < 3.0.19 Multiple Vulnerabilities

Firefox < 3.0.8 Multiple Vulnerabilities

Firefox < 3.0.9 Multiple Vulnerabilities

Firefox < 3.5.10 Multiple Vulnerabilities

Firefox < 3.5.11 Multiple Vulnerabilities

Firefox < 3.5.12 Multiple Vulnerabilities

Firefox < 3.5.14 Multiple Vulnerabilities

Firefox < 3.5.15 Buffer Overflow

Firefox < 3.5.16 Multiple Vulnerabilities

Firefox < 3.5.18 Invalid HTTP Certificates

Firefox < 3.5.19 Multiple Vulnerabilities

Firefox < 3.5.9 Multiple Vulnerabilities

Firefox < 30.0 Multiple Vulnerabilities

Firefox < 31.0 Multiple Vulnerabilities

Firefox < 32.0 Multiple Vulnerabilities

Firefox < 32.0.3 NSS Signature Verification Vulnerability

Firefox < 33.0 Multiple Vulnerabilities

Firefox < 34.0 Multiple Vulnerabilities

Firefox < 35 Multiple Vulnerabilities

Firefox < 36 Multiple Vulnerabilities

Firefox < 36.0.3 JIT Code Execution

Firefox < 36.0.4 SVG Bypass Privilege Escalation

Firefox < 37.0 Multiple Vulnerabilities

Firefox < 37.0.1 HTTP/2 Alt-Svc Header Certificate Verification Bypass

Firefox < 37.0.2 Failed Plugin Memory Corruption

Firefox < 38.0 Multiple Vulnerabilities

Firefox < 39.0 Multiple Vulnerabilities (Logjam)

Firefox < 39.0.3 PDF Reader Arbitrary File Access

Firefox < 4 CSS Browser History Disclosure Vulnerability

Firefox < 40 Multiple Vulnerabilities

Firefox < 40.0.3 Multiple Vulnerabilities

Firefox < 41 Multiple Vulnerabilities

Firefox < 41.0.2 'fetch' API Cross-Origin Bypass

Firefox < 42 Multiple Vulnerabilities

Firefox < 43 Multiple Vulnerabilities

Firefox < 44 Multiple Vulnerabilities

Firefox < 44.0.2 Service Workers Security Bypass

Firefox < 45 Multiple Vulnerabilities

Firefox < 46 Multiple Vulnerabilities

Firefox < 47 Multiple Vulnerabilities

Firefox < 48 Multiple Vulnerabilities

Firefox < 6.0 Multiple Vulnerabilities

Firefox < 6.0.1 Out-of-Date CA List

Firefox < 6.0.2 Untrusted CA

Firefox < 7.0 Multiple Vulnerabilities

Firefox < 8.0 Multiple Vulnerabilities

Firefox < 9.0 Multiple Vulnerabilities

Firefox Browser Extension Enumeration

Firefox ESR 17.x < 17.0.1 Multiple Vulnerabilities

Firefox ESR 17.x < 17.0.2 Multiple Vulnerabilities

Firefox ESR 17.x < 17.0.3 Multiple Vulnerabilities

Firefox ESR 17.x < 17.0.4 nsHTMLEditor Use-After-Free

Firefox ESR 17.x < 17.0.5 Multiple Vulnerabilities

Firefox ESR 17.x < 17.0.6 Multiple Vulnerabilities

Firefox ESR 17.x < 17.0.7 Multiple Vulnerabilities

Firefox ESR 17.x < 17.0.8 Multiple Vulnerabilities

Firefox ESR 17.x < 17.0.9 Multiple Vulnerabilities

Firefox ESR 24.x < 24.1 Multiple Vulnerabilities

Firefox ESR 24.x < 24.1.1 NSS and NSPR Multiple Vulnerabilities

Firefox ESR 24.x < 24.2 Multiple Vulnerabilities

Firefox ESR 24.x < 24.3 Multiple Vulnerabilities

Firefox ESR 24.x < 24.4 Multiple Vulnerabilities

Firefox ESR 24.x < 24.5 Multiple Vulnerabilities

Firefox ESR 24.x < 24.6 Multiple Vulnerabilities

Firefox ESR 24.x < 24.7 Multiple Vulnerabilities

Firefox ESR 24.x < 24.8 Multiple Vulnerabilities

Firefox ESR 24.x < 24.8.1 NSS Signature Verification Vulnerability

Firefox ESR 31.x < 31.1 Multiple Vulnerabilities

Firefox ESR 31.x < 31.1.1 NSS Signature Verification Vulnerability

Firefox ESR 31.x < 31.2 Multiple Vulnerabilities

Firefox ESR 31.x < 31.3 Multiple Vulnerabilities

Firefox ESR 31.x < 31.4 Multiple Vulnerabilities

Firefox ESR 31.x < 31.5 Multiple Vulnerabilities

Firefox ESR 31.x < 31.5.2 JIT Code Execution

Firefox ESR 31.x < 31.5.3 SVG Bypass Privilege Escalation

Firefox ESR 31.x < 31.6 Multiple Vulnerabilities

Firefox ESR 31.x < 31.7 Multiple Vulnerabilities

Firefox ESR 45.x < 45.1 Multiple Vulnerabilities

Firefox ESR 45.x < 45.2 Multiple Vulnerabilities

Firefox ESR 45.x < 45.3 Multiple Vulnerabilities

Firefox ESR < 17.0.10 Multiple Vulnerabilities

Firefox ESR < 17.0.11 Null\_Cipher Code Execution

Firefox ESR < 31.8 Multiple Vulnerabilities (Logjam)

Firefox ESR < 38.1 Multiple Vulnerabilities (Logjam)

Firefox ESR < 38.1.1 PDF Reader Arbitrary File Access

Firefox ESR < 38.2 Multiple Vulnerabilities

Firefox ESR < 38.2.1 Multiple Vulnerabilities

Firefox ESR < 38.3 Multiple Vulnerabilities

Firefox ESR < 38.4 Multiple Vulnerabilities

Firefox ESR < 38.5 Multiple Vulnerabilities

Firefox ESR < 38.6 Multiple Vulnerabilities

Firefox ESR < 38.6.1 Multiple Graphite 2 Library RCE

Firefox ESR < 38.7 Multiple Vulnerabilities

Firefox ESR < 38.8 Multiple Vulnerabilities

First Response < 1.1.1 Multiple Vulnerabilities

First4Internet XCP Uninstallation CodeSupport.ocx ActiveX Control Arbitrary Code Execution

Flash Cookie History

Flash Player 9.0.159.0 / 10.0.22.87 Multiple Vulnerabilities (APSB09-01)

Flash Player < 10.0.45.2 Multiple Vulnerabilities (APSB10-06)

Flash Player < 10.2.152.26 Multiple Vulnerabilities (APSB11-02)

Flash Player < 10.2.153.1 Unspecified Memory Corruption (APSB11-05)

Flash Player < 10.2.159.1 ActionScript Predefined Class Prototype Addition Remote Code Execution (APSB11-07)

Flash Player < 10.3.181.14 Multiple Vulnerabilities (APSB11-12)

Flash Player < 10.3.181.22 XSS (APSB11-13)

Flash Player < 10.3.181.26 Multiple Vulnerabilities (APSB11-18)

Flash Player < 6.0.79.0 Multiple Unspecified Overflows

Flash Player < 7.0.19.0 Predictable Data Location Weakness

Flash Player < 7.0.60.0 / 8.0.22.0 Multiple Vulnerabilities

Flash Player < 7.0.73.0 / 9.0.115.0 Multiple Vulnerabilities (APSB07-20)

Flash Player < 8.0.42.0 / 9.0.124.0 Multiple Vulnerabilities (APSB08-11)

Flash Player < 9.0.151.0 / 10.0.12.36 Multiple Vulnerabilities (APSB08-18 / APSB08-20 / APSB08-22)

Flash Player < 9.0.246.0 / 10.0.32.18 Multiple Vulnerabilities (APSB09-10)

Flash Player < 9.0.260 / 10.0.42.34 Multiple Vulnerabilities (APSB09-19)

Flash Player < 9.0.277.0 / 10.1.53.63 Multiple Vulnerabilities (ASPB10-14)

Flash Player < 9.0.280 / 10.1.82.76 Multiple Vulnerabilities (APSB10-16)

Flash Player < 9.0.283 / 10.1.85.3 Unspecified Code Execution (APSB10-22)

Flash Player < 9.0.289 / 10.1.102.64 Multiple Vulnerabilities (APSB10-26)

Flash Player <= 10.3.181.36 Multiple Vulnerabilities (APSB11-21)

Flash Player <= 10.3.183.10 / 11.0.1.152 Multiple Vulnerabilities (APSB11-28)

Flash Player <= 10.3.183.14 / 11.1.102.55 Multiple Vulnerabilities (APSB12-03)

Flash Player <= 10.3.183.15 / 11.1.102.62 Multiple Vulnerabilities (APSB12-05)

Flash Player <= 10.3.183.16 / 11.1.102.63 Multiple Memory Corruption Vulnerabilities (APSB12-07)

Flash Player <= 10.3.183.18 / 11.2.202.233 Object Confusion Vulnerability (APSB12-09)

Flash Player <= 10.3.183.19 / 11.3.300.256 Multiple Vulnerabilities (APSB12-14)

Flash Player <= 10.3.183.22 / 11.4.402.264 Multiple Vulnerabilities (APSB12-19)

Flash Player <= 10.3.183.23 / 11.4.402.278 Multiple Vulnerabilities (APSB12-22)

Flash Player <= 10.3.183.29 / 11.4.402.287 Multiple Vulnerabilities (APSB12-24)

Flash Player <= 10.3.183.43 / 11.5.502.110 Multiple Vulnerabilities (APSB12-27)

Flash Player <= 10.3.183.48 / 11.5.502.135 Buffer Overflow (APSB13-01)

Flash Player <= 10.3.183.50 / 11.5.502.146 Multiple Vulnerabilities (APSB13-04)

Flash Player <= 10.3.183.51 / 11.5.502.149 Multiple Vulnerabilities (APSB13-05)

Flash Player <= 10.3.183.63 / 11.6.602.168 Multiple Vulnerabilities (APSB13-08)

Flash Player <= 10.3.183.67 / 11.6.602.171 Multiple Vulnerabilities (APSB13-09)

Flash Player <= 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilities (APSB13-11)

Flash Player <= 10.3.183.7 Multiple Vulnerabilities (APSB11-26)

Flash Player <= 10.3.183.75 / 11.7.700.169 Multiple Vulnerabilities (APSB13-14)

Flash Player <= 10.3.183.86 / 11.7.700.202 Memory Corruption (APSB13-16)

Flash Player <= 10.3.183.90 / 11.7.700.224 Multiple Vulnerabilities (APSB13-17)

Flash Player <= 11.3.300.270 Code Execution (APSB12-18)

Flash Player <= 11.7.700.232 / 11.8.800.94 Memory Corruptions (APSB13-21)

Flash Player <= 11.7.700.242 / 11.9.900.117 Memory Corruptions (APSB13-26)

Flash Player <= 11.7.700.252 / 11.9.900.152 Multiple Vulnerabilities (APSB13-28)

Flash Player <= 11.7.700.257 / 11.9.900.170 Multiple Vulnerabilities (APSB14-02)

Flash Player <= 11.7.700.260 / 12.0.0.43 Unspecified Remote Code Execution (APSB14-04)

Flash Player <= 11.7.700.261 / 12.0.0.44 Multiple Vulnerabilities (APSB14-07)

Flash Player <= 11.7.700.269 / 12.0.0.70 Multiple Vulnerabilities (APSB14-08)

Flash Player <= 11.7.700.272 / 12.0.0.77 Multiple Vulnerabilities (APSB14-09)

Flash Player <= 11.7.700.275 / 13.0.0.182 Pixel Bender Component Buffer Overflow (APSB14-13)

Flash Player <= 13.0.0.206 Multiple Vulnerabilities (APSB14-14)

Flash Player <= 13.0.0.214 Multiple Vulnerabilities (APSB14-16)

Flash Player <= 14.0.0.125 Multiple Vulnerabilities (APSB14-17)

Flash Player <= 14.0.0.145 Multiple Vulnerabilities (APSB14-18)

Flash Player <= 14.0.0.179 Multiple Vulnerabilities (APSB14-21)

Flash Player <= 15.0.0.167 Multiple Vulnerabilities (APSB14-22)

Flash Player <= 15.0.0.189 Multiple Vulnerabilities (APSB14-24)

Flash Player <= 15.0.0.223 Dereferenced Memory Pointer RCE (APSB14-26)

Flash Player <= 15.0.0.239 Multiple Vulnerabilities (APSB14-27)

Flash Player <= 16.0.0.235 Multiple Vulnerabilities (APSB15-01)

Flash Player <= 16.0.0.257 Information Disclosure (APSB15-02)

Flash Player <= 16.0.0.287 Unspecified Code Execution (APSA15-01 / APSB15-03)

Flash Player <= 16.0.0.296 Unspecified Code Execution (APSA15-02 / APSB15-04)

Flash Player <= 16.0.0.305 Multiple Vulnerabilities (APSB15-05)

Flash Player Detection

Flash Player HTTP Header CRLF Injection (APSB06-18)

Flash Player Multiple Vulnerabilities (APSB06-11)

Flash Player Multiple Vulnerabilities (APSB07-12)

Flash Player swf Processing Multiple Unspecified Code Execution (APSB06-03)

FlashFXP < 2.1b923 Multiple Remote Overflows

FlashFXP < 4.2.0.1730 ListIndex TListBox Handling Remote Overflow

FlashFXP Detection

FlexCell Grid FlexCell.Grid ActiveX Control Multiple Method Arbitrary File Overwrite

Flexera AdminStudio LaunchProcess Function ActiveX Control Remote Command Execution

Flexera InstallShield Installed

Flexera ISGrid ActiveX Control Remote Code Execution Vulnerabilities

FLEXnet Connect Update Service ActiveX Control Multiple Code Execution Vulnerabilities

FLEXnet Connect Update Service Agent ActiveX (isusweb.dll) Overflow

FlexNet License Multiple Vulnerabilities

FlexNet License Server Installed

FlipViewer ActiveX Control < 4.1 Buffer Overflow Vulnerabilities

Fortinet FortiClient 6.2.x < 6.2.1 Missing Encryption Of Sensitive Data Vulnerability

Fortinet FortiClient < 6.2.0 Information Disclosure MitM (FG-IR-18-100)

Fortinet FortiClient Crafted VPN Connection Name Handling Local Format String

Fortinet FortiClient Host Security fortimon.sys Crafted Request Local Privilege Escalation

Fortinet FortiClient Installed

Fortinet FortiClient Local Privilege Escalation

Fortinet FortiClient NDIS Miniport Driver Null Pointer Dereference

Fortinet FortiClient OpenSSL Security Bypass

Fortinet FortiClient Unsupported Version Detection

Foxit 3D Plugin (U3DBrowser) Installed (Windows)

Foxit 3D Plugin Beta 9.7.0.29430 NULL Pointer Dereference Vulnerability

Foxit Advanced PDF Editor 3.x < 3.0.4.0 Security Cookie Stack-based Buffer Overflow

Foxit Advanced PDF Editor Installed

Foxit History

Foxit PDF SDK ActiveX < 5.5.1 Multiple Vulnerabilities

Foxit PDF SDK ActiveX Installed (Windows)

Foxit Phantom < 2.2.0.926 Multiple Vulnerabilities

Foxit PhantomPDF 8.x < 8.3.12 / 9.x < 9.7 Multiple Vulnerabilities

Foxit PhantomPDF < 7.2 Multiple Vulnerabilities

Foxit PhantomPDF < 7.3.11 Multiple Vulnerabilities

Foxit PhantomPDF < 7.3.13 Multiple Vulnerabilities

Foxit PhantomPDF < 7.3.15 Multiple Vulnerabilities

Foxit PhantomPDF < 7.3.17 Multiple Vulnerabilities

Foxit PhantomPDF < 7.3.4 Multiple Vulnerabilities

Foxit PhantomPDF < 7.3.9 Multiple Vulnerabilities

Foxit PhantomPDF < 8.0 Multiple Vulnerabilities

Foxit PhantomPDF < 8.0.2 Multiple Vulnerabilities

Foxit PhantomPDF < 8.1 Multiple Vulnerabilities

Foxit PhantomPDF < 8.1.1 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.1 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.10 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.11 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.2 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.5 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.6 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.7 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.8 Multiple Vulnerabilities

Foxit PhantomPDF < 8.3.9 Multiple Vulnerabilities

Foxit PhantomPDF < 9.0 Multiple Vulnerabilities

Foxit PhantomPDF < 9.1 Multiple Vulnerabilities

Foxit PhantomPDF < 9.1 Multiple Vulnerabilities

Foxit PhantomPDF < 9.2 Multiple Vulnerabilities

Foxit PhantomPDF < 9.3 Multiple Vulnerabilities

Foxit PhantomPDF < 9.4 Multiple Vulnerabilities

Foxit PhantomPDF < 9.5 Multiple Vulnerabilities

Foxit PhantomPDF < 9.5.0 Multiple Vulnerabilities

Foxit PhantomPDF < 9.6 Multiple Vulnerabilities

Foxit PhantomPDF < 9.7 Multiple Vulnerabilities

Foxit PhantomPDF < 9.7.1 Multiple Vulnerabilities

Foxit PhantomPDF Detection

Foxit Reader 2.x < 2.3 Build 3902 / 3.x < 3.0 Build 1506 Multiple Vulnerabilities

Foxit Reader 9.0 < 9.6.0.25114 Security Bypass Vulnerability

Foxit Reader < 2.3 Build 2923 util.printf() Floating Point Specifier RCE

Foxit Reader < 3.2.1 Arbitrary Program Execution

Foxit Reader < 4.0.0.0619 FreeType Engine RCE

Foxit Reader < 4.1.1.0805 FreeType CFF Opcodes RCE

Foxit Reader < 4.2.0.0928 Multiple Vulnerabilities

Foxit Reader < 4.3.1.0218 Multiple Vulnerabilities

Foxit Reader < 5.0.2.0718 Multiple Vulnerabilities

Foxit Reader < 5.1.3.1201 Memory Corruption RCE

Foxit Reader < 5.3 Cross-References RCE

Foxit Reader < 5.4 Trojan DLL Injection

Foxit Reader < 5.4.3 Trojan DLL Injection

Foxit Reader < 6.1.4 Trojan DLL Injection

Foxit Reader < 7.2 Multiple Vulnerabilities

Foxit Reader < 7.3.4 Multiple Vulnerabilities

Foxit Reader < 8.3.1 Multiple Vulnerabilities

Foxit Reader < 8.3.2 Multiple Vulnerabilities

Foxit Reader < 8.3.7 Multiple Vulnerabilities

Foxit Reader < 9.0 Multiple Vulnerabilities

Foxit Reader < 9.1 Multiple Vulnerabilities

Foxit Reader < 9.2 Multiple Vulnerabilities

Foxit Reader < 9.3 Multiple Vulnerabilities

Foxit Reader < 9.4 Multiple Vulnerabilities

Foxit Reader < 9.5 Multiple Vulnerabilities

Foxit Reader < 9.5.0 Multiple Vulnerabilities

Foxit Reader < 9.6 Multiple Vulnerabilities

Foxit Reader < 9.7 Multiple Vulnerabilities

Foxit Reader < 9.7.1 Multiple Vulnerabilities

Foxit Reader Detection

Foxit Reader Firefox Plugin Reloading RCE

Foxit Reader Firefox Plugin URL File Name RCE

Foxit Reader JPEG2000 / JBIG Decoder Add-On < 2.0.2009.616 Multiple Vulnerabilities

Foxit Studio Photo < 3.6.6.909 Multiple Vulnerabilities

Foxit Studio Photo < 3.6.6.913 Multiple Vulnerabilities

Foxit Studio Photo < 3.6.6.916 Out-of-Bounds Read Vulnerability

Foxit Studio Photo Installed (Windows)

Free Community Detection

FTP Voyager LIST Command File List Handling Remote Overflow

GAMSoft TelSrv 1.4/1.5 Username Overflow DoS

GATOR Detection

GdPicture Multiple ActiveX Control SaveAsPDF Method Arbitrary File Overwrite

GEAR Software CD DVD Filter Driver Insecure Method Local Privilege Escalation

GFI MailSecurity HTTP Management Interface Request Header Overflow

Git for Windows .git/config Command Execution

Git for Windows 2.13.x < 2.13.7 / 2.14.x < 2.14.4 / 2.15.x < 2.15.2 / 2.16.x < 2.16.4 / 2.17.x < 2.17.1 Remote Code Execution

Git for Windows 2.7.x < 2.7.6 / 2.8.x < 2.8.6 / 2.9.x < 2.9.5 / 2.10.x < 2.10.4 / 2.11.x < 2.11.13 / 2.12.x < 2.12.4 / 2.13.x < 2.13.5 / 2.14.x < 2.14.1 Malicious SSH URL Command Execution

Git for Windows Detection

GitHub for Windows < 2.6.5 .git/config Command Execution

GitHub for Windows Installed

GO-Global for Windows \_USERSA\_ Remote Overflow

GO-Global for Windows \_USERSA\_ Remote Overflow (credentialed check)

Google Apps Directory Sync < 3.1.6 Weak Stored Credential Local Disclosure

Google Apps Directory Sync Detection (Windows)

Google Chrome < 0.2.149.29 Multiple Vulnerabilities

Google Chrome < 0.3.154.9 Address Bar Spoofing

Google Chrome < 1.0.154.46 Multiple Vulnerabilities

Google Chrome < 1.0.154.48 Cross-browser Command Execution

Google Chrome < 1.0.154.53 Multiple Vulnerabilities

Google Chrome < 1.0.154.59 ChromeHTML URI Handling Privilege Escalation

Google Chrome < 1.0.154.64 Multiple Overflows

Google Chrome < 1.0.154.65 WebKit SVGList Object Handling Memory Corruption

Google Chrome < 10.0.648.127 Multiple Vulnerabilities

Google Chrome < 10.0.648.133 Code Execution

Google Chrome < 10.0.648.204 Multiple Vulnerabilities

Google Chrome < 10.0.648.205 Multiple Vulnerabilities

Google Chrome < 11.0.696.57 Multiple Vulnerabilities

Google Chrome < 11.0.696.68 Multiple Vulnerabilities

Google Chrome < 11.0.696.71 Multiple Vulnerabilities

Google Chrome < 12.0.742.112 Multiple Vulnerabilities

Google Chrome < 12.0.742.91 Multiple Vulnerabilities

Google Chrome < 13.0.782.107 Multiple Vulnerabilities

Google Chrome < 13.0.782.215 Multiple Vulnerabilities

Google Chrome < 13.0.782.218 Out of Date CA List

Google Chrome < 13.0.782.220 Untrusted CA

Google Chrome < 14.0.835.163 Multiple Vulnerabilities

Google Chrome < 14.0.835.186 Multiple Adobe Flash Player Vulnerabilities

Google Chrome < 14.0.835.202 Multiple Vulnerabilities

Google Chrome < 15.0.874.102 Multiple Vulnerabilities

Google Chrome < 15.0.874.120 Multiple Vulnerabilities

Google Chrome < 15.0.874.121 V8 Out-of-bounds Write Unspecified Remote Memory Corruption

Google Chrome < 16.0.912.63 Multiple Vulnerabilities

Google Chrome < 16.0.912.75 Multiple Vulnerabilities

Google Chrome < 16.0.912.77 Multiple Vulnerabilities

Google Chrome < 17.0.963.46 Multiple Vulnerabilities

Google Chrome < 17.0.963.56 Multiple Vulnerabilities

Google Chrome < 17.0.963.65 Multiple Vulnerabilities

Google Chrome < 17.0.963.78 Multiple Vulnerabilities

Google Chrome < 17.0.963.79 Memory Corruption Vulnerabilities

Google Chrome < 17.0.963.83 Multiple Vulnerabilities

Google Chrome < 18.0.1025.142 Multiple Vulnerabilities

Google Chrome < 18.0.1025.151 Multiple Vulnerabilities

Google Chrome < 18.0.1025.168 Multiple Vulnerabilities

Google Chrome < 19.0.1084.46 Multiple Vulnerabilities

Google Chrome < 19.0.1084.52 Multiple Vulnerabilities

Google Chrome < 2.0.172.31 WebKit Multiple Vulnerabilities

Google Chrome < 2.0.172.33 Multiple Vulnerabilities

Google Chrome < 2.0.172.37 Multiple Vulnerabilities

Google Chrome < 2.0.172.43 Multiple Vulnerabilities

Google Chrome < 20.0.1132.43 Multiple Vulnerabilities

Google Chrome < 20.0.1132.57 Multiple Vulnerabilities

Google Chrome < 21.0.1180.60 Multiple Vulnerabilities

Google Chrome < 21.0.1180.75 Multiple PDF Viewer Vulnerabilities

Google Chrome < 21.0.1180.89 Multiple Vulnerabilities

Google Chrome < 22.0.1229.79 Multiple Vulnerabilities

Google Chrome < 22.0.1229.92 Multiple Vulnerabilities

Google Chrome < 22.0.1229.94 Multiple Vulnerabilities

Google Chrome < 23.0.1271.64 Multiple Vulnerabilities

Google Chrome < 23.0.1271.91 Multiple Vulnerabilities

Google Chrome < 23.0.1271.95 Multiple Vulnerabilities

Google Chrome < 23.0.1271.97 Multiple Vulnerabilities

Google Chrome < 24.0.1312.52 Multiple Vulnerabilities

Google Chrome < 24.0.1312.56 Multiple Vulnerabilities

Google Chrome < 25.0.1364.152 Multiple Vulnerabilities

Google Chrome < 25.0.1364.160 WebKit Type Confusion Code Execution

Google Chrome < 25.0.1364.97 Multiple Vulnerabilities

Google Chrome < 26.0.1410.43 Multiple Vulnerabilities

Google Chrome < 27.0.1453.110 Multiple Vulnerabilities

Google Chrome < 27.0.1453.116 Flash Click-Jacking

Google Chrome < 27.0.1453.93 Multiple Vulnerabilities

Google Chrome < 28.0.1500.71 Multiple Vulnerabilities

Google Chrome < 28.0.1500.95 Multiple Vulnerabilities

Google Chrome < 29.0.1547.57 Multiple Vulnerabilities

Google Chrome < 3.0.195.21 Multiple Vulnerabilities

Google Chrome < 3.0.195.24 dtoa Implementation Remote Overflow

Google Chrome < 3.0.195.32 Multiple Vulnerabilities

Google Chrome < 3.0.195.33 Multiple Vulnerabilities

Google Chrome < 30.0.1599.101 Multiple Vulnerabilities

Google Chrome < 30.0.1599.66 Multiple Vulnerabilities

Google Chrome < 31.0.1650.48 Multiple Vulnerabilities

Google Chrome < 31.0.1650.57 Multiple Memory Corruptions

Google Chrome < 31.0.1650.63 Multiple Vulnerabilities

Google Chrome < 32.0.1700.102 Multiple Vulnerabilities

Google Chrome < 32.0.1700.76 Multiple Vulnerabilities

Google Chrome < 33.0.1750.117 Multiple Vulnerabilities

Google Chrome < 33.0.1750.146 Multiple Vulnerabilities

Google Chrome < 33.0.1750.149 Multiple Vulnerabilities

Google Chrome < 33.0.1750.154 Multiple Vulnerabilities

Google Chrome < 34.0.1847.116 Multiple Vulnerabilities

Google Chrome < 34.0.1847.131 Multiple Vulnerabilities

Google Chrome < 34.0.1847.137 Multiple Vulnerabilities

Google Chrome < 35.0.1916.114 Multiple Vulnerabilities

Google Chrome < 35.0.1916.153 Multiple Vulnerabilities

Google Chrome < 36.0.1985.125 Multiple Vulnerabilities

Google Chrome < 36.0.1985.143 Multiple Vulnerabilities

Google Chrome < 37.0.2062.120 Multiple Vulnerabilities

Google Chrome < 37.0.2062.124 Multiple Vulnerabilities

Google Chrome < 37.0.2062.94 Multiple Vulnerabilities

Google Chrome < 38.0.2125.101 Multiple Vulnerabilities

Google Chrome < 38.0.2125.104 Multiple Vulnerabilities

Google Chrome < 38.0.2125.122 Multiple Vulnerabilities

Google Chrome < 39.0.2171.65 Multiple Vulnerabilities

Google Chrome < 39.0.2171.71 Flash Player Remote Code Execution

Google Chrome < 39.0.2171.95 Multiple Vulnerabilities

Google Chrome < 39.0.2171.99 Multiple Vulnerabilities

Google Chrome < 4.0.249.78 Multiple Vulnerabilities

Google Chrome < 4.0.249.89 Multiple Vulnerabilities

Google Chrome < 4.1.249.1036 Multiple Vulnerabilities

Google Chrome < 4.1.249.1059 Multiple Vulnerabilities

Google Chrome < 4.1.249.1064 Multiple Vulnerabilities

Google Chrome < 40.0.2214.111 Multiple Vulnerabilities

Google Chrome < 40.0.2214.91 Multiple Vulnerabilities

Google Chrome < 40.0.2214.93 Flash Player Multiple Remote Code Execution

Google Chrome < 41.0.2272.118 Multiple Vulnerabilities

Google Chrome < 41.0.2272.76 Multiple Vulnerabilities

Google Chrome < 42.0.2311.135 Multiple Vulnerabilities

Google Chrome < 42.0.2311.152 Multiple Vulnerabilities

Google Chrome < 42.0.2311.90 Multiple Vulnerabilities

Google Chrome < 43.0.2357.124 Multiple Vulnerabilities

Google Chrome < 43.0.2357.130 Multiple Vulnerabilities

Google Chrome < 43.0.2357.132 Multiple Vulnerabilities

Google Chrome < 43.0.2357.134 Multiple RCE Vulnerabilities

Google Chrome < 43.0.2357.65 Multiple Vulnerabilities

Google Chrome < 44.0.2403.155 Multiple Vulnerabilities

Google Chrome < 44.0.2403.89 Multiple Vulnerabilities

Google Chrome < 45.0.2454.101 Multiple Vulnerabilities

Google Chrome < 45.0.2454.85 Multiple Vulnerabilities

Google Chrome < 45.0.2454.99 Multiple Vulnerabilities

Google Chrome < 46.0.2490.71 Multiple Vulnerabilities

Google Chrome < 46.0.2490.80 Multiple Vulnerabilities

Google Chrome < 46.0.2490.86 Multiple Vulnerabilities

Google Chrome < 47.0.2526.106 Multiple RCE

Google Chrome < 47.0.2526.73 Multiple Vulnerabilities

Google Chrome < 47.0.2526.80 Multiple Vulnerabilities

Google Chrome < 48.0.2564.109 Multiple Vulnerabilities

Google Chrome < 48.0.2564.116 Blink Same-Origin Policy Bypass

Google Chrome < 48.0.2564.82 Multiple Vulnerabilities

Google Chrome < 49.0.2623.108 Multiple Vulnerabilities

Google Chrome < 49.0.2623.75 Multiple Vulnerabilities

Google Chrome < 49.0.2623.87 Multiple RCE

Google Chrome < 5.0.375.125 Multiple Vulnerabilities

Google Chrome < 5.0.375.127 Multiple Vulnerabilities

Google Chrome < 5.0.375.55 Multiple Vulnerabilities

Google Chrome < 5.0.375.70 Multiple Vulnerabilities

Google Chrome < 5.0.375.86 Multiple Vulnerabilities

Google Chrome < 5.0.375.99 Multiple Vulnerabilities

Google Chrome < 50.0.2661.102 Multiple Vulnerabilities

Google Chrome < 50.0.2661.75 Multiple Vulnerabilities

Google Chrome < 50.0.2661.94 Multiple Vulnerabilities

Google Chrome < 51.0.2704.103 Multiple Vulnerabilities

Google Chrome < 51.0.2704.63 Multiple Vulnerabilities

Google Chrome < 51.0.2704.79 Multiple Vulnerabilities

Google Chrome < 52.0.2743.116 Multiple Vulnerabilities

Google Chrome < 52.0.2743.82 Multiple Vulnerabilities

Google Chrome < 53.0.2785.113 Multiple Vulnerabilities

Google Chrome < 53.0.2785.143 Multiple Vulnerabilities

Google Chrome < 53.0.2785.89 Multiple Vulnerabilities

Google Chrome < 54.0.2840.59 Multiple Vulnerabilities

Google Chrome < 54.0.2840.87 V8 Globals Stable Map Assumption Handling RCE

Google Chrome < 54.0.2840.99 Multiple Vulnerabilities

Google Chrome < 55.0.2883.75 Multiple Vulnerabilities

Google Chrome < 56.0.2924.76 Multiple Vulnerabilities

Google Chrome < 57.0.2987.133 Multiple Vulnerabilities

Google Chrome < 57.0.2987.98 Multiple Vulnerabilities

Google Chrome < 58.0.3029.81 Multiple Vulnerabilities

Google Chrome < 58.0.3029.96 WebRTC Frame Order Handling Race Condition

Google Chrome < 59.0.3071.104 Multiple Vulnerabilities

Google Chrome < 59.0.3071.86 Multiple Vulnerabilities

Google Chrome < 6.0.472.53 Multiple Vulnerabilities

Google Chrome < 6.0.472.59 Multiple Vulnerabilities

Google Chrome < 6.0.472.62 Multiple Vulnerabilities

Google Chrome < 60.0.3112.78 Multiple Vulnerabilities

Google Chrome < 61.0.3163.100 Multiple Vulnerabilities

Google Chrome < 61.0.3163.110 Multiple Vulnerabilities

Google Chrome < 61.0.3163.79 Multiple Vulnerabilities

Google Chrome < 62.0.3202.62 Multiple Vulnerabilities

Google Chrome < 62.0.3202.89 Multiple Vulnerabilities

Google Chrome < 62.0.3202.94 Out of bounds read flaw in V8

Google Chrome < 63.0.3239.108 Multiple Vulnerabilities

Google Chrome < 63.0.3239.84 Multiple Vulnerabilities

Google Chrome < 64.0.3282.119 Multiple Vulnerabilities (Spectre)

Google Chrome < 64.0.3282.140 V8 Factory::NewFunction() RCE

Google Chrome < 64.0.3282.167 V8 JSFunction::CalculateInstanceSizeForDerivedClass() RCE

Google Chrome < 65.0.3325.146 Multiple Vulnerabilities

Google Chrome < 66.0.3359.117 Multiple Vulnerabilities

Google Chrome < 66.0.3359.170 Multiple Vulnerabilities

Google Chrome < 67.0.3396.62 Multiple Vulnerabilities

Google Chrome < 68.0.3440.75 Multiple Vulnerabilities

Google Chrome < 69.0.3497.100 Vulnerability

Google Chrome < 69.0.3497.81 Multiple Vulnerabilities

Google Chrome < 69.0.3497.92 Vulnerability

Google Chrome < 7.0.517.41 Multiple Vulnerabilities

Google Chrome < 7.0.517.44 Multiple Vulnerabilities

Google Chrome < 70.0.3538.102 Vulnerability

Google Chrome < 70.0.3538.110 Vulnerability

Google Chrome < 70.0.3538.67 Multiple Vulnerabilities

Google Chrome < 71.0.3578.80 Multiple Vulnerabilities

Google Chrome < 71.0.3578.98

Google Chrome < 72.0.3626.121 Vulnerability

Google Chrome < 72.0.3626.81 Multiple Vulnerabilities

Google Chrome < 72.0.3626.96 Vulnerability

Google Chrome < 73.0.3683.103 Heap Corruption

Google Chrome < 73.0.3683.75 Multiple Vulnerabilities

Google Chrome < 74.0.3729.108 Multiple Vulnerabilities

Google Chrome < 74.0.3729.131 Multiple Vulnerabilities

Google Chrome < 74.0.3729.157 Vulnerability

Google Chrome < 75.0.3770.142 Multiple Vulnerabilities

Google Chrome < 75.0.3770.80 Multiple Vulnerabilities

Google Chrome < 75.0.3770.90 Vulnerability

Google Chrome < 76.0.3809.100 Multiple Vulnerabilities

Google Chrome < 76.0.3809.132 Use-After-Free Vulnerability

Google Chrome < 76.0.3809.87 Multiple Vulnerabilities

Google Chrome < 77.0.3865.120 Multiple Vulnerabilities

Google Chrome < 77.0.3865.75 Multiple Vulnerabilities

Google Chrome < 77.0.3865.90 Multiple Vulnerabilities

Google Chrome < 78.0.3904.108 Multiple Vulnerabilities

Google Chrome < 78.0.3904.70 Multiple Vulnerabilities

Google Chrome < 78.0.3904.87 Multiple Vulnerabilities

Google Chrome < 78.0.3904.97 Vulnerability

Google Chrome < 79.0.3945.117 Multiple Vulnerabilities

Google Chrome < 79.0.3945.130 Multiple Vulnerabilities

Google Chrome < 79.0.3945.79 Multiple Vulnerabilities

Google Chrome < 79.0.3945.88 Vulnerability

Google Chrome < 8.0.552.215 Multiple Vulnerabilities

Google Chrome < 8.0.552.224 Multiple Vulnerabilities

Google Chrome < 8.0.552.237 Multiple Vulnerabilities

Google Chrome < 80.0.3987.116 Multiple Vulnerabilities

Google Chrome < 80.0.3987.122 Multiple Vulnerabilities

Google Chrome < 80.0.3987.132 Multiple Vulnerabilities

Google Chrome < 80.0.3987.149 Multiple Vulnerabilities

Google Chrome < 80.0.3987.162 Multiple Vulnerabilities

Google Chrome < 80.0.3987.87 Multiple Vulnerabilities

Google Chrome < 81.0.4044.113 Vulnerability

Google Chrome < 81.0.4044.92 Multiple Vulnerabilities

Google Chrome < 9.0.597.107 Multiple Vulnerabilities

Google Chrome < 9.0.597.84 Multiple Vulnerabilities

Google Chrome < 9.0.597.94 Multiple Vulnerabilities

Google Chrome Detection (Windows)

Google Chrome Frame < 26.0.1410.28 Denial of Service

Google Chrome Frame < 4.0.245.1

Google Chrome Frame Detection (Windows)

Google Cloud Platform Compute Engine Instance Metadata Enumeration (Windows)

Google Desktop Advanced Search Internal Web Server XSS

Google Desktop Detection

Google Picasa < 3.6 Build 105.41

Google Picasa < 3.8 Path Subversion Arbitrary DLL Injection Code Execution

Google Picasa < 3.9 Build 136.17 Multiple Vulnerabilities

Google Picasa < 3.9 Build 137.69 Multiple Vulnerabilities

Google Picasa <= 3.6 Build 105.61 JPEG Image Handling Remote Code Execution

Google Picasa Detection (Windows)

Google Secure Access VPN Client Installed

Google SketchUp < 13.0.3689 SKP Multiple Vulnerabilities

Google SketchUp < 7.1 M2 Remote Code Execution Vulnerabilities

Google SketchUp < 8.0 SKP File Malformed Edge Geometry Handling Remote Code Execution

Google SketchUp < 8.0.11752 MAC Pict Buffer Overflow

Google SketchUp < 8.0.14346 Multiple Vulnerabilities

Google Toolbar < 2.0.114.1 Multiple Vulnerabilities

Google/Trimble SketchUp Detection

Gracenote CDDBControl ActiveX Control Option String Overflow

Gracenote CDDBControl ActiveX Proxy Configuration Parameters Multiple Overflows

Groove Virtual Office / Workspace Multiple Vulnerabilities

GroupWise Internet Agent < 8.0.2 HP1 Multiple Flaws

GroupWise Internet Agent < 8.0.2 HP2 Email Message VCALENDAR Data TZID Variable Remote Overflow

GroupWise Internet Agent < 8.0.2 HP3 Multiple Vulnerabilities

Gupta SQLBase EXECUTE Command Remote Overflow

H3C / HPE Intelligent Management Center PLAT < 7.3 E0504P04 Multiple Vulnerabilities

Hexamail Server pop3 Service USER Command Remote Overflow

Hexamail Server pop3 Service USER Command Remote Overflow (credentialed check)

hMailServer < 4.4.2 build 279 IMAP Command Handling Remote DoS

HP B-series SAN Network Advisor < 12.1.1 Remote Code Execution (Windows)

HP B-series SAN Network Advisor Installed (Windows)

HP Client Automation radexecd.exe Remote Command Execution

HP Data Protector <= A.06.20 Multiple Vulnerabilities (credentialed check)

HP Data Protector Express 5.x < 5.0.0 Build 59287 / 6.x < 6.0.0 Build 11974 Multiple Vulnerabilities

HP Data Protector Express < 4.x build 56906 / 3.x build 56936 Multiple Vulnerabilities

HP Data Protector Express Crafted Traffic Remote Memory Disclosure

HP Data Protector Express Installed

HP Data Protector Installed (Windows) (credentialed check)

HP Data Protector Media Operations Server 'DBServer.exe' Remote Code Execution

HP Easy Printer Care Software ActiveX Control Remote Code Execution Vulnerabilities

HP HPeDiag ActiveX Control Multiple Vulnerabilities

HP Info Center ActiveX Control Multiple Remote Vulnerabilities

HP iNode Management Center Remote Code Execution (HPSB3C02687)

HP Insight Control Performance Management < 6.3 Multiple Vulnerabilities

HP Insight Control Performance Management Installed

HP Insight Control Power Management < 6.1 Local Unauthorized Access

HP Insight Control Power Management Detection

HP Insight Control Server Migration 7.3.0 and 7.3.1 OpenSSL Heartbeat Information Disclosure (Heartbleed)

HP Insight Control Server Migration Detection (Windows)

HP Insight Management Agents Multiple Vulnerabilities

HP Instant Support Driver Check HPSDDX Class (SDD) ActiveX (sdd.dll) queryHub Function Overflow

HP Instant Support HPISDataManager.dll ActiveX Control < 1.0.0.24 Vulnerabilities

HP Intelligent Management Center < 5.0 E0101-L02 Multiple Vulnerabilities

HP Intelligent Management Center Application Detection

HP Intelligent Management Center Java Object Deserialization RCE

HP LoadRunner 11.52 / 12.00 / 12.01 / 12.02 / 12.50 Multiple Vulnerabilities

HP LoadRunner 11.52 / 12.00 / 12.01 / 12.02 / 12.50 Virtual Table Server RCE

HP LoadRunner 11.52 Buffer Overflow RCE

HP LoadRunner 11.52.x < 11.52 Patch 2 / 12.00.x < 12.00 Patch 1 Heartbeat Information Disclosure (Heartbleed)

HP LoadRunner < 11.00 Patch 4 Code Execution Vulnerability

HP LoadRunner < 11.52 Patch 1 Multiple Vulnerabilities

HP LoadRunner < 12.50 Scenario File Local Code Execution

HP LoadRunner Detect

HP LoadRunner lrLRIServices ActiveX Control Code Execution Vulnerability

HP LoadRunner MMS Protocol Buffer Overflow RCE

HP LoadRunner Unspecified Arbitrary Remote Code Execution

HP MFP Digital Sending Software 4.91.0 Local Authentication Bypass

HP MFP Digital Sending Software 4.9x <= 4.91.21 Local Workflow Metadata Information Disclosure

HP MFP Digital Sending Software < 4.18.3 Local Unspecified Authentication Bypass

HP MFP Digital Sending Software Detection

HP Network Node Manager i (NNMi) XSS (HPSBMU03035)

HP Network Node Manager i Remote Code Execution (HPSBMU03075)

HP NNMi 8.x / 9.0x / 9.1x / 9.20 Unspecified XSS

HP OpenView Network Node Manager Multiple Vulnerabilities

HP Operations Manager for Windows 8.x and 9.0 Java Object Deserialization RCE

HP Operations Manager for Windows Installed

HP Operations Manager i (OMi) 9.1 / 9.2 RCE

HP Operations Manager i (OMi) Detection

HP Operations Manager i Installed (deprecated)

HP Operations Manager SourceView ActiveX LoadFile / SaveFile Stack Overflows

HP OPOS CCO Drivers RCE Vulnerabilities

HP OVIS Probe Builder Service (PBOVISServer.exe) Arbitrary Remote Process Termination

HP Performance Center 11.52.x / 12.x < 12.53 Multiple Vulnerabilities

HP Performance Center < 12.53 Patch 4 libxdrutil.dll mxdr\_string() RCE

HP Performance Center Detect

HP Performance Center MMS Protocol Buffer Overflow RCE

HP PKI ActiveX Control KillProcess Denial of Service

HP ProCurve Manager Remote Unauthorized Access to Data (HPSBMA02420 SSRT071458)

HP SiteScope Installation Detection

HP Software Update HPRulesEngine.ContentCollection ActiveX (RulesEngine.dll) Multiple Insecure Methods

HP Sprinter Installed

HP Sprinter Remote Code Execution

HP Support Assistant < 8.1.52.1 Unspecified Local Authentication Bypass

HP Support Assistant < 8.7.50.3 DLL Loading Vulnerability

HP Support Assistant < 8.8 Multiple Vulnerabilities

HP Support Assistant Installed

HP Systems Insight Manager 7.2.x < 7.2 Hotfix 37 / 7.3.x < 7.3 Hotfix 34 OpenSSL Multiple Vulnerabilities

HP Systems Insight Manager < 2.5.2.0 WMI Mapper Component Multiple Flaws

HP Systems Insight Manager < 7.0 Multiple Vulnerabilities

HP Systems Insight Manager < 7.2 Multiple Vulnerabilities

HP Systems Insight Manager < 7.3 Multiple Vulnerabilities

HP Systems Insight Manager < 7.4 Multiple Vulnerabilities

HP Systems Insight Manager Detection (credentialed check)

HP Unified Functional Testing < 12.0 Remote Code Execution (HPSBMU02967)

HP Unified Functional Testing Detection

HP Version Control Agent (VCA) < 7.3.3 Multiple SSL Vulnerabilities

HP Version Control Agent (VCA) Heartbeat Information Disclosure (Heartbleed)

HP Version Control Repository Agent Installed

HP Version Control Repository Manager (VCRM) Heartbeat Information Disclosure (Heartbleed)

HP Version Control Repository Manager < 7.5.0 Multiple Vulnerabilities (HPSBMU03396) (FREAK)

HP Version Control Repository Manager < 7.6.0 Multiple Vulnerabilities

HP Version Control Repository Manager Installed

HP Version Control Repository Manager Multiple Vulnerabilities (HPSBMU03056)

HP Virtual Machine Manager Detection

HP Virtual Machine Manager For Windows < 6.0.0.0

HP Virtual Rooms Client < 7.0.1 ActiveX Control Dangerous Methods

HP Virtual Rooms WebHPVCInstall.HPVirtualRooms14 ActiveX Control Buffer Overflow Vulnerabilities

HP Virtual Server Environment Detection

HP Virtual Server Environment Remote Privilege Escalation

HP WebInspect Installed

HP WebInspect XXE Unauthorized Information Disclosure

HPE LoadRunner < 12.50 mchan.dll Packet Handling Invalid Memory Access DoS

HPE LoadRunner < 12.53 Patch 4 libxdrutil.dll mxdr\_string() RCE

HPE Network Node Manager i (NNMi) Detection (credentialed check)

HPE Network Node Manager i (NNMi) Multiple Vulnerabilities (HPESBGN03762)

HPE Smart Storage Administrator < 2.60.18.0 RCE

HPE Smart Storage Administrator Installed

HTTP RPC Endpoint Mapper (http-rpc-epmap) Detection

Hummingbird STR Service Buffer Overflow

Husdawg System Requirements Lab Multiple ActiveX Remote Code Execution

I-Nav VUpdater.Install ActiveX Buffer Overflow

IA eMailServer IMAP SEARCH Command Remote Overflow

IA eMailServer IMAP4 LIST Command Format String Remote DoS

IBM Access Support ActiveX Control GetXMLValue Method Overflow

IBM AFP Viewer Plug-in SRC Property Buffer Overflow

IBM Connections Portlets for WebSphere Portal Reflected XSS

IBM Data Studio 3.1 / 3.1.1 Help System Multiple Vulnerabilities

IBM Data Studio Detection

IBM DB2 10.1 < Fix Pack 3 Multiple Vulnerabilities (credentialed check)

IBM DB2 10.1.x < 10.1.400.770 Information Disclosure (credentialed check)

IBM DB2 10.5 < Fix Pack 7 Multiple Vulnerabilities (Bar Mitzvah) (FREAK) (Logjam)

IBM DB2 10.5 < Fix Pack 8 Multiple DoS

IBM DB2 10.5 < FP8 Special Build 36828 / 11.1.2.2 < FP2 Special Build 36792 Multiple Vulnerabilities (Windows)

IBM DB2 10.5.x < 10.5.500.109 Information Disclosure (credentialed check)

IBM DB2 9.7 < FP11 39672 / 10.1 < FP6 39678 / 10.5 < FP10 39688 / 11.1.4 < FP5 39693 / 11.5 < FP0 39711 Multiple Vulnerabilities (Windows)

IBM DB2 9.7 < FP11 Special Build 35317 / 10.1 < FP5 Special Build 35316 / 10.5 < FP7 Special Build 35315 Multiple Vulnerabilities (Windows)

IBM DB2 9.7 < FP11 Special Build 36621 / 10.1 < FP6 Special Build 36610 / 10.5 < FP8 Special Build 36605 / 11.1.2 < FP2 Multiple Vulnerabilities (Windows)

IBM DB2 9.7 < FP11 Special Build 36792 / 10.1 < FP6 Special Build 36792 / 10.5 < FP8 Special Build 36792 / 11.1.2.2 < FP2 Special Build 36792 Multiple Vulnerabilities (Windows)

IBM DB2 9.7 < FP11 Special Build 37314 / 10.1 < FP6 Special Build 37313 / 10.5 < FP10 / 11.1.3 < FP3 JDBC Driver Unsafe Deserialization Local Privilege Escalation (Windows)

IBM DB2 9.7 < FP11 Special Build 38744 / 10.1 < FP6 Special Build 38745 / 10.5 < FP10 Special Build 38746 / 11.1.4 < FP4a Special Build 38747 Buffer Overflow Vulnerability (Windows)

IBM DB2 9.7.x < 9.7.1000.568 Information Disclosure (credentialed check)

IBM DB2 and DB2 Connect Detection (credentialed)

IBM DB2 Connect 9.7 < FP11 Special Build 35317 / 10.1 < FP5 Special Build 35316 / 10.5 < FP7 Special Build 35315 Multiple Vulnerabilities (Windows)

IBM DB2 Connect 9.7 < FP11 Special Build 36621 / 10.1 < FP6 Special Build 36610 / 10.5 < FP8 Special Build 36605 / 11.1.2 < FP2 Multiple Vulnerabilities (Windows)

IBM Domino 8.0.x / 8.5.x / 9.0.x with IBM Java < 1.6 SR15 FP1 Multiple Vulnerabilities (credentialed check)

IBM Domino 8.5.3 < 8.5.3 Fix Pack 5 Interim Fix 1 iNotes Buffer Overflow (credentialed check)

IBM Domino 8.5.3 FP6 / 9.0.1 < 8.5.3 FP6 IF2 / 9.0.1 FP1 iNotes XSS (credentialed check)

IBM Domino 8.5.x < 8.5.3 Fix Pack 6 Interim Fix 4 GIF Code Execution (credentialed check)

IBM Domino 8.5.x < 8.5.3 FP5 Multiple Vulnerabilities

IBM Domino 8.5.x < 8.5.3 FP6 IF17 / 9.0.x < 9.0.1 FP8 IF2 IMAP EXAMINE Command Handling RCE (EMPHASISMINE) (credentialed check)

IBM Domino 8.5.x < 8.5.3 FP6 iNotes Multiple XSS (credentialed check)

IBM Domino 9.0.0 < 9.0.0 Interim Fix 4 iNotes Buffer Overflow (credentialed check)

IBM Domino 9.0.x < 9.0.1 Fix Pack 2 Multiple Vulnerabilities (credentialed check) (POODLE)

IBM Domino 9.0.x < 9.0.1 Fix Pack 3 Interim Fix 2 GIF Code Execution (credentialed check)

IBM Domino 9.x < 9.0.1 Multiple Vulnerabilities (credentialed check)

IBM Domino Installed

IBM Domino SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

IBM eGatherer ActiveX RunEgatherer Function Overflow

IBM Forms Viewer Installed

IBM Forms Viewer Stack Buffer Overflow

IBM General Parallel File System 3.4 < 3.4.0.27 / 3.5 < 3.5.0.16 DoS (Windows)

IBM General Parallel File System 3.5 < 3.5.0.17 Multiple OpenSSL Vulnerabilities (Heartbleed)

IBM General Parallel File System Detection

IBM General Parallel File System Multiple Vulnerabilities (Windows) (POODLE)

IBM General Parallel File System OpenSSH Memory Corruption

IBM General Parallel File System OpenSSL Security Bypass (Windows)

IBM Global Security Kit 7 < 7.0.4.50 / 8.0.14.x < 8.0.14.43 / 8.0.50.x < 8.0.50.20 Multiple Vulnerabilities

IBM GSKit Installed

IBM Informix Genero < 2.41 png\_decompress\_chunk Integer Overflow

IBM Informix Genero Detection

IBM Installation Manager Detection (Windows)

IBM Integration Bus 8.x < 8.0.0.8 / 9.x < 9.0.0.6 / 10.x < 10.0.0.5 SOAP FLOWS XXE DoS

IBM Integration Bus 8.x < 8.0.0.8 / 9.x < 9.0.0.7 / 10.x < 10.0.0.7 Clickjacking

IBM Integration Bus 8.x < 8.0.0.9 / 9.x < 9.0.0.8 / 10.x < 10.0.0.8 Multiple Vulnerabilities

IBM Integration Bus 8.x < 8.0.0.9 / 9.x < 9.0.0.9 / 10.x < 10.0.0.10 Multiple Vulnerabilities

IBM Integration Bus 8.x <= 8.0.0.9 / 9.x < 9.0.0.11 / 10.x < 10.0.0.12 JDBC XA switch load files Vulnerability (CVE-2017-1418)

IBM Integration Bus Installed

IBM iSeries Cached Passwords

IBM Lotus Domino Web Access ActiveX Control Buffer Overflow Vulnerabilities

IBM Lotus iNotes Upload Module ActiveX Control Attachment\_Times() Method Buffer Overflow

IBM Lotus Notes / Domino Client Memory Mapped Files Privilege Escalation

IBM Lotus Notes 8.5.1 / 8.5.2 / 8.5.3 < 8.5.3 FP3 Multiple Vulnerabilities

IBM Lotus Notes < 8.5.3 FP2 URL Handler Unspecified Remote Code Execution

IBM Lotus Notes Attachment Handling Multiple Buffer Overflows

IBM Lotus Sametime Connect Audio / Video Chat Information Disclosure

IBM Lotus Sametime Connect Client Information Disclosure

IBM Lotus Sametime Connect Client Installed

IBM Lotus Sametime Connect Client Mouseover XSS

IBM Lotus Sametime Connect Client Password Disclosure

IBM Lotus Symphony < 3.0 Fix Pack 3 Multiple Vulnerabilities

IBM Lotus Symphony < 3.0.1 Embedded Image File Handling Remote Overflows

IBM Lotus Symphony < 3.0.1 Fix Pack 2 Multiple Vulnerabilities

IBM Lotus Symphony Detection

IBM MQ 8.0.0.x < 8.0.0.11 / 9.0.0.x < 9.0.0.6 / 9.1.0.x < 9.1.0.2 / 9.1.1 TLS Key Renegotiation DoS

IBM MQ 8.0.0.x < 8.0.0.14 / 9.0.0.x < 9.0.0.8 LTS Unspecified DoS (CVE-2019-4568)

IBM MQ 8.0.0.x < 8.0.0.14 / 9.1.0.x < 9.1.0.4 LTS / 9.1.x < 9.1.4 CD Security Restrictions Bypass (CVE-2019-4620)

IBM MQ 8.x < 8.0.0.3 Multiple Information Disclosure (credentialed check)

IBM MQ 9.0.2 - 9.0.5 / 9.1.0.x < 9.1.0.1 Console Cross Site Scripting (XSS) Vulnerability (CVE-2018-1836)

IBM MQ 9.1.0.x LTS < 9.1.0.2 LTS / 9.1.1 CD Console Weak Cryptography Man in the Middle Vulnerability (CVE-2018-1925)

IBM MQ < 8.0.0.13 / 9.0.0.8 LTS / 9.1.0.4 LTS / 9.1.4 CD Channels DoS (CVE-2019-4560)

IBM MQ Server and Client Detection

IBM MQ Unsupported Version Detection (credentialed check)

IBM Notes 8.0.x / 8.5.x / 9.0.x with IBM Java < 1.6 SR15 FP1 Multiple Vulnerabilities

IBM Notes 8.5 < 8.5.3 IF4 HF2 / 9.0 < 9.0 IF2 Password Disclosure

IBM Notes 8.5.x < 8.5.3 FP5 Multiple Vulnerabilities

IBM Notes 8.x < 8.5.3 IF4 HF2 / 9.x < 9.0 IF2 Code Execution

IBM Notes 9.0.x < 9.0.1 Fix Pack 2 Multiple Vulnerabilities

IBM Notes Accepts JavaScript Tags Inside HTML Emails

IBM Notes Client Detection

IBM Notes PNG Integer Overflow

IBM Notes Single Sign On Password Disclosure

IBM Rational Business Developer 8.x < 8.0.1.4 Information Disclosure

IBM Rational Business Developer Installed

IBM Rational ClearQuest 7.1.1.x / 7.1.2.x < 7.1.2.13.01 / 8.0.0.x < 8.0.0.10.01 / 8.0.1.x < 8.0.1.3.01 OpenSSL Library Multiple Vulnerabilities (credentialed check) (Heartbleed)

IBM Rational ClearQuest 7.1.1.x < 7.1.1.4 / 7.1.2.x < 7.1.2.1 Multiple Vulnerabilities (credentialed check)

IBM Rational ClearQuest 7.1.1.x < 7.1.1.9 / 7.1.2.x < 7.1.2.6 / 8.0.0.x < 8.0.0.2 Multiple Vulnerabilities (credentialed check)

IBM Rational ClearQuest 7.1.x < 7.1.2.10 / 8.0.0.x < 8.0.0.6 Web Client Unspecified XSS (credentialed check)

IBM Rational ClearQuest 7.1.x < 7.1.2.12 / 8.0.0.x < 8.0.0.8 / 8.0.1.x < 8.0.1.1 Multiple Vulnerabilities (credentialed check)

IBM Rational ClearQuest 7.1.x < 7.1.2.15 / 8.0.0.x < 8.0.0.12 / 8.0.1.x < 8.0.1.5 Multiple Vulnerabilities (credentialed check)

IBM Rational ClearQuest 7.1.x < 7.1.2.16 / 8.0.0.x < 8.0.0.13 / 8.0.1.x < 8.0.1.6 Multiple Vulnerabilities (credentialed check) (POODLE)

IBM Rational ClearQuest 7.1.x < 7.1.2.8 / 8.0.0.x < 8.0.0.4 GSKit Spoofing (credentialed check)

IBM Rational ClearQuest 7.1.x < 7.1.2.9 / 8.0.0.x < 8.0.0.5 Multiple Vulnerabilities (credentialed check)

IBM Rational ClearQuest 7.x < 7.1.2.7 / 8.0.0.x < 8.0.0.3 Multiple Vulnerabilities (credentialed check)

IBM Rational ClearQuest 8.0.0.x < 8.0.0.9 / 8.0.1.x < 8.0.1.2 Information Disclosure (credentialed check)

IBM Rational ClearQuest Installed

IBM Rational ClearQuest Unsupported

IBM Rational Collaborative Lifecycle Management Installed

IBM Rational Collaborative Lifecycle Management Products Unspecified Remote Code Execution

IBM Security Directory Server < 6.1.0.61 / 6.2.0.36 / 6.3.0.30 / 6.3.1.2 with GSKit < 7.0.4.50 / 8.0.50.20 SSL CPU Utilization DoS

IBM Security Directory Server Installed (credentialed check)

IBM solidDB < 4.5.182 / 6.0.1069 / 6.3.49 / 6.5.0.4 Denial of Service

IBM Spectrum Protect / Tivoli Storage Manager Client Installed

IBM Spectrum Protect / Tivoli Storage Manager Installed

IBM SPSS SamplePower 3.0 < 3.0 FP 1 Multiple ActiveX Controls Arbitrary Code Execution

IBM SPSS SamplePower 3.0.1 < 3.0.1 IF1 ActiveX Control Remote Code Execution

IBM SPSS SamplePower 3.0.1 < 3.0.1 IF2 vsflex8l ActiveX Control Remote Code Execution

IBM SPSS SamplePower Detection

IBM Tivoli Directory Server 6.0.x / 6.1 < 6.1.0.58 / 6.2 < 6.2.0.33 / 6.3 < 6.3.0.25 Javadoc Frame Injection

IBM Tivoli Directory Server 6.2 < 6.2.0.29 / 6.3 < 6.3.0.21 SSL / TLS DoS

IBM Tivoli Directory Server < 6.0.0.72 / 6.1.0.55 / 6.2.0.30 / 6.3.0.22 with GSKit < 7.0.4.45 / 8.0.14.27 TLS Side-Channel Timing Information Disclosure

IBM Tivoli Directory Server < 6.1.0.47 / 6.2.0.22 / 6.3.0.11 Multiple Vulnerabilities (credentialed check)

IBM Tivoli Directory Server < 6.1.0.59 / 6.2.0.34 / 6.3.0.26 with GSKit < 7.0.4.48 / 8.0.50.16 X.509 Certificate Chain DoS

IBM Tivoli Directory Server ldapinst.log DB2 Admin Password Disclosure

IBM Tivoli Directory Server Vulnerabilities (credentialed check)

IBM Tivoli Endpoint Manager Client Detection

IBM Tivoli Federated Identity Manager 6.2.2 < 6.2.2 FP16 XSS (swg21974157)

IBM Tivoli Federated Identity Manager 6.2.x < 6.2.2 FP17 Multiple Vulnerabilities

IBM Tivoli Federated Identity Manager Installation Detection

IBM Tivoli Federated Identity Manager Unspecified XSS

IBM Tivoli Federated Identity Manager XML Signature Validation Bypass

IBM Tivoli Monitoring Java Unspecified Vulnerability

IBM Tivoli Monitoring SOAP Interface Insecure Configuration Remote SOAP Query Information Disclosure

IBM Tivoli Provisioning Manager Express for Software Distribution Isig.isigCtl.1 ActiveX RunAndUploadFile Method Boundary Error Remote Overflow

IBM Tivoli Provisioning Manager for OS Deployment TFTPD Malformed PRQ Request DoS

IBM Tivoli Storage Manager Client 6.2.x < 6.2.5.2 / 6.3.x < 6.3.2 / 6.4 < 6.4.1.3 Local Buffer DoS

IBM Tivoli Storage Manager Client 6.3 < 6.3.1.0 / 6.4 < 6.4.0.1 Unauthorized Access

IBM Tivoli Storage Manager Client 6.3.1.x < 6.3.2.0 / 6.4.x < 6.4.1.0 ReFS Insecure File Permissions

IBM Tivoli Storage Manager Client Denial of Service

IBM Tivoli Storage Manager Client Multiple Buffer Overflows (swg21457604)

IBM Tivoli Storage Manager Express Backup Server Service (dsmsvc.exe) Packet Handling Remote Overflow

IBM Tivoli Storage Manager for Virtual Environments Installed.

IBM Tivoli Storage Manager HSM Client < 5.5.1.8 / 5.4.2.6

IBM TXSeries for Multiplatforms CICS Listener Crafted CICSAS eci Response Timeout DoS

IBM WebSphere 9.0.0.x < 9.0.0.3 / 9.0.0 < 9.0.5 Multiple Vulnerabilities

IBM WebSphere MQ 6.x < 6.0.2.7 / 7.x < 7.0.1.0 Queue Manager Buffer Overflow RCE

IBM WebSphere MQ 6.x < 6.0.2.9 / 7.x < 7.0.1.1 'userid' and 'password' Information Disclosure

IBM WebSphere MQ 7.0 / 7.1 / 7.5 / 8.0 PCF Query DoS

IBM WebSphere MQ 7.0 / 7.1 / 7.5 Global Security Toolkit Vulnerabilities

IBM WebSphere MQ 7.0.0.x / 8.0.0.x Password Handling Remote Access Vulnerability

IBM WebSphere MQ 7.0.1.x / 7.1.0.x < 7.1.0.9 / 7.5.0.x < 7.5.0.8 / 8.0.0.x < 8.0.0.6 / 9.0.0.x < 9.0.0.1 Multiple Vulnerabilities

IBM WebSphere MQ 7.0.1.x <= 7.0.1.14 / 7.1.0.x <= 7.1.0.8 / 7.5.0.x <= 7.5.0.8 / 8.0.0.x <= 8.0.0.7 / 9.0.0.x <= 9.0.0.1 / 9.0.1.x <= 9.0.3.0 Privilege Escalation Vulnerability

IBM WebSphere MQ 7.0.1.x ROBOT Vulnerability

IBM WebSphere MQ 7.1 / 7.5 Multiple Vulnerabilities

IBM WebSphere MQ 7.1 < 7.1.0.1 MQ SVRCONN Channels Security Configuration Bypass

IBM WebSphere MQ 7.1 < 7.1.0.5 / 7.5 < 7.5.0.3 Multiple Vulnerabilities

IBM WebSphere MQ 7.1 < 7.1.0.8 / 7.5 < 7.5.0.7 / 8.0 < 8.0.0.5 Multiple Vulnerabilities

IBM WebSphere MQ 7.5.x / 8.0.0.x < 8.0.0.8 / 9.0.x < 9.0.4 / 9.0.0.x < 9.0.0.2 Multiple Vulnerabilities

IBM WebSphere MQ 8.0 < 8.0.0.2 WebSockets XSS

IBM WebSphere MQ 9.0.1 < 9.0.3 Multiple Vulnerabilities

IBM WebSphere MQ Client 6.x < 6.0.2.7 / 7.x < 7.0.1.0 CCDT Buffer Overflow

IBM WebSphere Portal 7.0.0.x Unified Task List Portlet < 6.0.1 Multiple Vulnerabilities (PI18909)

IBM WebSphere Portal 8.5.0 < 8.5.0 CF14 / 9.0.0 < 9.0.0 CF14 Multiple Vulnerabilities

IBM WebSphere Portal Installed (Windows)

IBM WebSphere Portal Unspecified Information Disclosure (PI17768)

IBM WebSphere Service Registry and Repository 6.3 < 6.3.0.5 Multiple Vulnerabilities

IBM WebSphere Service Registry and Repository 7.0 < 7.0.0 FP1 Authentication Bypass

IBM WebSphere Service Registry and Repository 7.0 < 7.0.0.5 Multiple Vulnerabilities

IBM WebSphere Service Registry and Repository 7.5 < 7.5.0 FP4 Script Injection

IBM WebSphere Service Registry and Repository 7.5 < 7.5.0.4 Multiple Vulnerabilities

IBM WebSphere Service Registry and Repository 8.0 < 8.0.0.3 Multiple Vulnerabilities

IBM WebSphere Service Registry and Repository 8.5 < 8.5.0.1 Multiple Vulnerabilities

IBM WebSphere Service Registry and Repository 8.5 < 8.5.6.2 Information Disclosure Vulnerability

IBM WebSphere Service Registry and Repository Installed

iCloud Detection (Windows)

ICQ < 2003b Multiple Vulnerabilities

ICQ < 6 Build 6059 Message Processing Format String

ICQ Detection

ICUII Detection

IDA Kernel Database TIL Section Parsing Unspecified Issue

IDA Pro IDB Loader Code Execution

IDA Pro Mach-O Loader Buffer Overflow

IDA Pro Multiple Memory Corruption Vulnerabilities

IDA Pro QNX File Loader Denial of Service

IDrive Online Backup ActiveX Control < 3.4.1 Arbitrary File Overwrite

ImageMagick 6.x < 6.9.4-0 / 7.x < 7.0.1-2 Multiple Vulnerabilities

ImageMagick 6.x < 6.9.4-3 / 7.x < 7.0.1-4 Multiple Vulnerabilities

ImageMagick 6.x < 6.9.4-5 / 7.x < 7.0.1-7 Multiple DoS

ImageMagick 6.x < 6.9.6-5 TIFFGetProperties() NULL Pointer Dereference DoS

ImageMagick 6.x < 6.9.6-6 ReadSGIImage() SGI File Handling DoS

ImageMagick 6.x < 6.9.7-3 ReadPSDLayers() Function PSB File Handling RCE

ImageMagick 6.x < 6.9.7-5 / 7.x < 7.0.4-5 tga.c WriteTGAImage() Assertion Failure DoS

ImageMagick 6.x < 6.9.7-8 / 7.x < 7.0.4-8 Multiple DoS

ImageMagick 6.x < 6.9.7-9 / 7.x < 7.0.4-10 webp.c ReadWEBPImage() File Descriptor Exhaustion DoS

ImageMagick 6.x < 6.9.8-10 / 7.x < 7.0.5-9 Multiple Vulnerabilities

ImageMagick 7.x < 7.0.1-10 Multiple Vulnerabilities

ImageMagick 7.x < 7.0.2-0 ReadSUNImage() Function SUN Image Handling DoS

ImageMagick 7.x < 7.0.3-6 WaveletDenoiseImage() Heap Buffer Overflow RCE

ImageMagick 7.x < 7.0.3-7 TIFFGetProperties() NULL Pointer Dereference DoS

ImageMagick 7.x < 7.0.3-9 ReadSGIImage() SGI File Handling DoS

ImageMagick 7.x < 7.0.4-3 Multiple Vulnerabilities

ImageMagick < 6.5.2-9 magick/xwindow.c XMakeImage() Function TIFF File Handling Overflow

ImageMagick < 6.7.5-1 Multiple Vulnerabilities

ImageMagick < 6.7.5-8 Multiple Vulnerabilities

ImageMagick < 6.7.6-3 Multiple Vulnerabilities

ImageMagick < 6.7.6-4 profile.c Heap-Based Buffer Overflow

ImageMagick < 6.7.8-8 gif.c Memory Corruption

ImageMagick < 6.8.7-6 WritePSDImage PSD Handling Memory Corruption

ImageMagick < 6.8.8-5 Multiple PSD Handling Buffer Overflows

ImageMagick < 6.8.9-9 Multiple Vulnerabilities

ImageMagick < 7.0.1-1 / 6.x < 6.9.3-10 Multiple Vulnerabilities (ImageTragick)

ImageMagick < 7.0.7-28 Denial of service vulnerability

ImageMagick < 7.0.8-25 Multiple Vulnerabilities

ImageMagick < 7.0.8-35 Multiple vulnerabilities

ImageMagick < 7.0.8-44 Multiple vulnerabilities

ImageMagick < 7.0.8-56 Multiple vulnerabilities

ImageMagick Detection

iMesh IMWeb.IMWebControl ActiveX (IMWeb.dll) SetHandler Method Arbitrary Code Execution

Insecure Windows Service Permissions

InstallShield InstallFromTheWeb ActiveX Control Multiple Overflows

Intel Active Management Technology (AMT) detection

Intel Common Base Agent CreateProcessA() Function Remote Command Execution

Intel Converged Security Management Engine (CSME) Active Management Technology (AMT) Multiple Vulnerabilities (INTEL-SA-00112)

Intel Driver Update Utility 2.x < 2.4 Cleartext Download MitM

Intel Driver Update Utility Installed

Intel Management Engine Insecure Read / Write Operations RCE (INTEL-SA-00075)

Intel Management Engine Multiple WPA2 Vulnerabilities (INTEL-SA-00101)

Intel Management Engine Unspecified Multiple Vulnerabilities (INTEL-SA-00086)

Intel PRO/Wireless 2100 Network Connection Driver Local Privilege Escalation Vulnerability

Intel PRO/Wireless Network Connection Drivers Remote Code Execution Vulnerabilities

Intel Wireless Driver Wi-Fi Protected Access II (WPA2) Multiple Vulnerabilities (KRACK)

Internet Explorer .mht XML External Entity Vulnerability

Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2020-0674) (Deprecated)

Internet Explorer Typed URLs

Intuit QuickBooks Help System Multiple Vulnerabilities

Intuit QuickBooks Installed

Intuit QuickBooks Online Edition < 10 ActiveX Multiple Vulnerabilities

Investintech Able2Doc < 6.0.8.22 Multiple Vulnerabilities

Investintech Able2Doc Detection

Investintech Able2Extract < 7.0.8.22 Multiple Vulnerabilities

Investintech Able2Extract Detection

Investintech SlimPDF Detection

Investintech SlimPDF Reader < 1.0.1.12 Multiple Vulnerabilities

iParty Client Extended Character Handling Remote Overflow DoS

IPINSIGHT Detection

Ipswitch IM Server < 2.07 Multiple Function Remote DoS

Ipswitch IMail Client Multipart MIME Email Message Handling Overflow

Ipswitch IMail IMAP Service DELETE Command Remote Overflow

Ipswitch IMail Server < 2006.2 Multiple Remote Overflows

Ipswitch IMail Server < 2006.21 Multiple Vulnerabilities

Ipswitch IMail Server < 8.13 Multiple Remote DoS

Ipswitch IMail Server IMAP LIST Command Remote Overflow DoS

Ipswitch IMail Server/Collaboration Suite IMAP FETCH Command Overflow

Ipswitch MOVEit DMZ < 8.2 Multiple Vulnerabilities

Ipswitch MOVEit DMZ Detection

Ipswitch WhatsUp Gold < 16.4 Multiple Vulnerabilities

Ipswitch WhatsUp Gold < 16.5.0 WrFreeFormText.asp sUniqueID Parameter Blind SQLi (credentialed)

Ipswitch WhatsUp Gold Detection

Ipswitch WhatsUp Gold Multiple Vulnerabilities

IRCXPro Plaintext Passwords Local Disclosure

IrfanView < 4.32 Buffer Overflow

IrfanView < 4.33 Boundary Error Multiple Image File Handling Remote Overflow

IrfanView < 4.35 Multiple Heap-Based Buffer Overflows

IrfanView < 4.36 Multiple Vulnerabilities

IrfanView < 4.37 Multiple Buffer Overflow Vulnerabilities

IrfanView Detection

IrfanView DjVu Plugin DjVu Image File Decompression Overflow

IrfanView FlashPix Plugin < 4.36 Summary Information Property Set Handling Integer Overflow

IrfanView FlashPix Plugin Heap Based Buffer Overflow

IrfanView Formats Plugin ECW Plugin File Handling Buffer Overflow Vulnerability

IrfanView Formats Plugin TTF File Buffer Overflow Vulnerability

IrfanView ImXCF.dll XCF File Handling Overflow

IrfanView JLS Plugin JLS Compressed Image File Handling Overflow

IrfanView JPEG-2000 Plugin Remote Stack-based Buffer Overflow

IrfanView MrSID Plugin < 4.37 Multiple Buffer Overflows

IS Decisions RemoteExec '.rec' Remote Buffer Overflow

ISS BlackICE Multiple Remote Vulnerabilities

ISS BlackICE/PC Protection Unprivileged User Local DoS

JanaServer < 2.4.5 Multiple Remote DoS

JAR File Detection for Windows

JavaScript Enabled in Adobe Reader

Jenkins Installed (Windows)

JIRA Service Desk Installed (Windows)

Jordan's Windows Telnet Server Password Handling Remote Overflow

Juniper Installer Service 7.4 < 7.4r6 Privilege Escalation (JSA10644)

Juniper Installer Service Detection

Juniper Junos Pulse Client Detection

Juniper Junos Pulse Client Privilege Escalation (JSA10644)

Juniper NetScreen VPN Client Detection

Juniper NetScreen VPN Client Multiple Buffer Overflow Vulnerabilities

Kaspersky Anti-Virus < 6.0.2.614 Multiple Vulnerabilities

Kaspersky Anti-Virus Detection and Status

Kaspersky Anti-Virus for Check Point FireWall-1 Unspecified DoS

Kaspersky Anti-Virus PE File Handling DoS

Kaspersky Anti-Virus UPX File Decompression DoS

Kaspersky Internet Security / Anti-Virus External Script Unspecified Protection Mechanism Bypass

Kaspersky Internet Security Heartbeat Information Disclosure (Heartbleed)

Kaspersky Labs Anti-Virus IOCTL Local Privilege Escalation

Kaspersky Multiple Products 'Bases' Directory Insecure Permissions

Kaspersky Multiple Products kl1.sys Driver Local Overflow

Kaspersky Online Scanner kavwebscan.CKAVWebScan ActiveX (kavwebscan.dll) Format String Arbitrary Code Execution

Kaspersky Password Manager 5.x < 5.0.0.169 HTML Injection

Kaspersky Password Manager Installed (credentialed check)

KB 3137909: Vulnerabilities in ASP.NET Templates Could Allow Tampering

KB2915720: Changes in Windows Authenticode Signature Verification

KB4017094: Security Update for the libjpeg Information Disclosure Vulnerability for Microsoft Silverlight 5 (April 2017)

KB4023307: Security Update for the Windows Uniscribe Remote Code Execution Vulnerability for Microsoft Silverlight 5 (June 2017)

KB4036996: Security Update for SQL Server (August 2017) (uncredentialed check)

Kerio Control < 7.1.0 Build 1689 Remote Cache Poisoning

Kerio Control Detection

Kerio Control Web Filter Unspecified Issue

KeyWorks KeyHelp ActiveX Control Multiple Vulnerabilities

Komodia SSL Digestor Root CA Certificate Installed (Superfish)

KpyM Telnet Server DoS

LANDesk Management Suite Alert Service (aolnsrvr.exe) Remote Overflow

LANDesk Multiple Products QIP Server Service (qipsrvr.exe) Heal Request Packet Handling Overflow

Last Boot Time (WMI)

LastPass Firefox Extension 4.0 < 4.1.21a Message Hijacking

LeapFTP < 2.7.4.x PASV Reply Remote Overflow

Learn2 STRunner ActiveX Control Multiple Buffer Overflow Vulnerabilities

Lenovo Mouse Suite < 6.73 Local Privilege Elevation

Lenovo Mouse Suite Installed

Lenovo Rescue and Recovery tvtumon.sys Filename Handling Local Overflow

Lenovo System Update < 5.06.0034 Multiple Vulnerabilities

Lenovo System Update Installed

Lenovo ThinkPad Bluetooth with Enhanced Data Rate Arbitrary DLL Injection Code Execution Vulnerability

Lenovo ThinkPad Bluetooth with Enhanced Data Rate Detection

LibreOffice 4.2.x < 4.2.3 OpenSSL Multiple Vulnerabilities (Heartbleed)

LibreOffice 4.3.x < 4.3.1 Multiple Vulnerabilities

LibreOffice 4.3.x < 4.3.3 Impress Remote RCE

LibreOffice 4.x < 4.2.6-secfix (4.2.6.3) Multiple Vulnerabilities

LibreOffice 4.x < 4.2.7 Impress Remote RCE

LibreOffice 6.1.x < 6.1.3.2 Arbitrary Code Execution

LibreOffice 6.2.6 / 6.3.1 Security Control Bypass (Windows)

LibreOffice < 3.3.3 / 3.4.0 LWP File Handling Overflow

LibreOffice < 3.4.6 / 3.5.1 XML External Entity RDF Document Handling Information Disclosure

LibreOffice < 3.5.3 Multiple Memory Corruption Vulnerabilities

LibreOffice < 3.5.5 Multiple Heap-Based Buffer Overflows

LibreOffice < 3.5.7 / 3.6.1 Multiple Denial of Service Vulnerabilities

LibreOffice < 3.6.7 / 4.0.4 / 4.1.0 .docm Import DoS

LibreOffice < 4.1.5 / 4.2.0 Python Multiple Vulnerabilities

LibreOffice < 4.2.5 Unspecified Macro Code Execution

LibreOffice < 4.2.8 / 4.3.5 RTF File Handling Code Execution

LibreOffice < 4.4.5 Multiple Vulnerabilities

LibreOffice < 4.4.6 / 5.x < 5.0.1 Document Bookmark Arbitrary Code Execution

LibreOffice < 5.0.5 Multiple RCE

LibreOffice < 5.1.4 RTF Character Style Index RCE

LibreOffice < 5.1.6 / 5.2.5 / 5.3.0 Multiple Vulnerabilities

LibreOffice < 5.4.5 or 6.x < 6.0.1 Multiple Vulnerabilities

LibreOffice < 5.4.6 and < 6.0.2 Heap Buffer Overflow

LibreOffice < 5.4.7 or 6.x < 6.0.4 Information Disclosure

LibreOffice < 6.1.6, 6.2.x < 6.2.3 Hyperlink Processing Vulnerability (Windows)

LibreOffice < 6.2.5 Multiple Vulnerabilities (Windows)

LibreOffice < 6.2.6 / 6.3 Input Validation (Windows)

LibreOffice < 6.2.7 / 6.3.x < 6.3.1 Multiple Vulnerabilities (Windows)

LibreOffice Detection

LibreOffice Unsupported Version Detection

Local Administrator Password Solution Installed

Logical Drive Insecure Filesystem Enumeration (WMI)

Logitech Unifying Receiver Key Injection (MouseJack)

LogMeIn Agent Detection

LogMeIn Client Installed (Windows)

LogMeIn Control Panel Installed (Windows)

LogMeIn Detection (Windows)

LOP.COM Detection

Lorex Technologies Edge Series Security DVR ActiveX Buffer Overflow

Lotus CC:Mail Installed (EASYPI)

Lotus Notes Client < 7.0.3 / 8.0.1 Multiple Overflows

Lotus Quickr for Domino qp2.dll ActiveX Control Integer Overflow Remote Code Execution

Lotus Quickr for Domino qp2.dll ActiveX Control Unspecified Stack Overflow

LPViewer ActiveX Control Multiple Buffer Overflow Vulnerabilities

LuraWave JP2 ActiveX Control < 2.1.5.11 jp2\_x.dll Remote Buffer Overflow

LuraWave JP2 Browser Plug-In < 2.1.1.11 npjp2.dll Remote Buffer Overflow

Lyris ListManager MSDE Weak sa Password

Macrovision FLEXnet DWUpdateService ActiveX (agent.exe) Multiple Method Arbitrary Command Execution

Macrovision InstallShield InstallScript One-Click Install ActiveX Arbitrary Code Execution

Macrovision SafeDisc secdrv.sys Crafted METHOD\_NEITHER IOCTL Local Overflow

Magic Winmail Server PASS Command Remote Format String

MagniComp SysInfo Installed (Windows)

MailEnable < 1.7 IMAP Server Multiple Vulnerabilities (ME-100008)

MailEnable Detection

MailEnable IMAP / SMTP Multiple Remote Vulnerabilities

MailEnable IMAP EXAMINE Command Remote Overflow

MailEnable IMAP Server (meimaps.exe) Crafted RENAME Command Remote DoS

MailEnable IMAP Server EXAMINE Command Remote DoS

MailEnable IMAP Server Multiple Buffer Overflow Vulnerabilities (ME-10021)

MailEnable IMAP Server Multiple Buffer Overflow Vulnerabilities (ME-10025)

MailEnable IMAP Server Multiple Remote Buffer Overflows

MailEnable IMAP Server SEARCH Command Remote DoS

MailEnable IMAP Server Unspecified Buffer Overflow (ME-10018)

MailEnable IMAP Server W3C Logging Overflow

MailEnable IMAP STATUS Command Remote Overflow

MailEnable POP Server PASS Command Remote Overflow (ME-10026)

MailEnable POP3 Server APOP Command Remote Buffer Overflow

MailEnable POP3 Server Authentication Vulnerabilities

MailEnable Webmail Malformed Encoded Quoted-printable Email DoS (CVE-2006-1338)

MailEnable Webmail Malformed Quoted-printable Email DoS (CVE-2006-0504)

MailMarshal tar Archive Traversal Arbitrary File Overwrite

Malicious File Detection

Malicious File Detection Using Yara

Malicious File Detection: APT1 Software on System

Malicious File Detection: Invalid Directories

Malicious File Detection: Malware Signed By Stolen Bit9 Certificate

Malicious File Detection: Potentially Unwanted Software

Malicious File Detection: User Defined Malware

Malicious Process Detection

Malicious Process Detection: APT1 Software Running

Malicious Process Detection: Authenticode Microsoft Manufacturer

Malicious Process Detection: Authenticode Not Signed

Malicious Process Detection: Authenticode Not Verified

Malicious Process Detection: Authenticode Signed

Malicious Process Detection: Authenticode Signed Bad Date

Malicious Process Detection: Authenticode With Invalid Signature

Malicious Process Detection: Malware Signed By Stolen Bit9 Certificate

Malicious Process Detection: Potentially Unwanted Software

Malicious Process Detection: User Defined Malware Running

Malwarebytes Anti-Exploit < 1.04.1.1012 RCE

Malwarebytes Anti-Exploit < 1.05.1.1014 DoS

Malwarebytes Anti-Exploit Installed

MapQuest Toolbar Detection

MarkAny Content SAFER ActiveX Arbitrary Download and Execution

McAfee Agent Detection

McAfee Antivirus Detection and Status

McAfee Antivirus Engine Out of Date

McAfee Antivirus TAR / PDF Scan Evasion (SB10003)

McAfee Antivirus ZIP / RAR Scan Evasion

McAfee Application Control / Change Control Installed

McAfee Application Control 6.x < 6.2.0.567 / 7.0.x < 7.0.1.275 Unauthorized IOCTL Use Local Privilege Escalation (SB10175)

McAfee Application Control swin.sys Memory Corruption (SB10145)

McAfee Cloud Single Sign On < 4.0.1 Information Disclosure (SB10066) (Windows)

McAfee Cloud Single Sign On Detection

McAfee Common Management Agent 3.6.0 UDP Packet Handling Format String (credentialed check)

McAfee Common Management Agent Installation Detection

McAfee Data Loss Prevention Endpoint Agent Detection

McAfee DLPe Agent 11.x < 11.1.210.32 / 11.2.x / 11.3.x < 11.3.2.8 Multiple Vulnerabilities (SB10295)

McAfee DLPe Agent < 10.0.500 / 11.x < 11.0.400 Master Bypass Vulnerability (SB10233)

McAfee DLPe Agent < 11.1.200 / 11.2.x Multiple Vulnerabilities (SB10289) (SB10290)

McAfee DLPe Agent Privilege Escalation Vulnerability on Windows XP (SB10097)

McAfee E-Business Server Administration Client Length Remote DoS

McAfee E-Business Server Authentication Packet Remote Overflow

McAfee Endpoint (Drive) Encryption Installed (credentialed check)

McAfee Endpoint Security and Module Detection

McAfee Endpoint Security for Windows 10.5.x / 10.6.x / 10.7.0.x Improper Access Control (SB10314)

McAfee Endpoint Security for Windows 10.5.x < 10.5.5 October 2019 Update / 10.6.x < 10.6.1 February 2020 Update / 10.7.x < 10.7.0 February 2020 Update Multiple Vulnerabilities (SB10299)

McAfee ePO DLPe Extension < 9.3.400 Multiple Vulnerabilities (SB10098)

McAfee ePO DLPe Extension < 9.3.416.4 Multiple Vulnerabilities (SB10111)

McAfee ePO Extension for McAfee Agent Multiple Blind SQL Injection (SB10043)

McAfee ePolicy Orchestrator 4.x < 4.6.9 / 5.x < 5.1.2 Multiple Vulnerabilities (SB10095)

McAfee ePolicy Orchestrator 5.1.x < 5.1.3 HF1167014 / 5.3.x < 5.3.1 HF1179709 / 5.3.x < 5.3.2 HF1167013 Blind SQL Injection (SB10187)

McAfee ePolicy Orchestrator 5.1.x < 5.1.3 HF1193124 / 5.3.x < 5.3.1 HF1194398 / 5.3.2 < 5.3.2 HF1193123 / 5.9.x < 5.9.0 HF1193951 Path Traversal RCE (SB10196)

McAfee ePolicy Orchestrator < 4.6.7 HF940148 XML Entity Injection (SB10065)

McAfee ePolicy Orchestrator Installed (credentialed check)

McAfee ePolicy Orchestrator Java Object Deserialization RCE

McAfee ePolicy Orchestrator Unsupported Version Detection

McAfee Host Intrusion Prevention Installed

McAfee Host Intrusion Prevention Services < 8.0.0.3828 Authentication Bypass (SB10173)

McAfee Managed Agent 4.6.x < 4.8.0.1938 / 5.0.x < 5.0.1 Log View Clickjacking (SB10094) (credentialed check)

McAfee Managed Agent FrameworkService.exe Denial of Service (SB10055) (credentialed check)

McAfee Security Scan Plus < 3.11.474.2 Multiple Vulnerabilities (TS102593 / TS102614)

McAfee Security Scan Plus < 3.11.587.1 Protection Level UI Element Download MitM Command Execution (TS102714)

McAfee Security Scan Plus < 3.11.599.3 LiveSafe Non-certificate-based Authentication HTTP Backend-response Handling MitM Registry Value Manipulation (TS102723)

McAfee Security Scan Plus Detection

McAfee Security-as-a-Service (SaaS) < 5.2.2 ActiveX Controls Arbitrary Code Execution (SB10016)

McAfee Security-as-a-Service (SaaS) mcCIOScn.dll ShowReport Method Remote Command Execution

McAfee SmartFilter Administration < 4.2.1.01 Unauthenticated Access to JBOSS RMI (SB10029)

McAfee SmartFilter Administration Installed

McAfee Virtual Technician ActiveX Control GetObject() Method Remote Command Execution (SB10028)

McAfee Virtual Technician McHealthCheck.dll ActiveX Control Save() Method Arbitrary File Overwrite (SB10040)

McAfee VirusScan Enterprise 8.5 / 8.7 hcp:// Security Bypass (SB10012)

McAfee VirusScan Enterprise 8.8 < 8.8 Patch 1 DoS

McAfee VirusScan Enterprise 8.8 Patch 2 < HF778101 Local Privilege Escalation (SB10038)

McAfee VirusScan Enterprise < 8.8 / 8.7 HF643440 CLI Local Privilege Escalation (SB10014)

McAfee VirusScan Enterprise < 8.8 Patch 11 Privilege Escalation Vulnerability (SB10237)

McAfee VirusScan Enterprise < 8.8 Patch 6 Buffer Overflow Protection (BOP) Security Bypass (SB10142)

McAfee VirusScan Enterprise < 8.8 Patch 6/7 Hotfix 1123565 Protection Bypass Vulnerability (SB10158)

McAfee VirusScan Enterprise < 8.8 Patch 7 Protected Resource Access Bypass (SB10151)

McAfee VirusScan Enterprise < 8.8 Patch 9 Scriptscan COM Object DoS (SB10194)

McAfee VirusScan Enterprise Local Privilege Escalation (SB10034)

McAfee VirusScan Enterprise Path Subversion Arbitrary DLL Injection Code Execution

McAfee VirusScan Enterprise Unsupported Version Detection

McAfee Vulnerability Manager Enterprise Manager Multiple Vulnerabilities (SB10061)

McAfee Vulnerability Manager Installed (credentialed check)

McAfee Web Reporter Installed (credentialed check)

MDaemon < 9.0.6 POP3 Server USER / APOP Command Remote Overflow

MDaemon Content Filter Traversal Arbitrary File Write

MDaemon IMAP Server CREATE Command Mailbox Name Handling Overflow

MDaemon IMAP Server FETCH Command Remote Buffer Overflow

MDaemon IMAP Server Mail Folder Name Format String

MDaemon IMAP Server Multiple Command Local DoS

MDaemon POP Server Multiple Command Remote Overflow DoS

MDaemon POP Server User Name Overflow DoS

MDaemon Server DomainPOP Malformed Message DoS

MDaemon Webconfig IMAP Malformed URL DoS

MERCUR Mailserver SMTP / IMAP / POP3 Servers Remote Overflows

MERCUR Messaging < 2005 SP4 Multiple Remote DoS Vulnerabilities

MERCUR Messaging Control Server Multiple Buffer Overflows

Microsoft .NET Core for Windows

Microsoft .NET Core SDK for Windows

Microsoft .NET Framework Detection

Microsoft .NET Framework Service Pack Out of Date

Microsoft .NET Framework Unsupported

Microsoft .NET Security Rollup Enumeration

Microsoft Access Installed (credentialed check)

Microsoft Access Unsupported Version Detection

Microsoft ActiveSync WideCharToMultiByte() Function NULL Dereference Remote DoS

Microsoft ASP .NET Core for Windows

Microsoft Azure AD Connect Installed

Microsoft Azure Instance Metadata Enumeration (Windows)

Microsoft BizTalk Server Installed

Microsoft Commerce Server Installed

Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161)

Microsoft Dynamics 365 (on-premises) 8.x < 8.2.3.0008 multiple vulnerabilities

Microsoft Dynamics 365 Detection (Windows)

Microsoft Dynamics AX Installed

Microsoft Dynamics GP < 10.0 Multiple Vulnerabilities

Microsoft Edge Browser Installed (Windows)

Microsoft Edge Browser Unsupported Version Detection

Microsoft EMET 3.x >= 3.5 / 4.x < 4.0.4913.26122 ASLR Security Bypass

Microsoft EMET < 5.5 Security Bypass Vulnerability

Microsoft Enhanced Mitigation Experience Toolkit (EMET) Installed

Microsoft Excel Viewer Installed (credentialed check)

Microsoft Excel Viewer Unsupported Version Detection

Microsoft Exchange Client Access Server Information Disclosure

Microsoft Exchange Installed

Microsoft Exchange Server Elevation of Privilege Vulnerability (November 2018)

Microsoft Exchange Server Unsupported Version Detection

Microsoft Exchange Server Unsupported Version Detection (Uncredentialed)

Microsoft FAST Search Server Installed

Microsoft Forefront Client Security Unsupported

Microsoft Forefront Endpoint Protection / System Center Endpoint Protection / Anti-malware Client Detection and Status

Microsoft Forefront Protection for Exchange Server Installed

Microsoft Forefront Unified Access Gateway Installed

Microsoft Groove Server Installed

Microsoft Host Integration Server Installed

Microsoft Identity Manager Detection

Microsoft Internet Explorer Enhanced Protection Mode (EPM) Detection

Microsoft Internet Explorer Enhanced Security Configuration Detection

Microsoft Internet Explorer Unsupported Version Detection

Microsoft Internet Explorer Version Detection

Microsoft Lync Installed

Microsoft Lync Server 2010 reachLocale Parameter XSS

Microsoft Malicious Software Removal Tool Installed

Microsoft Malware Protection Engine < 1.1.13804 Multiple Vulnerabilities

Microsoft Malware Protection Engine < 1.1.13903 RCE

Microsoft Malware Protection Engine < 1.1.14405.2 RCE

Microsoft Malware Protection Engine < 1.1.14700.5 RCE

Microsoft Malware Protection Engine Elevation of Privilege Vulnerability

Microsoft Office 365 Unsupported Channel Version Detection

Microsoft Office ActiveX Controls Enabled Without Restrictions Or Prompting

Microsoft Office Compatibility Pack Installed (credentialed check)

Microsoft Office Compatibility Pack Unsupported Version Detection

Microsoft Office Detection

Microsoft Office File History

Microsoft Office Macros Configuration

Microsoft Office Protected View Disabled

Microsoft Office Service Pack Out of Date

Microsoft Office Trust Access to VBA Project Model Object Enabled

Microsoft Office Unsupported Version Detection

Microsoft Office Web Apps Installed (credentialed check)

Microsoft OneNote Detection

Microsoft Outlook Attachment Previewing Enabled

Microsoft Paint Recent File History

Microsoft PowerPoint Viewer Installed (credentialed check)

Microsoft PowerPoint Viewer Unsupported Version Detection

Microsoft Project Installed (credentialed check)

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Microsoft Remote Desktop Connection Installed

Microsoft Remote Desktop Gateway Multiple RCE Vulnerabilities (uncredentialed check)

Microsoft Revoked Digital Certificates Enumeration

Microsoft Security Advisory 4033453: Vulnerability in Azure AD Connect Could Allow Elevation of Privilege

Microsoft Security Rollup Enumeration

Microsoft Service Bus for Windows Server Installed

Microsoft SharePoint Installed (credentialed check)

Microsoft SharePoint Server Unsupported Version Detection

Microsoft Silverlight Detection

Microsoft Silverlight Unsupported Version Detection (Windows)

Microsoft SMS/SCCM Installed

Microsoft SQL Server Management Studio (SSMS) Installed

Microsoft SQL Server Management Studio 18.x < 18.3.1 Multiple Vulnerabilities (October 2019)

Microsoft SQL Server Management Studio Multiple vulnerabilities (October 2018)

Microsoft System Center Configuration Manager Client Installed

Microsoft System Center Configuration Manager Database Information

Microsoft System Center Configuration Manager Management Point Detection

Microsoft System Center Operations Manager Component Installed

Microsoft System Center Virtual Machine Manager Installed

Microsoft Update Installed

Microsoft Visio Installed (credentialed check)

Microsoft Visio Unsupported Version Detection

Microsoft Visio Viewer Installed (credentialed check)

Microsoft Visio Viewer Unsupported Version Detection

Microsoft Visual FoxPro Installed

Microsoft Visual FoxPro Unsupported Version Detection

Microsoft Visual Studio .git\config Command Execution

Microsoft Visual Studio Code Installed

Microsoft Visual Studio Code Installed (Windows)

Microsoft Visual Studio Installed

Microsoft Visual Studio Integrated Shell Installed

Microsoft Visual Studio Isolated Shell Installed

Microsoft Visual Studio Team Foundation Server / Azure DevOps Server Detection (credentialed check)

Microsoft Whale Client Components ActiveX (WhlMgr.dll) Multiple Method Overflows

Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Microsoft Windows 10 Version 1507 Unsupported Version Detection

Microsoft Windows 10 Version 1511 Unsupported Version Detection

Microsoft Windows 10 Version 1607 Unsupported Version Detection

Microsoft Windows 10 Version 1703 Unsupported Version Detection

Microsoft Windows 10 Version 1709 Unsupported Version Detection

Microsoft Windows 2000 SP4 Update Rollup 1 Missing

Microsoft Windows 2000 Unsupported Installation Detection

Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection

Microsoft Windows 8 Unsupported Installation Detection

Microsoft Windows 95/98/ME Unsupported Installation Detection

Microsoft Windows 98 Malformed oshare Packet DoS

Microsoft Windows Administrator Default Password Detection (W32/Deloder Worm Susceptibility)

Microsoft Windows Alerter Service Social Engineering Weakness

Microsoft Windows AppLocker Configuration

Microsoft Windows ARP Table

Microsoft Windows AutoRuns Appinit DLLs

Microsoft Windows AutoRuns Boot Execute

Microsoft Windows AutoRuns Codecs

Microsoft Windows AutoRuns Explorer

Microsoft Windows AutoRuns Internet Explorer

Microsoft Windows AutoRuns Known DLLs

Microsoft Windows AutoRuns Logon

Microsoft Windows AutoRuns LSA Providers

Microsoft Windows AutoRuns Network Providers

Microsoft Windows AutoRuns Print Monitor

Microsoft Windows AutoRuns Registry Hijack Possible Locations

Microsoft Windows AutoRuns Report

Microsoft Windows AutoRuns Scheduled Tasks

Microsoft Windows AutoRuns Services and Drivers

Microsoft Windows AutoRuns Setup

Microsoft Windows AutoRuns Unique Entries

Microsoft Windows AutoRuns Winlogon

Microsoft Windows AutoRuns Winsock Provider

Microsoft Windows Current Groups

Microsoft Windows Current Sessions

Microsoft Windows Current Users

Microsoft Windows Current Users Last Password Change

Microsoft Windows Default Credentials (PCI wordlist)

Microsoft Windows Device Logs

Microsoft Windows DNS Cache

Microsoft Windows Environment Variables

Microsoft Windows Essentials Installed

Microsoft Windows Hosts File

Microsoft Windows ICMP Type 9 Packet Remote DoS

Microsoft Windows Installed Hotfixes

Microsoft Windows Installed Software Enumeration (credentialed check)

Microsoft Windows Known Bad AutoRuns / Scheduled Tasks Deprecated

Microsoft Windows Last Boot Time

Microsoft Windows LM / NTLMv1 Authentication Enabled

Microsoft Windows Messenger Detection

Microsoft Windows Messenger Service Social Engineering Weakness

Microsoft Windows Mounted Devices

Microsoft Windows NetBIOS NULL Source Name Remote DoS

Microsoft Windows NetBIOS over TCP/IP Info

Microsoft Windows Network Adapters

Microsoft Windows NT 4.0 Unsupported Installation Detection

Microsoft Windows NT SCM Malformed Resource Enumeration Request DoS

Microsoft Windows NT WINS Service Malformed Data DoS

Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Microsoft Windows Portable Devices

Microsoft Windows PowerShell Execution Policy

Microsoft Windows PPTP Server Malformed Control Packet Remote DoS (179107)

Microsoft Windows Process Information

Microsoft Windows Process Module Information

Microsoft Windows Process Unique Process Name

Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Microsoft Windows Remote Listeners Enumeration (WMI)

Microsoft Windows Scripting Host Settings

Microsoft Windows Search Remote Code Execution Vulnerability (CVE-2017-8543)

Microsoft Windows Security Center Settings

Microsoft Windows Server 2003 Unsupported Installation Detection

Microsoft Windows Server 2008 Unsupported Version Detection

Microsoft Windows shlwapi.dll Malformed HTML Tag Handling Null Pointer DoS

Microsoft Windows SMB : Suspicious Software Detection

Microsoft Windows SMB : WindowsUpdate Disabled

Microsoft Windows SMB : WSUS Client Configured

Microsoft Windows SMB Blank Administrator Password

Microsoft Windows SMB Guessable User Credentials

Microsoft Windows SMB Guest Account Local User Access

Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Microsoft Windows SMB Last Logged On User Disclosure

Microsoft Windows SMB Log In Possible

Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration

Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials

Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Microsoft Windows SMB NULL Session Authentication

Microsoft Windows SMB Registry : Autologon Enabled

Microsoft Windows SMB Registry : Classic Logon Screen

Microsoft Windows SMB Registry : Dial-In Enabled

Microsoft Windows SMB Registry : Enumerate the list of SNMP communities

Microsoft Windows SMB Registry : Key Permission Weakness Admin Privilege Escalation

Microsoft Windows SMB Registry : Key Permissions Path Subversion Local Privilege Escalation

Microsoft Windows SMB Registry : Last Logged User Name Disclosure

Microsoft Windows SMB Registry : McAfee EPO GUID

Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Microsoft Windows SMB Registry : NT MTS Package Administration Registry Key Permission Weakness

Microsoft Windows SMB Registry : NT RAS Administration Registry Key Permission Weakness Local Privilege Escalation

Microsoft Windows SMB Registry : NT4 Service Pack Version Detection

Microsoft Windows SMB Registry : OS Version and Processor Architecture

Microsoft Windows SMB Registry : Registry HKLM\_LOCAL\_MACHINE Permissions

Microsoft Windows SMB Registry : Remote PDC/BDC Detection

Microsoft Windows SMB Registry : Schedule Key Permission Weakness Local Privilege Escalation

Microsoft Windows SMB Registry : SFCDisable Key Permission Weakness

Microsoft Windows SMB Registry : SNMP Registry Key Permission Weakness Local Privilege Escalation

Microsoft Windows SMB Registry : Vista / Server 2008 Service Pack Detection

Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection

Microsoft Windows SMB Registry : Windows 2000 Service Pack Detection

Microsoft Windows SMB Registry : Windows 2003 Server Service Pack Detection

Microsoft Windows SMB Registry : Windows 8 / Server 2012 Service Pack Detection

Microsoft Windows SMB Registry : Windows 8.1 / Server 2012 R2 Service Pack Detection

Microsoft Windows SMB Registry : Winlogon Cached Password Weakness

Microsoft Windows SMB Registry : Winlogon Key Permission Weakness

Microsoft Windows SMB Registry : Winreg Registry Key Detection

Microsoft Windows SMB Registry : WinVNC's Key Permissions

Microsoft Windows SMB Registry : XP Service Pack Detection

Microsoft Windows SMB Registry Not Fully Accessible Detection

Microsoft Windows SMB Registry Remotely Accessible

Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)

Microsoft Windows SMB Service Config Enumeration

Microsoft Windows SMB Service Detection

Microsoft Windows SMB Service Enumeration

Microsoft Windows SMB Service Enumeration via \srvsvc

Microsoft Windows SMB Sessions

Microsoft Windows SMB Share Hosting Office Files

Microsoft Windows SMB Share Hosting Possibly Copyrighted Material

Microsoft Windows SMB Share Permissions Enumeration

Microsoft Windows SMB Shares Access

Microsoft Windows SMB Shares Enumeration

Microsoft Windows SMB Shares Unprivileged Access

Microsoft Windows SMB svcctl MSRPC Interface SCM Service Enumeration

Microsoft Windows SMB Versions Supported (remote check)

Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Microsoft Windows SMBv1 Multiple Vulnerabilities

Microsoft Windows SMBv3 Compression RCE (ADV200005)(CVE-2020-0796)(Deprecated)

Microsoft Windows SMBv3 Compression RCE (ADV200005)(CVE-2020-0796)(Remote)

Microsoft Windows SMBv3 Compression RCE (ADV200005)(CVE-2020-0796)(Remote)

Microsoft Windows Startup Software Enumeration

Microsoft Windows Time Zone Information

Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)

Microsoft Windows Unquoted Service Path Enumeration

Microsoft Windows Update Reboot Required

Microsoft Windows USB Device Usage Report

Microsoft Windows Vista Unsupported Installation Detection

Microsoft Windows Wireless Network History

Microsoft Windows XP Unsupported Installation Detection

Microsoft Word Viewer Installed (credentialed check)

Microsoft Word Viewer Unsupported Version Detection

Microsoft XML Parser (MSXML) and XML Core Services Unsupported

mIRC Detection

mIRC PRIVMSG Handling Remote Buffer Overflow

Mobipocket Reader CHM File Handling Remote Overflow

Modem Enumeration (WMI)

Morovia Barcode ActiveX Control < 3.6.0 Arbitrary File Overwrite

Mozilla < 1.7.3 / Thunderbird < 0.8 Multiple Vulnerabilities

Mozilla Browser < 1.7.12 Multiple Vulnerabilities

Mozilla Browser < 1.7.6 Multiple Vulnerabilities

Mozilla Browser < 1.7.7 Multiple Vulnerabilities

Mozilla Browser < 1.7.8 Multiple Vulnerabilities

Mozilla Browser < 1.7.9 Multiple Vulnerabilities

Mozilla Browsers Multiple Vulnerabilities

Mozilla Browsers shell: URI Arbitrary Command Execution

Mozilla Firefox 48.x / 49.x < 49.0.2 Multiple Vulnerabilities

Mozilla Firefox 49.x < 50.0.1 HTTP Redirect Handling Same-origin Policy Bypass

Mozilla Firefox < 49 Multiple Vulnerabilities

Mozilla Firefox < 49.0 Multiple Vulnerabilities

Mozilla Firefox < 50.0 Multiple Vulnerabilities

Mozilla Firefox < 50.0.2 nsSMILTimeContainer.cpp SVG Animation RCE

Mozilla Firefox < 50.1 Multiple Vulnerabilities

Mozilla Firefox < 51.0 Multiple Vulnerabilities

Mozilla Firefox < 52.0 Multiple Vulnerabilities

Mozilla Firefox < 52.0.1 CreateImageBitmap RCE

Mozilla Firefox < 53 Multiple Vulnerabilities

Mozilla Firefox < 53.0.2 ANGLE Graphics Library RCE

Mozilla Firefox < 54 Multiple Vulnerabilities

Mozilla Firefox < 55 Multiple Vulnerabilities

Mozilla Firefox < 56 Multiple Vulnerabilities

Mozilla Firefox < 57 Multiple Vulnerabilities

Mozilla Firefox < 57.0.1 Multiple Vulnerabilities

Mozilla Firefox < 57.0.2 ANGLE Graphics Library RCE

Mozilla Firefox < 57.0.4 Speculative Execution Side-Channel Attack Vulnerability (Spectre)

Mozilla Firefox < 58 Multiple Vulnerabilities

Mozilla Firefox < 58.0.1 Arbitrary Code Execution

Mozilla Firefox < 59 Multiple Vulnerabilities

Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities

Mozilla Firefox < 60 Multiple Critical Vulnerabilities

Mozilla Firefox < 61 Multiple Critical Vulnerabilities

Mozilla Firefox < 62 Multiple Critical Vulnerabilities

Mozilla Firefox < 62.0.2 Vulnerability

Mozilla Firefox < 62.0.3 Multiple Vulnerabilities

Mozilla Firefox < 63 Multiple Vulnerabilities

Mozilla Firefox < 64.0 Multiple Vulnerabilities

Mozilla Firefox < 65.0

Mozilla Firefox < 65.0.1

Mozilla Firefox < 66.0

Mozilla Firefox < 66.0.1

Mozilla Firefox < 67.0

Mozilla Firefox < 67.0.2

Mozilla Firefox < 67.0.3

Mozilla Firefox < 67.0.4

Mozilla Firefox < 68.0

Mozilla Firefox < 68.0.2

Mozilla Firefox < 69.0

Mozilla Firefox < 69.0.1

Mozilla Firefox < 70.0 Multiple Vulnerabilities

Mozilla Firefox < 71.0

Mozilla Firefox < 72.0 Multiple Vulnerabilities

Mozilla Firefox < 72.0.1

Mozilla Firefox < 73.0

Mozilla Firefox < 74.0 Multiple Vulnerabilities

Mozilla Firefox < 74.0.1

Mozilla Firefox < 75.0 (mfsa2020-12)

Mozilla Firefox ESR 45.x < 45.4 Multiple Vulnerabilities

Mozilla Firefox ESR 45.x < 45.5 Multiple Vulnerabilities

Mozilla Firefox ESR 45.x < 45.5.1 nsSMILTimeContainer.cpp SVG Animation RCE

Mozilla Firefox ESR 45.x < 45.6 Multiple Vulnerabilities

Mozilla Firefox ESR 45.x < 45.9 Multiple Vulnerabilities

Mozilla Firefox ESR 52.x < 52.1 Multiple Vulnerabilities

Mozilla Firefox ESR 52.x < 52.1.1 ANGLE Graphics Library RCE

Mozilla Firefox ESR 68.x < 68.2 Multiple vulnerabilities

Mozilla Firefox ESR 68.x < 68.3 Multiple vulnerabilities

Mozilla Firefox ESR < 45.7 Multiple Vulnerabilities

Mozilla Firefox ESR < 45.8 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.0.1 CreateImageBitmap RCE

Mozilla Firefox ESR < 52.2 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.3 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.4 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.5 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.5.2 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.6 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.7 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.7.2 Multiple Code Execution Vulnerabilities

Mozilla Firefox ESR < 52.7.3 Denial of Service Vulnerability

Mozilla Firefox ESR < 52.8 Multiple Critical Vulnerabilities

Mozilla Firefox ESR < 52.9 Multiple Critical Vulnerabilities

Mozilla Firefox ESR < 59.0.2 Denial of Service Vulnerability

Mozilla Firefox ESR < 60.1 Multiple Critical Vulnerabilities

Mozilla Firefox ESR < 60.2 Multiple Critical Vulnerabilities

Mozilla Firefox ESR < 60.2.1 Multiple Vulnerabilities

Mozilla Firefox ESR < 60.2.2 Multiple Vulnerabilities

Mozilla Firefox ESR < 60.3 Multiple Vulnerabilities

Mozilla Firefox ESR < 60.4 Multiple Vulnerabilities

Mozilla Firefox ESR < 60.5

Mozilla Firefox ESR < 60.5.1

Mozilla Firefox ESR < 60.6

Mozilla Firefox ESR < 60.6.1

Mozilla Firefox ESR < 60.7

Mozilla Firefox ESR < 60.7.1

Mozilla Firefox ESR < 60.7.2

Mozilla Firefox ESR < 60.8

Mozilla Firefox ESR < 60.9

Mozilla Firefox ESR < 68.0.2

Mozilla Firefox ESR < 68.1

Mozilla Firefox ESR < 68.4 Multiple Vulnerabilities

Mozilla Firefox ESR < 68.4.1

Mozilla Firefox ESR < 68.5 Multiple Vulnerabilities

Mozilla Firefox ESR < 68.6 Multiple Vulnerabilities

Mozilla Firefox ESR < 68.6.1

Mozilla Firefox ESR < 68.7 Multiple Vulnerabilities (mfsa2020-13)

Mozilla Foundation Application Detection

Mozilla Foundation Unsupported Application Detection

Mozilla Multiple Browsers CA Certificate SSL Page DoS

Mozilla Multiple Products XPInstall Arbitrary File Overwrite

Mozilla nsNNTPProtocol.cpp NNTP news:// URI Handling Overflow DoS

Mozilla SOAPParameter Object Constructor Overlow

Mozilla Thunderbird 10.0.x < 10.0.3 Multiple Vulnerabilities

Mozilla Thunderbird 10.0.x < 10.0.4 Multiple Vulnerabilities

Mozilla Thunderbird 10.0.x < 10.0.5 Multiple Vulnerabilities

Mozilla Thunderbird 10.0.x < 10.0.6 Multiple Vulnerabilities

Mozilla Thunderbird 10.0.x < 10.0.7 Multiple Vulnerabilities

Mozilla Thunderbird 10.0.x < 10.0.8 Multiple Vulnerabilities

Mozilla Thunderbird 10.x < 10.0.1 Memory Corruption

Mozilla Thunderbird 10.x < 10.0.10 Multiple Vulnerabilities

Mozilla Thunderbird 10.x < 10.0.11 Multiple Vulnerabilities

Mozilla Thunderbird 10.x < 10.0.12 Multiple Vulnerabilities

Mozilla Thunderbird 10.x < 10.0.2 'png\_decompress\_chunk' Integer Overflow

Mozilla Thunderbird 10.x < 10.0.9 Multiple Vulnerabilities

Mozilla Thunderbird 17.x < 17.0.5 Multiple Vulnerabilities

Mozilla Thunderbird 17.x through 23.x Multiple Vulnerabilities

Mozilla Thunderbird 24.x < 24.7 Multiple Vulnerabilities

Mozilla Thunderbird 24.x < 24.8 Multiple Vulnerabilities

Mozilla Thunderbird 24.x < 24.8.1 NSS Signature Verification Vulnerability

Mozilla Thunderbird 3.1 < 3.1.10 Multiple Vulnerabilities

Mozilla Thunderbird 3.1 < 3.1.11 Multiple Vulnerabilities

Mozilla Thunderbird 3.1 < 3.1.12 Multiple Vulnerabilities

Mozilla Thunderbird 3.1 < 3.1.3 Multiple Vulnerabilities

Mozilla Thunderbird 3.1 < 3.1.5 Multiple Vulnerabilities

Mozilla Thunderbird 3.1 < 3.1.6 Buffer Overflow

Mozilla Thunderbird 3.1 < 3.1.8 Multiple Vulnerabilities

Mozilla Thunderbird 3.1 < 3.1.9 Invalid HTTP Certificates

Mozilla Thunderbird 3.1.x < 3.1.1 Multiple Vulnerabilities

Mozilla Thunderbird 3.1.x < 3.1.14 Untrusted CA

Mozilla Thunderbird 3.1.x < 3.1.16 Multiple Vulnerabilities

Mozilla Thunderbird 3.1.x < 3.1.18 Multiple Vulnerabilities

Mozilla Thunderbird 3.1.x < 3.1.19 'png\_decompress\_chunk' Integer Overflow

Mozilla Thunderbird 3.1.x < 3.1.20 Multiple Vulnerabilities

Mozilla Thunderbird 3.1.x < 3.1.7 Multiple Vulnerabilities

Mozilla Thunderbird 3.1.x Out-of-Date CA List

Mozilla Thunderbird < 1.0.2 Browser GIF Processing Overflow

Mozilla Thunderbird < 1.0.6 Multiple Vulnerabilities

Mozilla Thunderbird < 1.0.7 IDN URL Domain Name Overflow

Mozilla Thunderbird < 1.5 Attachment Extension Spoofing

Mozilla Thunderbird < 1.5.0.10 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.12 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.13 / 2.0.0.6 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.14 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.4 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.5 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.7 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.8 Multiple Vulnerabilities

Mozilla Thunderbird < 1.5.0.9 Multiple Vulnerabilities

Mozilla Thunderbird < 10.0 Multiple Vulnerabilities

Mozilla Thunderbird < 12.0 Multiple Vulnerabilities

Mozilla Thunderbird < 13.0 Multiple Vulnerabilities

Mozilla Thunderbird < 14.0 Multiple Vulnerabilities

Mozilla Thunderbird < 15.0 Multiple Vulnerabilities

Mozilla Thunderbird < 16.0 Multiple Vulnerabilities

Mozilla Thunderbird < 16.0.1 Multiple Vulnerabilities

Mozilla Thunderbird < 16.0.2 Multiple Vulnerabilities

Mozilla Thunderbird < 17.0 Multiple Vulnerabilities

Mozilla Thunderbird < 17.0.2 Multiple Vulnerabilities

Mozilla Thunderbird < 17.0.3 Multiple Vulnerabilities

Mozilla Thunderbird < 17.0.4 nsHTMLEditor Use-After-Free

Mozilla Thunderbird < 17.0.5 Multiple Vulnerabilities

Mozilla Thunderbird < 17.0.7 Multiple Vulnerabilities

Mozilla Thunderbird < 17.0.8 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.12 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.14 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.16 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.17 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.18 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.19 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.21 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.22 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.23 Certificate Authority (CA) Common Name Null Byte Handling SSL MiTM Weakness

Mozilla Thunderbird < 2.0.0.24 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.5 Multiple Vulnerabilities

Mozilla Thunderbird < 2.0.0.9 Multiple Vulnerabilities

Mozilla Thunderbird < 24.1 Multiple Vulnerabilities

Mozilla Thunderbird < 24.1.1 NSS and NSPR Multiple Vulnerabilities

Mozilla Thunderbird < 24.2 Multiple Vulnerabilities

Mozilla Thunderbird < 24.3 Multiple Vulnerabilities

Mozilla Thunderbird < 24.4 Multiple Vulnerabilities

Mozilla Thunderbird < 24.5 Multiple Vulnerabilities

Mozilla Thunderbird < 24.6 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.1 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.10 Buffer Overflow

Mozilla Thunderbird < 3.0.11 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.2 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.4 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.5 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.6 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.7 Multiple Vulnerabilities

Mozilla Thunderbird < 3.0.9 Multiple Vulnerabilities

Mozilla Thunderbird < 31.0 Multiple Vulnerabilities

Mozilla Thunderbird < 31.1 Multiple Vulnerabilities

Mozilla Thunderbird < 31.1.2 NSS Signature Verification Vulnerability

Mozilla Thunderbird < 31.2 Multiple Vulnerabilities

Mozilla Thunderbird < 31.3 Multiple Vulnerabilities

Mozilla Thunderbird < 31.4 Multiple Vulnerabilities

Mozilla Thunderbird < 31.5 Multiple Vulnerabilities

Mozilla Thunderbird < 31.6 Multiple Vulnerabilities

Mozilla Thunderbird < 31.7 Multiple Vulnerabilities

Mozilla Thunderbird < 38.1 Multiple Vulnerabilities (Logjam)

Mozilla Thunderbird < 38.4 Multiple Vulnerabilities

Mozilla Thunderbird < 45.5.1 nsSMILTimeContainer.cpp SVG Animation RCE

Mozilla Thunderbird < 45.6 Multiple Vulnerabilities

Mozilla Thunderbird < 45.7 Multiple Vulnerabilities

Mozilla Thunderbird < 45.8 Multiple Vulnerabilities

Mozilla Thunderbird < 52.1 Multiple Vulnerabilities

Mozilla Thunderbird < 52.2 Multiple Vulnerabilities

Mozilla Thunderbird < 52.5 Multiple Vulnerabilities

Mozilla Thunderbird < 52.5.2 Multiple Vulnerabilities

Mozilla Thunderbird < 52.6 Multiple Vulnerabilities

Mozilla Thunderbird < 52.8 Multiple Vulnerabilities (EFAIL)

Mozilla Thunderbird < 52.9 Multiple Vulnerabilities

Mozilla Thunderbird < 6.0 Multiple Vulnerabilities

Mozilla Thunderbird < 6.0.1 Out-of-Date CA List

Mozilla Thunderbird < 6.0.2 Untrusted CA

Mozilla Thunderbird < 60.0 Multiple Vulnerabilities

Mozilla Thunderbird < 60.2.1 Multiple Vulnerabilities

Mozilla Thunderbird < 60.3 Multiple Vulnerabilities

Mozilla Thunderbird < 60.5

Mozilla Thunderbird < 60.5.1

Mozilla Thunderbird < 60.6

Mozilla Thunderbird < 60.6.1

Mozilla Thunderbird < 60.7

Mozilla Thunderbird < 60.7.1

Mozilla Thunderbird < 60.7.2

Mozilla Thunderbird < 60.8

Mozilla Thunderbird < 60.9 Multiple Vulnerabilities

Mozilla Thunderbird < 68.0

Mozilla Thunderbird < 68.1 Multiple Vulnerabilities

Mozilla Thunderbird < 68.1.1

Mozilla Thunderbird < 68.2

Mozilla Thunderbird < 68.3

Mozilla Thunderbird < 68.4.1

Mozilla Thunderbird < 68.5

Mozilla Thunderbird < 68.7.0

Mozilla Thunderbird < 7.0 Multiple Vulnerabilities

Mozilla Thunderbird < 8.0 Multiple Vulnerabilities

Mozilla Thunderbird < 9.0 Multiple Vulnerabilities

Mozilla Thunderbird ESR 17.x < 17.0.3 Multiple Vulnerabilities

Mozilla Thunderbird ESR 17.x < 17.0.4 nsHTMLEditor Use-After-Free

Mozilla Thunderbird ESR 17.x < 17.0.5 Multiple Vulnerabilities

Mozilla Thunderbird ESR 17.x < 17.0.6 Multiple Vulnerabilities

Mozilla Thunderbird ESR 17.x < 17.0.7 Multiple Vulnerabilities

Mozilla Thunderbird ESR 17.x < 17.0.8 Multiple Vulnerabilities

Mozilla Thunderbird ESR 17.x < 17.0.9 Multiple Vulnerabilities

Mozilla Thunderbird ESR < 17.0.10 Multiple Vulnerabilities

Mozilla Thunderbird ESR < 17.0.11 Null\_Cipher Code Execution

MS 2562937: Update Rollup for ActiveX Kill Bits (2562937)

MS 2647518: Update Rollup for ActiveX Kill Bits (2647518)

MS 2695962: Update Rollup for ActiveX Kill Bits (2695962)

MS 2736233: Update Rollup for ActiveX Kill Bits (2736233)

MS Blaster Worm (msblast.exe) Infection Detection

MS KB2219475: Windows Help Center hcp:// Protocol Handler Arbitrary Code Execution

MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution

MS KB2286198: Windows Shell Shortcut Icon Parsing Arbitrary Code Execution (EASYHOOKUP)

MS KB2401593: Microsoft Outlook Web Access (OWA) CSRF

MS KB2488013: Internet Explorer CSS Import Rule Processing Arbitrary Code Execution

MS KB2491888: Microsoft Malware Protection Engine (MMPE) Privilege Escalation

MS KB2506014: Update for the Windows Operating System Loader

MS KB2526954: Microsoft Silverlight 4.0 < 4.0.60310 Multiple Vulnerabilities

MS KB2532445: AppLocker Rules Bypass

MS KB2661254: Update For Minimum Certificate Key Length

MS KB2719662: Vulnerabilities in Gadgets Could Allow Remote Code Execution

MS KB2755399: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2758994: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2785605: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2794220: Vulnerability in Internet Explorer Could Allow Remote Code Execution (deprecated)

MS KB2796096: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2805940: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2811522: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2813430: Update to Improve Cryptography and Digital Certificate Handling in Windows

MS KB2819372: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2819682: Security Updates for Microsoft Windows Store Applications

MS KB2820197: Update Rollup for ActiveX Kill Bits

MS KB2824670: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2833510: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2837385: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2847928: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2857645: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2861855: Updates to Improve Remote Desktop Protocol Network-Level Authentication

MS KB2862152: Vulnerability in DirectAccess Could Allow Security Feature Bypass

MS KB2862966: Updates to Improve Cryptography and Digital Certificate Handling in Windows

MS KB2862973: Update for Deprecation of MD5 Hashing Algorithm for Microsoft Root Certificate Program

MS KB2868725: Update for Disabling RC4

MS KB2871690: Update to Revoke Non-compliant UEFI Modules

MS KB2871997: Update to Improve Credentials Protection and Management

MS KB2880289: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2898108: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2905247: Insecure ASP.NET Site Configuration Could Allow Elevation of Privilege

MS KB2907997: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

MS KB2916626: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2927432: Visual Studio Update 2 for Debug Interface Access SDK

MS KB2929825: Update for Vulnerability in Adobe Flash Player in Internet Explorer

MS KB2934802: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2938527: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2942844: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2957151: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2960358: Update for Disabling RC4 in .NET TLS

MS KB2961887: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2962393: Update for Vulnerability in Juniper Networks Windows In-Box Junos Pulse Client (Heartbleed)

MS KB2962824: Update Rollup of Revoked Non-Compliant UEFI Modules

MS KB2966072: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2974008: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2977292: Update for Microsoft EAP Implementation that Enables the Use of TLS

MS KB2982794: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB2987114: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3001237: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3004150: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3008925: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)

MS KB3018943: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3021953: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3024663: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3033408: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3033929: Availability of SHA-2 Code Signing Support for Windows 7 and Windows Server 2008 R2

MS KB3035034: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3042058: Update to Default Cipher Suite Priority Order

MS KB3044132: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3045755: Update to Improve PKU2U Authentication

MS KB3049508: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3061904: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3062760: Update for Vulnerability in Juniper Networks Windows In-Box Junos Pulse Client (FREAK)

MS KB3065820: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3065823: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3074162: Vulnerability in Microsoft Malicious Software Removal Tool Could Allow Elevation of Privilege

MS KB3074219: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3079777: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3083992: Update to Improve AppLocker Publisher Rule Enforcement

MS KB3087040: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge

MS KB3087916: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

MS KB3097966: Inadvertently Disclosed Digital Certificates Could Allow Spoofing

MS KB3099406: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge

MS KB3103688: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge

MS KB3105216: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge

MS KB3108638: Update for Windows Hyper-V to Address CPU Weakness

MS KB3109853: Update to Improve TLS Session Resumption Interoperability

MS KB3118753: Update for ActiveX Kill Bits

MS KB3119147: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge

MS KB3119884: Improperly Issued Digital Certificates Could Allow Spoofing

MS KB3123040: Improperly Issued Digital Certificates Could Allow Spoofing

MS KB3123479: Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program

MS KB3132372: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge

MS KB3152550: Update to Improve Wireless Mouse Input Filtering

MS KB3155527: Update to Cipher Suites for FalseStart

MS KB3179528: Update for Kernel Mode Blacklist

MS KB821724: ISA Server 2000 May Send Basic Credentials Over an External HTTP Connection

MS KB870669: ADODB.Stream object from Internet Explorer

MS KB892313: DRM Update in Windows Media Player May Facilitate Spyware Infections

MS KB900930: Microsoft Outlook Express Multiple Vulnerabilities

MS KB953839: Cumulative Security Update of ActiveX Kill Bits

MS KB955759: Security Enhancements for the Indeo Codec

MS KB956391: Cumulative Security Update of ActiveX Kill Bits

MS KB960715: Cumulative Security Update of ActiveX Kill Bits

MS KB969898: Cumulative Security Update of ActiveX Kill Bits

MS KB979267: Flash 6 ActiveX Control On Windows XP Multiple Vulnerabilities

MS KB982316: Elevation of Privilege Using Windows Service Isolation Bypass

MS Security Advisory 2846338: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution

MS Security Advisory 2974294: Vulnerability in Microsoft Malware Protection Engine Could Allow Denial of Service

MS Security Advisory 4022344: Security Update for Microsoft Malware Protection Engine

MS00-013: Microsoft Windows Media Server Malformed Handshake Sequence DoS (253943) (intrusive check)

MS02-004: Microsoft Telnet Server Protocol Option Handling Remote Overflow (307298) (intrusive check)

MS02-018: Microsoft Windows Distributed Transaction Coordinator (DTC) Malformed Input DoS (319733) (intrusive check)

MS02-045: Microsoft Windows SMB Protocol SMB\_COM\_TRANSACTION Packet Remote Overflow DoS (326830) (uncredentialed check)

MS03-010: Microsoft Windows RPC Endpoint Manager Malformed Packet DoS (331953) (intrusive check)

MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)

MS03-034: Flaw in NetBIOS Could Lead to Information Disclosure (824105) (uncredentialed check)

MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)

MS03-039: Microsoft Windows RPC DCOM Interface epmapper Pipe Hijack Local Privilege Escalation (824146) (intrusive check)

MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)

MS04-006: WINS Server Remote Overflow (830352) (uncredentialed check)

MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (HTTP)

MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)

MS04-011: Microsoft Windows SSL Library Malformed Message Remote DoS (835732) (uncredentialed check)

MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)

MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check)

MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check)

MS04-031: Vulnerability NetDDE Could Allow Code Execution (841533) (uncredentialed check)

MS04-035: WINS Code Execution (870763) (uncredentialed check)

MS04-036: Microsoft NNTP Component Remote Overflow (883935) (uncredentialed check)

MS04-042: Windows NT Multiple DHCP Vulnerabilities (885249) (uncredentialed check)

MS05-007: Vulnerability in Windows Could Allow Information Disclosure (888302) (uncredentialed check)

MS05-017: Vulnerability in MSMQ Could Allow Code Execution (892944) (uncredentialed check)

MS05-019: Vulnerabilities in TCP/IP Could Allow Remote Code Execution (893066) (uncredentialed check)

MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)

MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)

MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589) (uncredentialed check)

MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)

MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution (902400) (uncredentialed check)

MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution (911927) (uncredentialed check)

MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow DoS (913580) (uncredentialed check)

MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution (911280) (uncredentialed check)

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

MS06-056: Vulnerabilities in ASP.NET could allow information disclosure (922770) (uncredentialed check)

MS07-039: Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122) (uncredentialed check)

MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212) (uncredentialed check)

MS07-063: Vulnerability in SMBv2 Could Allow Remote Code Execution (942624) (uncredentialed check)

MS07-065: Vulnerability in Message Queuing Could Allow Remote Code Execution (937894) (uncredentialed check)

MS08-039: Outlook Web Access for Exchange Server Privilege Escalation (Uncredentialed)

MS08-040: Microsoft SQL Server Multiple Privilege Escalation (941203) (uncredentialed check)

MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593) (uncredentialed check)

MS08-059: Microsoft Host Integration Server (HIS) SNA RPC Request Remote Overflow (956695) (uncredentialed check)

MS08-065: Microsoft Windows Message Queuing Service RPC Request Handling Remote Code Execution (951071) (uncredentialed check)

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check / IPS)

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

MS09-003: Microsoft Exchange Remote Code Execution (959239) (Uncredentialed)

MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) (uncredentialed check)

MS09-039: Vulnerabilities in WINS Could Allow Remote Code Execution (969883) (uncredentialed check)

MS09-050: Microsoft Windows SMB2 \_Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (uncredentialed check)

MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488) (uncredentialed check)

MS09-064: Vulnerability in the License Logging Service (974783) (uncredentialed check)

MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)

MS10-024: Microsoft Exchange Denial of Service (uncredentialed)

MS10-025: Vulnerability in Microsoft Windows Media Services Could Allow Remote Code Execution (980858) (uncredentialed check)

MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)

MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) (EMERALDTHREAD) (uncredentialed check)

MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure (2418042) (uncredentialed check)

MS10-075: Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679) (uncredentialed check)

MS10-106: Microsoft Exchange Server Denial of Service (uncredentialed)

MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) (uncredentialed check)

MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)

MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

MS11-035: Vulnerability in WINS Could Allow Remote Code Execution (2524426) (uncredentialed check)

MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275) (remote check)

MS11-049: Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893) (uncredentialed check)

MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (remote check)

MS11-064: Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894) (uncredentialed check)

MS11-082: Vulnerabilities in Host Integration Server Could Allow Denial of Service (2607670) (uncredentialed check)

MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939) (uncredentialed check)

MS12-070: Vulnerability in SQL Server Could Allow Elevation of Privilege (2754849) (uncredentialed check)

MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check)

MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220) (uncredentialed check)

MS14-044: Vulnerability in SQL Server Could Allow Elevation of Privilege (2984340) (uncredentialed check)

MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)

MS15-058: Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718) (uncredentialed check)

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

MS16-136: Security Update for SQL Server (3199641) (uncredentialed check)

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

MUICache Program Execution History

MusicMatch < 9.0.5066 / 10.0.2048 Multiple Vulnerabilities

MW6 Technologies ActiveX Multiple Buffer Overflows

MySpace Uploader ActiveX Control < 1.0.0.6 Action Property Buffer Overflow

National Instruments LabVIEW 2015 < 2015 SP1 f7 / 2016 < 2016 f2 LvVarientUnflatten VI File Handling Arbitrary Code Execution

National Instruments LabVIEW Installed

NCR Aloha POS SMB Default Credentials

Nessus Client 4.x < 4.2.0 QtWeb Path Subversion DLL Injection Local Code Execution

Nessus Windows < 3.0.6 GUI Unspecified XSS

Nessus Windows < 3.0.6.1 ScanCtrl ActiveX Multiple Method File Manipulation

NetBIOS Multiple IP Address Enumeration

NetIQ Access Manager Detect

netOctopus Agent nantsys.sys MSR Write Local Privilege Escalation

Netop Remote Control dws File Handling Overflow

Netop Remote Control Guest Detection

NetSarang Xftp 5 Backdoor Trojan (ShadowPad)

NetSarang Xlpd 5 Backdoor Trojan (ShadowPad)

NetSarang Xmanager 5 Backdoor Trojan (ShadowPad)

NetSarang Xmanager Enterprise 5 Backdoor Trojan (ShadowPad)

NetSarang Xshell 5 Backdoor Trojan (ShadowPad)

Netscape Browser < 8.0.4 Multiple Vulnerabilities

Netscape Browser < 9.0.0.4 Multiple Vulnerabilities

Netscape Browser < 9.0.0.6 Multiple Vulnerabilities

Netscape Browser Detection

Netscape Browser Unsupported Version Detection

NetSupport Manager < 11.00.0005

NetSupport Manager Client Spoofing Remote Authentication Bypass

NetSupport NSM / NSS Initial Connection Setup Configuration Exchange Remote Overflow

NetVault Report Manager Scheduler File Name Handling Overflow

Network Interfaces Enumeration (WMI)

Network Virtualization for HP LoadRunner Information Disclosure

Nitro Pro <= 7.5.0.29 Memory Corruption

Nitro Pro Insecure Library Loading

Nitro Pro Installed

Nitro Reader <= 2.5.0.45 Memory Corruption

Nitro Reader Installed

No-IP Windows Dynamic Update Client Detection

NOD32 3.0/ESET Smart Security < 3.0.684 Local Privilege Escalation

NOD32 Antivirus < 1.1743 Multiple File Processing Vulnerabilities

NOD32 Antivirus ARJ Archive Filename Handling Overflow

NOD32 Antivirus Detection and Status

NOD32 Antivirus Directory Name Handling Multiple Operation Overflows

NOD32 Antivirus Restore To Feature Local File Creation

NOD32 Antivirus Run-Time Decompressors Multiple Vulnerabilities

Node.js Installed (Windows)

Non-administrators can shut down Windows XP SP1 thru TSShutdn.exe (889323)

Notepad++ Ruby Source File Handling Overflow

NovaStor NovaNET < 13 Multiple Vulnerabilities

Novell Client / Client 2 Multiple Vulnerabilities

Novell Client 2 Vba32 AntiRootKit DoS

Novell Client for Windows DPRPC library (DPRPCW32.DLL) ndps\_xdr\_array Function Remote Overflow

Novell Client nicm.sys Local Privilege Escalation

Novell Client nwfs.sys Local Privilege Escalation

Novell Client nwspool.dll RPC Printer Functions Remote Overflow (300870)

Novell Client srvloc.sys Crafted Packet Unspecified Remote DoS

Novell Client TS/Citrix Session Arbitrary User Profile Invocation

Novell Distributed Print Services (NDPS) Print Provider (NDPPNT.DLL) Remote Overflow

Novell eDirectory eMBox Utility Unauthorized Access

Novell exteNd Director LocalExec ActiveX (LocalExec.ocx) launch() Method Arbitrary Command Execution

Novell File Reporter Agent XML Tag Handling Buffer Overflow

Novell File Reporter Engine RECORD Element Tag Parsing Overflow (credentialed check)

Novell GroupWise / Oracle Outside In Lotus 123 v4 Parser Unspecified Remote Code Execution

Novell GroupWise Authentication Credentials MiTM Disclosure

Novell GroupWise Client 8.x < 8.0.3 / 2012.x < 2012 SP1 Unspecified File Handling Arbitrary Code Execution

Novell GroupWise Client 8.x < 8.0.3 Hot Patch 2 / 2012.x < 2012 SP1 Hot Patch 1 Multiple Vulnerabilities

Novell GroupWise Client 8.x < 8.0.3 Hot Patch 3 / 2012.x < 2012 SP2 XSS

Novell GroupWise Client 8.x < 8.0.3 Hot Patch 4 / 2012 < 2012 SP3 / 2014 < 2014 SP1 Multiple Dereference Vulnerabilities

Novell GroupWise Client Address Book File Handling Email Address Field Remote Overflow

Novell GroupWise Client Installed

Novell GroupWise Internet Agent 8.x < 8.0.3 / 12.x < 12.0.1 Multiple Vulnerabilities

Novell GroupWise Internet Agent 8.x <= 8.0.2 HP3 / 12.x < 12.0.1 Multiple Vulnerabilities

Novell GroupWise Internet Agent < 7.03 HP3 / 8.0 HP2 Multiple Buffer Overflows

Novell GroupWise Internet Agent Detection

Novell GroupWise Messenger Client < 2.0.3 HP1 Multiple Remote Overflows

Novell GroupWise Unsupported Version Detection

Novell GroupWise WebAccess 12.0.x < 12.0.4 / 14.0.x < 14.0.2 Multiple XSS Vulnerabilities

Novell GroupWise WebAccess 2012 < 2012 SP4 / 2014 < 2014 SP2 Multiple XSS (7016653)

Novell GroupWise WebAccess 8.x < 8.0.3 Multiple XSS Vulnerabilities

Novell GroupWise WebAccess Arbitrary File Download (local check)

Novell GroupWise WebAccess Detection

Novell GroupWise WebAccess Directory.Item Parameters XSS

Novell GroupWise Windows Client Arbitrary Email Access

Novell iPrint Client < 5.32 Multiple Overflows

Novell iPrint Client < 5.42 Multiple Flaws

Novell iPrint Client < 5.44 Multiple Vulnerabilities

Novell iPrint Client < 5.56 Multiple Vulnerabilities

Novell iPrint Client < 5.64 Multiple Vulnerabilities

Novell iPrint Client < 5.72 nipplib.dll GetDriverSettings Function Buffer Overflow

Novell iPrint Client < 5.78 Multiple Code Execution Vulnerabilities

Novell iPrint Client < 5.82 Remote Code Execution

Novell iPrint Client < 5.90 Stack-Based Buffer Overflow

Novell iPrint Client < 5.93 DoS

Novell iPrint Client ActiveX Control Multiple Vulnerabilities

Novell iPrint Client for Windows ienipp.ocx ActiveX Multiple Variable Overflow

Novell iPrint Client nipplib.dll ActiveX (ienipp.ocx) IppCreateServerRef Function Overflow

Novell iPrint Control ActiveX (ienipp.ocx) ExecuteRequest() Method Overflow

Novell Messenger Client Detection

Novell Messenger Client Import Command Remote Code Execution

Novell Messenger Server Memory Information Disclosure

Novell NetIdentity Agent < 1.2.4 Arbitrary Pointer De-reference Code Execution

Novell NetIQ Sentinel Agent Manager NQMcsVarSet ActiveX DumpToFile() Remote Code Execution

Novell NetWare Client Print Provider (nwspool.dll) Multiple Function Overflow

Novell Privileged User Manager Library Injection Arbitrary Code Execution (credentialed check)

Novell SecureLogin < 6.0.106 Multiple Vulnerabilities

Novell ZENworks Configuration Management 10.3 < 10.3.4 Multiple Vulnerabilities

Novell ZENworks Configuration Management < 10 SP3 Multiple Flaws

Novell ZENworks Configuration Management < 11.2.3a Monthly Update 1 Multiple Vulnerabilities (credentialed check)

Novell ZENworks Configuration Management < 11.3.0.35304 PreBoot Service Directory Traversal

Novell ZENworks Configuration Management PreBoot Service Opcode Request Parsing Vulnerabilities

Novell ZENworks Control Center File Upload Remote Code Execution

Novell ZENworks Detection

Novell ZENworks ESM Security Client STEngine Privilege Escalation

Novell ZENworks Handheld Management Common.dll messageID Request Field Parsing Traversal Arbitrary File Creation

Novell ZENworks Handheld Management ZfHIPCND.exe Crafted TCP Request Remote Overflow

Novell ZENworks Handheld Management ZfHIPCND.exe Unspecified Buffer Overflow

Novell ZENworks Handheld Management ZfHSrvr.exe Multiple Remote Code Execution Vulnerabilities

Now SMS/MMS Gateway < 2008.02.22 Multiple Remote Overflows

NTR ActiveX Control < 2.0.4.8 Multiple Vulnerabilities

Nuance PDF Reader Installed

Nuance PDF Reader pdfcore8.dll Heap Buffer Overflow

Nuance PDF Viewer Plus Installed

NVIDIA Display Driver 174.x < 307.78 / 310.x < 311.00 Multiple Vulnerabilities

NVIDIA Display Driver Service Remote Stack Buffer Overflow (credentialed check)

NVIDIA GeForce Experience < 3.20.2 Local Privilege Escalation Vulnerability

NVIDIA GeForce Experience Installed

NVIDIA Graphics Driver 340.x < 341.92 / 352.x < 354.35 / 358.x < 358.87 Multiple Vulnerabilities

NVIDIA Graphics Driver 340.x < 341.95 / 352.x < 354.74 Multiple Vulnerabilities

NVIDIA Graphics Driver 340.x < 341.96 / 352.x < 354.99 / 361.x < 362.77 / 367.x < 368.39 Multiple Vulnerabilities

NVIDIA Graphics Driver Local Privilege Escalation

NVIDIA Graphics Driver Unspecified Privilege Escalation (Windows)

NVIDIA Linux GPU Display Driver Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver (August 2019)

NVIDIA Windows GPU Display Driver (Feb 2020)

NVIDIA Windows GPU Display Driver 340.x / 341.x / 342.x < 342.00 / 375.x < 375.63 Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver 340.x < 342.01 / 375.x < 376.33 Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver 34x.x < 342.00 / 367.x < 369.73 / 367.x < 369.71 (GRID) / 375.x < 375.63 Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver 375.x / 384.x < 385.08 Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver 375.x < 376.67 / 378.x < 378.52 Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver 375.x < 377.35 / 382.x < 382.05 Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver 375.x < 377.55 / 384.x < 384.94 / 385.x < 385.08 Multiple Vulnerabilities

NVIDIA Windows GPU Display Driver 384.x / 385.x / 386.x < 386.07 / 390.x < 390.65 Multiple Vulnerabilities (Meltdown)(Spectre)

NVIDIA Windows GPU Display Driver Multiple Vulnerabilities (February 2019)

NVIDIA Windows GPU Display Driver Multiple Vulnerabilities (May 2019)

OFF2000: Office Programs Can Browse Restricted Drives (302753)

Office Viewer Component < 5.0 Multiple Vulnerabilities

Office Viewer Component ActiveX (officeviewer.ocx) HttpDownloadFile Method Traversal Arbitrary File Overwrite

Okta AD Agent Detection

Okta Browser Plugin Detection

OnSSI Ocularis Recorder 5.5 < Patch 10 / 5.4 < Patch 19 / 5.3 < Patch 19 Denial of Service (DoS) Vulnerability

OnSSI Ocularis Recorder Installed

OpenOffice < 2.0.3 Multiple Vulnerabilities

OpenOffice < 2.4.1 rtl\_allocateMemory() Function Crafted Document Handling Integer Overflow

OpenOffice < 2.4.2 WMF and EMF File Handling Buffer Overflows

OpenOffice < 3.1.1 Multiple Buffer Overflows

OpenOffice Detection

OpenOffice XML External Entity RDF Document Handling Information Disclosure

OpenSaveMRU History

OpenVPN 2.3.12 < 2.3.15 / 2.4.x < 2.4.2 Denial of Service Vulnerability (Windows)

OpenVPN 2.3.x < 2.3.17 & 2.4.x < 2.4.3 Multiple Denial of Service Vulnerabilites (Windows)

OpenVPN 2.3.x Heartbeat Information Disclosure (Heartbleed)

OpenVPN 2.4.x < 2.4.6 Denial of Service Vulnerability (Windows)

OpenVPN 2.x < 2.2.3 / 2.3.6 Control Channel Packet Handling DoS

OpenVPN 2.x < 2.3. 18/ 2.4.x < 2.4.4 Buffer Overflow Vulnerability w/ key-method 1

OpenVPN < 2.0.1 Multiple Vulnerabilities (Windows)

OpenVPN < 2.3.1 Information Disclosure Vulnerability (Windows)

OpenVPN < 2.3.15 / 2.4.x < 2.4.2 Denial of Service Vulnerability (Windows)

OpenVPN < 2.3.15 Weak Cryptographic Cipher Vulnerability (Windows)

OpenVPN Client 2.0.x < 2.0.6 Remote Code Execution Vulnerability

OpenVPN Client Installed

OpenVPN Server 2.0.x < 2.0.3 Remote Code Execution Vulnerability

OpenVPN Server 2.0.x < 2.0.4 Denial of Service Vulnerability

OpenVPN Server Installed

Opera < 10.0 Multiple Vulnerabilities

Opera < 10.01 Multiple Vulnerabilities

Opera < 10.10 Multiple Vulnerabilities

Opera < 10.50 Multiple Vulnerabilities

Opera < 10.51 Multiple Vulnerabilities

Opera < 10.53 Asynchronous Content Modification Uninitialized Memory Access

Opera < 10.54 Multiple Vulnerabilities

Opera < 10.60 Multiple Vulnerabilities

Opera < 10.61 Multiple Vulnerabilities

Opera < 10.62 Path Subversion Arbitrary DLL Injection Code Execution

Opera < 10.63 Multiple Vulnerabilities

Opera < 11 Multiple Vulnerabilities

Opera < 11.01 Multiple Vulnerabilities

Opera < 11.10 Multiple Vulnerabilities

Opera < 11.11 Multiple Vulnerabilities

Opera < 11.50 Multiple Vulnerabilities

Opera < 11.51 Multiple Vulnerabilities (BEAST)

Opera < 11.52 Multiple Vulnerabilities

Opera < 11.60 Multiple Vulnerabilities (BEAST)

Opera < 11.61 Multiple Vulnerabilities

Opera < 11.62 Multiple Vulnerabilities

Opera < 11.64 URL Parsing Memory Corruption

Opera < 12 Multiple Vulnerabilities

Opera < 12.01 Multiple Vulnerabilities

Opera < 12.02 Truncated Dialog Vulnerability

Opera < 12.10 Multiple Vulnerabilities

Opera < 12.11 Multiple Vulnerabilities

Opera < 12.12 Multiple Vulnerabilities

Opera < 12.13 Multiple Vulnerabilities

Opera < 12.15 Multiple Vulnerabilities

Opera < 12.17 opera\_autoupdate.exe MITM Vulnerability

Opera < 15 UTF-8 Encoding XSS

Opera < 16 Multiple Vulnerabilities

Opera < 17 Multiple Vulnerabilities

Opera < 18 Multiple Vulnerabilities

Opera < 19 Multiple Vulnerabilities

Opera < 20 Multiple Vulnerabilities

Opera < 21 Address Bar Spoofing Vulnerabilities

Opera < 22 Multiple Chromium Vulnerabilities

Opera < 7.03 Multiple Vulnerabilities

Opera < 7.11 Filename Extension Handling Overflow

Opera < 7.20 news URL Handling DoS

Opera < 7.21 HREF Escaped Character Overflow

Opera < 7.22 Multiple Vulnerabilities

Opera < 7.23 File Download Encoded Traversal Arbitrary File Deletion

Opera < 7.23 Zip File Processing Crafted File Handling Overflow

Opera < 7.24 getElementsByTagName JavaScript Method DoS

Opera < 7.50 File Download Extension Spoofing

Opera < 7.50 JavaScript Engine Array Handling DoS

Opera < 7.50 onUnload Address Bar Spoofing

Opera < 7.51 favicon.ico Address Bar Spoofing

Opera < 7.53 Multiple Vulnerabilities

Opera < 7.54 Download File Type Dialog Spoofing

Opera < 7.54 Empty Embedded Object DoS

Opera < 7.54 location Object Crafted URL Arbitrary Local File Access

Opera < 7.54 Multiple Function Address Bar Spoofing

Opera < 8.01 Multiple Vulnerabilities

Opera < 8.02 Multiple Vulnerabilities

Opera < 8.50 Multiple Vulnerabilities

Opera < 8.54 Multiple Vulnerabilities

Opera < 9.00 Multiple Vulnerabilities

Opera < 9.02 Multiple Vulnerabilities

Opera < 9.10 Multiple Vulnerabilities

Opera < 9.20 Multiple Vulnerabilities

Opera < 9.21 Transfer Manager Torrent File Handling Overflow

Opera < 9.22 Multiple Vulnerabilities

Opera < 9.23 Crafted Javascript Arbitrary Code Execution

Opera < 9.24 Multiple Vulnerabilities

Opera < 9.25 Multiple Vulnerabilities

Opera < 9.26 Multiple Vulnerabilities

Opera < 9.27 Multiple Vulnerabilities

Opera < 9.50 Multiple Vulnerabilities

Opera < 9.51 Multiple Vulnerabilities

Opera < 9.52 Multiple Vulnerabilities

Opera < 9.60 Multiple Vulnerabilities

Opera < 9.61 Multiple Vulnerabilities

Opera < 9.62 Multiple Vulnerabilities

Opera < 9.63 Multiple Vulnerabilities

Opera < 9.64 Multiple Vulnerabilities

Opera Browser Detection

Oracle Access Manager Unspecified Vulnerability (credentialed check, April 2014 CPU)

Oracle BI Publisher Mobile Service Unspecified Remote Information Disclosure (July 2014 CPU)

Oracle Business Intelligence Publisher Information Disclosure (Oct 2016 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (Apr 2019 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (Apr 2020 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (April 2016 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (April 2018 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (January 2016 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (January 2018 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (Jul 2016 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (Jul 2017 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (Jul 2019 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (July 2018 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (Oct 2019 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (October 2017 CPU)

Oracle Business Intelligence Publisher Multiple Vulnerabilities (October 2018 CPU)

Oracle Data Quality and Profiling Client Detection

Oracle Data Quality and Profiling Client Multiple Vulnerabilities (April 2014 CPU)

Oracle Document Capture Multiple Vulnerabilities

Oracle Forms Recognition Detection

Oracle Forms Recognition Multiple ActiveX Control Arbitrary File Overwrite Vulnerabilities

Oracle Fusion Middleware Web Services Component Remote Information Disclosure

Oracle Fusion Middleware Web Services Manager Unspecified Remote Information Disclosure

Oracle Fusion Middleware WebLogic Detection (credentialed check)

Oracle Glassfish Installed (Windows)

Oracle Installed Software Enumeration (Windows)

Oracle iPlanet Web Proxy Server 4.0 < 4.0.23 Unspecified Vulnerability

Oracle iPlanet Web Proxy Server 4.0 < 4.0.24 Multiple Vulnerabilities

Oracle iPlanet Web Proxy Server 4.0 < 4.0.25 NSS Signature Verification Vulnerability

Oracle iPlanet Web Proxy Server 4.0.x < 4.0.26 NSS Signature Handling Remote Code Injection

Oracle iPlanet Web Proxy Server 4.0.x < 4.0.27 NSS ASN.1 Decoder RCE (April 2016 CPU)

Oracle iPlanet Web Proxy Server Detection

Oracle Java File Detection for Windows

Oracle Java JDK / JRE 5 < Update 41 Remote Code Execution (Windows)

Oracle Java JDK / JRE 6 < Update 20 Multiple Vulnerabilities

Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities

Oracle Java JDK / JRE 6 < Update 35 SunToolKit getField() and getMethod() Access Issue

Oracle Java JDK / JRE 6 < Update 43 Remote Code Execution (Windows)

Oracle Java JDK / JRE 7 < Update 17 Remote Code Execution (Windows)

Oracle Java JRE Enabled (Google Chrome)

Oracle Java JRE Enabled (Internet Explorer)

Oracle Java JRE Enabled (Mozilla Firefox)

Oracle Java JRE Enabled (Opera)

Oracle Java JRE Premier Support and Extended Support Version Detection

Oracle Java JRE Universally Enabled

Oracle Java JRE Unsupported Version Detection

Oracle Java Runtime Environment (JRE) Detection

Oracle Java SE 1.7.0\_221 / 1.8.0\_211 / 1.11.0\_3 / 1.12.0\_1 Multiple Vulnerabilities (Apr 2019 CPU)

Oracle Java SE 1.7.0\_231 / 1.8.0\_221 / 1.11.0\_4 / 1.12.0\_2 Multiple Vulnerabilities (Jul 2019 CPU)

Oracle Java SE 1.7.0\_241 / 1.8.0\_231 / 1.11.0\_5 / 1.13.0\_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows)

Oracle Java SE 1.7.0\_251 / 1.8.0\_241 / 1.11.0\_6 / 1.13.0\_2 Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Java SE 1.7.0\_261 / 1.8.0\_251 / 1.11.0\_7 / 1.14.0\_1 Multiple Vulnerabilities (Apr 2020 CPU)

Oracle Java SE 1.7.x < 1.7.0\_211 / 1.8.x < 1.8.0\_201 / 1.11.x < 1.11.0\_2 Multiple Vulnerabilities (January 2019 CPU)

Oracle Java SE 7 < Update 11 Multiple Vulnerabilities

Oracle Java SE 7 < Update 7 Multiple Vulnerabilities

Oracle Java SE Hotspot JSR 292 Method Handles RCE

Oracle Java SE Installer on Windows Arbitrary Code Execution

Oracle Java SE Multiple Vulnerabilities (April 2013 CPU)

Oracle Java SE Multiple Vulnerabilities (April 2014 CPU)

Oracle Java SE Multiple Vulnerabilities (April 2015 CPU) (FREAK)

Oracle Java SE Multiple Vulnerabilities (April 2016 CPU)

Oracle Java SE Multiple Vulnerabilities (April 2017 CPU)

Oracle Java SE Multiple Vulnerabilities (April 2018 CPU)

Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)

Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)

Oracle Java SE Multiple Vulnerabilities (February 2013 CPU Update 1)

Oracle Java SE Multiple Vulnerabilities (February 2013 CPU)

Oracle Java SE Multiple Vulnerabilities (January 2014 CPU)

Oracle Java SE Multiple Vulnerabilities (January 2015 CPU) (POODLE)

Oracle Java SE Multiple Vulnerabilities (January 2016 CPU) (SLOTH)

Oracle Java SE Multiple Vulnerabilities (January 2017 CPU) (SWEET32)

Oracle Java SE Multiple Vulnerabilities (January 2018 CPU)

Oracle Java SE Multiple Vulnerabilities (July 2014 CPU)

Oracle Java SE Multiple Vulnerabilities (July 2015 CPU) (Bar Mitzvah)

Oracle Java SE Multiple Vulnerabilities (July 2016 CPU)

Oracle Java SE Multiple Vulnerabilities (July 2017 CPU)

Oracle Java SE Multiple Vulnerabilities (July 2018 CPU)

Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)

Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)

Oracle Java SE Multiple Vulnerabilities (June 2013 CPU)

Oracle Java SE Multiple Vulnerabilities (March 2010 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2010 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2011 CPU) (BEAST)

Oracle Java SE Multiple Vulnerabilities (October 2012 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2013 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2014 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2015 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2016 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2017 CPU)

Oracle Java SE Multiple Vulnerabilities (October 2018 CPU)

Oracle JInitiator beans.ocx ActiveX Multiple Buffer Overflows

Oracle JRockit Detection

Oracle JRockit JDK R28.3.19 Multiple Vulnerabilities (October 2018 CPU)

Oracle JRockit R27 < R27.7.2.5 / R28 < R28.2.3.13 Multiple Vulnerabilities (April 2012 CPU)

Oracle JRockit R27 < R27.7.3.6 / R28 < R28.2.4.14 Unspecified Vulnerability (July 2012 CPU)

Oracle JRockit R27 < R27.7.4.5 / R28 < R28.2.5.20 Multiple Vulnerabilities (October 2012 CPU)

Oracle JRockit R27 < R27.7.6 / R28 < R28.2.8 Unspecified Vulnerability (July 2013 CPU)

Oracle JRockit R27 < R27.8.2 / R28 < R28.3.2 Multiple Vulnerabilities (April 2014 CPU)

Oracle JRockit R27 < R27.8.3.9 / R28 < R28.3.3.10 Multiple Vulnerabilities (July 2014 CPU)

Oracle JRockit R27.8.3 / R28.3.3 Multiple Vulnerabilities (October 2014 CPU)

Oracle JRockit R27.8.4 / R28.3.4 Multiple Vulnerabilities (January 2015 CPU) (POODLE)

Oracle JRockit R28 < R28.3.7 Multiple Vulnerabilities (July 2015 CPU) (Bar Mitzvah) (Logjam)

Oracle JRockit R28 < R28.3.8 Multiple Vulnerabilities (October 2015 CPU)

Oracle JRockit R28 < R28.3.9 Multiple Vulnerabilities (January 2016 CPU) (SLOTH)

Oracle JRockit R28.3.10 Multiple Vulnerabilities (July 2016 CPU)

Oracle JRockit R28.3.12 Multiple Vulnerabilities (January 2017 CPU)

Oracle JRockit R28.3.13 Multiple Vulnerabilities (April 2017 CPU)

Oracle JRockit R28.3.14 Multiple Vulnerabilities (July 2017 CPU)

Oracle JRockit R28.3.15 Multiple Vulnerabilities (October 2017 CPU)

Oracle JRockit R28.3.16 Multiple Vulnerabilities (January 2018 CPU)

Oracle JRockit R28.3.17 Multiple Vulnerabilities (April 2018 CPU)

Oracle JRockit R28.3.18 Multiple Vulnerabilities (July 2018 CPU)

Oracle JRockit R28.3.5 Multiple Vulnerabilities (April 2015 CPU) (FREAK)

Oracle JRockit R28.3.9 Multiple Vulnerabilities (April 2016 CPU)

Oracle MySQL Connectors Installed (Windows)

Oracle OpenOffice.org < 3.2.1 Multiple Vulnerabilities

Oracle OpenOffice.org < 3.3 Multiple Vulnerabilities

Oracle OpenSSO Agent Detection

Oracle Siebel CRM Server Detection

Oracle Siebel Multiple Vulnerabilities (July 2014 CPU)

Oracle Siebel UI Framework CVE-2014-2468 Remote Security Vulnerability (April 2014 CPU)

Oracle VirtualBox 4.1 < 4.1.22 Task-Gate IDT Call NULL Pointer Dereference Local DoS

Oracle VirtualBox Unsupported Version Detection (Windows)

Oracle VM VirtualBox 3.x / 4.0.x < 4.0.10 Local Integer Overflows

Oracle VM VirtualBox 4.1.x < 4.1.8 Unspecified Local Issues

Oracle VM VirtualBox 5.2.x < 5.2.34 / 6.0.x < 6.0.14 (Oct 2019 CPU)

Oracle VM VirtualBox < 3.2.18 / 4.0.20 / 4.1.28 / 4.2.18 Local DoS

Oracle VM VirtualBox < 3.2.20 / 4.0.22 / 4.1.30 / 4.2.20 / 4.3.4 Multiple Vulnerabilities

Oracle VM VirtualBox < 3.2.20 / 4.0.22 / 4.1.30 / 4.2.22 / 4.3.6 Local Vulnerability

Oracle VM VirtualBox < 3.2.22 / 4.0.24 / 4.1.32 / 4.2.24 / 4.3.8 Multiple Memory Corruption

Oracle VM VirtualBox < 3.2.24 / 4.0.26 / 4.1.34 / 4.2.26 / 4.3.14 Multiple Unspecified Vulnerabilities

Oracle VM VirtualBox < 3.2.26 / 4.0.28 / 4.1.36 / 4.2.28 / 4.3.20 Multiple Vulnerabilities (January 2015 CPU)

Oracle VM VirtualBox < 3.2.28 / 4.0.30 / 4.1.38 / 4.2.30 / 4.3.28 QEMU FDC Overflow RCE (VENOM)

Oracle VM VirtualBox < 4.1.32 / 4.2.24 / 4.3.10 WDDM Graphics Driver Flaw

Oracle VM VirtualBox < 4.1.34 / 4.2.26 / 4.3.14 WDDM DoS (October 2014 CPU)

Oracle VM VirtualBox Core Subcomponent < 4.0.18 / 4.1.24 / 4.2.6 Local Issue

Oracle VM VirtualBox Detection

Oracle WebCenter Sites Apache Xalan-Java Library Security Bypass (January 2016 CPU)

Oracle WebCenter Sites Local Installation Detection

Oracle WebCenter Sites Local Vulnerability (Oct 2017 CPU)

Oracle WebCenter Sites Multiple Vulnerabilities (April 2015 CPU)

Oracle WebCenter Sites Multiple Vulnerabilities (April 2020 CPU)

Oracle WebCenter Sites Multiple Vulnerabilities (October 2012 CPU)

Oracle WebCenter Sites Multiple Vulnerabilities (October 2015 CPU)

Oracle WebCenter Sites Remote Vulnerability (April 2018 CPU)

Oracle WebCenter Sites Remote Vulnerability (April 2019 CPU)

PacketTrap pt360 TFTP Server < 1.0.3302.0 Multiple Vulnerabilities

Palo Alto Networks User-ID Agent < 7.0.4 TLS-Secured API Invocation Credential Disclosure (PAN-SA-2016-0007)

Palo Alto Networks User-ID Agent Version Detection

Panda AdminSecure Communications Agent < 4.2 Packet Handling Remote Heap Overflow

Panda AdminSecure Communications Agent < 4.50.0.10 Directory Traversal

Panda Antivirus Detection and Status

Panda Antivirus EXE File Parsing Overflow

Panda Antivirus TAR / CAB Scan Evasion

Panda Products RKPavProc.sys IOCTL Handling Vulnerabilities

Panda Security cpoint.sys Kernel Memory Corruption

Patchlink Detection

PDF-XChange Detection

PDF-XChange Viewer < 2.5 Build 208 JPEG Processing Buffer Overflow

PDF-XChange Viewer/PDF-XChange PDF File Handling Memory Corruption

Persistent Systems Radia Client Automation Agent Command Injection

PFTP Cleartext Local Password Disclosure

PGP Desktop < 9.10 Multiple Local DoS

PGP Desktop PGPserv Crafted Data Object Arbitrary Code Execution

Photo Upload Plugin ActiveX Multiple Buffer Overflows

PhotoParade Player PhPInfo ActiveX (PhPCtrl.dll) FileVersionof Property Overflow

PicoZip ZipInfo.dll Filename Handling Buffer Overflow

Pidgin < 2.10.0 Multiple Vulnerabilities

Pidgin < 2.10.1 Multiple Vulnerabilities

Pidgin < 2.10.10 Multiple Vulnerabilities

Pidgin < 2.10.2 Multiple DoS

Pidgin < 2.10.4 Multiple DoS Vulnerabilities

Pidgin < 2.10.5 mxit\_show\_message Function RX Message Inline Image Parsing Remote Overflow

Pidgin < 2.10.7 Multiple Vulnerabilities

Pidgin < 2.10.8 Multiple Vulnerabilities

Pidgin < 2.11.0 Multiple Vulnerabilities

Pidgin < 2.12.0 libpurple/util.c purple\_markup\_unescape\_entity() XML Entity Handling RCE

Pidgin < 2.5.6 Multiple Buffer Overflows

Pidgin < 2.5.9 'msn\_slplink\_process\_msg()' Memory Corruption

Pidgin < 2.6.1 Multiple Vulnerabilities

Pidgin < 2.7.10 Information Disclosure

Pidgin < 2.7.6 Multiple Vulnerabilities

Pidgin < 2.9.0 gdk\_pixbuf\_\_gif\_image\_load() Denial of Service

Pidgin Detection (Windows)

Pidgin MSN Custom Smileys Feature Emoticon Request Traversal Arbitrary File Disclosure

Pidgin OTR < 3.2.1 Format String

Pidgin OTR Plugin Detection

Pidgin X-Status NULL Pointer Denial of Service

Piriform CCleaner Cloud 1.07.3191 Backdoor

Piriform CCleaner Cloud Installed

Piriform CCleaner Installed

Plaxo Client Detection

Portrait Display SDK PdiService Insecure Privileges Local Privilege Escalation

POWER SEARCH Detection

PowerArchiver 14.02.03 Incorrect PKZIP Encryption Usage

PowerArchiver by ConeXware Installed

PowerArchiver paiso.dll ISO Image Handling Buffer Overflow

Presto! PageManager Network Group Service Packet Network Request Parsing Arbitrary File Access

Prevx Pro 2005 <= 1.0.0.1 Multiple Vulnerabilities

PrivDog Installed

ProgramChecker sasatl.dll ActiveX Control Multiple Overflows

Programmer's Notepad ctags Processing Buffer Overflow

PsExec Service Installed

PuTTY 0.52 to 0.62 Multiple Vulnerabilities

PuTTY < 0.64 Multiple Information Disclosure Vulnerabilities

PuTTY < 0.67 PSCP Server Header Handling Stack Buffer Overflow

PuTTY < 0.71 Multiple Vulnerabilities

PuTTY Detection

PuTTY Password Local Information Disclosure

QlikView < 11.20 SR1 qvw File Format Parser Integer Overflow

QlikView Installed

QLogic QConvergeConsole Installed (Windows)

Quake 3 Arena Malformed Connection Packet DoS

Quest Defender Desktop Login Component Installed

Quest Defender Desktop Login Component Unspecified Vulnerability

QuickTime < 6.1 URL Handling Overflow (Windows)

QuickTime < 6.5.1 .mov File sample-to-chunk Table Data Handling Overflow (Windows)

QuickTime < 6.5.2 PictureViewer Malformed JPEG Overflow (Windows)

QuickTime < 7.0.3 Multiple Vulnerabilities (Windows)

QuickTime < 7.0.4 Multiple Vulnerabilities (Windows)

QuickTime < 7.1 Multiple Vulnerabilities (Windows)

QuickTime < 7.1.3 Multiple Vulnerabilities (Windows)

QuickTime < 7.1.5 Multiple Vulnerabilities (Windows)

QuickTime < 7.1.6 quicktime.util.QTHandleRef toQTPointer Method Arbitrary Code Execution (Windows)

QuickTime < 7.1.6 Security Update (Windows)

QuickTime < 7.2 Multiple Vulnerabilities (Windows)

QuickTime < 7.2 Security Update (Windows)

QuickTime < 7.3 Multiple Vulnerabilities (Windows)

QuickTime < 7.3.1 Multiple Vulnerabilities (Windows)

QuickTime < 7.4 Multiple Vulnerabilities (Windows)

QuickTime < 7.4.1 RTSP Response Long Reason-Phrase Arbitrary Remote Code Execution (Windows)

QuickTime < 7.4.5 Multiple Vulnerabilities (Windows)

QuickTime < 7.5 Multiple Vulnerabilities (Windows)

QuickTime < 7.5.5 Multiple Vulnerabilities (Windows)

QuickTime < 7.6 Multiple Vulnerabilities (Windows)

QuickTime < 7.6.2 Multiple Vulnerabilities (Windows)

QuickTime < 7.6.4 Multiple Vulnerabilities (Windows)

QuickTime < 7.6.6 Multiple Vulnerabilities (Windows)

QuickTime < 7.6.7 QuickTimeStreaming.qtx SMIL File Debug Logging Overflow (Windows)

QuickTime < 7.6.8 Multiple Vulnerabilities (Windows)

QuickTime < 7.6.9 Multiple Vulnerabilities (Windows)

QuickTime < 7.7 Multiple Vulnerabilities (Windows)

QuickTime < 7.7.1 Multiple Vulnerabilities (Windows)

QuickTime < 7.7.2 Multiple Vulnerabilities (Windows)

QuickTime < 7.7.3 Multiple Vulnerabilities (Windows)

QuickTime < 7.7.4 Multiple Vulnerabilities (Windows)

QuickTime < 7.7.5 Multiple Vulnerabilities (Windows)

QuickTime < 7.7.6 Multiple Vulnerabilities (Windows)

QuickTime for Windows Detection

QuickTime RTSP URL Handler Buffer Overflow (Windows)

R-Viewer < 1.6.3768 Multiple Vulnerabilities

RADIATE Detection

RARLAB WinRAR < 5.70 Beta 1 Multiple Vulnerabilities

RARLAB WinRAR Installed (Windows)

Real Video Server Telnet Malformed Data Remote DoS

RealPage Module Upload ActiveX Control Multiple Vulnerabilities

RealPlayer / RealOne Player for Windows Multiple Vulnerabilities (2005-06-23)

RealPlayer ActiveX (ierpplug.dll) Playlist Handling Buffer Overflow

RealPlayer ActiveX (rmoc3260.dll) Console Property Memory Corruption Arbitrary Code Execution

RealPlayer Detection

RealPlayer Enterprise for Windows < Build 6.0.12.1823 Multiple Vulnerabilities

RealPlayer File Handler Arbitrary Code Execution

RealPlayer for Windows < 15.0.0 Multiple Vulnerabilities

RealPlayer for Windows < 15.0.2.71 Multiple Vulnerabilities

RealPlayer for Windows < 15.0.4.53 Multiple Vulnerabilities

RealPlayer for Windows < 15.0.6.14 Multiple Vulnerabilities

RealPlayer for Windows < 16.0.0.282 Multiple Vulnerabilities

RealPlayer for Windows < 16.0.1.18 MP4 Heap-Based Buffer Overflow

RealPlayer for Windows < 16.0.3.51 Multiple Vulnerabilities

RealPlayer for Windows < 17.0.4.61 RMP Buffer Overflow

RealPlayer for Windows < Build 12.0.0.319 Multiple Buffer Overflows

RealPlayer for Windows < Build 12.0.0.879 Multiple Vulnerabilities

RealPlayer for Windows < Build 12.0.1.609 Multiple Vulnerabilities

RealPlayer for Windows < Build 12.0.1.633 Multiple Remote Code Execution Vulnerabilities

RealPlayer for Windows < Build 12.0.1.647 Multiple Vulnerabilities

RealPlayer for Windows < Build 12.0.1.666 Multiple Vulnerabilities

RealPlayer for Windows < Build 6.0.12.1483 Multiple Vulnerabilities

RealPlayer for Windows < Build 6.0.12.1578 Multiple Vulnerabilities

RealPlayer for Windows < Build 6.0.12.1662 Multiple Vulnerabilities

RealPlayer for Windows < Build 6.0.14.806 / 6.0.12.1675 Multiple Vulnerabilities

RealPlayer for Windows <= 17.0.8.22 MP4 Multiple Memory Corruptions

RealPlayer for Windows Multiple Overflows

RealPlayer Multiple Remote Overflows

RealPlayer Multiple Remote Overflows (2005-03-01)

RealPlayer Multiple Remote Vulnerabilities (2004-09-28)

RealPlayer PNG Deflate Algorithm Heap Corruption Arbitrary Code Execution

RealPlayer Skin File Remote Buffer Overflow

Realtek HD Audio Codec Drivers Multiple Local Privilege Escalation Vulnerabilities

RealVNC VNC Viewer < 4.1.3/4.4.3 Arbitrary Command Execution

Recent File History

Recycle Bin Files

Registry Editor Last Accessed

Remote Code Execution in DiskPulse Server

Reputation of Windows Executables: Known Process(es)

Reputation of Windows Executables: Never seen process(es)

Reputation of Windows Executables: Unknown Process(es)

Retrospect Backup Server Authentication Module Password Hash Weakness (ESA-08-009)

Rhapsody Detection

Rhapsody SWF File Handling Buffer Overflow

Rhapsody vidplin.dll AVI Processing Heap Overflow Vulnerability

RoboHelp Server Help Errors Multiple Vulnerabilities (APSB08-16)

RoboHelp Server Multiple XSS (APSB09-02 Update 2)

Rocket Software UniData < 7.3 unidata72 Remote Command Execution (credentialed check)

Rocket Software UniData Detection

Rocket Software UniData/UniVerse unirpc32.dll Uni RPC Service Packet Header Remote Overflow

Rocket Software UniVerse Detection

Roxio Creator 9.x <= 9.0.136 Image Handling Integer Overflow

Roxio Creator Installed

RSA Authentication Agent 7.1.x < 7.1.2 Authentication Bypass

RSA Authentication Agent for Web for IIS 7.1.x < 7.1.2 Filter Bypass

RSA Authentication Agent for Web for IIS 8.x < 8.0.2 Multiple Vulnerabilities

RSA Authentication Agent for Web for IIS Installed

RSA Authentication Agent Installed

RSA Authentication Client 3.5 < 3.5.6 Local Authentication Bypass

RSA SecurID Software Token < 4.1.1 Insecure Library Loading

RSA SecurID Software Token Converter XML-Formatted .sdtid Buffer Overflow

RSA SecurID Software Token Installed

RSA SecurID Software Token Unsupported Version Detection

RTI Connext DDS 5.1.1.x < 5.1.1.5 / 5.2.3.x < 5.2.3.17 / 5.2.7 Multiple Vulnerabilities

RTI Connext DDS Installed

Safari < 3.1.1 Multiple Vulnerabilities

Safari < 3.1.2 Multiple Vulnerabilities

Safari < 3.2 Multiple Vulnerabilities

Safari < 3.2.2 Multiple Vulnerabilities

Safari < 3.2.3 Multiple Vulnerabilities

Safari < 4.0 Multiple Vulnerabilities

Safari < 4.0.2 Multiple Vulnerabilities

Safari < 4.0.3 Multiple Vulnerabilities

Safari < 4.0.4 Multiple Vulnerabilities

Safari < 4.0.5 Multiple Vulnerabilities

Safari < 5.0 Multiple Vulnerabilities

Safari < 5.0.1 Multiple Vulnerabilities

Safari < 5.0.2 Multiple Vulnerabilities

Safari < 5.0.3 Multiple Vulnerabilities

Safari < 5.0.4 Multiple Vulnerabilities

Safari < 5.0.5 Multiple Vulnerabilities

Safari < 5.1 Multiple Vulnerabilities

Safari < 5.1.1 Multiple Vulnerabilities

Safari < 5.1.4 Multiple Vulnerabilities

Safari < 5.1.7 Multiple Vulnerabilities

Safari Detection (Windows)

Safari Unsupported

SAHAGENT Detection

Samsung Kies < 2.5.0.12094\_27\_11 Multiple ActiveX Control Vulnerabilities

Samsung Kies SyncService ActiveX PrepareSync() Buffer Overflow

SAP GUI Detection

SAP GUI DLL Loading Arbitrary Code Execution (Note 1511179)

SAP GUI KWEdit ActiveX Control SaveDocumentAs() Insecure Method

SAP GUI Moniker Creation Multiple Vulnerabilities

SAP GUI saplogon.ini File Buffer Overflow (Note 1504547)

SAP SAPgui MDrmSap ActiveX (mdrmsap.dll) Buffer Overflow

SAP SAPgui SAPIrRfc ActiveX (sapirrfc.dll) Accept Function Overflow

SAP Sybase Adaptive Server Enterprise Authorization Bypass (SAP Note 1849356)

SAP Sybase Adaptive Server Enterprise Detection

SAP Sybase Adaptive Server Enterprise Directory Traversal (SAP Note 1893556)

SAP Sybase Adaptive Server Enterprise DoS (SAP Note 1887342)

SAP Sybase Adaptive Server Enterprise DoS (SAP Note 1893561)

SAP Sybase Adaptive Server Enterprise Information Disclosure (SAP Note 1809246)

SAP Sybase Adaptive Server Enterprise Information Disclosure (SAP Note 1887341)

SAP Sybase Adaptive Server Enterprise Information Disclosure (SAP Note 1893562)

SAP Sybase Adaptive Server Enterprise Remote Code Execution (SAP Note 1893558)

SAP Sybase Adaptive Server Enterprise Remote Code Execution (SAP Note 1893560)

SAP Sybase Adaptive Server Enterprise SQL Injection (SAP Note 1893440)

SAPlpd < 6.29 Multiple Vulnerabilities (credentialed check)

SAS Integration Technologies Client ActiveX Stack Buffer Overflow

SaveNOW Detection

Schneider Electric InduSoft Web Studio RCE (Apr 2018)

Schneider Electric InTouch Machine Edition RCE (Apr 2018)

Scientific Toolworks Understand 'wintab32.dll' DLL Loading Arbitrary Code Execution

ScriptLogic $LOGS Share Remote Information Disclosure

ScriptLogic Multiple Service Remote Privilege Escalation

SeaMonkey < 1.0 Multiple Vulnerabilities

SeaMonkey < 1.0.1 Multiple Vulnerabilities

SeaMonkey < 1.0.2 Multiple Vulnerabilities

SeaMonkey < 1.0.3 Multiple Vulnerabilities

SeaMonkey < 1.0.5 Multiple Vulnerabilities

SeaMonkey < 1.0.6 Multiple Vulnerabilities

SeaMonkey < 1.0.7 Multiple Vulnerabilities

SeaMonkey < 1.0.8 Multiple Vulnerabilities

SeaMonkey < 1.0.9 / 1.1.2 Multiple Vulnerabilities

SeaMonkey < 1.1.10 Multiple Vulnerabilities

SeaMonkey < 1.1.11 CSSValue Array Memory Corruption

SeaMonkey < 1.1.12 Multiple Vulnerabilities

SeaMonkey < 1.1.13 Multiple Vulnerabilities

SeaMonkey < 1.1.14 Multiple Vulnerabilities

SeaMonkey < 1.1.15 Multiple Vulnerabilities

SeaMonkey < 1.1.16 Multiple Vulnerabilities

SeaMonkey < 1.1.17 Multiple Vulnerabilities

SeaMonkey < 1.1.18 Multiple Vulnerabilities

SeaMonkey < 1.1.19 Multiple Vulnerabilities

SeaMonkey < 1.1.3 Multiple Vulnerabilities

SeaMonkey < 1.1.4 Multiple Vulnerabilities

SeaMonkey < 1.1.5 Multiple Vulnerabilities

SeaMonkey < 1.1.7 Multiple Vulnerabilities

SeaMonkey < 1.1.8 Multiple Vulnerabilities

SeaMonkey < 1.1.9 Multiple Vulnerabilities

SeaMonkey < 2.0 Multiple Vulnerabilities

SeaMonkey < 2.0.1 Multiple Vulnerabilities

SeaMonkey < 2.0.10 Buffer Overflow

SeaMonkey < 2.0.11 Multiple Vulnerabilities

SeaMonkey < 2.0.12 Multiple Vulnerabilities

SeaMonkey < 2.0.13 Invalid HTTP Certificates

SeaMonkey < 2.0.14 Multiple Vulnerabilities

SeaMonkey < 2.0.3 Multiple Vulnerabilities

SeaMonkey < 2.0.4 Multiple Vulnerabilities

SeaMonkey < 2.0.5 Multiple Vulnerabilities

SeaMonkey < 2.0.6 Multiple Vulnerabilities

SeaMonkey < 2.0.7 Multiple Vulnerabilities

SeaMonkey < 2.0.9 Multiple Vulnerabilities

SeaMonkey < 2.1 CSS Browser History Disclosure Vulnerability

SeaMonkey < 2.10.0 Multiple Vulnerabilities

SeaMonkey < 2.11.0 Multiple Vulnerabilities

SeaMonkey < 2.12.0 Multiple Vulnerabilities

SeaMonkey < 2.13 Multiple Vulnerabilities

SeaMonkey < 2.13.1 Multiple Vulnerabilities

SeaMonkey < 2.13.2 Multiple Vulnerabilities

SeaMonkey < 2.14 Multiple Vulnerabilities

SeaMonkey < 2.15 Multiple Vulnerabilities

SeaMonkey < 2.16 Multiple Vulnerabilities

SeaMonkey < 2.16.1 nsHTMLEditor Use-After-Free

SeaMonkey < 2.17 Multiple Vulnerabilities

SeaMonkey < 2.2.0 Multiple Vulnerabilities

SeaMonkey < 2.20 Multiple Vulnerabilities

SeaMonkey < 2.21 Multiple Vulnerabilities

SeaMonkey < 2.22 Multiple Vulnerabilities

SeaMonkey < 2.22.1 NSS and NSPR Multiple Vulnerabilities

SeaMonkey < 2.23 Multiple Vulnerabilities

SeaMonkey < 2.24 Multiple Vulnerabilities

SeaMonkey < 2.25 Multiple Vulnerabilities

SeaMonkey < 2.26 Multiple Vulnerabilities

SeaMonkey < 2.26.1 Multiple Vulnerabilities

SeaMonkey < 2.29.1 NSS Signature Verification Vulnerability

SeaMonkey < 2.3.0 Multiple Vulnerabilities

SeaMonkey < 2.3.2 Out-of-Date CA List

SeaMonkey < 2.3.3 Untrusted CA

SeaMonkey < 2.32 Vulnerability

SeaMonkey < 2.33.1 Multiple Vulnerabilities

SeaMonkey < 2.4.0 Multiple Vulnerabilities

SeaMonkey < 2.6.0 Multiple Vulnerabilities

SeaMonkey < 2.7.0 Multiple Vulnerabilities

SeaMonkey < 2.7.1 Memory Corruption

SeaMonkey < 2.7.2 'png\_decompress\_chunk' Integer Overflow

SeaMonkey < 2.8.0 Multiple Vulnerabilities

SeaMonkey < 2.9.0 Multiple Vulnerabilities

SecureCRT SSH-1 Protocol Version String Remote Overflow

SecureCRT telnet URI Arbitrary Configuration Folder Remote Command Execution

Security Update ASP .NET Core September 2017

Security Update for .NET Core (February 2019)

Security Update for .NET Core (January 2018)

Security Update for .NET Core (January 2019)

Security Update for .NET Core (January 2020)

Security Update for .NET Core (March 2018)

Security Update for .NET Core (May 2019)

Security Update for .NET Core (November 2018)

Security Update for .NET Core (October 2018)

Security Update for .NET Core (Sep 2019)

Security Update for .NET Core SDK (January 2020)

Security Update for .NET Core SDK (July 2019)

Security Update for .NET Core SDK (March 2019)

Security Update for .NET Core SDK (May 2018)

Security Update for .NET Core SDK (May 2019)

Security Update for .NET Core SDK (October 2018)

Security Update for .NET Core SDK (Sep 2019)

Security Update for ASP.NET Core (March 2018)

Security Update for ASP.NET Core (May 2018)

Security Update for ASP.NET Core January 2018

Security Update for Microsoft ASP.NET Core (DoS) (January 2019)

Security Update for Microsoft ASP.NET Core (DoS) (May 2019)

Security Update for Microsoft ASP.NET Core (January 2020)

Security Update for Microsoft ASP.NET Core (July 2019)

Security Update for Microsoft ASP.NET Core (Sep 2019)

Security Update for Microsoft Dynamics 365 (on-premises) (May 2019)

Security Update for Microsoft Identity Manager Software

Security Update for Microsoft Visual Studio Code (CVE-2019-1414)

Security Update for Microsoft Visual Studio Code (February 2019)

Security Update for Microsoft Windows Admin Center (March 2019)

Security Updates for Exchange (Jun 2018)

Security Updates for Microsoft Defender (April 2020)

Security Updates for Microsoft Dynamics 365 (on-premises) (August 2019)

Security Updates for Microsoft SQL Server (May 2019)

Security Updates for Microsoft SQL Server (Uncredentialed Check) (February 2020)

Security Updates for Microsoft SQL Server (Uncredentialed Check) (July 2019)

Security Updates for Microsoft SQL Server 2016 and 2017 x64 (August 2018) (uncredentialed check)

Security Updates for Windows Defender (April 2020)

Server Message Block (SMB) Protocol Version 1 Enabled

sethc.exe Possible Backdoor

Shibboleth 2.0 < 2.6 XMLTooling-C DTD Processing Forgery Vulnerability

Shibboleth Identity Provider Installed

Shibboleth Service Provider Installed

Shockwave Player < 11.5.0.601 Multiple Vulnerabilities (APSB09-11)

Shockwave Player < 11.5.6.606 Multiple Vulnerabilities (APSB10-03)

Shockwave Player < 11.5.7.609 Multiple Vulnerabilities (APSB10-12)

Shockwave Player < 11.5.8.612

Shockwave Player < 11.5.9.615

Shockwave Player < 11.5.9.620 (APSB11-01)

Shockwave Player < 11.6.0.626 (APSB11-17)

Shockwave Player < 11.6.1.629 Multiple Memory Corruption Vulnerabilities (APSB11-19)

Shockwave Player <= 11.5.1.601 Multiple Vulnerabilities (APSB09-16)

Shockwave Player <= 11.6.1.629 Multiple Memory Corruption Vulnerabilities (APSB11-27)

Shockwave Player <= 11.6.3.633 Multiple Code Execution Vulnerabilities (APSB12-02)

Shockwave Player <= 11.6.4.634 Multiple Memory Corruption Vulnerabilities (APSB12-13)

Shockwave Player <= 11.6.5.635 Multiple Memory Corruption Vulnerabilities (APSB12-17)

Shockwave Player <= 11.6.7.637 Multiple Vulnerabilities (APSB12-23)

Shockwave Player <= 11.6.8.638 Multiple Vulnerabilities (APSB13-06)

Shockwave Player <= 12.0.0.112 Multiple Vulnerabilities (APSB13-12)

Shockwave Player <= 12.0.2.122 Memory Corruption (APSB13-18)

Shockwave Player <= 12.0.3.133 Memory Corruption Vulnerabilities (APSB13-23)

Shockwave Player <= 12.0.6.147 Memory Corruptions (APSB13-29)

Shockwave Player <= 12.0.7.148 Multiple Memory Corruption Vulnerabilities (APSB14-06)

Shockwave Player <= 12.0.9.149 Unspecified Memory Corruption Vulnerabilities (APSB14-10)

ShockWave Player ActiveX Installer Buffer Overflow

Shockwave Player Crafted Director File Handling Remote Code Execution (APSB09-08)

Siemens Solid Edge SEListCtrlX ActiveX Control SetItemReadOnly Method Memory Address Write Arbitrary Code Execution

Siemens Solid Edge WPHelper ActiveX Control OpenInEditor Method Arbitrary Command Execution

SigPlus Pro ActiveX Control < 4.29 Multiple Vulnerabilities

SigPlus Pro ActiveX Control LCDWriteString() Method HexString Parameter Overflow

SiteKiosk < 6.5.150 Multiple Vulnerabilities

SizerOne ActiveX Control AddTab Method Remote Buffer Overflow

Skype 7.2.x / 7.35.x / 7.36.x < 7.37 MSFTEDIT.DLL RDP Session Clipboard Handling RCE

Skype < 1.4.0.84 Multiple Remote Overflows (credentialed check)

Skype < 1.4.0.84 Multiple Vulnerabilities (uncredentialed check)

Skype < 6.3.0.105 Multiple Vulnerabilities (credentialed check)

Skype Extras Manager (skypePM.exe) skype-plugin: URI Arbitrary XML File Deletion (credentialed check)

Skype Extras Manager (skypePM.exe) skype-plugin: URI Arbitrary XML File Deletion (uncredentialed check)

Skype Extras Manager Unspecified Vulnerability (uncredentialed check)

Skype file: URI Handling Security Bypass Arbitrary Code Execution (uncredentialed check)

Skype Installed

Skype skype4com URI Handler Remote Heap Corruption (uncredentialed check)

Skype skype: URI Handling /Datapath Argument Injection Settings Manipulation (credentialed check)

Skype skype: URI Handling /Datapath Argument Injection Settings Manipulation (uncredentialed check)

Skype URI Handling Arbitrary File Download (uncredentialed check)

Skype User Configuration Files

Skype Web Content Zone Multiple Field Remote Code Execution (uncredentialed check)

Slack Installed (Windows)

SmartFTP 'filename' Unspecified Vulnerability

SmartFTP Detection

SmartFTP Multiple Command Response Overflow

SMB Insecurely Configured Service

SMB Password Encryption Not Required

SMB QuickFixEngineering (QFE) Enumeration

SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks)

SMB Share Files Enumeration

SMB Shares File Enumeration (via WMI)

Snagit DLL Preloading Arbitrary Code Execution

Snagit Installed

SNMPc < 7.1.1 UDP Packet Handling Buffer Overflow

SNMPc Management Server Login Packet Remote DoS

SolarWinds DameWare Mini Remote Client Agent < 12.0.3 Stack Buffer Overflow

SolarWinds DameWare Mini Remote Control < 12.0 Hotfix 1 DWRCC.exe RCE

SolarWinds DameWare Mini Remote Control < 12.0 Hotfix 2 SSLv3 Padding Oracle On Downgraded Legacy Encryption (POODLE)

SolarWinds Dameware Mini Remote Control Client Public Key Buffer Over-read

SolarWinds DameWare Mini Remote Control Detection (credentialed check)

SolarWinds Dameware Mini Remote Control Unauthenticated RCE

SolarWinds Storage Manager < 5.7.2 Remote Code Execution

SolarWinds Storage Resource Monitor / SolarWinds Storage Manager Detection (credentialed check)

SolarWinds Storage Resource Monitor < 6.2 ProcessFileUpload.jsp File Upload RCE

SolarWinds Storage Resource Monitor Profiler < 6.2.3 Hotfix 1 RulesMetaData SQLi RCE

SolarWinds Storage Resource Monitor Profiler < 6.2.3 Multiple Vulnerabilities (Logjam) (POODLE)

SolarWinds TFTP Server < 10.4.0.13 DoS

SolarWinds TFTP Server < 10.4.0.14 DoS

SolarWinds TFTP Server Installed

SolidWorks Sldimdownload ActiveX Control Arbitrary Code Execution

Songbird Detection

SonicWALL Global VPN Client < 4.0.0.830 Format String Vulnerabilities

SonicWALL Global VPN Client Detection

SonicWALL SSL-VPN NetExtender NELaunchCtrl ActiveX Control Multiple Overflows

Sony ImageStation AxRUploadServer.AxRUploadControl ActiveX (AxRUploadServer.dll) SetLogging Method Overflow

Sony VAIO Wireless Manager ActiveX Control WifiMan.dll Multiple Buffer Overflows

Sophos Anti-Virus < 10.0.9 / 10.2.1 Multiple Vulnerabilities

Sophos Anti-Virus CAB, RAR and LZH Scanning Evasion

Sophos Anti-Virus Detection and Status

Sophos Anti-Virus Engine < 3.50.1 System Objects DoS

Sophos Anti-Virus For Windows CAB File Scan Evasion

Sophos Anti-Virus Installed (Windows)

Sophos Anti-Virus SAVOnAccessFilter Local Privilege Escalation

Sophos Anti-Virus UPX and BZIP File Multiple Vulnerabilities

Sophos PureMessage < 3.0.2 Multiple Vulnerabilities

SourceTree by Atlassian Detection

Spring Framework 4.3.x < 4.3.15 / 5.0.x < 5.0.5 Windows Directory Traversal Vulnerability (CVE-2018-1271)

Spybot Search & Destroy Detection

Spybot Search & Destroy Signature Update Check

Steam Client Installed (Windows)

StudioLine Photo Basic Detection

StudioLine Photo Basic NMSDVDXU.dll ActiveX EnableLog() Arbitrary File Overwrite

stunnel 4.21 - 4.54 Multiple Vulnerabilities

stunnel 4.46 < 5.34 Improper Level 4 Peer Certificate Validation Security Bypass

stunnel 4.4x < 4.42 Unspecified Memory Corruption

stunnel < 4.23 Local Privilege Escalation

stunnel < 5.00 PRNG State Security Weakness

stunnel < 5.01 OpenSSL Heartbeat Information Disclosure (Heartbleed)

stunnel < 5.02 OpenSSL Multiple Vulnerabilities

stunnel < 5.03 OpenSSL Multiple Vulnerabilities

stunnel < 5.06 OpenSSL Multiple Vulnerabilities (POODLE)

stunnel < 5.12 OpenSSL Multiple Vulnerabilities

stunnel < 5.14 Authentication Bypass Vulnerability

stunnel Detection

Subversion Client/Server Detection (Windows)

SumatraPDF < 2.1 Multiple Vulnerabilities

SumatraPDF Detection

Sun Java Applet Invocation Version Specification

Sun Java Enterprise Server NSS Remote Code Execution Vulnerabilities

Sun Java J2SE 1.4.2 < Update 18 Multiple Vulnerabilities

Sun Java JDK/JRE 5 < Update 16 Multiple Vulnerabilities

Sun Java JDK/JRE 6 < Update 7 Multiple Vulnerabilities

Sun Java JRE / Web Start Java Plug-in Untrusted Applet Privilege Escalation

Sun Java JRE / Web Start Multiple Vulnerabilities (103072, 103073, 103078, 103079, 103112)

Sun Java JRE Applet Handling Privilege Escalation (231261)

Sun Java JRE External XML Entities Restriction Bypass (231246)

Sun Java JRE Font Parsing Privilege Escalation (103024)

Sun Java JRE GIF Image Handling Buffer Overflow (102760)

Sun Java JRE Image Parsing Vulnerabilities (102934)

Sun Java JRE jpiexp32.dll NULL Pointer Remote DoS

Sun Java JRE Multiple Vulnerabilities (102729 / 102732)

Sun Java JRE Multiple Vulnerabilities (233321-233327)

Sun Java JRE Multiple Vulnerabilities (244986 et al)

Sun Java JRE Multiple Vulnerabilities (254569 / 254611 / 254608 ..)

Sun Java JRE Multiple Vulnerabilities (263408 / 263409 / 263428 ..)

Sun Java JRE Multiple Vulnerabilities (269868 / 269869 / 270476 ..)

Sun Java JRE Plug-in Capability Arbitrary Package Access

Sun Java JRE XML Signature Command Injection (102993)

Sun Java Media Framework (JMF) Arbitrary Code Execution

Sun Java System Application Server 8.1 / 8.2 DoS

Sun Java System Application Server Information Disclosure

Sun Java Web Start JNLP File Handling Overflow (102996)

Sun Java Web Start PersistenceService Application Traversal Arbitrary File Overwrite (102957)

Sun Java Web Start Unauthorized Access (102881)

Sun OpenOffice.org < 2.2 Multiple Vulnerabilities

Sun OpenOffice.org < 2.3 TIFF Parser Buffer Overflow Vulnerabilities

Sun OpenOffice.org < 2.3.1 Database HSQLDB Database Document Handling Arbitrary Java Code Execution

Sun OpenOffice.org < 2.4 Multiple Vulnerabilities

Sun OpenOffice.org < 3.2 Multiple Vulnerabilities

Sun OpenOffice.org RTF Parser prtdata Tag Buffer Overflow

Sun xVM VirtualBox < 1.6.4 Local Privilege Escalation

Sun xVM VirtualBox < 3.0.4 Multiple Local Denial of Service Vulnerabilities

Sun xVM VirtualBox Guest Additions < 2.0.12 / 3.0.10 Local DoS

Super Micro Detection (Windows)

SwiftView Viewer Plugin < 8.3.5 Buffer Overflow

Symantec Alert Management System 2 Multiple Vulnerabilities (SYM11-002, SYM11-003)

Symantec Alert Management System 2 RCE (SYM09-007)

Symantec Antivirus Engine 20151.1.0.32 Malformed PE Header Parser Memory Access Violation (SYM16-008)

Symantec AntiVirus Management Interface Remote Overflow (SYM06-010)

Symantec AntiVirus Multiple Vulnerabilities (SYM10-002 / SYM10-003 / SYM10-004)

Symantec AntiVirus Scan Engine Detection

Symantec Antivirus Scan Engine RAR and CAB Parsing Multiple Vulnerabilities

Symantec AntiVirus Scan Engine Web Service Administrative Interface Buffer Overflow

Symantec Antivirus Software Detection and Status

Symantec AppStream / Workspace Streaming Remote Code Execution (SYM10-008)

Symantec AppStream Client LaunchObj ActiveX Control Multiple Unsafe Methods (SYM09-001)

Symantec Backup Exec Calendar ActiveX Control Multiple Vulnerabilities (SYM08-007)

Symantec Backup Exec for Windows Multiple Vulnerabilities

Symantec Backup Exec for Windows RPC Crafted ncacn\_ip\_tcp Request Remote Overflow

Symantec Backup Exec for Windows Servers Denial of Service Vulnerabilities

Symantec Backup Exec Multiple Heap Overflow RCE (SYM06-014)

Symantec Backup Exec Server / System Recovery Installed

Symantec Backup Exec Server Multiple Vulnerabilities (SYM13-009)

Symantec Backup Exec Server Unauthorized Access (SYM11-006)

Symantec Critical System Protection 5.2.9.x < 5.2.9 MP6 Multiple Vulnerabilities (SYM15-001 / SYM16-009)

Symantec Critical System Protection 8.0 < 8.0 MP2 Authentication Bypass (SYMSA1498)

Symantec Critical System Protection for Windows Security Bypass (SYM14-008)

Symantec Critical System Protection Installed

Symantec Data Insight Detection

Symantec Decomposer Multiple Vulnerabilities (SYM08-006)

Symantec Deployment Solution AClient <= 6.9 Buffer Overflow

Symantec Deployment Solution Client Service Installed

Symantec Encryption Desktop 10.x < 10.3.2 MP3 DoS

Symantec Encryption Desktop 10.x < 10.4.1 MP2 DoS

Symantec Encryption Desktop 10.x =< 10.4.1 MP2HF1 (SYM17-010)

Symantec Encryption Desktop Detection

Symantec Encryption Desktop Installed

Symantec Encryption Desktop Local Access Elevation of Privilege Vulnerabilities

Symantec Encryption Desktop Multiple DoS Vulnerabilities

Symantec Encryption Desktop Unquoted Search Path

Symantec Endpoint Encryption 11.x < 11.1.1 Unquoted Search Path Local Privilege Escalation (SYM16-006)

Symantec Endpoint Encryption < 11.1.3 HF3 (SYM17-010)

Symantec Endpoint Encryption < 11.1.3 MP1 (SYM17-012)

Symantec Endpoint Encryption < 11.2.1 MP1 (SYMSA1478)

Symantec Endpoint Encryption Client Installed

Symantec Endpoint Protection Client 12.1.x / 14.x < 14.2 MP1 DLL Preloading Vulnerability (SYMSA1468)

Symantec Endpoint Protection Client 12.1.x / 14.x < 14.2.3332.1000 Kernel Memory Disclosure (SYMSA1479)

Symantec Endpoint Protection Client 12.1.x < 12.1 RU6 MP10 / 14.0.x < 14.0 RU1 MP1 Multiple Vulnerabilities (SYMSA1454)

Symantec Endpoint Protection Client 12.1.x < 12.1 RU6 MP5 Multiple Vulnerabilities (SYM16-010)

Symantec Endpoint Protection Client 12.1.x < 12.1 RU6 MP7 / 14.0.x < 14.0 MP1 Command Injection (SYM17-002)

Symantec Endpoint Protection Client 12.1.x < 12.1 RU6 MP7 Local Privilege Escalation (SYM17-002)

Symantec Endpoint Protection Client 12.1.x < 12.1 RU6 MP9 / 14.0.x < 14.0 RU1 Multiple Vulnerabilities (SYM17-011)

Symantec Endpoint Protection Client 12.1.x < 12.1.6 MP6 Multiple DoS (SYM16-015)

Symantec Endpoint Protection Client 12.1.x < 12.1.7454.7000 / 14.x < 14.2 Multiple Vulnerabilities (SYMSA1468)

Symantec Endpoint Protection Client 12.x < 12.1.7454.7000 / 14.x < 14.2.5323.2000 Multiple Vulnerabilities (SYMSA1488)

Symantec Endpoint Protection Client 14.x < 14.2.5569.2100 Multiple Vulnerabilities (SYMSA1505)

Symantec Endpoint Protection Client < 11.0.7.4 / 12.1.2 (SYM14-001)

Symantec Endpoint Protection Client < 12.1 RU4 MP1b (SYM14-013)

Symantec Endpoint Protection Client < 12.1 RU6 MP4 SysPlant.sys Driver RCE (SYM16-003)

Symantec Endpoint Protection Client < 22.8.0.50 Elevation of Privilege (SYM16-021)

Symantec Endpoint Protection Manager 11.x / 12.x < 12.1 RU6 MP1 Multiple Vulnerabilities (SYM15-007)

Symantec Endpoint Protection Manager 12.1.x < 12.1 RU6 MP5 Multiple Vulnerabilities (SYM16-011)

Symantec Endpoint Protection Manager 14.x < 14.2 RU2 MP1 Multiple Out-of-Bounds Read Vulnerabilities (SYMSA1505)

Symantec Endpoint Protection Manager < 11 RU7 MP2 (SYM12-007 / SYM12-008) (credentialed check)

Symantec Endpoint Protection Manager < 11.0 RU7-MP4a / 12.1 RU4a Multiple Vulnerabilities (SYM14-004)

Symantec Endpoint Protection Manager < 11.0.7.4 / 12.1.2 RU2 (SYM14-001)

Symantec Endpoint Protection Manager < 12.1 RU1 MP1 (SYM12-008) (credentialed check)

Symantec Endpoint Protection Manager < 12.1 RU3 (SYM13-005) (credentialed check)

Symantec Endpoint Protection Manager < 12.1 RU4 MP1a OpenSSL Heartbeat Information Disclosure (Heartbleed)

Symantec Endpoint Protection Manager < 12.1 RU5 Multiple Vulnerabilities (SYM14-015)

Symantec Endpoint Protection Manager < 12.1 RU6 MP3 Multiple Vulnerabilities (SYM15-011)

Symantec Endpoint Protection Manager < 12.1 RU6 MP4 Multiple Vulnerabilities (SYM16-003)

Symantec Endpoint Protection Manager < 12.1 RU6 Multiple Vulnerabilities (SYM15-005)

Symantec Endpoint Protection Manager Installed (credentialed check)

Symantec Enterprise Security Manager Unquoted Search Path (SYM12-020)

Symantec Enterprise Vault / Oracle Outside In Multiple Vulnerabilities (SYM11-011)

Symantec Enterprise Vault / Oracle Outside In Multiple Vulnerabilities (SYM12-004)

Symantec Enterprise Vault < 10.0.2 Multiple Vulnerabilities in Oracle Outside-In Libraries (SYM12-015)

Symantec Enterprise Vault Detection

Symantec Fax Viewer Control ActiveX Control AppendFax Overflow

Symantec Ghost Solution Suite Backup File Handling Memory Corruption (SYM12-016)

Symantec Ghost Solution Suite Installed

Symantec IM Manager 8.x < 8.3.14 (SYM10-005 and SYM10-006)

Symantec IM Manager < 8.4.16 Multiple SQL Injections (SYM10-010)

Symantec IM Manager < 8.4.18 Multiple Vulnerabilities (SYM11-012)

Symantec IM Manager Detection

Symantec IM Manager IMAdminSchedTask.asp Eval Code Injection Remote Code Execution (SYM11-004)

Symantec IM Manager whereClause Parameter SQL Injection (SYM10-010)

Symantec Legacy Decomposer Code Execution (SYM12-017)

Symantec LiveUpdate Administrator Insecure Permissions Local Privilege Escalation (credentialed check)

Symantec LiveUpdate Administrator Installed (credentialed check)

Symantec Mail Security Autonomy Verity Keyview Filter Vulnerabilities (SYM11-013)

Symantec Mail Security Autonomy Verity Keyview Filter Vulnerabilities (SYM12-018)

Symantec Mail Security for Domino Arbitrary Mail Relay

Symantec Mail Security for Domino Installed

Symantec Mail Security for Domino Unsupported

Symantec Mail Security for Exchange / Domino Autonomy KeyView Module Multiple Buffer Overflows

Symantec Mail Security for Exchange / Domino Decomposer Engine Multiple Vulnerabilities (SYM16-010)

Symantec Mail Security for Exchange / Domino RAR and CAB Multiple Vulnerabilities

Symantec Mail Security for Exchange and Domino Decomposer Engine Multiple DoS (SYM16-015)

Symantec Mail Security for Exchange Live Update Priviledge Escalation Vulnerability (SYMSA1488)

Symantec Mail Security for Microsoft Exchange Installed

Symantec Mail Security for Microsoft Exchange Unsupported Version Detection

Symantec Mail Security for SMTP < 5.0.1 Patch 200 Unspecified DoS

Symantec Mail Security for SMTP Autonomy KeyView Module Multiple Buffer Overflows

Symantec Mail Security for SMTP Detection

Symantec Mail Security for SMTP File Parsing Vulnerabilities

Symantec Mail Security for SMTP KeyView Excel SST Parsing RCE

Symantec Mail Security for SMTP libdayzero.dll Executable Parsing DoS

Symantec Mail Security for SMTP Message Handling Arbitrary Code Execution

Symantec Mail Security for SMTP RAR and CAB Parsing Multiple Vulnerabilities

Symantec Mail Security KeyView PRZ Processing Buffer Overflow

Symantec Management Console File Name Handling Path Traversal Remote Access (SYM17-013)

Symantec Management Console Installed

Symantec Management Console Multiple XSS and XXE Vulnerabilities (SYM17-005)

Symantec pcAnywhere awhost32 Denial of Service (SYM12-003)

Symantec pcAnywhere CHF File Pathname Format String Denial of Service

Symantec pcAnywhere Installed

Symantec pcAnywhere Launch with Windows Caller Properties Local Privilege Escalation

Symantec pcAnywhere Multiple Vulnerabilities (SYM12-002)

Symantec pcAnywhere Service Unrestricted Access

Symantec Products Intel Alert Handler Remote DoS

Symantec Protection Engine 7.0.x < 7.0.5 HF01 / 7.5.x < 7.5.3 HF03 / 7.8.x < 7.8.0 HF01 Multiple Vulnerabilities (SYM16-010)

Symantec Protection Engine 7.0.x < 7.0.5 HF02 / 7.5.x < 7.5.5 HF01 / 7.8.x < 7.8.0 HF03 Multiple DoS (SYM16-015)

Symantec Protection for SharePoint Servers 6.0.3 - 6.0.5 < HF2.5 / 6.0.6 < HF2.6 / 6.0.7 < HF2.7 Multiple DoS (SYM16-015)

Symantec Protection for SharePoint Servers 6.0.3 to 6.0.5 < HF1.5 / 6.0.6 < HF1.6 Multiple Vulnerabilities (SYM16-010)

Symantec Protection for SharePoint Servers Detection

Symantec SAVCE RTVScan Component Local Privilege Escalation (SYM07-017)

Symantec SONAR < 12.0.2 Security Bypass (SYMSA1494)

Symantec System Recovery 2011 imapi.dll Path Subversion Arbitrary DLL Injection Code Execution (SYM12-012)

Symantec Veritas Enterprise Administrator Service (vxsvc) Multiple Integer Overflows (SYM11-010)

Symantec Workspace Streaming < 7.5 SP1 XMLRPC Request Remote Code Execution (SYM14-009)

Symantec Workspace Streaming Agent Unquoted Service Path Local Privilege Escalation (SYM15-004)

Symantec Workspace Streaming Server Detection

Symantec Workspace Virtualization 6.x < 6.4.1953 Local Privilege Escalation (SYM13-011)

Symantec Workspace Virtualization Agent Detection

Synaptics SynTP.sys Driver Keylogger Vulnerability

SyncBack Profile File Remote Buffer Overflow

TeamSpeak Client 2.x < 2.0.33.7 Buffer Overflow

TeamViewer Bypass Brute-force Authentication

TeamViewer Connection Handling Remote Overflow Denial of Service

TeamViewer Exposure of Sensitive Information

TeamViewer Insecure Directory Permissions Privilege Escalation

TeamViewer Path Subversion Arbitrary DLL Injection Code Execution

TeamViewer Permissions Vulnerability (Windows)

TeamViewer Version Detection

TeamViewer Windows Service DLL Sideloading Vulnerability

Telerik UI for ASP.NET AJAX Cryptographic Weakness

Telerik UI for ASP.NET AJAX Installed

Telerik UI for ASP.NET AJAX RadAsyncUpload Multiple Vulnerabilities

Tenable Log Correlation Engine (LCE) Windows Client Installed (credentialed check)

Tenable Log Correlation Engine Windows Client Unsupported Version Detection

Tenable Nessus 6.8.x < 6.10.2 Arbitrary File Upload (TNS-2017-06)

Tenable Nessus < 7.0.3 Sub-directory Missing Secure Permission Local Privilege Escalation (TNS-2018-01)

Tenable Passive Vulnerability Scanner Installed (Windows) (credentialed check)

Tenable Windows Nessus Agent Installed

Terminal Services History

TestDirector (TD) for Mercury Quality Center SPIDERLib.Loader ActiveX Control (Spider90.ocx) ProgColor Property Overflow

Tftpd32 GET/PUT Command File Name Handling Overflow

TheGreenBow VPN Client TGB File OpenScriptAfterUp Parameter Local Overflow

ThinkVantage System Update < 3.14 SSL Certificate Issuer Spoofing

TightVNC Viewer < 1.3.10 Multiple Integer Overflows

Timbuktu Pro < 8.6.5 Multiple Vulnerabilities

Timbuktu Pro < 8.6.7 PlughNTCommand Named Pipe Remote Stack Buffer Overflow

Tom Sawyer Software GET Extension Factory COM Object Instantiation Memory Corruption

TOM-Skype Detection

Total Commander Detection

Total Commander FTP Client Traversal Arbitrary File Overwrite

Trend Micro Antivirus Detection and Status

Trend Micro Apex One Server Installed (Windows)

Trend Micro Control Manager 6.x < 6.0 SP3 Hotfix 3328 Multiple Vulnerabilities

Trend Micro Control Manager AdHocQuery\_Processor.aspx id Parameter SQL Injection

Trend Micro Control Manager CasLogDirectInsertHandler.cs Remote Code Execution

Trend Micro Control Manager CmdProcessor.exe Remote Buffer Overflow

Trend Micro Control Manager Detection

Trend Micro Control Manager mrf.exe Stack Overflow

Trend Micro Deep Security Agent Installed (Windows)

Trend Micro Deep Security Manager Installed (Windows)

Trend Micro DirectPass < 1.6.0.1015 Multiple Vulnerabilities

Trend Micro Internet Security Pro UfProxyBrowserCtrl ActiveX extSetOwner Function Arbitrary Code Execution

Trend Micro InterScan Web Security Suite < 3.1 Build 1237 Multiple Flaws

Trend Micro InterScan Web Security Virtual Appliance (IWSVA) Information Disclosure Vulnerability (1122250)

Trend Micro Malware Sample Detection Bypass Vulnerability (1118797)

Trend Micro Multiple Products TmComm.sys IOCTL Handler Local Privilege Escalation

Trend Micro Multiple Products Token Prediction Security Bypass

Trend Micro OfficeScan 'cgiRecvFile.exe' ComputerName Parameter Buffer Overflow

Trend Micro OfficeScan cgiShowClientAdm Remote Memory Corruption

Trend Micro OfficeScan Client Firewall Multiple Vulnerabilities

Trend Micro OfficeScan Directory Traversal Vulnerability (000151730)

Trend Micro OfficeScan Directory Traversal Vulnerability (1122250)

Trend Micro OfficeScan HTTP Request Remote Buffer Overflow

Trend Micro OfficeScan Multiple CGI Module Vulnerabilities

Trend Micro OfficeScan Multiple Vulnerabilities (000245571)

Trend Micro OfficeScan OfficeScanSetupINI.dll Remote Buffer Overflow

Trend Micro OfficeScan tmlisten.exe Malformed Data Remote DoS

Trend Micro OfficeScan TMTDI Module Local Privilege Escalation

Trend Micro OfficeScan Web Interface Detection

Trend Micro Scan Engine Tmxpflt.sys Buffer Overflow

Trend Micro ScanMail for Exchange 10.2 < Build 3318 / 11.x < Build 4180 Predictable Session IDs

Trend Micro ScanMail for Exchange 12.x < SP1 Patch 1 CP1755

Trend Micro ScanMail for Exchange Installation Detection

Trend Micro ServerProtect AgRpcCln.dll Buffer Overflow

Trend Micro ServerProtect Detection and Status (credentialed check)

Trend Micro ServerProtect EarthAgent RPC Request Remote Buffer Overflow

Trend Micro ServerProtect for Windows (SpntSvc.exe) StRpcSrv.dll Arbitrary Remote Code Execution

Trend Micro ServerProtect Multiple Remote Overflows

Trend Micro Titanium Security 8.x < 8.0.2063 / 10.x < 10.0.1265 Multiple Vulnerabilities

Trend Micro UPX File Parsing Overflow

Trend Micro VSAPI ARJ Handling Heap Overflow

Trend Micro VsapiNT.sys UPX File Parsing DoS

Trend Micro Worry-Free Business Security (WFBS) Directory Traversal Vulnerability (1122250)

Trend Micro Worry-Free Business Security (WFBS) Multiple Vulnerabilities (1114098)

Trend Micro Worry-Free Business Security Advanced Server Installed (Windows)

TRENDnet SecurView UltraMJCam ActiveX Control OpenFileDlg Method WideCharToMultiByte() Call Remote Overflow

Trillian < 3.1.10.0 Multiple Vulnerabilities

Trillian < 3.1.12.0 Multiple Vulnerabilities

Trillian < 3.1.5.1 Multiple Vulnerabilities

Trillian < 3.1.5.1 XMPP Decoding Heap Overflow

Trillian < 3.1.6.0 Multiple Vulnerabilities

Trillian aim:// URI Handler Vulnerabilities

Trillian Detection

Trillian DirectIM Packet Remote Overflow

Trillian MSN Overflow

Trillian Multiple HTTP Responses Buffer Overflow Vulnerabilities

Tumbleweed SecureTransport vcst\_eu.dll ActiveX Control Buffer Overflows

Ubisoft uPlay < 2.0.4 Browser Plugin RCE

Ubisoft uPlay Detection

UltraVNC Viewer < 1.0.5.4 Multiple Integer Overflows

Unisys Business Information Server Stack Overflow

Unsupported Windows OS (remote)

Untrusted Microsoft Office Macro Execution Enabled

UPnP TCP Helper Detection

USB Device Wireless Key Injection or DoS (MouseJack)

USB Drives Enumeration (WMI)

User Download Folder Files

User Shell Folders Settings

UserAssist Execution History

VeriSign ConfigChk ActiveX Control (VSCnfChk.dll) Buffer Overflow

Veritas Backup Exec Agent Browser 8.x < 8.60.3878 HF 68 / 9.0.x < 9.0.4454 HF 30 / 9.1.x < 9.1.4691 HF 40 RCE

VERITAS Backup Exec Agent for Windows CONNECT\_CLIENT\_AUTH Remote Overflow

Veritas Backup Exec Remote Agent 14.1.x < 14.1.1786.1126 / 14.2.x < 14.2.1180.3160 / 16.0.x < 16.0.1142.1327 Use-after-free RCE (VTS17-006)

Veritas Backup Exec Remote Agent Installed

Veritas NetBackup 7.7.x / 8.0.x Multiple Vulnerabilities (VTS17-004)

Veritas NetBackup 7.x < 7.7.2 Multiple Vulnerabilities (VTS16-001)

Veritas NetBackup Installed

VERITAS NetBackup Volume Manager Daemon Buffer Overflow

VERITAS Storage Foundation NULL NTLMSSP Authentication Bypass (SYM08-015)

Virus Infection Detection (deprecated)

Viscosity VPN Client Detection

VisiWave Site Survey Report VWR File Handling Overflow

Visnetic AntiVirus Plug-in for MailServer Local Privilege Escalation

VLC 2.x < 2.1.2 parseRTSPRequestString Function RTSP Command Parsing Overflow

VLC 3.0.x < 3.0.2 Heap Use-After-Free / Remote Code Execution Vulnerability

VLC < 2.0.5 Multiple Vulnerabilities

VLC < 2.0.6 ASF Demuxer Buffer Overflow

VLC < 2.0.7 Multiple Vulnerabilities

VLC < 2.0.9 Buffer Overflow

VLC < 3.0.7 Multiple Vulnerabilities

VLC < 3.0.8 Multiple Vulnerabilities

VLC Detection

VLC get\_chunk\_header Function TiVo File Remote Code Execution

VLC Media Player 0.5.0 to 0.9.5 Stack-Based Buffer Overflows

VLC Media Player 0.5.0 to 1.1.10 Multiple Buffer Overflows

VLC Media Player 0.9.x < 0.9.8a RealMedia Processing Remote Integer Overflow

VLC Media Player < 0.8.6f Multiple Vulnerabilities

VLC Media Player < 0.8.6h Multiple Vulnerabilities

VLC Media Player < 0.8.6i WAV File Handling Integer Overflow

VLC Media Player < 0.9.3 XSPF Playlist Handling Memory Corruption

VLC Media Player < 1.0.1 real\_get\_rdt\_chunk() Function Overflow

VLC Media Player < 1.0.2 Multiple Remote Buffer Overflows

VLC Media Player < 1.0.6 Multiple Vulnerabilities

VLC Media Player < 1.1.4 Path Subversion Arbitrary DLL Injection Code Execution

VLC Media Player < 1.1.5 Buffer Overflow

VLC Media Player < 1.1.6 Multiple Vulnerabilities

VLC Media Player < 1.1.7 MKV Input Validation Vulnerability

VLC Media Player < 1.1.8 Multiple Buffer Overflows

VLC Media Player < 1.1.9 Multiple Vulnerabilities

VLC Media Player < 2.0.1 Multiple Vulnerabilities

VLC Media Player < 2.0.2 Ogg\_DecodePacket Function OGG File Handling Overflow

VLC Media Player < 2.1.5 Multiple Vulnerabilities

VLC Media Player < 2.2.5 Multiple Vulnerabilities

VLC Media Player < 2.2.7 Overflow Condition

VLC Media Player <= 2.2.8 Use-After-Free RCE

VLC Media Player XSPF Playlist Integer Overflow

VMnc Media Codec Multiple Heap Overflows (VMSA-2009-0012)

VMSA-2010-0012 : VMware vCenter Update Manager Fix for Jetty Web Server

VMware ACE detection (Windows)

VMware Carbon Black Cloud Endpoint Standard Installed (Windows)

VMware Horizon View 6.x < 6.2.4 / 7.x < 7.1.0 Unspecified Buffer Overflow RCE (VMSA-2017-0008)

VMware Horizon View 6.x < 6.2.8 / 7.x (CR) < 7.8.0 / 7.5.x (ESB) < 7.5.2 Information Disclosure (VMSA-2019-0003)

VMware Horizon View Agent 6.x < 6.2.7 / 7.x < 7.5.1 Local Information Disclosure Vulnerability (VMSA-2018-0019)

VMware Horizon View Agent 7.x < 7.5.1 Local Information Disclosure Vulnerability (VMSA-2018-0018)

VMware Horizon View Agent 7.x < 7.5.4 / 7.10.1 / 7.11.0 Privilege Escalation (VMSA-2019-0023)

VMware Horizon View Client 3.2.x < 3.2.1 / 3.3.x < 3.4.0 / or 5.x < 5.4.2 Multiple Vulnerabilities (VMSA-2015-0004)

VMware Horizon View Client 4.x < 4.4.0 Multiple Vulnerabilities (VMSA-2017-0008)

VMware Horizon View Client 4.x < 4.6.1 Multiple Vulnerabilities (VMSA-2017-0018)

VMware Horizon View Client 4.x < 4.7.0 Multiple Vulnerabilities (VMSA-2018-0003)

VMware Horizon View Client 4.x < 4.8.1 Information Disclosure Vulnerability (VMSA-2018-0019)

VMware Horizon View Client 5.x < 5.4.2 DACL Privilege Escalation (VMSA-2015-0005)

VMware Horizon View Client < 3.0.0 Multiple SSL Vulnerabilities (VMSA-2014-0006)

VMware Horizon View Client Detection

VMware Horizon View Client Detection (Linux)

VMware Horizon View Directory Traversal File Disclosure (VMSA-2016-0015)

VMware Horizon View Installed

VMware Horizon View Multiple Vulnerabilities (VMSA-2014-0006)

VMware Horizon View Multiple Vulnerabilities (VMSA-2015-0003) (VMSA-2015-0008) (POODLE)

VMware Movie Decoder < 9.0 Path Subversion Arbitrary DLL Injection Code Execution (VMSA-2012-0014)

VMware Movie Decoder Installed

VMware OVF Tool 2.1 File Handling Format String Vulnerability (VMSA-2012-0015)

VMware OVF Tool 3.x < 3.5.2 Multiple OpenSSL Vulnerabilities (VMSA-2014-0006)

VMware OVF Tool Installed

VMware Player 12.1.x < 12.1.1 Shared Folders (HGFS) Guest DLL Hijacking Arbitrary Code Execution (VMSA-2016-0010)

VMware Player 12.x < 12.5.2 Drag-and-Drop Feature Arbitrary Code Execution (VMSA-2016-0019)

VMware Player 12.x < 12.5.4 Drag-and-Drop Feature Guest-to-Host Code Execution (VMSA-2017-0005)

VMware Player 12.x < 12.5.8 Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre)

VMware Player 12.x < 12.5.9 / 14.x < 14.1.1 Multiple Vulnerabilities (VMSA-2018-0004) (VMSA-2018-0005) (Spectre)

VMware Player 14.x < 14.1.2 Multiple DoS (VMSA-2018-0013)

VMware Player 14.x < 14.1.3 Out-of-Bounds Write (VMSA-2018-022)

VMware Player 4.x < 4.0.5 Multiple Vulnerabilities (VMSA-2012-0015)

VMware Player 5.x < 5.0.1 VMX Process DoS (VMSA-2014-0001)

VMware Player 5.x < 5.0.3 LGTOSYNC.SYS Guest Privilege Escalation (VMSA-2013-0014)

VMware Player 6.x < 6.0.2 OpenSSL Library Multiple Vulnerabilities (VMSA-2014-0004) (Heartbleed)

VMware Player 6.x < 6.0.2 Windows 8.1 Guest Privilege Escalation (VMSA-2014-0005)

VMware Player 6.x < 6.0.5 Multiple Vulnerabilities (VMSA-2015-0001) (Windows)

VMware Player 6.x < 6.0.6 Multiple Vulnerabilities (VMSA-2015-0004)

VMware Player 6.x < 6.0.7 / 7.x < 7.1.1 DACL Privilege Escalation (VMSA-2015-0005)

VMware Player 7.x < 7.1.1 Multiple Vulnerabilities (VMSA-2015-0004)

VMware Player 7.x < 7.1.2 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001)

VMware Player 7.x < 7.1.3 Host Privilege Escalation (VMSA-2016-0005)

VMware Player < 5.0.4 / 6.0.3 OpenSSL Library Multiple Vulnerabilities (Windows)

VMware Player detection (Windows)

VMware Player Local Privilege Escalation (VMSA-2012-0007)

VMware Player Multiple Vulnerabilities (VMSA-2012-0009)

VMware Player Multiple Vulnerabilities (VMSA-2012-0011)

VMware Products Local Privilege Escalation (VMSA-2012-0007)

VMware Products Multiple Vulnerabilities (VMSA-2008-0005)

VMware Products Multiple Vulnerabilities (VMSA-2008-0008)

VMware Products Multiple Vulnerabilities (VMSA-2008-0009)

VMware Products Multiple Vulnerabilities (VMSA-2008-0014)

VMware Products Multiple Vulnerabilities (VMSA-2008-0018/VMSA-2008-0019)

VMware Products Multiple Vulnerabilities (VMSA-2009-0005/VMSA-2009-0007)

VMware Products Multiple Vulnerabilities (VMSA-2010-0007)

VMware Products Multiple Vulnerabilities (VMSA-2010-0018)

VMware Products Multiple Vulnerabilities (VMSA-2011-0009)

VMware Products Privilege Escalation Vulnerability (VMSA-2009-0015)

VMware Server Detection (Windows)

VMware Tools 10.2.x / 10.3.x < 10.3.10 Information Disclosure / Denial of Service Vulnerability (VMSA-2019-0009)

VMware Tools 10.x < 10.2.0 Multiple Vulnerabilities (VMSA-2018-0003)

VMware Tools 10.x < 10.3.0 Multiple Vulnerabilities (VMSA-2018-0017)

VMware Tools 10.x < 11.0.0 Privilege Escalation (VMSA-2020-0002)

VMware Tools Detection

VMware vCenter Chargeback Manager Installed

VMware vCenter Chargeback Manager Multiple Java Vulnerabilities (VMSA-2015-0003) (POODLE)

VMware vCenter Chargeback Manager Multiple OpenSSL Vulnerabilities (VMSA-2014-0006)

VMware vCenter Chargeback Manager Remote Code Execution (VMSA-2013-0008)

VMware vCenter Converter 5.1.x < 5.1.2 / 5.5.x < 5.5.3 Multiple Vulnerabilities (VMSA-2014-0010) (Shellshock)

VMware vCenter Converter Installed

VMware vCenter Converter Multiple Vulnerabilities (VMSA-2014-0006)

VMware vCenter Operations Manager Installed (Windows)

VMware vCenter Orchestrator Installed

VMware vCenter Update Manager Detection (credentialed check)

VMware vCenter Update Manager Multiple Java Vulnerabilities (VMSA-2014-0008)

VMware vCenter Update Manager Multiple Java Vulnerabilities (VMSA-2014-0012)

VMware vCenter Update Manager Multiple Vulnerabilities (VMSA-2012-0013)

VMware vCenter Update Manager Multiple Vulnerabilities (VMSA-2014-0006)

VMware View 4.x < 4.6.2 / 5.x < 5.1.2 VMCI Privilege Escalation (VMSA-2013-0002)

VMware View Agent Detection

VMware View Multiple Vulnerabilities (VMSA-2012-0004)

VMware View Server Detection

VMware View Server Directory Traversal Vulnerability (VMSA-2012-0017)

VMware View Server Unsupported Version Detection

VMware VIX API Multiple Buffer Overflow Vulnerabilities

VMware vmnat.exe/vmnet-natd Multiple FTP Command Remote Overflow

VMware vRealize Operations for Horizon Adapter Multiple Vulerabilities (VMSA-2020-0003)

VMware vRealize Operations for Horizon Desktop Agent 6.x < 6.5.1 Privilege Escalation Vulnerability (VMSA-2018-0003)

VMware vRealize Operations for Horizon Desktop Agent Installed (Windows)

VMware vRealize Operations for Published Applications Desktop Agent 6.x < 6.5.1 Privilege Escalation Vulnerability (VMSA-2018-0003)

VMware vRealize Operations for Published Applications Desktop Agent Installed (Windows)

VMware vSphere Client Installed

VMware vSphere Client Memory Corruption (VMSA-2013-0001)

VMware vSphere Client Multiple Vulnerabilities (VMSA-2014-0003)

VMware vSphere Client Multiple Vulnerabilities (VMSA-2014-0006)

VMware vSphere Client XXE Injection Information Disclosure (VMSA-2016-0022)

VMware vSphere Update Manager Java Vulnerability (VMSA-2015-0003)

VMware Workstation 10.x < 10.0.2 OpenSSL Library Multiple Vulnerabilities (VMSA-2014-0004) (Heartbleed)

VMware Workstation 10.x < 10.0.2 Windows 8.1 Guest Privilege Escalation (VMSA-2014-0005)

VMware Workstation 10.x < 10.0.5 Multiple Vulnerabilities (VMSA-2015-0001 / VMSA-2015-0004) (Windows)

VMware Workstation 10.x < 10.0.6 / 11.x < 11.1.1 Multiple Vulnerabilities (VMSA-2015-0004) (Windows)

VMware Workstation 10.x < 10.0.7 / 11.x < 11.1.1 DACL Privilege Escalation (VMSA-2015-0005)

VMware Workstation 11.x < 11.1.2 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001)

VMware Workstation 11.x < 11.1.3 Host Privilege Escalation (VMSA-2016-0005)

VMware Workstation 12.1.x < 12.1.1 Shared Folders (HGFS) Guest DLL Hijacking Arbitrary Code Execution (VMSA-2016-0010)

VMware Workstation 12.x / 14.x < 14.1.0 Multiple Vulnerabilities (VMSA-2018-0003)

VMware Workstation 12.x < 12.5.0 Multiple Vulnerabilities (VMSA-2016-0014)

VMware Workstation 12.x < 12.5.2 Drag-and-Drop Feature Arbitrary Code Execution (VMSA-2016-0019)

VMware Workstation 12.x < 12.5.3 Multiple Vulnerabilities (VMSA-2017-0003)

VMware Workstation 12.x < 12.5.3 Multiple Vulnerabilities (VMSA-2017-0008)

VMware Workstation 12.x < 12.5.4 Drag-and-Drop Feature Guest-to-Host Code Execution (VMSA-2017-0005)

VMware Workstation 12.x < 12.5.5 Multiple Vulnerabilities (VMSA-2017-0006)

VMware Workstation 12.x < 12.5.6 vstor2 Driver NULL Pointer Dereference DoS (VMSA-2017-0009)

VMware Workstation 12.x < 12.5.7 Multiple Vulnerabilities (VMSA-2017-0015)

VMware Workstation 12.x < 12.5.8 Multiple Vulnerabilities (VMSA-2017-0018)

VMware Workstation 12.x < 12.5.8 Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre)

VMware Workstation 12.x < 12.5.9 / 14.x < 14.1.1 Multiple Vulnerabilities (VMSA-2018-0004) (VMSA-2018-0005) (Spectre)

VMware Workstation 14.0.x < 14.1.6 / 15.0.x < 15.0.3 Pixel Shader out-of-bounds read/write vulnerabilities (VMSA-2019-0012)

VMware Workstation 14.x < 14.1.2 Multiple DoS (VMSA-2018-0013)

VMware Workstation 14.x < 14.1.3 Out-of-Bounds Read Vulnerability (VMSA-2018-0026)

VMware Workstation 14.x < 14.1.3 Out-of-Bounds Write (VMSA-2018-0022)

VMware Workstation 14.x < 14.1.3 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020)

VMware Workstation 15.0.x < 15.5.1 Multiple Vulnerabilities (VMSA-2019-0020, VMSA-2019-0021)

VMware Workstation 15.0.x < 15.5.2 Multiple Vulnerabilities (VMSA-2020-0004)

VMware Workstation 15.x < 15.1.0 DLL-hijacking Vulnerability (VMSA-2019-0007)

VMware Workstation 8.x < 8.0.5 / 9.x < 9.0.1 VMCI Privilege Escalation (VMSA-2013-0002)

VMware Workstation 8.x < 8.0.5 Multiple Vulnerabilities (VMSA-2012-0015)

VMware Workstation 9.x < 9.0.1 VMX Process DoS (VMSA-2014-0001)

VMware Workstation < 5.5.4 Build 44386 Multiple Vulnerabilities

VMware Workstation < 5.5.5 and Server < 1.0.4 Multiple Vulnerabilities

VMware Workstation < 9.0.4 / 10.0.3 OpenSSL Library Multiple Vulnerabilities (Windows)

VMware Workstation Detection

VMware Workstation Multiple Vulnerabilities (VMSA-2012-0009)

VMware Workstation Multiple Vulnerabilities (VMSA-2012-0011)

Web3000 Detection

WebEx Downloader ActiveX Control Command Injection

WebEx Meeting Manager WebexUCFObject ActiveX Control Buffer Overflow

WEBGATE ActiveX Controls Multiple Buffer Overflows

WebGate Webeye ActiveX Control Stack Based Buffer Overflow Vulnerability

WEBHANCER Detection

Webroot SpySweeper Enterprise Detection

Websense Email Security < 7.1 Hotfix 4

Websense Email Security Heartbeat Information Disclosure (Heartbleed)

Websense Email Security Installed

Websense Email Security SMTP Component Weak SSL/TLS Ciphers

Websense Triton 7.1.x < 7.1.3 / 7.5.x < 7.5.3 / 7.6.0 < 7.6.1 / 7.6.2 < 7.6.3 Remote Command Execution

Websense Triton 7.7.3 < 7.7.3 Hotfix 31 Information Disclosure

Websense TRITON 7.8 Multiple Vulnerabilities

Websense TRITON Installed

Websense Web Security Heartbeat Information Disclosure (Heartbleed)

WebWasher Remote ARJ Decoder Malformed Archive Handling DoS

WibuKey Runtime ActiveX Control DisplayMessageDialog Method String Parsing Overflow

WILDTANGENT detection

Winamp < 3.0b Multiple File Handling DoS

Winamp < 5.0.5 Skin File (.WSZ) Local Zone Arbitrary Code Execution

Winamp < 5.0.7 Multiple File Handling DoS

Winamp < 5.0.8c Multiple Unspecified Vulnerabilities

Winamp < 5.03 Filename Handler Local Buffer Overflow

Winamp < 5.07 IN\_CDDA.dll m3u Playlist Processing Overflow

Winamp < 5.093 Malformed ID3v2 Tag Handling Buffer Overflow

Winamp < 5.13 Playlist Handling Multiple Overflows

Winamp < 5.2 Multiple Vulnerabilities

Winamp < 5.22 Malformed Midi File Handling Buffer Overflow

Winamp < 5.24 in\_midi.dll MIDI File Processing Overflow

Winamp < 5.31 Multiple Buffer Overflows

Winamp < 5.34 Multiple Vulnerabilities

Winamp < 5.35 MP4 File Handling Buffer Overflow

Winamp < 5.5 FLAC Plug-in Multiple Buffer Overflows

Winamp < 5.52 Ultravox Streaming Metadata in\_mp3.dll Multiple Tag Overflow

Winamp < 5.541 NowPlaying Feature Metadata XSS

Winamp < 5.55 AIFF File Handling Overflow

Winamp < 5.552 Modern Skins Support Module (gen\_ff.dll) MAKI File Handling Overflow

Winamp < 5.57 Multiple Vulnerabilities

Winamp < 5.58 Buffer Overflow

Winamp < 5.59 build 3033 Multiple Vulnerabilities

Winamp < 5.6 Multiple Vulnerabilities

Winamp < 5.601 MIDI Timestamp Stack-based Buffer Overflow

Winamp < 5.622 Multiple Vulnerabilities

Winamp < 5.623 Multiple Integer Overflows

Winamp < 5.63 Multiple Vulnerabilities

Winamp < 5.64 Multiple Vulnerabilities

Winamp < 5.666 Multiple Memory Corruptions

Windows Admin Center Installed

Windows AppLocker Installed

Windows AutoRuns JavaScript MSHTML

Windows ComputerSystemProduct Enumeration (WMI)

Windows Credential Guard Disabled

Windows Defender Advanced Threat Protection Installed (Windows)

Windows Defender Antimalware/Antivirus Signature Definition Check

Windows Defender Installed

Windows Deployment Services TFTP Server Remote Code Execution Vulnerability

Windows Display Driver Enumeration

Windows DNS Server Enumeration

Windows Explorer Recently Executed Programs

Windows Explorer Typed Paths

Windows Flamer / Skywiper Malware Detection

Windows Live OneCare Unsupported Application Detection

Windows Management Instrumentation (WMI) Available

Windows Mapped Network Drives

Windows NetBIOS / SMB Remote Host Information Disclosure

Windows NetBIOS / SMB Remote Host Report Tag

Windows NetBIOS Remote Host Information Disclosure

Windows OS Not Activated (WMI)

Windows OS Partial Product Key (WMI)

Windows Prefetch Folder

Windows Product Key Retrieval

Windows Server 2008 Critical RCE Vulnerabilities (uncredentialed) (PCI/DSS)

Windows Service Pack Out-of-Date

Windows Speculative Execution Configuration Check

Windows Store Application Enumeration

Windows Terminal Services Enabled

Windows Wireless SSID (WMI)

Windows XP SP2 Firewall Critical Update (886185)

WinGate DNS Compressed Name Pointer DoS

WinGate IMAP Server Directory Traversal Vulnerabilities

WinGate Invalid SMTP State Format String DoS

WinGate Passwordless Default Installation

WinGate POST Request Buffer Overflow

WinGate Proxy POP3 USER Overflow

WinGate Telnet Proxy localhost Connection Saturation DoS

WinPcap NPF.SYS bpf\_filter\_init Arbitrary Array Indexing Local Privilege Escalation

WinPcap NPF.SYS Local Privilege Escalation

WinProxy < 6.1a Telnet Proxy Remote DoS

WinProxy < 6.1r1c HTTP CONNECT Request Remote Overflow

WinRAR < 3.71 Archive Handling Vulnerabilities

WinRAR History

WinRAR LHA Filename Handling Buffer Overflows

WinSCP 5.x < 5.5.4 Multiple Vulnerabilities

WinSCP 5.x < 5.5.5 Multiple Vulnerabilities

WinSCP < 5.1.6 RSA Signature Blob Integer Overflow

WinSCP < 5.1.7 Multiple Vulnerabilities

WinSCP Heartbeat Information Disclosure (Heartbleed)

WinSCP History

WinSCP Installed

WinSCP URI Handler Arbitrary File Access

WinSCP URL Protocol Handler Arbitrary File Transfer

WinSyslog Long Syslog Message Remote DoS

WinZip 11.x 'gdiplus.dll' Unspecified Vulnerability

WinZip <= 9.0 Multiple Unspecified Overflows

WinZip FileView ActiveX Control Vulnerabilities

WinZip Installed

WinZip Unsupported Version Detection

Wireshark / Ethereal 0.9.0 to 1.2.4 Multiple Vulnerabilities

Wireshark / Ethereal 0.9.2 to 1.0.9 Multiple Vulnerabilities

Wireshark / Ethereal 0.9.2 to 1.2.0 Multiple Vulnerabilities

Wireshark / Ethereal 0.9.6 to 1.2.1 Multiple Vulnerabilities

Wireshark / Ethereal 0.99.2 to 1.0.6 Multiple Vulnerabilities

Wireshark / Ethereal 0.99.6 to 1.0.5 Multiple Denial of Service Vulnerabilities

Wireshark / Ethereal < 1.0.14 / 1.2.9 Multiple Vulnerabilities

Wireshark / Ethereal < 1.0.15 / 1.2.10 Multiple Vulnerabilities

Wireshark / Ethereal < 1.0.3 Multiple Vulnerabilities

Wireshark / Ethereal < 1.2.11 / 1.0.16 Path Subversion Arbitrary DLL Injection Code Execution

Wireshark / Ethereal Detection (Windows)

Wireshark / Ethereal Dissector LWRES Multiple Buffer Overflows

Wireshark 1.10.x < 1.10.1 Multiple Vulnerabilities

Wireshark 1.10.x < 1.10.10 Multiple DoS Vulnerabilities

Wireshark 1.10.x < 1.10.11 Multiple DoS Vulnerabilities

Wireshark 1.10.x < 1.10.12 / 1.12.x < 1.12.3 Multiple DoS Vulnerabilities

Wireshark 1.10.x < 1.10.13 / 1.12.x < 1.12.4 Multiple DoS Vulnerabilities

Wireshark 1.10.x < 1.10.14 / 1.12.x < 1.12.5 Multiple DoS Vulnerabilities

Wireshark 1.10.x < 1.10.2 Multiple DoS

Wireshark 1.10.x < 1.10.3 Multiple DoS Vulnerabilities

Wireshark 1.10.x < 1.10.4 Multiple DoS

Wireshark 1.10.x < 1.10.6 Multiple Vulnerabilities

Wireshark 1.10.x < 1.10.7 DoS

Wireshark 1.10.x < 1.10.8 Metadissector DoS

Wireshark 1.10.x < 1.10.9 Multiple DoS Vulnerabilities

Wireshark 1.12.x < 1.12.1 Multiple DoS Vulnerabilities

Wireshark 1.12.x < 1.12.10 Multiple Vulnerabilities

Wireshark 1.12.x < 1.12.11 Multiple DoS

Wireshark 1.12.x < 1.12.12 Multiple DoS

Wireshark 1.12.x < 1.12.13 Multiple DoS

Wireshark 1.12.x < 1.12.2 Multiple DoS Vulnerabilities

Wireshark 1.12.x < 1.12.6 Multiple DoS Vulnerabilities

Wireshark 1.12.x < 1.12.7 Multiple DoS

Wireshark 1.12.x < 1.12.8 pcapng File Parser DoS

Wireshark 1.12.x < 1.12.9 Multiple DoS

Wireshark 1.4.5 Denial of Service

Wireshark 1.4.x < 1.4.10 Multiple Vulnerabilities

Wireshark 1.4.x < 1.4.11 Multiple Vulnerabilities

Wireshark 1.4.x < 1.4.12 Multiple Denial of Service Vulnerabilities

Wireshark 1.4.x < 1.4.13 Multiple Denial of Service Vulnerabilities

Wireshark 1.4.x < 1.4.14 Multiple Denial of Service Vulnerabilities

Wireshark 1.4.x < 1.4.15 Multiple Vulnerabilities

Wireshark 1.4.x < 1.4.9 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.10 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.11 DRDA DoS

Wireshark 1.6.x < 1.6.12 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.13 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.14 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.15 ASN.1 BER Dissector Malformed Packet Handling DoS

Wireshark 1.6.x < 1.6.16 Multiple DoS Vulnerabilities

Wireshark 1.6.x < 1.6.2 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.3 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.5 Multiple Vulnerabilities

Wireshark 1.6.x < 1.6.6 Multiple Denial of Service Vulnerabilities

Wireshark 1.6.x < 1.6.8 Multiple Denial of Service Vulnerabilities

Wireshark 1.6.x < 1.6.9 Multiple Denial of Service Vulnerabilities

Wireshark 1.8.x < 1.8.1 Multiple Denial of Service Vulnerabilities

Wireshark 1.8.x < 1.8.10 Multiple DoS

Wireshark 1.8.x < 1.8.11 Multiple DoS Vulnerabilities

Wireshark 1.8.x < 1.8.12 Multiple DoS

Wireshark 1.8.x < 1.8.13 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.2 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.3 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.4 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.5 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.6 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.7 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.8 Multiple Vulnerabilities

Wireshark 1.8.x < 1.8.9 Multiple Vulnerabilities

Wireshark 2.0.0 Multiple DoS

Wireshark 2.0.x < 2.0.10 / 2.2.x < 2.2.4 Multiple DoS

Wireshark 2.0.x < 2.0.11 / 2.2.x < 2.2.5 Multiple DoS

Wireshark 2.0.x < 2.0.12 / 2.2.x < 2.2.6 Multiple DoS

Wireshark 2.0.x < 2.0.13 / 2.2.x < 2.2.7 Multiple DoS

Wireshark 2.0.x < 2.0.14 / 2.2.x < 2.2.8 Multiple DoS

Wireshark 2.0.x < 2.0.15 Multiple DoS

Wireshark 2.0.x < 2.0.16 DMP dissector DoS

Wireshark 2.0.x < 2.0.2 Multiple Vulnerabilities

Wireshark 2.0.x < 2.0.3 Multiple DoS

Wireshark 2.0.x < 2.0.4 Multiple DoS

Wireshark 2.0.x < 2.0.5 Multiple DoS

Wireshark 2.0.x < 2.0.6 Multiple DoS

Wireshark 2.0.x < 2.0.8 / 2.2.x < 2.2.2 Multiple DoS

Wireshark 2.2.x < 2.2.1 Multiple DoS

Wireshark 2.2.x < 2.2.10 Multiple DoS

Wireshark 2.2.x < 2.2.11 / 2.4.x < 2.4.3 DoS Vulnerabilities

Wireshark 2.2.x < 2.2.12 / 2.4.x < 2.4.4 DoS Vulnerabilities

Wireshark 2.2.x < 2.2.13 / 2.4.x < 2.4.5 Multiple DoS Vulnerabilities

Wireshark 2.2.x < 2.2.14 / 2.4.x < 2.4.6 Multiple Vulnerabilities

Wireshark 2.2.x < 2.2.15 / 2.4.x < 2.4.7 / 2.6.x < 2.6.1 Multiple Vulnerabilities

Wireshark 2.2.x < 2.2.16 / 2.4.x < 2.4.8 / 2.6.x < 2.6.2 Multiple Vulnerabilities

Wireshark 2.2.x < 2.2.17 / 2.4.x < 2.4.9 / 2.6.x < 2.6.3 Multiple Vulnerabilities

Wireshark 2.2.x < 2.2.9 Multiple DoS

Wireshark 2.4.x < 2.4.1 Multiple DoS

Wireshark 2.4.x < 2.4.10 Multiple Vulnerabilities

Wireshark 2.4.x < 2.4.11 Multiple Vulnerabilities

Wireshark 2.4.x < 2.4.12 Multiple Vulnerabilities

Wireshark 2.4.x < 2.4.13 Multiple Vulnerabilities

Wireshark 2.4.x < 2.4.14 Multiple Vulnerabilities

Wireshark 2.4.x < 2.4.15 A Vulnerability

Wireshark 2.4.x < 2.4.16 DoS Vulnerability

Wireshark 2.4.x < 2.4.2 Multiple DoS

Wireshark 2.6.x < 2.6.10 DoS Vulnerability

Wireshark 2.6.x < 2.6.11 Gryphon Dissector DoS Vulnerability

Wireshark 2.6.x < 2.6.13 A Vulnerability

Wireshark 2.6.x < 2.6.15 Multiple Vulnerabilities

Wireshark 2.6.x < 2.6.4 Multiple Vulnerabilities

Wireshark 2.6.x < 2.6.5 Multiple Vulnerabilities

Wireshark 2.6.x < 2.6.6 Multiple Vulnerabilities

Wireshark 2.6.x < 2.6.7 Multiple Vulnerabilities

Wireshark 2.6.x < 2.6.8 Multiple Vulnerabilities

Wireshark 2.6.x < 2.6.9 A Vulnerability

Wireshark 3.0.x < 3.0.1 Multiple Vulnerabilities

Wireshark 3.0.x < 3.0.2 A Vulnerability

Wireshark 3.0.x < 3.0.3 DoS Vulnerability

Wireshark 3.0.x < 3.0.4 Gryphon Dissector DoS Vulnerability

Wireshark 3.0.x < 3.0.7 A Vulnerability

Wireshark 3.0.x < 3.0.8 Denial of Service (DoS) Vulnerability

Wireshark 3.0.x < 3.0.9 Multiple Vulnerabilities

Wireshark 3.2.x < 3.2.1 Denial of Service (DoS) Vulnerability

Wireshark 3.2.x < 3.2.2 Multiple Vulnerabilities

Wireshark < 1.2.12 / 1.4.1 ASN.1 BER Dissector Denial of Service

Wireshark < 1.2.13 / 1.4.2 Multiple Vulnerabilities

Wireshark < 1.2.14 / 1.4.3 Multiple Vulnerabilities

Wireshark < 1.2.15 / 1.4.4 Multiple Vulnerabilities

Wireshark < 1.2.16 / 1.4.5 Multiple Vulnerabilities

Wireshark < 1.2.17 / 1.4.7 Multiple DoS Vulnerabilities

Wireshark < 1.2.18 / 1.4.8 / 1.6.1 Multiple Denial of Service Vulnerabilities

WMI Anti-spyware Enumeration

WMI Antivirus Enumeration

WMI Bluetooth Network Adapter Enumeration

WMI EMET Configuration Enumeration

WMI Encryptable Volume Enumeration

WMI Firewall Enumeration

WMI Firewall Rule Enumeration

WMI IIS ISAPI Extension Enumeration

WMI QuickFixEngineering (QFE) Enumeration

WMI Trusted Platform Module Enumeration

WMI Windows Feature Enumeration

wodSFTP ActiveX Arbitrary File Access

WordPad History

WorldMail IMAP Server Traversal Arbitrary Mail Spool Access

Worldspan for Windows Gateway Res Manager Port 17990 Malformed Request DoS

WS\_FTP Pro Client ASCII Mode Directory Listing Handling Overflow

WS\_FTP Pro Client Weak Password Encrypted

WS\_FTP Pro HTTP Server Response Format String

Wyse Device Manager Buffer Overflow

XCP DRM Software Detection

Xftp < 3.0 Build 242 LIST Response Buffer Overflow

XnView 2.x < 2.03 Multiple Buffer Overflow Vulnerabilities

XnView 2.x < 2.04 Multiple Buffer Overflow Vulnerabilities

XnView 2.x < 2.13 Multiple Buffer Overflows

XnView < 1.98.1 Insecure Executable Loading

XnView < 1.98.5 Multiple Integer Overflow Vulnerabilities

XnView < 1.98.6 Multiple Buffer Overflow Vulnerabilities

XnView < 1.99.0 Multiple Buffer Overflow Vulnerabilities

XnView < 1.99.1 JPEG Compressed TIFF Image Multiple Header Value Handling Overflow

XnView RGBE File Handling Buffer Overflow

XUpload ActiveX Control AddFolder Method Buffer Overflow

Yahoo! Messenger < 11.5.0.155 CYImage::LoadJPG Method JPG File Handling Remote Integer Overflow

Yahoo! Messenger < 8.1.0.416 Multiple Vulnerabilities

Yahoo! Messenger AudioConf ActiveX Control (yacscom.dll) Multiple Property Overflow

Yahoo! Messenger Detection

Yahoo! Messenger Webcam ActiveX Buffer Overflows

Yahoo! Messenger YMMAPI.YMailAttach ActiveX (ymmapi.dll) Overflow

Yahoo! Messenger YVerInfo ActiveX Buffer Overflows

Yahoo! Music Jukebox ActiveX Controls Buffer Overflows

Yahoo! Widgets YDP YDPCTL.YDPControl.1 ActiveX (YDPCTL.dll) Buffer Overflow

ZipCentral ZIP File Handling Buffer Overflow

ZoIPer < 2.24 Crafted SIP INVITE Request Remote DoS

Zoom Client for Meetings 4.x < 4.1.34814.1119 Message Spoofing Vulnerability

Zoom Client for Meetings < 4.6.19253.0401 Multiple Vulnerabilities

Zoom Client for Meetings Installed (Windows)

Zoomify Viewer ActiveX Buffer Overflows

# Web Servers

04WebServer Multiple Vulnerabilities (XSS, DoS, more)

12Planet Chat Server Administration Authentication Cleartext Credential Disclosure

12Planet Chat Server Error Message Path Disclosure

4D WebStar Arbitrary Multiple Vulnerabilities

A-A-S Application Access Server Default Admin Password

A-A-S Application Access Server Detection

Abyss Web Server GET Request Multiple Vulnerabilities

Abyss Web Server Malformed GET Request Remote DoS

Abyss Web Server MS-DOS Device Name DoS

Acme mini\_httpd Protocol String Handling Memory Disclosure

Acme thttpd < 2.26 Multiple Vulnerabilities

Acme thttpd Detection

Alibaba Web Server 2.0 HTTP Request Overflow DoS

Allegro RomPager HTTP Cookie Management Remote Code Execution Vulnerability (Misfortune Cookie)

Allegro RomPager HTTP Cookie Management Remote Code Execution Vulnerability (Misfortune Cookie)

Allied Telesyn Router/Switch Web Interface Default Password

AnalogX SimpleServer:WWW /cgi-bin/ Long GET Request DoS

AnalogX SimpleServer:WWW Buffer Overflow

AnalogX SimpleServer:WWW Encoded Traversal Arbitrary File Access

AnalogX SimpleServer:WWW Short GET /cgi-bin Remote DoS

Anti-Nessus Defense Detection

Apache .htaccess and .htpasswd Disclosure

Apache 1.3.x < 1.3.41 Multiple Vulnerabilities (DoS, XSS)

Apache 1.3.x < 1.3.42 mod\_proxy Integer Overflow

Apache 2.0.x < 2.0.43 Multiple Vulnerabilities (Log Injection, Source Disc.)

Apache 2.0.x < 2.0.45 Multiple Vulnerabilities (DoS, File Write)

Apache 2.0.x < 2.0.46 Multiple DoS

Apache 2.0.x < 2.0.46 on OS/2 filestat.c Device Name Request DoS

Apache 2.0.x < 2.0.47 Multiple Vulnerabilities (DoS, Encryption)

Apache 2.0.x < 2.0.48 Multiple Vulnerabilities (OF, Info Disc.)

Apache 2.0.x < 2.0.49 mod\_ssl Plain HTTP Request DoS

Apache 2.0.x < 2.0.51 Multiple Vulnerabilities (OF, DoS)

Apache 2.0.x < 2.0.64 Multiple Vulnerabilities

Apache 2.0.x < 2.0.65 Multiple Vulnerabilities

Apache 2.2.x < 2.2.12 Multiple Vulnerabilities

Apache 2.2.x < 2.2.13 APR apr\_palloc Heap Overflow

Apache 2.2.x < 2.2.14 Multiple Vulnerabilities

Apache 2.2.x < 2.2.15 Multiple Vulnerabilities

Apache 2.2.x < 2.2.16 Multiple Vulnerabilities

Apache 2.2.x < 2.2.17 Multiple Vulnerabilities

Apache 2.2.x < 2.2.18 APR apr\_fnmatch DoS

Apache 2.2.x < 2.2.18 APR apr\_fnmatch DoS

Apache 2.2.x < 2.2.21 mod\_proxy\_ajp DoS

Apache 2.2.x < 2.2.22 Multiple Vulnerabilities

Apache 2.2.x < 2.2.23 Multiple Vulnerabilities

Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities

Apache 2.2.x < 2.2.25 Multiple Vulnerabilities

Apache 2.2.x < 2.2.27 Multiple Vulnerabilities

Apache 2.2.x < 2.2.28 Multiple Vulnerabilities

Apache 2.2.x < 2.2.32 Multiple Vulnerabilities (httpoxy)

Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities

Apache 2.2.x < 2.2.34 Multiple Vulnerabilities

Apache 2.2.x < 2.2.6 Multiple Vulnerabilities (DoS, XSS, Info Disc)

Apache 2.2.x < 2.2.8 Multiple Vulnerabilities (XSS, DoS)

Apache 2.2.x < 2.2.9 Multiple Vulnerabilities (DoS, XSS)

Apache 2.4.17 / 2.4.18 DoS

Apache 2.4.18 / 2.4.20 X.509 Certificate Authentication Bypass

Apache 2.4.6 Remote DoS

Apache 2.4.x < 2.4.10 Multiple Vulnerabilities

Apache 2.4.x < 2.4.12 Multiple Vulnerabilities

Apache 2.4.x < 2.4.16 Multiple Vulnerabilities

Apache 2.4.x < 2.4.2 'LD\_LIBRARY\_PATH' Insecure Library Loading

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)

Apache 2.4.x < 2.4.27 Multiple Vulnerabilities

Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)

Apache 2.4.x < 2.4.3 Multiple Vulnerabilities

Apache 2.4.x < 2.4.33 Multiple Vulnerabilities

Apache 2.4.x < 2.4.33 Multiple Vulnerabilities (deprecated)

Apache 2.4.x < 2.4.34 Multiple Vulnerabilities

Apache 2.4.x < 2.4.35 DoS

Apache 2.4.x < 2.4.38 Multiple Vulnerabilities

Apache 2.4.x < 2.4.39 Multiple Vulnerabilities

Apache 2.4.x < 2.4.4 Multiple XSS Vulnerabilities

Apache 2.4.x < 2.4.41 Multiple Vulnerabilities

Apache 2.4.x < 2.4.42 Multiple Vulnerabilities

Apache 2.4.x < 2.4.5 Multiple Vulnerabilities

Apache 2.4.x < 2.4.8 Multiple Vulnerabilities

Apache 2.x < 2.0.50 Multiple Remote DoS

Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)

Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)

Apache < 1.3.29 Multiple Modules Local Overflow

Apache < 1.3.31 / 2.0.49 Log Entry Terminal Escape Sequence Injection

Apache < 1.3.31 / 2.0.49 Socket Connection Blocking Race Condition DoS

Apache < 1.3.31 mod\_access IP Address Netmask Rule Bypass

Apache < 1.3.37 mod\_rewrite LDAP Protocol URL Handling Overflow

Apache < 2.0.44 DOS Device Name Multiple Remote Vulnerabilities (Code Exec, DoS)

Apache < 2.0.44 Illegal Character Default Script Mapping Bypass

Apache < 2.0.55 Multiple Vulnerabilities

Apache < 2.0.59 mod\_rewrite LDAP Protocol URL Handling Overflow

Apache < 2.0.63 Multiple XSS Vulnerabilities

Apache < 2.2.3 mod\_rewrite LDAP Protocol URL Handling Overflow

Apache <= 1.3.33 htpasswd Local Overflow

Apache <= 2.0.39 Win32 Crafted Traversal Arbitrary File Access

Apache <= 2.0.51 Satisfy Directive Access Control Bypass

Apache ASP module Apache::ASP source.asp Example File Arbitrary File Creation

Apache Auth Module SQL Injection

Apache Banner Linux Distribution Disclosure

Apache Chunked Encoding Remote Overflow

Apache Default Index Page

Apache Double Slash GET Request Forced Directory Listing

Apache for Windows Multiple Forward Slash Directory Listing

Apache HTTP Server 403 Error Page UTF-7 Encoded XSS

Apache HTTP Server Byte Range DoS

Apache HTTP Server Error Page Detection

Apache HTTP Server httpOnly Cookie Information Disclosure

Apache HTTP Server mod\_proxy Reverse Proxy HTTP 0.9 Information Disclosure

Apache HTTP Server mod\_proxy Reverse Proxy Information Disclosure

Apache HTTP Server Version

Apache Mixed Platform AddType Directive Information Disclosure

Apache mod\_fcgid Module < 2.3.9 fcgid\_header\_bucket\_read() Function Heap-Based Buffer Overflow

Apache mod\_fcgid Module fcgid\_header\_bucket\_read() Function Remote Stack Buffer Overflow

Apache mod\_imap Image Map Referer XSS

Apache mod\_include get\_tag() Function Local Overflow

Apache mod\_info /server-info Information Disclosure

Apache mod\_jk2 Host Header Multiple Fields Remote Overflow

Apache mod\_negotiation Multi-Line Filename Upload Vulnerabilities

Apache mod\_proxy Content-Length Overflow

Apache mod\_proxy\_ftp Directory Component Wildcard Character Globbing XSS

Apache mod\_ssl i2d\_SSL\_SESSION Function SSL Client Certificate Overflow

Apache mod\_ssl ssl\_compat\_directive Function Overflow

Apache mod\_ssl ssl\_engine\_log.c mod\_proxy Hook Function Remote Format String

Apache mod\_ssl ssl\_hook\_Access Error Handling DoS

Apache mod\_status /server-status Information Disclosure

Apache mod\_suexec Multiple Privilege Escalation Vulnerabilities

Apache mod\_wsgi < 3.5 Apache Process Privilege Escalation

Apache mod\_wsgi < 4.2.4 Privilege Dropping Privilege Escalation

Apache Multiviews Arbitrary Directory Listing

Apache on Mac OS X HFS+ Arbitrary File Source Disclosure

Apache on SuSE Linux cgi-bin-sdb Request Script Source Disclosure

Apache on Windows < 1.3.24 / 2.0.x < 2.0.34 DOS Batch File Arbitrary Command Execution

Apache on Windows php.exe Malformed Request Path Disclosure

Apache Server ETag Header Information Disclosure

Apache ServerTokens Information Disclosure

Apache Subversion 1.7.x < 1.7.19 / 1.8.x < 1.8.11 Multiple Remote DoS

Apache Tomcat 3.x < 3.2.2 JSP Error Condition XSS

Apache Tomcat 3.x < 3.2.2 Malformed URL JSP Source Disclosure

Apache Tomcat 3.x < 3.3.2 Multiple Vulnerabilities

Apache Tomcat 4.x < 4.1.0 Multiple Vulnerabilities

Apache Tomcat 4.x < 4.1.3 Denial of Service

Apache Tomcat 4.x < 4.1.32 Multiple Vulnerabilities

Apache Tomcat 4.x < 4.1.36 Multiple Vulnerabilities

Apache Tomcat 4.x < 4.1.37 Multiple Vulnerabilities

Apache Tomcat 4.x < 4.1.39 Multiple Vulnerabilities

Apache Tomcat 5.0.x <= 5.0.30 / 5.5.x < 5.5.23 Content-Length HTTP Request Smuggling

Apache Tomcat 5.0.x <= 5.0.30 / 5.5.x < 5.5.25 Multiple Vulnerabilities

Apache Tomcat 5.5.x < 5.5.30

Apache Tomcat 5.5.x < 5.5.32 HTML Manager Interface XSS

Apache Tomcat 5.5.x < 5.5.34 Multiple Vulnerabilities

Apache Tomcat 5.5.x < 5.5.36 DIGEST Authentication Multiple Security Weaknesses

Apache Tomcat 5.x < 5.5.1 Information Disclosure

Apache Tomcat 5.x < 5.5.21 Multiple Vulnerabilities

Apache Tomcat 5.x < 5.5.35 Hash Collision Denial of Service

Apache Tomcat 6.0 < 6.0.28 Multiple Vulnerabilities

Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure

Apache Tomcat 6.0.x < 6.0.24 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.30 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.33 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.36 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.37 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.39 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.40 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.42 Handling Request Smuggling DoS

Apache Tomcat 6.0.x < 6.0.43 Multiple Vulnerabilities (POODLE)

Apache Tomcat 6.0.x < 6.0.44 Multiple Vulnerabilities (FREAK)

Apache Tomcat 6.0.x < 6.0.45 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities

Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure

Apache Tomcat 6.x < 6.0.30 / 7.x < 7.0.5 Multiple XSS

Apache Tomcat 6.x < 6.0.35 Multiple Vulnerabilities

Apache Tomcat 6.x < 6.0.9 Information Disclosure

Apache Tomcat 7.0.0 < 7.0.85 Security Constraint Weakness

Apache Tomcat 7.0.0 < 7.0.91 Open Redirect Weakness

Apache Tomcat 7.0.0 < 7.0.94 Remote Code Execution Vulnerability (Windows)

Apache Tomcat 7.0.12 / 7.0.13 Security Constraint Bypass

Apache Tomcat 7.0.41 < 7.0.79 Cache Poisoning Vulnerability

Apache Tomcat 7.0.41 < 7.0.90 Multiple Vulnerabilities

Apache Tomcat 7.0.79 < 7.0.83 Insecure CGI Servlet Search Algorithm Description Weakness

Apache Tomcat 7.0.x < 7.0.28 Multiple DoS

Apache Tomcat 7.0.x < 7.0.30 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.32 XSRF Filter Bypass

Apache Tomcat 7.0.x < 7.0.33 Session Fixation

Apache Tomcat 7.0.x < 7.0.40 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.47 / 8.0.x < 8.0.0-RC3 Information Disclosure

Apache Tomcat 7.0.x < 7.0.50 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.52 Content-Type DoS

Apache Tomcat 7.0.x < 7.0.53 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.54 XML Parser Information Disclosure

Apache Tomcat 7.0.x < 7.0.55 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.57 Multiple Vulnerabilities (POODLE)

Apache Tomcat 7.0.x < 7.0.59 Security Manager Bypass

Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK)

Apache Tomcat 7.0.x < 7.0.65 / 8.0.x < 8.0.27 Directory Traversal

Apache Tomcat 7.0.x < 7.0.68 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service

Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control

Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation

Apache Tomcat 7.0.x < 7.0.81 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.82 Multiple Vulnerabilities

Apache Tomcat 7.0.x < 7.0.88 Denial of Service

Apache Tomcat 7.x < 7.0.11 @ServletSecurity Annotation Security Bypass

Apache Tomcat 7.x < 7.0.12 Multiple Vulnerabilities

Apache Tomcat 7.x < 7.0.17 Multiple Vulnerabilities

Apache Tomcat 7.x < 7.0.20 'jsvc' Information Disclosure

Apache Tomcat 7.x < 7.0.21 Arbitrary AJP Message Control

Apache Tomcat 7.x < 7.0.22 Multiple Vulnerabilities

Apache Tomcat 7.x < 7.0.23 Hash Collision DoS

Apache Tomcat 7.x < 7.0.4 SecurityManager Local Security Bypass

Apache Tomcat 7.x < 7.0.6 Manager Interface XSS

Apache Tomcat 8.0.0 < 8.0.53 Security Constraint Weakness

Apache Tomcat 8.0.0.RC1 < 8.0.32 Multiple Vulnerabilities

Apache Tomcat 8.0.0.RC1 < 8.0.45 Cache Poisoning

Apache Tomcat 8.0.0.RC1 < 8.0.47 Multiple Vulnerabilities

Apache Tomcat 8.0.0.RC1 < 8.0.50 Security Constraint Weakness

Apache Tomcat 8.0.45 < 8.0.48 Insecure CGI Servlet Search Algorithm Description Weakness

Apache Tomcat 8.0.x < 8.0.11 Multiple OpenSSL Vulnerabilities

Apache Tomcat 8.0.x < 8.0.15 Multiple Vulnerabilities (POODLE)

Apache Tomcat 8.0.x < 8.0.17 Security Manager Bypass

Apache Tomcat 8.0.x < 8.0.21 Multiple Vulnerabilities (FREAK)

Apache Tomcat 8.0.x < 8.0.3 Content-Type DoS

Apache Tomcat 8.0.x < 8.0.4 Multiple Vulnerabilities

Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service

Apache Tomcat 8.0.x < 8.0.6 XML Parser Information Disclosure

Apache Tomcat 8.0.x < 8.0.9 Multiple DoS

Apache Tomcat 8.5.0 < 8.5.32 Multiple Vulnerabilities

Apache Tomcat 8.5.0 < 8.5.40 Remote Code Execution Vulnerability (Windows)

Apache Tomcat 8.5.0 < 8.5.41 a vulnerability

Apache Tomcat 8.5.0 < 8.5.49 Privilege Escalation

Apache Tomcat 8.5.0 < 8.5.50 Privilege Escalation Vulnerability

Apache Tomcat 8.5.16 < 8.5.24 Insecure CGI Servlet Search Algorithm Description Weakness

Apache Tomcat 8.5.7 < 8.5.11 nextRequest Information Disclosure

Apache Tomcat 8.5.x < 8.5.13 / 9.0.x < 9.0.0.M19 Multiple Vulnerabilities

Apache Tomcat 8.5.x < 8.5.16 Multiple Vulnerabilities

Apache Tomcat 8.5.x < 8.5.28 Security Constraint Weakness

Apache Tomcat 8.5.x < 8.5.34 Open Redirect Weakness

Apache Tomcat 9.0.0 < 9.0.10 Multiple Vulnerabilites

Apache Tomcat 9.0.0.M1 < 9.0.1 Multiple Vulnerabilities

Apache Tomcat 9.0.0.M1 < 9.0.12 Open Redirect Weakness

Apache Tomcat 9.0.0.M1 < 9.0.16 a vulnerability

Apache Tomcat 9.0.0.M1 < 9.0.19 Remote Code Execution Vulnerability (Windows)

Apache Tomcat 9.0.0.M1 < 9.0.20 a vulnerability

Apache Tomcat 9.0.0.M1 < 9.0.30 Privilege Escalation Vulnerability

Apache Tomcat 9.0.0.M1 < 9.0.5 Insecure CGI Servlet Search Algorithm Description Weakness

Apache Tomcat 9.0.0.M1 < 9.0.8 Denial of Service Vulnerability

Apache Tomcat 9.0.0.M11 < 9.0.0.M17 nextRequest Information Disclosure

Apache Tomcat 9.0.0.M22 < 9.0.2 Insecure CGI Servlet Search Algorithm Description Weakness

Apache Tomcat 9.0.0M1 < 9.0.0.M22 Multiple Vulnerabilities

Apache Tomcat < 4.1.40 / 5.5.28 / 6.0.20 Multiple Vulnerabilities

Apache Tomcat < 5.5.26 Multiple Vulnerabilities

Apache Tomcat < 6.0.10 Directory Traversal

Apache Tomcat < 6.0.13 Multiple Vulnerabilities

Apache Tomcat < 6.0.14 Multiple Vulnerabilities

Apache Tomcat < 6.0.16 Multiple Vulnerabilities

Apache Tomcat < 6.0.18 Multiple Vulnerabilities

Apache Tomcat < 6.0.32 / 7.0.8 NIO Connector DoS

Apache Tomcat < 6.0.6 Cross-Site Scripting

Apache Tomcat < 7.0.100 / 8.5.x < 8.5.51 / 9.x < 9.0.31 Multiple Vulnerabilities

Apache Tomcat < 7.0.2 Denial of Service and Information Disclosure

Apache Tomcat < 7.0.67 Session Fixation

Apache Tomcat < 8.0.0-RC10 Multiple Vulnerabilities

Apache Tomcat < 8.0.30 Directory Disclosure

Apache Tomcat < 9.0.0.M3 Multiple Vulnerabilities

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Apache Tomcat AJP12 Protocol Malformed Packet Remote DoS

Apache Tomcat contextAdmin Arbitrary File Access

Apache Tomcat Cross-Application File Manipulation

Apache Tomcat Default Accounts

Apache Tomcat Default Files

Apache Tomcat Detection

Apache Tomcat Directory Traversal

Apache Tomcat Examples Web Root Path Disclosure

Apache Tomcat HTTP PUT JSP File Upload RCE

Apache Tomcat Installed (Windows)

Apache Tomcat JK Connector 1.2.x < 1.2.41 JkUnmount Directive Handling Remote Information Disclosure

Apache Tomcat JK Connector Content-Length Header Cross-User Information Disclosure

Apache Tomcat Local Detection

Apache Tomcat Long URL Information Disclosure

Apache Tomcat Manager Common Administrative Credentials

Apache Tomcat mod\_jk Invalid Transfer-Encoding Chunked Field DoS

Apache Tomcat MS-DOS Device Name Request DoS

Apache Tomcat WAR Deployment Multiple Vulnerabilities

Apache Tomcat XSRF Token Disclosure

Apache Traffic Server 3.0.x < 3.0.4 / 3.1.x < 3.1.3 Host HTTP Header Parsing Remote Overflow

Apache Traffic Server 4.x < 4.2.1.1 / 5.x < 5.0.1 Synthetic Health Check Vulnerability

Apache Traffic Server 5.1.x < 5.1.1 Multiple Vulnerabilities (POODLE)

Apache Traffic Server 5.1.x < 5.1.2 DoS

Apache Traffic Server 5.2.0 - 5.3.2 / 6.x < 6.2.2 / 7.x < 7.1.2 TLS Handshake DoS

Apache Traffic Server 5.3.x < 5.3.1 'url\_sig' Plugin Multiple Vulnerabilities

Apache Traffic Server 5.3.x < 5.3.2 HTTP2 Multiple Vulnerabilities

Apache Traffic Server 6.x < 6.2.2 / 7.x < 7.1.2 Host Header and Line Folding Vulnerability

Apache Traffic Server Unsupported

Apache Traffic Server Version

Apache UserDir Directive Username Enumeration

Apache WebDAV Module PROPFIND Arbitrary Directory Listing

Apache-SSL < 1.3.23+1.46 i2d\_SSL\_SESSION Function SSL Client Certificate Overflow

Apache-SSL ExpandCert() Function Certificate Handling Arbitrary Environment Variables Manipulation

Apache-SSL SSLVerifyClient SSLFakeBasicAuth Client Certificate Forgery

Apple Mac OS X Find-By-Content .DS\_Store Web Directory Listing

Appweb 3.1.x / 3.2.x / 3.3.x < 3.3.3 mprUrlEncode Function Heap Overflow Vulnerability

Appweb < 7.0.3 authCondition Authentication Bypass Vulnerability

Appweb HTTP Server Version

APSIS Pound Load Balancer Format String Overflow

ArGoSoft Mail Server HTTP Daemon GET Request Saturation DoS

Aspen < 0.22 Directory Traversal

Aspen HTTP Server Detection

Avirt Multiple Product HTTP Proxy Overflow (deprecated)

Backported Security Patch Detection (PHP)

BadBlue Connection Saturation Remote DoS

BadBlue ext.dll mfcisapicommand Parameter Remote Overflow

BadBlue Hex-encoded Null Byte Request Arbitrary File Access

BadBlue ISAPI Extension .hts Crafted File Extension Request Authentication Bypass

BadBlue ISAPI Extension ext.dll LoadPage Parameter Arbitrary File Access

BadBlue Malformed GET Request Remote DoS

BEA WebLogic <= 8.1 SP4 Multiple Vulnerabilities (XSS, DoS, ID, more)

Blue Coat Reporter Default Password (admin) for 'admin' Account

Blue Coat Reporter Detection

Boa Web Server Traversal Arbtirary File Access/Execution

Broken Web Server Detection

Broken Web Servers

BrowseGate HTTP MIME Headers Remote Overflow

Cabletron WebView Administrative Access

Caudium Web Server Malformed URI Remote DoS

CCProxy < 6.62 HTTP Proxy CONNECT Request Handling Remote Overflow

CCProxy Logging Compoent HTTP GET Request Remote Overflow

CERN httpd CGI Name Handling Remote Overflow

CERN httpd Double Slash Protected Webpage Bypass

CERN httpd Virtual Web Path Disclosure

Cherokee Web Server auth\_pam Authentication Format String

Cherokee Web Server Malformed POST Request Remote DoS

Cherokee Web Server Port Bind Privilege Drop Weakness

Cherokee Web Server URI Traversal Arbitrary File Access

CiscoSecure ACS for Windows CSAdmin Login Overflow DoS

Citrix NetScaler Management and Analytics System

Citrix NetScaler Management and Analytics System Default Administrator Credentials

Citrix NetScaler Web Management Interface Default Administrator Credentials

Citrix NetScaler Web Management Interface Detection

Citrix NFuse Server launch.asp Arbitrary Server/Port Redirect

CommuniGate Pro HTTP Configuration Port Remote Overflow

Compaq WBEM HTTP Server Remote Overflow

Compaq Web-Based Management Agent Remote Overflow DoS

Compaq Web-enabled Management Software Default Account

Compaq Web-enabled Management Software HTTP Server Arbitrary Traffic Proxy

CUPS Memory Information Disclosure

DD-WRT HTTP Daemon Metacharacter Injection Remote Code Execution

Default nginx HTTP Server Settings

Device Information (devinfo.xml)

Easy File Sharing Web Server Crafted Request ADS Arbitrary File Access

Easy File Sharing Web Server disk\_c Virtual Folder Request Arbitrary File Access

Easy File Sharing Web Server Multiple Remote Vulnerabilities (FS, XSS, Upload)

Embedded Web Server Detection

Enhydra Multiserver Default Password

ePolicy Orchestrator HTTP /spipe/pkg/ Source Header Remote Overflow

ePolicy Orchestrator HTTP GET Request Remote Format String

ePolicy Orchestrator Multiple Remote Vulnerabilities (OF, FS)

ePolicy Orchestrator Symlink Arbitrary Privileged File Access

Eserv GET Request Traversal Arbitrary File Access

Eserv Web Server /? Request Forced Directory Listing

External URLs

Eye-Fi Helper < 3.4.23 Directory Traversal

Eye-Fi Helper Detection

F5 BIG-IP Cookie Remote Information Disclosure

F5 BIG-IP Web Management Interface Detection

Fastream NETFile FTP/Web Server HEAD Request Saturation DoS

Fixed HTTP Session Cookies

FTPGate Web Proxy Traversal Arbitrary File Access

GeoHttpServer Unauthorized Image Access Vulnerability

GoAhead Embedded Web Server websNormalizeUriPath() Directory Traversal Vulnerability

Google Search Appliance Detection

GPON ONT Home Gateway Authenticated Remote Command Execution (CVE-2019-3919)

GPON ONT Home Gateway Authenticated Remote Command Execution (CVE-2019-3920)

GPON ONT Home Gateway Remote Enabling of Telnet (CVE-2019-3917)

GPON ONT Home Gateway Router is vulnerable to authenticated remote command execution (CVE-2018-10562)

GPON ONT Home Gateway Router is vulnerable to authentication bypass (CVE-2018-10561)

Hiawatha 'setuid' Local Privilege Escalation

Hiawatha < 3.6 URL Handling Weakness

Hiawatha < 6.5 str2int Integer Overflow

Hiawatha < 7.3 Multiple Unspecified Issues

Hiawatha < 8.5 Connection Saturation DoS

Hiawatha < 8.8 Mixed Case DenyBody Security Bypass

Hiawatha Detection

Hiawatha fetch\_request Integer Overflow DoS

Hiawatha Tomahawk poll DoS

HMAP Web Server Fingerprinting

HP OfficeJet Printer Heartbeat Information Disclosure (Heartbleed)

HP OfficeJet Printer Security Bypass (HPSBPI03107)

HP OfficeJet Pro 8500 XSS

HP OfficeJet Pro Wi-Fi Direct Support Printer Configuration Unauthenticated Access

HP System Management Homepage (SMH) AddXECert Remote DoS

HP System Management Homepage 7.3.x / 7.4.x < 7.5.0 Multiple Vulnerabilities (FREAK)

HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities

HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities

HP System Management Homepage < 6.2 Multiple Vulnerabilities

HP System Management Homepage < 6.3 Multiple Vulnerabilities

HP System Management Homepage < 7.0 Multiple Vulnerabilities

HP System Management Homepage < 7.1.1 Multiple Vulnerabilities

HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution

HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities (BEAST)

HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL Multiple Vulnerabilities

HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE)

HP System Management Homepage < 7.2.6 Multiple Vulnerabilities (FREAK)

HP System Management Homepage < 7.3 Multiple Vulnerabilities

HP System Management Homepage < 7.4 Multiple Vulnerabilities

HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam)

HP System Management Homepage < 7.5.4.3 AddCertsToTrustCfgList DoS

HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy)

HP System Management Homepage < 7.6.1 Multiple Vulnerabilities (HPSBMU03753)

HP System Management Homepage Detection

HP System Management Homepage ginkgosnmp.inc Command Injection

HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593)

HP System Management Homepage OpenSSL Multiple Vulnerabilities (Heartbleed)

HP System Management Homepage Single Sign On Parameter Handling RCE

HP Virtual Table Server Detection

HSTS Missing From HTTPS Server

HTTP Header Name Remote Format String

HTTP Header Value Remote Format String

HTTP Method Remote Format String

HTTP Methods Allowed (per directory)

HTTP Protocol Version Detection

HTTP Proxy CONNECT Loop DoS

HTTP Reverse Proxy Detection (Deprecated)

HTTP Server Cookies Set

HTTP Server Type and Version

HTTP Session Cookies

HTTP TRACE / TRACK Methods Allowed

HTTP URI Handling Format String

HTTP/2 Cleartext Detection

HTTP\_PROXY Environment Variable Namespace Collision Vulnerability (httpoxy)

HyperText Transfer Protocol (HTTP) Information

HyperText Transfer Protocol (HTTP) Redirect Information

IBM BigFix Compliance Detection

IBM BigFix Platform 9.1.x < 9.1.1328.0 / 9.2.x < 9.2.11.19 Multiple Vulnerabilities

IBM BigFix Platform 9.2.x < 9.2.12 / 9.5.x < 9.5.7 Multiple Vulnerabilities

IBM BigFix Platform 9.2.x < 9.2.15 / 9.5.x < 9.5.10 Multiple Vulnerabilities

IBM BigFix Platform 9.2.x <= 9.2.16 / 9.5.x <= 9.5.11 Information Disclosure

IBM BigFix Platform 9.5.x < 9.5.10 Plain Text Credentials

IBM BigFix Platform 9.5.x < 9.5.12 Multiple Vulnerabilities

IBM BigFix Platform 9.x < 9.1.9.1301 / 9.2.9.36 / 9.5.4.38 Multiple Vulnerabilities

IBM BigFix Platform 9.x < 9.5.3 Remote Command Injection

IBM BigFix Server 9.1.x < 9.1.1275.0 Multiple XSS

IBM BigFix Server 9.2.x < 9.2.7.53 BES Gather XSS

IBM BigFix Server 9.2.x < 9.2.8.74 .beswrpt File Handling XSS

IBM BigFix Web Reports Detection

IBM Domino Password Protected DB Enumeration

IBM Domino ZMerge Database Security Bypass

IBM Endpoint Manager Web Server Detection

IBM HTTP Server 6.0 <= 6.0.2.43 (FP43) / 6.1 <= 6.1.0.47 (FP47) / 7.0 < 7.0.0.39 (FP39) / 8.0 < 8.0.0.11 (FP11) / 8.5 < 8.5.5.7 (FP7) Named Pipe DoS

IBM HTTP Server 6.1 <= 6.1.0.47 (FP47) / 7.0 < 7.0.0.39 (FP39) / 8.0 < 8.0.0.12 (FP12) / 8.5 < 8.5.5.7 (FP7) Multiple Vulnerabilities

IBM HTTP Server for z/OS 5.3.0 Command Execution

IBM HTTP Server on Windows Apache Portable Runtime (APR) Named Pipe DoS

IBM HTTP Server SSL/TLS RC4 Stream Cipher Key Invariance (Bar Mitzvah)

IBM Lotus Domino 6.0 Multiple Vulnerabilities

IBM Lotus Domino 8.5.x < 8.5.3 FP 4 Multiple Vulnerabilities

IBM Lotus Domino 8.5.x < 8.5.3 Multiple Vulnerabilities

IBM Lotus Domino 8.5.x Multiple Vulnerabilities

IBM Lotus Domino < 8.0.1 / 7.0.3 FP1 Multiple Vulnerabilities

IBM Lotus Domino ?open Forced Directory Listing

IBM Lotus Domino ?ReadDesign Request Design Element Disclosure

IBM Lotus Domino Banner Nonexistent .pl File Request Path Disclosure

IBM Lotus Domino Crafted .nsf Request Authentication Bypass

IBM Lotus Domino Directory Traversal Arbitrary File Access

IBM Lotus Domino HTML Hidden Field Encrypted Password Disclosure

IBM Lotus Domino HTTP /cgi-bin Relative URL Request DoS

IBM Lotus Domino HTTP Server Filesystem Setup Disclosure

IBM Lotus Domino Server Crafted .nsf Request Traversal Arbitrary File Access

IBM Lotus Domino Web Service NLSCCSTR.DLL Malformed GET Request Overflow DoS

IBM RSA Default Credentials

IBM Sametime Detection

IBM Tivoli Endpoint Manager Server 8.2.x < 8.2.1445.0 / 9.0.x < 9.0.853.0 / 9.1.x < 9.1.1088.0 Unspecified XXE File Disclosure

IBM Tivoli Endpoint Manager Server 9.0.777 (patch 2) LDAP and AD Authentication

IBM Tivoli Endpoint Manager Server 9.1.x < 9.1.1117.0 OpenSSL Security Bypass

IBM Tivoli Management Framework Endpoint addr URL Default Credentials

IBM Tivoli Management Framework Endpoint addr URL Remote Buffer Overflow

IBM Tivoli Management Framework Endpoint Web Detection

IBM Tivoli Provisioning Manager OS Deployment < 5.1.0.3 Interim Fix 3 HTTP Server Logging Functionality Remote Overflow

IBM Tivoli Provisioning Manager OS Deployment Multiple Stack Overflows

IBM Tivoli Provisioning Manager OS Deployment Multiple Unspecified Input Validation Vulnerabilities

IBM Tivoli SecureWay WebSEAL Proxy Policy Director Encoded URL DoS

IBM Tivoli Storage Manager Client Multiple Vulnerabilities (swg21268775)

IBM WebSphere Application Server 6.0 < 6.0.2.17 Multiple Vulnerabilities

IBM WebSphere Application Server 6.0 < 6.0.2.19 HTTP Response Splitting

IBM WebSphere Application Server 6.0 < 6.0.2.21 Multiple Vulnerabilities

IBM WebSphere Application Server 6.0 < 6.0.2.23 Unspecified Vulnerability (PK45726)

IBM WebSphere Application Server 6.0 < 6.0.2.25 Multiple Vulnerabilities

IBM WebSphere Application Server 6.0 < 6.0.2.39 Multiple Vulnerabilities

IBM WebSphere Application Server 6.0 < 6.0.2.41 Multiple Vulnerabilities

IBM WebSphere Application Server 6.0 < 6.0.2.43 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.13 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.31 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.33 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.35 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.37 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.39 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.41 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.43 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.7 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < 6.1.0.9 Cross-session Information Disclosure

IBM WebSphere Application Server 6.1 < Fix Pack 19 Multiple Flaws

IBM WebSphere Application Server 6.1 < Fix Pack 21 Multiple Flaws

IBM WebSphere Application Server 6.1 < Fix Pack 45 Multiple Vulnerabilities

IBM WebSphere Application Server 6.1 < Fix Pack 47 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < 7.0.0.39 (FP39) / 8.0 < 8.0.0.11 (FP11) / 8.5 < 8.5.5.6 (FP6) Multiple Vulnerabilities (Bar Mitzvah) (FREAK)

IBM WebSphere Application Server 7.0 < 7.0.0.41 / 8.0 < 8.0.0.12 / 8.5 < 8.5.5.9 OAuth Provider XSS

IBM WebSphere Application Server 7.0 < 7.0.0.43 / 8.0 < 8.0.0.13 / 8.5 < 8.5.5.10 / 9.0 < 9.0.0.1 / Liberty 16.0 < 16.0.0.3 Information Disclosure

IBM WebSphere Application Server 7.0 < 7.0.0.43 / 8.0 < 8.0.0.13 / 8.5 < 8.5.5.10 / Liberty 16.0 < 16.0.0.2 CRLF Sequences HTTP Response Splitting

IBM WebSphere Application Server 7.0 < 7.0.0.43 / 8.0 < 8.0.0.13 / 8.5 < 8.5.5.10 Information Disclosure

IBM WebSphere Application Server 7.0 < 7.0.0.43 / 8.0 < 8.0.0.13 / 8.5 < 8.5.5.11 / 9.0 < 9.0.0.2 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < 7.0.0.43 / 8.0 < 8.0.0.14 / 8.5 < 8.5.5.12 / 9.0 < 9.0.0.3 Admin Console Multiple XSS

IBM WebSphere Application Server 7.0 < 7.0.0.45 / 8.0 < 8.0.0.14 / 8.5 < 8.5.5.12 / 9.0 < 9.0.0.4 / Liberty 17.0 < 17.0.0.2 OAuth Service Provider XSRF

IBM WebSphere Application Server 7.0 < 7.0.0.45 / 8.0 < 8.0.0.14 / 8.5 < 8.5.5.12 / 9.0 < 9.0.0.5 Insecure File Permissions (PI79343)

IBM WebSphere Application Server 7.0 < 7.0.0.45 / 8.0 < 8.0.0.14 / 8.5 < 8.5.5.12 / 9.0 < 9.0.0.5 Unspecified XSS (PI82078)

IBM WebSphere Application Server 7.0 < 7.0.0.45 / 8.0 < 8.0.0.14 / 8.5 < 8.5.5.13 / 9.0 < 9.0.0.5 Information Disclosure (PI82630)

IBM WebSphere Application Server 7.0 < Fix Pack 1

IBM WebSphere Application Server 7.0 < Fix Pack 11 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 13 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 15 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 17 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 19 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 21 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 23 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 25 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 27 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 29 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 3

IBM WebSphere Application Server 7.0 < Fix Pack 31 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 33 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 35 Multiple Vulnerabilities

IBM WebSphere Application Server 7.0 < Fix Pack 37 Multiple Vulnerabilities (POODLE)

IBM WebSphere Application Server 7.0 < Fix Pack 5

IBM WebSphere Application Server 7.0 < Fix Pack 7

IBM WebSphere Application Server 7.0 < Fix Pack 9

IBM WebSphere Application Server 7.0.0.0 < 7.0.0.45 / 8.0.0.0 < 8.0.0.15 / 8.5.0.0 < 8.5.5.14 / 9.0.0.0 < 9.0.0.7 Admin Console Unspecified Insecure Security Remote Privilege Escalation

IBM WebSphere Application Server 7.0.0.0 <= 7.0.0.45 / 8.0.0.0 <= 8.0.0.15 / 8.5.0.0 <= 8.5.5.17 / 9.0.0.0 <= 9.0.5.3 Privilege Escalation (CVE-2020-4362)

IBM WebSphere Application Server 7.0.0.x < 7.0.0.43 / 8.0.0.x < 8.0.0.14 / 8.5.x < 8.5.5.12 / 9.0.0.x < 9.0.0.4 SOAP Connectors DoS

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.10 Admin Console Directory Traversal Vulnerability (CVE-2018-1770)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.10 Admin Console Directory Traversal Vulnerability (CVE-2018-1770)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.10 Remote Code Execution (CVE-2018-1567)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.15 Form Login Spoofing Vulnerability (CVE-2018-1695)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.16 / 9.0.0.x < 9.0.0.11 / Liberty < 19.0.0.4 Request Header Denial of Service (DoS) Vulnerability (CVE-2019-4046)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.16 / 9.0.0.x < 9.0.0.11 Admin Console Denial of Service (DoS) Vulnerability (CVE-2019-4080)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.16 / 9.0.0.x < 9.0.0.11 Information Disclosure Vulnerability (CVE-2018-1996)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.17 / 9.0.x < 9.0.5.2 / Liberty < 19.0.0.11 Information Disclosure (CVE-2019-4441)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.17 / 9.0.x < 9.0.5.3 Command Execution (CVE-2020-4163)

IBM WebSphere Application Server 7.0.0.x <= 7.0.0.45 / 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.18 / 9.0.x < 9.0.5.4 Privilege Escalation (CVE-2020-4276)

IBM WebSphere Application Server 7.0.x / 8.0.0.x / 8.5.x < 8.5.5.17 / 9.0.0.x < 9.0.5.2 Directory Traversal Vulnerability

IBM WebSphere Application Server 7.0.x / 8.0.0.x / 8.5.x < 8.5.5.17 / 9.0.0.x < 9.0.5.2 Information Disclosure (CVE-2019-4477)

IBM WebSphere Application Server 8.0 < 8.0.0.14 / 8.5 < 8.5.5.12 Administrative Console Information Disclosure

IBM WebSphere Application Server 8.0 < Fix Pack 1 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 10 Multiple Vulnerabilities (POODLE)

IBM WebSphere Application Server 8.0 < Fix Pack 2 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 3 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 4 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 5 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 6 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 7 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 8 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0 < Fix Pack 9 Multiple Vulnerabilities

IBM WebSphere Application Server 8.0.0.10 < 8.0.0.14 / 8.5.5.3 < 8.5.5.12 / 9.0.0.0 < 9.0.0.4 OIDC Privilege Escalation

IBM WebSphere Application Server 8.0.0.x <= 8.0.0.15 / 8.5.x < 8.5.5.14 / 9.0.0.x < 9.0.0.9 Installation Verification Tool Cross-site Scripting (XSS) Vulnerability (CVE-2018-1643)

IBM WebSphere Application Server 8.5 < Fix Pack 1 Multiple Vulnerabilities

IBM WebSphere Application Server 8.5 < Fix Pack 2 Multiple Vulnerabilities

IBM WebSphere Application Server 8.5 < Fix Pack 8.5.5 Multiple Vulnerabilities

IBM WebSphere Application Server 8.5 < Fix Pack 8.5.5.1 Multiple Vulnerabilities

IBM WebSphere Application Server 8.5 < Fix Pack 8.5.5.2 Multiple Vulnerabilities

IBM WebSphere Application Server 8.5 < Fix Pack 8.5.5.3 Multiple Vulnerabilities

IBM WebSphere Application Server 8.5 < Fix Pack 8.5.5.4 Multiple Vulnerabilities (POODLE)

IBM WebSphere Application Server 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.10 Cross-Site Request Forgery (CVE-2018-1926)

IBM WebSphere Application Server 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.10 Information Disclosure (CVE-2018-1614)

IBM WebSphere Application Server 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.10 Privilege Escalation (CVE-2018-1840)

IBM WebSphere Application Server 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.10 Privilege Escalation (CVE-2018-1901)

IBM WebSphere Application Server 8.5.x < 8.5.5.15 / 9.0.0.x < 9.0.0.9 TLS Downgrade Vulnerability (CVE-2018-1719)

IBM WebSphere Application Server 9.0.0.0 < 9.0.0.8 Spoof Attack Vulnerability

IBM WebSphere Application Server 9.0.0.x < 9.0.0.10 XML External Entity Injection (XXE) Vulnerability (CVE-2018-1905)

IBM WebSphere Application Server 9.0.x < 9.0.5.0 Information Disclosure (CVE-2019-4269)

IBM WebSphere Application Server < 6.0.2.31 Multiple Vulnerabilities

IBM WebSphere Application Server < 6.0.2.33 Multiple Vulnerabilities

IBM WebSphere Application Server < 6.0.2.35 Multiple Vulnerabilities

IBM WebSphere Application Server < 6.1.0.15 Multiple Vulnerabilities

IBM WebSphere Application Server < 6.1.0.17 Multiple Vulnerabilities

IBM WebSphere Application Server < 6.1.0.23 Multiple Flaws

IBM WebSphere Application Server < 6.1.0.25 Multiple Vulnerabilities

IBM WebSphere Application Server < 6.1.0.27 Multiple Vulnerabilities

IBM WebSphere Application Server < 6.1.0.29 Multiple Vulnerabilities

IBM WebSphere Application Server Denial of Service (CVE-2019-4720)

IBM WebSphere Application Server Detection

IBM WebSphere Application Server Liberty Detection

IBM WebSphere Application Server Multiple Vulnerabilities

IBM WebSphere Application Server Multiple Vulnerabilities

IBM WebSphere Application Server Remote Code Execution Vulnerability (CVE-2018-1904)

IBM WebSphere Application Server Virtual Enterprise 7.0.x / Network Deployment 8.5.x < 8.5.5.16 / Network Deployment 9.0.0.x <= 9.0.0.11 Remote Code Execution Vulnerability (CVE-2019-4279)

IBM WebSphere Application Server Virtual Enterprise 7.0.x <= 7.0.0.6 / Virtual Enterprise 8.0.x / 8.5.5.x < 8.5.5.17 / 9.0.x < 9.0.5.1 Information Disclosure (CVE-2019-4505)

IBM WebSphere Edge Caching Proxy DoS

IBM WebSphere HTTP Request Header Remote Overflow

IBM WebSphere Java Object Deserialization RCE

Icecast / libshout Multiple Remote Overflows

Icecast Crafted URI Remote DoS

Icecast HTTP Basic Authorization Remote Overflow DoS

Icecast HTTP Header Processing Remote Overflow

Icecast Multiple Unspecified Remote Overflows

Icecast utils.c fd\_write Function Format String

IceWarp Webmail Detection

iChat Server Traversal Arbitrary File Access

IIS Detailed Error Information Disclosure

IMail Host: Header Field Handling Remote Overflow

Intel Active Management Technology (AMT) Web UI Clickjacking Weakness (INTEL-SA-00081) (remote check)

Intel Management Engine Active Management Technology (AMT) Remote Access Enabled

Intel Management Engine Authentication Bypass (INTEL-SA-00075) (remote check)

Intel Management Engine Insecure Read / Write Operations RCE (INTEL-SA-00075) (remote check)

Intrusion.com SecureNet Provider Detection

Intrusion.com SecureNet Sensor Detection

iPlanet Application Server Prefix Remote Overflow

iPlanet Certificate Management Traversal Arbitrary File Access

iPlanet Chunked Encoding Processing Remote Overflow

iPlanet Directory Server Traversal Arbitrary File Access

iPlanet Search Engine search CGI Arbitrary File Access

iPlanet Web Server Enterprise Edition URL-encoded Host: Information Disclosure

iPlanet Web Server shtml File Handling Remote Overflow

ipMonitor Encoded Traversal Arbitrary File Access

Ipswitch IMail Web Calendaring Server GET Request Traversal Arbitrary File Access

JBoss Administration Console Default Credentials

JBoss Enterprise Application Platform '/jmx-console' Authentication Bypass

JBoss Enterprise Application Platform '/web-console' Authentication Bypass

JBoss Enterprise Application Platform doFilter() Method Insecure Deserialization RCE

JBoss Java Object Deserialization RCE

Jetty < 4.2.19 HTTP Server HttpRequest.java Content-Length Handling Remote Overflow DoS

Jetty HttpParser Error Remote Memory Disclosure

Jigsaw < 2.2.4 Unspecified URI Parsing Unspecified Vulnerability

Jigsaw Webserver MS/DOS Device Request Remote DoS

JRun Multiple Vulnerabilities (OF, XSS, ID, Hijacking)

Kerio MailServer < 6.0.1 Embedded HTTP Server Unspecified Issue

Kernel vulnerabilities detected in banner reporting (PCI-DSS check)

KeyFocus (KF) Web Server Null Byte Request Restricted File / Directory Access

LabVIEW Web Server HTTP Get Newline DoS

lighttpd 1.4.31 http\_request\_split\_value Function Header Handling DoS

lighttpd < 1.3.8 Null Byte Request CGI Script Source Code Disclosure

lighttpd < 1.4.16 Multiple Vulnerabilities

lighttpd < 1.4.19 Multiple Vulnerabilities

lighttpd < 1.4.20 Multiple Vulnerabilities

lighttpd < 1.4.26 or 1.5.0 Denial of Service

lighttpd < 1.4.28 Insecure Temporary File Creation

lighttpd < 1.4.30 base64\_decode Function Out-of-Bounds Read Error DoS

lighttpd < 1.4.34 Multiple Vulnerabilities

lighttpd < 1.4.35 Multiple Vulnerabilities

lighttpd < 1.4.36 Multiple Vulnerabilities

lighttpd < 1.4.50 Multiple Vulnerabilities

lighttpd < 1.4.51 Multiple Vulnerabilities

lighttpd HTTP Server Detection

lighttpd mod\_fastcgi HTTP Request Header Remote Overflow

lighttpd on Windows < 1.4.10a Crafted Filename Request Script Source Disclosure

lighttpd PHP File Trailing Slash Request Source Disclosure

lighttpd Status Module Remote Information Disclosure

LiteServe HTTP Service Malformed URL Decoding Remote DoS

LiteSpeed Web Server Source Code Information Disclosure

LocalWeb2000 2.1.0 Multiple Remote Vulnerabilities

MDaemon WebConfig HTTP Server URL Overflow DoS

MDaemon WorldClient HTTP Server URL Overflow DoS

MDG Web Server 4D GET Request Remote Overflow

MetaInfo Web Server Traversal Arbitrary Command Execution

Microsoft .NET Custom Errors Not Set

Microsoft .NET Handlers Enumeration

Microsoft .NET Version Information Disclosure

Microsoft ASP.NET MS-DOS Device Name DoS

Microsoft ASP.NET MS-DOS Device Name DoS (PCI-DSS check)

Microsoft ASP.NET ValidateRequest Filters Bypass

Microsoft Content Management Server (MCMS) 2001 Multiple Remote Vulnerabilities

Microsoft Data Access Components RDS Data Stub Remote Overflow

Microsoft FrontPage dvwssr.dll Multiple Vulnerabilities

Microsoft FrontPage Extensions authors.pwd Information Disclosure

Microsoft FrontPage Extensions Check

Microsoft FrontPage Extensions MS-DOS Device Request DoS

Microsoft FrontPage Server Extensions (fp30reg.dll) Debug Function Remote Overflow (MS03-051 / 813360)

Microsoft FrontPage Unpassworded Installation

Microsoft IIS .HTR Filter Multiple Overflows (MS02-028)

Microsoft IIS .HTR ISAPI Filter Enabled

Microsoft IIS .IDA ISAPI Filter Enabled

Microsoft IIS / Site Server codebrws.asp Arbitrary Source Disclosure

Microsoft IIS / Site Server viewcode.asp Arbitrary File Access

Microsoft IIS /iisadmin Unrestricted Access

Microsoft IIS /iisadmpwd/aexp2.htr Password Policy Bypass

Microsoft IIS 404 Response Service Pack Signature

Microsoft IIS 5 .printer ISAPI Filter Enabled

Microsoft IIS 5.0 ServerVariables\_Jscript.asp Path Disclosure

Microsoft IIS 5.0 WebDAV Malformed PROPFIND Request Remote DoS

Microsoft IIS 6.0 Unsupported Version Detection

Microsoft IIS 7.0 Vulnerabilities (uncredentialed) (PCI/DSS)

Microsoft IIS ASP ISAPI Filter Multiple Overflows

Microsoft IIS ASP::$DATA ASP Source Disclosure

Microsoft IIS Authentication Method Enumeration

Microsoft IIS bdir.htr Arbitrary Directory Listing

Microsoft IIS Cookie information disclosure

Microsoft IIS Frontpage Server Extensions (FPSE) Malformed Form DoS

Microsoft IIS FrontPage Server Extensions (FPSE) shtml.exe Path Disclosure

Microsoft IIS ISAPI Filter Multiple Vulnerabilities (MS01-044)

Microsoft IIS ISM.DLL HTR Request Remote Overflow

Microsoft IIS Malformed File Extension URL DoS

Microsoft IIS Malformed HTTP Request Header Remote DoS

Microsoft IIS MDAC RDS (msadcs.dll) Arbitrary Remote Command Execution

Microsoft IIS Multiple .cnf File Information Disclosure

Microsoft IIS Multiple Remote DoS (MS02-018 / Q319733)

Microsoft IIS perl.exe HTTP Path Disclosure

Microsoft IIS repost.asp File Upload

Microsoft IIS Source Fragment Disclosure

Microsoft IIS Traversal GET Request Remote DoS

Microsoft IIS Unicode Remote Command Execution

Microsoft IIS WebDAV Malformed PROPFIND Request Remote DoS

Microsoft IIS WebDAV ntdll.dll Remote Overflow (MS03-007)

Microsoft IIS WebDAV SEARCH Method Arbitrary Directory Forced Listing

Microsoft IIS WebDAV Unicode Request Directory Security Bypass

Microsoft IIS WebHits null.htw .asp Source Disclosure

Microsoft IIS webhits.dll Hit-Highlighting Authentication Bypass

Microsoft IIS/PWS %2e Request ASP Source Disclosure

Microsoft Media Services ISAPI nsiislog.dll Multiple Overflows

Microsoft SharePoint Server Detection

Microsoft Windows IIS Default Index Page

Microsoft Windows Server 2003 IIS 6.0 WebDAV PROPFIND Request Handling RCE (EXPLODINGCAN)

Microsoft Windows Server 2003 R2 IIS 6.0 WebDAV PROPFIND Request Handling RCE (EXPLODINGCAN)

MikroTik RouterOS with Blank Password (HTTP)

MiniShare Webserver HTTP GET Request Remote Overflow

MiniWebsvr GET Request Traversal Arbitrary File Access

mod\_auth\_any for Apache Metacharacter Remote Command Execution

mod\_frontpage for Apache fpexec Remote Overflow

mod\_gzip Debug Mode mod\_gzip\_printf Remote Format String

mod\_gzip Detection

mod\_mylo for Apache mylo\_log Logging Function HTTP GET Overflow

mod\_ntlm for Apache Multiple Remote Vulnerabilities

mod\_perl Apache::Status Info Disclosure

mod\_perl Apache::Status URI XSS

mod\_python < 2.7.8 Module Importing Privilege Function Execution

mod\_python < 2.7.9 / 3.0.4 Malformed Query String DoS

mod\_ssl ssl\_util\_uuencode\_binary Remote Overflow

mod\_survey For Apache ENV Tags SQL Injection

Mongoose URI Trailing Slash Request Source Code Disclosure

Monkey HTTP Daemon (monkeyd) Post\_Method Function Crafted Content-Length Header DoS

Monkey HTTP Daemon (monkeyd) PostMethod() Function Remote Overflow

MS00-006: Microsoft IIS IDA/IDQ Multiple Vulnerabilities (uncredentialed check)

MS00-019: Microsoft IIS ISAPI Virtual Directory UNC Mapping ASP Source Disclosure (uncredentialed check)

MS01-023: Microsoft IIS 5.0 Malformed HTTP Printer Request Header Remote Buffer Overflow (953155) (uncredentialed check)

MS01-026 / MS01-044: Microsoft IIS Remote Command Execution (uncredentialed check)

MS01-035: Microsoft IIS FrontPage fp30reg.dll Remote Overflow (uncredentialed check)

MS02-053: Microsoft FrontPage Extensions shtml.exe Remote Overflow (uncredentialed check)

MS12-026: Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Information Disclosure (2663860) (uncredentialed check)

Multi-Threaded HTTP Server v1.1 for Zimbra

Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure

Multiple Web Server on Windows MS/DOS Device Request Remote DOS

Multiple Web Server ~nobody/ Request Arbitrary File Access

MultiTech Proxy Server Default Null Password

MyServer 0.4.3 / 0.7 Crafted Traversal Arbitrary File Access

MyServer <= 0.4.2 Multiple Remote DoS

MyServer HTTP POST Request Remote Overflow DoS

NaviCOPA ::$DATA Extension Request Source Code Disclosure

NaviCOPA < 3.01 6th February 2009 Multiple Vulnerabilities

NaviCOPA Encoded Space Request Source Code Disclosure

NaviCOPA Trailing Dot Source Code Disclosure

NetApp SANtricity Web Services Proxy Detection

NetApp SANtricity Web Services Proxy Unauthenticated RCE

NETGEAR ProSafe VPN Firewall Web Server Malformed Basic Authorization Header Remote DoS

NetScaler Unencrypted Web Management Interface

NetScaler Web Management Interface Cookie Credentials Encryption Weakness

NetScaler Web Management Interface IP Address Cookie Information Disclosure

NetScaler Web Management Successful Authentication

Netscape / iPlanet .perf Remote Information Disclosure

Netscape Administration Server /admin-serv/config/admpw Admin Password Disclosure

Netscape Enterprise Server Accept Header Remote Overflow

Netscape Enterprise Server Basic Authentication Buffer Overflow RCE (EGGBASKET/XP\_NS-HTTPD)

Netscape Enterprise Server Long Traversal Request Remote DoS

Netscape Enterprise Server SSL Handshake DoS

Netscape Enterprise Web Publishing INDEX Command Arbitrary Directory Listing

Netscape FastTrack get Command Forced Directory Listing

Netscape Server ?PageServices Request Forced Directory Listing

Netscape Server ?wp-\* Publishing Tags Forced Directory Listing

Network Camera Web Server Detection

NetworkActiv Web Server Encoded URL Request Remote DoS

nginx 0.8.x < 0.8.33 / 0.7.x < 0.7.65 Windows Filename Pseudonyms (CORE-2010-0121)

nginx 1.0.7 - 1.0.14 / 1.1.3 - 1.1.18 ngx\_http\_mp4\_module Buffer Overflow

nginx 1.5.10 SPDY Memory Corruption

nginx 1.9.5 < 1.16.1 / 1.17.x < 1.17.3 Multiple Vulnerabilties

nginx 1.9.x < 1.9.6 HTTPv2 PRI Double-Free DoS

nginx 1.x < 1.14.1 / 1.15.x < 1.15.6 Multiple Vulnerabilties

nginx < 0.7.63 / 0.8.x < 0.8.17 Directory Traversal

nginx < 0.7.64 / 0.8.x < 0.8.23 Multiple Vulnerabilities

nginx < 0.7.66 / 0.8.x < 0.8.40 Information Disclosure

nginx < 0.7.67 / 0.8.x < 0.8.41 DoS

nginx < 1.0.10 ngx\_resolver\_copy Function DNS Response Parsing Buffer Overflow

nginx < 1.0.14 / 1.1.17 HTTP Header Response Memory Disclosure

nginx < 1.10.1 / 1.11.x < 1.11.1 Denial-of-Service Vulnerability

nginx < 1.13.2 Integer Overflow Vulnerability

nginx < 1.17.7 Information Disclosure

nginx < 1.4.4 / 1.5.7 ngx\_parse\_http Security Bypass

nginx < 1.4.7 / 1.5.12 SPDY Heap Buffer Overflow

nginx < 1.6.1 / 1.7.4 SMTP STARTTLS Command Injection

nginx < 1.6.2 / 1.7.5 SSL Session Reuse

nginx < 1.8.1 / 1.9.x < 1.9.10 Multiple Vulnerabilities

nginx <= 1.3.13 Insecure Log Permissions

nginx Data Disclosure Vulnerability

nginx HTTP Request Multiple Vulnerabilities

nginx HTTP Server Detection

nginx ngx\_http\_proxy\_module.c Memory Disclosure

nginx ngx\_http\_proxy\_module.c Multiple Vulnerabilities

nginx on Windows Directory Aliases Access Restriction Bypass

NGINX Unit 0.x > 0.3 / 1.x < 1.7.1 Heap Buffer Overflow (CVE-2019-7401)

NGINX Unit HTTP Server Detection

Nonexistent Page (404) Physical Path Disclosure

Nortel Contivity HTTP Server cgiproc Special Character DoS

Novell eDirectory < 8.8 SP3 FTF3 iMonitor HTTP Accept-Language Header Overflow

Novell eDirectory DHost Predictable Session ID

Novell File Reporter Agent Detection

Novell File Reporter Engine Detection

Novell GroupWise Document Viewer Agent Web Console Accessible

Novell GroupWise Enhancement Pack Java Server URL Handling Overflow DoS

Novell GroupWise Internet Agent Accessible

Novell GroupWise MTA Web Console Accessible

Novell GroupWise WebAccess Accessible

Novell Messenger Server Process Memory Remote Information Disclosure

Novell Open Enterprise Server Remote Manager (novell-nrm) POST Request Content-Length Overflow

Null httpd Content-Length Header Handling Remote Overflow

OmniHTTPd Pro Long POST Request DoS

oops WWW Proxy Server Reverse DNS Response Overflow

OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability

OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service

OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities

OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities

OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)

OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)

OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities

OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities

OpenSSL 0.9.8 < 0.9.8zh X509\_ATTRIBUTE Memory Leak DoS

OpenSSL 0.9.8s DTLS Denial of Service

OpenSSL 1.0.0 < 1.0.0-beta2 DoS

OpenSSL 1.0.0 < 1.0.0h Multiple Vulnerabilities

OpenSSL 1.0.0 < 1.0.0i ASN.1 asn1\_d2i\_read\_bio Memory Corruption

OpenSSL 1.0.0 < 1.0.0j DTLS CBC Denial of Service

OpenSSL 1.0.0 < 1.0.0k Multiple Vulnerabilities

OpenSSL 1.0.0 < 1.0.0l DTLS Security Bypass

OpenSSL 1.0.0 < 1.0.0m Multiple Vulnerabilities

OpenSSL 1.0.0 < 1.0.0n Multiple Vulnerabilities

OpenSSL 1.0.0 < 1.0.0p Multiple Vulnerabilities (FREAK)

OpenSSL 1.0.0 < 1.0.0r Multiple Vulnerabilities

OpenSSL 1.0.0 < 1.0.0s Multiple Vulnerabilities

OpenSSL 1.0.0 < 1.0.0t Multiple DoS

OpenSSL 1.0.0 < 1.0.1o Multiple Vulnerabilities (POODLE)

OpenSSL 1.0.0f DTLS Denial of Service

OpenSSL 1.0.1 < 1.0.1a ASN.1 asn1\_d2i\_read\_bio Memory Corruption

OpenSSL 1.0.1 < 1.0.1c TLS/DTLS CBC Denial of Service

OpenSSL 1.0.1 < 1.0.1d Multiple Vulnerabilities

OpenSSL 1.0.1 < 1.0.1e Information Disclosure

OpenSSL 1.0.1 < 1.0.1f Multiple Vulnerabilities

OpenSSL 1.0.1 < 1.0.1g Multiple Vulnerabilities (Heartbleed)

OpenSSL 1.0.1 < 1.0.1h Multiple Vulnerabilities

OpenSSL 1.0.1 < 1.0.1i Multiple Vulnerabilities

OpenSSL 1.0.1 < 1.0.1j Multiple Vulnerabilities (POODLE)

OpenSSL 1.0.1 < 1.0.1k Multiple Vulnerabilities (FREAK)

OpenSSL 1.0.1 < 1.0.1m Multiple Vulnerabilities

OpenSSL 1.0.1 < 1.0.1n Multiple Vulnerabilities (Logjam)

OpenSSL 1.0.1 < 1.0.1o ASN.1 Encoder Negative Zero Value Handling RCE

OpenSSL 1.0.1 < 1.0.1p Multiple Vulnerabilities

OpenSSL 1.0.1 < 1.0.1q Multiple DoS

OpenSSL 1.0.1 < 1.0.1r Multiple Vulnerabilities (Logjam)

OpenSSL 1.0.1 < 1.0.1s Multiple Vulnerabilities (DROWN)

OpenSSL 1.0.1 < 1.0.1t Multiple Vulnerabilities

OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities (SWEET32)

OpenSSL 1.0.2 < 1.0.2a Multiple Vulnerabilities

OpenSSL 1.0.2 < 1.0.2b Multiple Vulnerabilities (Logjam)

OpenSSL 1.0.2 < 1.0.2c ASN.1 Encoder Negative Zero Value Handling RCE

OpenSSL 1.0.2 < 1.0.2d Multiple Vulnerabilities

OpenSSL 1.0.2 < 1.0.2e Multiple Vulnerabilities

OpenSSL 1.0.2 < 1.0.2f Multiple Vulnerabilities (Logjam)

OpenSSL 1.0.2 < 1.0.2g Multiple Vulnerabilities (DROWN)

OpenSSL 1.0.2 < 1.0.2h Multiple Vulnerabilities

OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32)

OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities

OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities

OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities

OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability

OpenSSL 1.0.2i CRL Handling NULL Pointer Dereference DoS

OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue

OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities

OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities

OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities

OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability

OpenSSL 1.1.0 < 1.1.0a Multiple Vulnerabilities

OpenSSL 1.1.0 < 1.1.0c Multiple Vulnerabilities

OpenSSL 1.1.0 < 1.1.0d Multiple Vulnerabilities

OpenSSL 1.1.0 < 1.1.0e Encrypt-Then-Mac Extension DoS

OpenSSL 1.1.0 < 1.1.0g RSA/DSA Unspecified Carry Issue

OpenSSL 1.1.0 < 1.1.0h AVX2 Montgomery Multiplication Private Key Derivation Weakness

OpenSSL 1.1.0 < 1.1.0i Multiple Vulnerabilities

OpenSSL 1.1.0 < 1.1.0j Multiple Vulnerabilities

OpenSSL 1.1.0 < 1.1.0k Vulnerability

OpenSSL 1.1.0 < 1.1.0l Multiple Vulnerabilities

OpenSSL 1.1.0a read\_state\_machine() Function Message Handling RCE

OpenSSL 1.1.1 < 1.1.1a Multiple Vulnerabilities

OpenSSL 1.1.1 < 1.1.1c Vulnerability

OpenSSL 1.1.1 < 1.1.1d Multiple Vulnerabilities

OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability

OpenSSL 1.x < 1.0.0e Multiple Vulnerabilities

OpenSSL 1.x < 1.0.0f Multiple Vulnerabilities

OpenSSL < 0.9.2b Session Reuse

OpenSSL < 0.9.5a /dev/random Check Failure

OpenSSL < 0.9.6b Predictable Random Generator

OpenSSL < 0.9.6e Multiple Vulnerabilities

OpenSSL < 0.9.6f Denial of Service

OpenSSL < 0.9.6j / 0.9.7b Multiple Vulnerabilities

OpenSSL < 0.9.6k Denial of Service

OpenSSL < 0.9.6l Denial of Service

OpenSSL < 0.9.6m / 0.9.7d Denial of Service

OpenSSL < 0.9.6m / 0.9.7d Multiple Remote DoS

OpenSSL < 0.9.7-beta3 Buffer Overflow

OpenSSL < 0.9.7c ASN.1 Decoding Vulnerabilities

OpenSSL < 0.9.7f Insecure Temporary File Creation

OpenSSL < 0.9.7h / 0.9.8a Protocol Version Rollback

OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability

OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities

OpenSSL < 0.9.8 Weak Default Configuration

OpenSSL < 0.9.8f Multiple Vulnerabilities

OpenSSL < 0.9.8h Multiple Vulnerabilities

OpenSSL < 0.9.8i Denial of Service

OpenSSL < 0.9.8j Signature Spoofing

OpenSSL < 0.9.8k Multiple Vulnerabilities

OpenSSL < 0.9.8k Signature Repudiation

OpenSSL < 0.9.8l Multiple Vulnerabilities

OpenSSL < 0.9.8m Multiple Vulnerabilities

OpenSSL < 0.9.8n Multiple Vulnerabilities

OpenSSL < 0.9.8o / 1.0.0a Multiple Vulnerabilities

OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow

OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability

OpenSSL < 0.9.8q / 1.0.0c Multiple Vulnerabilities

OpenSSL < 0.9.8s Multiple Vulnerabilities

OpenSSL < 0.9.8u Multiple Vulnerabilities

OpenSSL < 0.9.8w ASN.1 asn1\_d2i\_read\_bio Memory Corruption

OpenSSL < 0.9.8y Multiple Vulnerabilities

OpenSSL < 1.0.2i Default Weak 64-bit Block Cipher (SWEET32)

OpenSSL < vA.00.09.07l on HP-UX Local Denial of Service

OpenSSL AES Timing Attack

OpenSSL OCSP Stapling Denial of Service

OpenSSL Unsupported

OpenSSL Version Detection

OpenText FirstClass HTTP Daemon /Search Large Request Remote DoS

OpenVMS WASD HTTP Server Multiple Vulnerabilities

Operating System Unsupported Version Detection in banner reporting (PCI-DSS check)

Oracle Application Express (Apex) Administration Interface is Accessible

Oracle Application Express (Apex) CVE-2008-4005

Oracle Application Express (Apex) CVE-2009-0981

Oracle Application Express (Apex) CVE-2009-1993

Oracle Application Express (Apex) CVE-2010-0076

Oracle Application Express (Apex) CVE-2010-0892

Oracle Application Express (Apex) CVE-2011-3525

Oracle Application Express (Apex) CVE-2012-1708

Oracle Application Express (Apex) Detection

Oracle Application Express (Apex) Unspecified Issues (pre 2.2.1)

Oracle Application Express (Apex) Unspecified Issues (pre 3.0.1)

Oracle Application Express (Apex) Unspecified Issues (pre 3.1)

Oracle Application Express (Apex) Version Detection

Oracle Application Server Multiple Vulnerabilities

Oracle Fusion Middleware HTTP Server (July 2012 CPU)

Oracle Fusion Middleware Oracle HTTP Server (Apr 2019 CPU)

Oracle Fusion Middleware Oracle HTTP Server (Apr 2020 CPU)

Oracle Fusion Middleware Oracle HTTP Server (Jan 2020 CPU)

Oracle Fusion Middleware Oracle HTTP Server (Jul 2019 CPU)

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities (January 2015 CPU)

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities (January 2018 CPU)

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities (January 2019 CPU)

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities (July 2014 CPU)

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities (July 2016 CPU)

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities (October 2015 CPU)

Oracle Fusion Middleware Oracle HTTP Server Multiple Vulnerabilities (October 2018 CPU)

Oracle Fusion Middleware Security Service Information Disclosure (January 2015 CPU) (BEAST)

Oracle Fusion Middleware WebLogic Component DoS

Oracle GlassFish Embedded Server Vulnerabilities (January 2016 CPU)

Oracle GlassFish HTTP Server Version

Oracle GlassFish Server 2.1.1 < 2.1.1 Patch15 Administration Component Unspecified Vulnerability

Oracle GlassFish Server 2.1.1 < 2.1.1.14 / 3.0.1 < 3.0.1.4 / 3.1.1 < 3.1.1.1 Web Container Component Unspecified Vulnerability

Oracle GlassFish Server 2.1.1 < 2.1.1.15 / 3.0.1 < 3.0.1.5 / 3.1.1 < 3.1.1.2 Hash Collision DoS

Oracle GlassFish Server 2.1.1.x < 2.1.1.27 NSS ASN.1 Decoder RCE (April 2016 CPU)

Oracle GlassFish Server 2.1.1.x < 2.1.1.28 Information Disclosure (July 2016 CPU)

Oracle GlassFish Server 2.1.1.x < 2.1.1.29 / 3.0.1.x < 3.0.1.14 / 3.1.2.x < 3.1.2.15 Java Server Faces RCE (October 2016 CPU)

Oracle GlassFish Server 2.1.1.x < 2.1.1.29 Mozilla NSS ASN.1 Structure Handling RCE (October 2016 CPU)

Oracle GlassFish Server 2.1.1.x < 2.1.1.30 / 3.0.1.x < 3.0.1.15 / 3.1.2.x < 3.1.2.16 Multiple Vulnerabilities (January 2017 CPU)

Oracle GlassFish Server 3.0.1 / 3.1.1 < 3.0.1.5 / 3.1.1.3 Administration Component Unspecified Vulnerability

Oracle GlassFish Server 3.0.1 / 3.1.2 / Enterprise 2.1.1 DoS

Oracle GlassFish Server 3.0.1 < 3.0.1.7 / 3.1.2 < 3.1.2.5 Multiple Vulnerabilities (April 2013 CPU)

Oracle GlassFish Server 3.0.1.x < 3.0.1.14 Multiple Vulnerabilities (July 2016 CPU)

Oracle GlassFish Server 3.0.1.x < 3.0.1.17 / 3.1.2.x < 3.1.2.18 (October 2017 CPU)

Oracle GlassFish Server 3.1.1 < 3.1.1.2 Administration Component Unspecified Vulnerability

Oracle GlassFish Server 3.1.1 < 3.1.1.3 Multiple Vulnerabilities (April 2012 CPU)

Oracle GlassFish Server 3.1.2.x < 3.1.2.15 Multiple Vulnerabilities (July 2016 CPU)

Oracle GlassFish Server 3.1.2.x < 3.1.2.17 Java Server Faces Information Disclosure (April 2017 CPU)

Oracle GlassFish Server 3.1.2.x < 3.1.2.19 (October 2018 CPU)

Oracle GlassFish Server < 3.0.1.22 Multiple Vulnerabilities

Oracle GlassFish Server Administration Console

Oracle GlassFish Server Administrative Console Authentication Bypass

Oracle GlassFish Server Multiple Vulnerabilities (April 2015 CPU) (POODLE)

Oracle GlassFish Server Multiple Vulnerabilities (July 2014 CPU)

Oracle GlassFish Server Multiple Vulnerabilities (July 2015 CPU)

Oracle GlassFish Server Multiple Vulnerabilities (October 2013 CPU)

Oracle GlassFish Server Unspecified Information Disclosure (October 2015 CPU)

Oracle GlassFish Server Unspecified Vulnerability (January 2015 CPU)

Oracle HTTP Server (January 2006 CPU)

Oracle HTTP Server (January 2007 CPU)

Oracle HTTP Server (October 2006 CPU)

Oracle HTTP Server Version

Oracle iPlanet Web Server 6.1.x < 6.1.21 / 7.0.x < 7.0.22 NSS Signature Handling Remote Code Injection

Oracle iPlanet Web Server 7.0.x < 7.0.15 Multiple Vulnerabilities

Oracle iPlanet Web Server 7.0.x < 7.0.20 Multiple Vulnerabilities

Oracle iPlanet Web Server 7.0.x < 7.0.21 NSS Signature Verification Vulnerability

Oracle iPlanet Web Server 7.0.x < 7.0.23 NSS ASN.1 Decoder RCE (April 2016 CPU)

Oracle iPlanet Web Server 7.0.x < 7.0.27 NSS Unspecified Vulnerability (January 2018 CPU)

Oracle iPlanet Web Server 7.0.x < 7.0.9 Multiple Vulnerabilities

Oracle iPlanet Web Server Detection

Oracle WebLogic Admin State Unspecified Privilege Escalation (CVE-2008-4011)

Oracle WebLogic Console / WLST Unspecified Privilege Escalation (CVE-2008-2577)

Oracle WebLogic Detection (Combined)

Oracle WebLogic DoS (CVE-2008-2582)

Oracle WebLogic ForeignJMS Component Unspecified Information Disclosure (CVE-2008-2576)

Oracle WebLogic HTTP Detection

Oracle WebLogic Java Object Deserialization RCE

Oracle WebLogic Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU)

Oracle WebLogic JSP Pages and Servlets Unspecified Information Disclosure (CVE-2008-5460)

Oracle WebLogic JSP Pages Unspecified Information Disclosure (CVE-2008-2580)

Oracle WebLogic Multiple Authorizer Unspecified Privilege Escalation (CVE-2008-4009)

Oracle WebLogic Plugins Unspecified Remote Issue (CVE-2008-2579)

Oracle WebLogic Portal Elevation of Privilege (CVE-2008-5462)

Oracle WebLogic Server 10.3.6.0 / 12.1.3.0 / 12.2.1.3 Java Object Deserialization RCE (CVE-2018-3191)

Oracle WebLogic Server Deserialization RCE (CVE-2018-2628)

Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)

Oracle WebLogic Server Deserialization RCE (CVE-2019-2729)

Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU)

Oracle WebLogic Server Java Object Deserialization RCE (CVE-2018-3245)

Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)

Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU)

Oracle WebLogic Server mod\_wl Invalid Parameter Remote Overflow (1150354)

Oracle WebLogic Server mod\_wl POST Request Remote Overflow

Oracle WebLogic Server Plug-in HTTP Injection

Oracle WebLogic Server Plug-in Remote Overflow (1166189)

Oracle WebLogic Server Servlet Container Session Fixation

Oracle WebLogic Server Servlets Unspecified Unauthenticated Remote Issue (CVE-2008-4013)

Oracle WebLogic Server Unspecified Information Disclosure (CVE-2008-2578)

Oracle WebLogic Server Web Services Security Policy not Enforced (CVE-2008-5459)

Oracle WebLogic UDDI Explorer Unspecified Vulnerability (CVE-2008-2581)

Oracle WebLogic WLS Unspecified Vulnerability (CVE-2008-5461)

Oracle WebLogic WLS9-async Remote Code Execution (remote check)

Oracle WebLogic WSAT Remote Code Execution

Orange Web Server Malformed HTTP Request Remote DoS

OS vulnerabilities detected in banner reporting (PCI-DSS check)

Personal Web Sharing Long HTTP Request DoS

PHP expose\_php Information Disclosure

PHP File Upload Capability Hidden Form Field Modification Arbitrary File Access

PHP mime\_split Function POST Request Overflow

PHP Version Detection

Pi3Web < 2.0.1 CGI Handler Long Parameter Handling Overflow

Pi3Web Malformed GET Request Remote Overflow

Pi3Web tstisap.dll Long URL Overflow

Pivotal Web Server 5.x < 5.4.1 Multiple OpenSSL Vulnerabilities

Pivotal Web Server Version Detection

Polipo < 0.9.9 Unspecified Traversal Arbitrary File Access

Polycom ViaVideo Web Server Incomplete HTTP Connection Saturation Remote DoS

Polycom Videoconferencing Unit Detection

Protected Web Page Detection

Proxomitron GET Request Overflow Remote DoS

Proxy Web Server XSS

Quest NetVault Backup Server Detection

RaidenHTTPD < 1.1.34 Multiple Remote Vulnerabilities

RaidenHTTPD Crafted Request Arbitrary File Access

RaidenHTTPD Crafted Request Script Source Disclosure

Remote Help Detection

Remote web server screenshot

Resin for Windows \WEB-INF Traversal Arbitrary File Access

Resin for Windows Encoded URI Traversal Arbitrary File Access

Resin MS-DOS Device Request Path Disclosure

Resin Status Page Information Disclosure

Resin Traversal Arbitrary File Access

Restricted Web Pages Detection

Roxen Web Server /%00/ Encoded Request Forced Directory Listing

Ruby on Rails Multiple Method Session Fixation

Samba SWAT HTTP Basic Auth base64 Overflow

Sambar Server Cleartext Password Transmission

Sambar Server Default Accounts

Sami HTTP Server 1.0.4 GET Request Remote Overflow

Sami HTTP Server Multiple Remote Vulnerabilities

Savant Web Server Malformed Content-Length DoS

Savant Web Server Multiple Percent Request Remote DoS

SBLIM-SFCB Multiple Buffer Overflows

Script Src Integrity Check

SEDUM HTTP Server Long HTTP Request Overflow DoS

Session Fixation Attack on HTTP Cookies

Shambala Web Server Malformed HTTP GET Request DoS

ShowOff! Digital Media Software <= 1.5.4 Multiple Remote Vulnerabilities

SilverStream Directory Listing

SimpleServer:WWW Encoded Traversal Arbitrary Command Execution

SMC 2652W AP Malformed HTTP Request Remote DoS

SolarWinds Storage Resource Monitor Profiler addNewRule SQL Injection RCE

Sonatype Nexus Repository Manager Detection

Splunk 6.x < 6.0.3 Multiple OpenSSL Vulnerabilities (Heartbleed)

Splunk Enterprise 4.3.x / 5.0.x < 5.0.9 / 6.0.x < 6.0.5 / 6.1.x < 6.1.2 Multiple OpenSSL Vulnerabilities

Splunk Enterprise 5.0.x < 5.0.11 Multiple Vulnerabilities (POODLE)

Splunk Management API Detection

Splunk Unsupported Version Detection

Splunk Web Detection

Sun AnswerBook2 Web Server dwhttpd GET Request Remote Format String

Sun GlassFish Enterprise < 2.1 Patch 02 Denial of Service

Sun Java System ASP Server < 4.0.3 Multiple Vulnerabilities

Sun Java System Web Proxy Server Multiple Unspecified Remote DoS

Sun Java System Web Proxy Server Unspecified Remote Overflow

Sun Java System Web Server ::$DATA Extension Request JSP Resource Disclosure

Sun Java Web Console < 3.0.5 Remote File Enumeration

Sun Java Web Console BeginLogin.jsp redirect\_url Parameter URI Redirection

Sun Java Web Console LibWebconsole\_Services.SO Remote Format String

SWS Web Server Unfinished Line Remote DoS

Symantec Endpoint Protection Manager Java Object Deserialization RCE (SYM15-011)

TeamSpeak Server Administration Detection

TelCondex Simple Webserver Buffer Overflow

Tembria Server Monitor < 5.6.1 Denial of Service

Tembria Server Monitor Detection

Tenable SecurityCenter Multiple Apache Vulnerabilities (TNS-2015-11)

thttpd 2.0.7 Directory Traversal (Windows)

thttpd 2.04 If-Modified-Since Header Remote Buffer Overflow

thttpd Double Slash Request Arbitrary File Access

thttpd Host Header Traversal Arbitrary File Access

TinyWeb cgi-bin Crafted HTTP GET Request DoS

Tomcat /status Information Disclosure

Tornado < 2.2.1 HTTP Response Splitting

TP-Link HTTP Server Detection

Trend Micro OfficeScan Client Traversal Arbitrary File Access

Unsupported linux kernel version detected in banner reporting (PCI-DSS check)

Unsupported Web Server Detection

URLScan for IIS Detection

Veritas Cluster Management Console Detection

VisualRoute Web Server Detection

VMware AirWatch Console 9.1.x < 9.1.5 / 9.2.x < 9.2.2 XSRF

VMware AirWatch Console 9.1.x < 9.1.5.6 / 9.2.x < 9.2.3.27 / 9.3.x < 9.3.0.25 / 9.4.x < 9.4.0.22 / 9.5.x < 9.5.0.16 / 9.6.x < 9.6.0.7 / 9.7.x < 9.7.0.3 SAML Security Bypass

Vulture Reverse Proxy Detection

WAS Target Discovery for PCI

WAS Target Scanning for PCI

Web Application Cookies Are Expired

Web Application Cookies Not Marked HttpOnly

Web Application Cookies Not Marked Secure

Web Application Potentially Vulnerable to Clickjacking

Web Application Session Cookies Not Marked HttpOnly

Web Application Session Cookies Not Marked Secure

Web Application Sitemap

Web Application Tests Disabled

Web Form Sending Credentials Using GET (PCI-DSS check)

Web mirroring

Web mirroring stub

Web Server / Application favicon.ico Vendor Fingerprinting

Web Server Allows Password Auto-Completion

Web Server Crafted Request Vendor/Version Information Disclosure

Web Server Directory Enumeration

Web Server Directory Traversal Arbitrary File Access

Web Server Error Page Information Disclosure

Web Server GET Request Saturation Remote DoS

Web Server Harvested Email Addresses

Web Server HTTP 1.0 Header Remote Overflow

Web Server HTTP 1.1 Header Remote Overflow

Web Server HTTP Authorization Header Remote Overflow

Web Server HTTP Basic Authorization Header Remote Overflow DoS

Web Server HTTP Cookie Header Remote Overflow

Web Server HTTP Dangerous Method Detection

Web Server HTTP GET Request Version Number Handling Remote Overflow

Web Server HTTP Header Handling Remote Overflow

Web Server HTTP Header Information Disclosure

Web Server HTTP Header Internal IP Disclosure

Web Server HTTP Header Memory Exhaustion DoS

Web Server HTTP Method Handling Remote Overflow

Web Server HTTP OPTIONS Method URL Handling Remote Overflow

Web Server HTTP POST Method Handling Remote Overflow DoS

Web Server HTTP User-Agent Header Handling Remote Overflow

Web Server Incomplete Basic Authentication DoS

Web Server Load Balancer Detection

Web Server Long URL Handling Remote Overflow DoS

Web Server No 404 Error Code Check

Web Server on Extended Support

Web Server Potentially Hosting Copyrighted Material

Web Server PROPFIND Method Internal IP Disclosure

Web Server Reverse Proxy Detection

Web Server robots.txt Information Disclosure

Web Server SSL Port HTTP Traffic Detection

Web Server Transmits Cleartext Credentials

Web Server UDDI Detection

Web Server Unconfigured - Default Install Page Present

Web Server Uses Basic Authentication over HTTPS

Web Server Uses Basic Authentication Without HTTPS

Web Server Uses Non Random Session IDs

Web Site Hosting Malicious Binaries

WebDAV Detection

WebDAV Directory Enumeration

WebLogic Crafted GET Request Hostname Disclosure

WebLogic Server Double Dot GET Request Remote Overflow

WebLogic Server Encoded Request Directory Listing

WebLogic SSL Certificate Chain User Spoofing

WebServer 4 Everyone Host Field Header Buffer Overflow

WebWasher Classic Server Mode Arbitrary Proxy CONNECT Request

WindWeb <= 2.0 Malformed GET Request Remote DoS

WS-Management Server Detection

WsMp3 Daemon (WsMp3d) HTTP Traversal Arbitrary File Execution/Access

Xeneo Web Server %A Request Remote DoS

Xeneo Web Server 2.2.9.0 GET Request Remote Overflow DoS

Xerver < 4.20 Multiple Vulnerabilities

Xerver HTTP Response Splitting

Xerver Web Server < 2.20 Crafted C:/ Request Remote DoS

Xitami Malformed POST Request Infinite Loop Remote DoS

Xitami Web Server Administration Port Remote Overflow

Yawcam Web Server Traversal Arbitrary File Access

Yaws Web Server .yaws Script Null Byte Request Source Code Disclosure

Zeus Web Server Null Byte Request CGI Source Disclosure

Zinwave Series 3000 DAS Web Interface Detection

Zope < 2.1.7 DocumentTemplate Unauthorized DTML Entity Modification

Zope < 2.3.3 ZClass Permission Mapping Modification Local Privilege Escalation

Zope < 2.6.3 Multiple Vulnerabilities

Zope Image and File Update Data Protection Bypass

Zope Invalid Query Path Disclosure

Zope Malformed XML RPC Request Path Disclosure

Zope ZClass Modification Local DoS

# VMware ESX Local Security Checks

VMSA-2007-0006 : Critical security updates for all supported versions of VMware ESX Server, VMware Server, VMware Workstation, VMware ACE, and VMware Player

VMSA-2008-0001 : Moderate OpenPegasus PAM Authentication Buffer Overflow and updated service console packages

VMSA-2008-0002 : Low severity security update for VirtualCenter and ESX

VMSA-2008-0003 : Moderate: Updated aacraid driver and samba and python Service Console updates

VMSA-2008-0004 : Low: Updated e2fsprogs service console package

VMSA-2008-0006 : Updated libxml2 service console package

VMSA-2008-0007 : Moderate Updated Service Console packages pcre, net-snmp, and OpenPegasus

VMSA-2008-0009 : Updates to VMware Workstation, VMware Player, VMware ACE, VMware Fusion, VMware Server, VMware VIX API, VMware ESX, VMware ESXi resolve critical security issues

VMSA-2008-0010 : Updated Tomcat and Java JRE packages for VMware ESX 3.5 and VirtualCenter

VMSA-2008-0011 : Updated ESX service console packages for Samba and vmnix

VMSA-2008-0013 : Updated ESX packages for OpenSSL, net-snmp, perl

VMSA-2008-0014 : Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX, VMware VCB address information disclosure, privilege escalation and other security issues.

VMSA-2008-0015 : Updated ESXi and ESX 3.5 packages address critical security issue in openwsman

VMSA-2008-0016 : VMware Hosted products, VirtualCenter Update 3 and patches for ESX and ESXi resolve multiple security issues

VMSA-2008-0017 : Updated ESX packages for libxml2, ucd-snmp, libtiff

VMSA-2008-0018 : VMware Hosted products and patches for ESX and ESXi resolve two security issues

VMSA-2008-0019 : VMware Hosted products and patches for ESX and ESXi resolve a critical security issue and update bzip2

VMSA-2009-0001 : ESX patches address an issue loading corrupt virtual disks and update Service Console packages

VMSA-2009-0002 : VirtualCenter Update 4 and ESX patch update Tomcat to version 5.5.27

VMSA-2009-0003 : ESX 2.5.5 patch 12 updates service console package ed

VMSA-2009-0004 : ESX Service Console updates for openssl, bind, and vim

VMSA-2009-0005 : VMware Hosted products, VI Client and patches for ESX and ESXi resolve multiple security issues

VMSA-2009-0006 : VMware Hosted products and patches for ESX and ESXi resolve a critical security vulnerability

VMSA-2009-0007 : VMware Hosted products and ESX and ESXi patches resolve security issues

VMSA-2009-0008 : ESX Service Console update for krb5

VMSA-2009-0009 : ESX Service Console updates for udev, sudo, and curl

VMSA-2009-0014 : VMware ESX patches for DHCP, Service Console kernel, and JRE resolve multiple security issues

VMSA-2009-0015 : VMware hosted products and ESX patches resolve two security issues

VMSA-2009-0016 : VMware vCenter and ESX update release and vMA patch release address multiple security issues in third party components.

VMSA-2009-0017 : VMware vCenter, ESX patch and vCenter Lab Manager releases address XSS issues

VMSA-2010-0001 : ESX Service Console and vMA updates for nss and nspr

VMSA-2010-0002 : VMware vCenter update release addresses multiple security issues in Java JRE

VMSA-2010-0003 : ESX Service Console update for net-snmp

VMSA-2010-0004 : ESX Service Console and vMA third-party updates

VMSA-2010-0006 : ESX Service Console updates for samba and acpid

VMSA-2010-0007 : VMware hosted products, vCenter Server and ESX patches resolve multiple security issues

VMSA-2010-0009 : ESXi ntp and ESX Service Console third-party updates

VMSA-2010-0010 : ESX 3.5 third-party update for Service Console kernel

VMSA-2010-0013 : VMware ESX third-party updates for Service Console

VMSA-2010-0015 : VMware ESX third-party updates for Service Console

VMSA-2010-0016 : VMware ESXi and ESX third-party updates for Service Console and Likewise components

VMSA-2010-0017 : VMware ESX third-party update for Service Console kernel

VMSA-2010-0018 : VMware hosted products and ESX patches resolve multiple security issues

VMSA-2010-0019 : VMware ESX third-party updates for Service Console

VMSA-2010-0020 : VMware ESXi 4.1 Update Installer SFCB Authentication Flaw

VMSA-2011-0001 : VMware ESX third-party updates for Service Console packages glibc, sudo, and openldap

VMSA-2011-0003 : Third-party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX

VMSA-2011-0004 : VMware ESX/ESXi SLPD denial of service vulnerability and ESX third-party updates for Service Console packages bind, pam, and rpm.

VMSA-2011-0007 : VMware ESXi and ESX Denial of Service and third-party updates for Likewise components and ESX Service Console

VMSA-2011-0008 : VMware vCenter Server and vSphere Client security vulnerabilities

VMSA-2011-0009 : VMware hosted product updates, ESX patches and VI Client update resolve multiple security issues

VMSA-2011-0010 : VMware ESX third-party updates for Service Console packages glibc and dhcp

VMSA-2011-0012 : VMware ESXi and ESX updates to third-party libraries and ESX Service Console

VMSA-2011-0013 : VMware third-party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX

VMSA-2012-0001 : VMware ESXi and ESX updates to third-party library and ESX Service Console

VMSA-2012-0003 : VMware VirtualCenter Update and ESX 3.5 patch update JRE

VMSA-2012-0005 : VMware vCenter Server, Orchestrator, Update Manager, vShield, vSphere Client, Workstation, Player, ESXi, and ESX address several security issues

VMSA-2012-0006 : VMware Workstation, ESXi, and ESX address several security issues

VMSA-2012-0007 : VMware hosted products and ESXi/ESX patches address privilege escalation

VMSA-2012-0008 : VMware ESX updates to ESX Service Console

VMSA-2012-0009 : VMware Workstation, Player, Fusion, ESXi and ESX patches address critical security issues

VMSA-2012-0011 : VMware hosted products and ESXi and ESX patches address security issues

VMSA-2012-0012 : VMware ESXi update to third-party library

VMSA-2012-0013 : VMware vSphere and vCOps updates to third-party libraries

VMSA-2012-0016 : VMware security updates for vSphere API and ESX Service Console

VMSA-2012-0018 : VMware security updates for vCSA and ESXi

VMSA-2013-0001 : VMware vSphere security updates for the authentication service and third-party libraries

VMSA-2013-0002 : VMware ESX, Workstation, Fusion, and View VMCI privilege escalation vulnerability

VMSA-2013-0003 : VMware vCenter Server, ESXi and ESX address an NFC Protocol memory corruption and third-party library security issues.

VMSA-2013-0004 : VMware ESXi and ESX security update for third-party library

VMSA-2013-0007 : VMware ESX third-party update for Service Console package sudo

VMSA-2013-0009 : VMware vSphere, ESX and ESXi updates to third-party libraries

VMSA-2013-0011 : VMware ESXi and ESX address an NFC Protocol Unhandled Exception

VMSA-2013-0012 : VMware vSphere updates address multiple vulnerabilities

VMSA-2013-0014 : VMware Workstation, Fusion, ESXi and ESX patches address a guest privilege escalation

VMSA-2013-0015 : VMware ESX updates to third-party libraries

VMSA-2013-0016 : VMware ESXi and ESX unauthorized file access through vCenter Server and ESX

VMSA-2014-0001 : VMware Workstation, Player, Fusion, ESXi, ESX and vCloud Director address several security issues

VMSA-2014-0002 : VMware vSphere updates to third-party libraries

VMSA-2014-0003 : VMware vSphere Client updates address security vulnerabilities

VMSA-2014-0004 : VMware product updates address OpenSSL security vulnerabilities

VMSA-2014-0005 : VMware Workstation, Player, Fusion, and ESXi patches address a guest privilege escalation

VMSA-2014-0006 : VMware product updates address OpenSSL security vulnerabilities

VMSA-2014-0008 : VMware vSphere product updates to third-party libraries

VMSA-2014-0010 : VMware product updates address critical Bash security vulnerabilities (Shellshock)

VMSA-2014-0012 : VMware vSphere product updates address security vulnerabilities

VMSA-2015-0001 : VMware vCenter Server, ESXi, Workstation, Player, and Fusion updates address security issues (POODLE)

VMSA-2015-0007 : VMware vCenter and ESXi updates address critical security issues

VMSA-2016-0001 : VMware ESXi, Workstation, Player, and Fusion updates address important guest privilege escalation vulnerability

VMSA-2016-0002 : VMware product updates address a critical glibc security vulnerability

VMSA-2016-0014 : VMware ESXi, Workstation, Fusion, &amp; Tools updates address multiple security issues

VMSA-2016-0023 : VMware ESXi updates address a cross-site scripting issue

VMSA-2017-0006 : VMware ESXi, Workstation and Fusion updates address critical and moderate security issues

VMSA-2017-0015 : VMware ESXi, vCenter Server, Fusion and Workstation updates resolve multiple security vulnerabilities

VMSA-2017-0021 : VMware ESXi, vCenter Server Appliance, Workstation and Fusion updates address multiple security vulnerabilities

VMSA-2018-0002 : VMware ESXi, Workstation and Fusion updates address side-channel analysis due to speculative execution. (Spectre)

VMSA-2018-0004 : VMware vSphere, Workstation and Fusion updates add Hypervisor-Assisted Guest Remediation for speculative execution issue (Spectre)

VMSA-2018-0012 : VMware vSphere, Workstation and Fusion updates enable Hypervisor-Assisted Guest Mitigations for Speculative Store Bypass issue (Spectre)

VMSA-2018-0016 : VMware ESXi, Workstation, and Fusion updates address multiple out-of-bounds read vulnerabilities

VMSA-2018-0018 : VMware Horizon View Agent, VMware ESXi, Workstation, and Fusion updates resolve multiple security issues

VMSA-2018-0026 : VMware ESXi, Workstation, and Fusion updates address an out-of-bounds read vulnerability

VMSA-2018-0027 : VMware ESXi, Workstation, and Fusion updates address uninitialized stack memory usage

VMSA-2019-0005 : VMware ESXi, Workstation and Fusion updates address multiple security issues

VMSA-2019-0006 : VMware ESXi, Workstation and Fusion updates address multiple out-of-bounds read vulnerabilities

VMSA-2019-0008 : MDS Vulnerabilities (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

VMSA-2019-0011 : ESXi patches address partial denial of service vulnerability in hostd process

VMSA-2019-0012 : Out-of-bounds pixel shader vulnerabilities

VMSA-2019-0013 : Command injection and information disclosure vulnerabilities

VMSA-2019-0014 : Use-after-free vulnerability

VMSA-2019-0019 : Denial-of-service vulnerability

VMSA-2019-0020 : Hypervisor-Specific Mitigations for Denial-of-Service and Speculative-Execution Vulnerabilities

VMSA-2019-0022 : VMware ESXi updates address OpenSLP remote code execution vulnerability

VMware Active Virtual Machines

VMware ESX / ESXi Third-Party Libraries and Components (VMSA-2010-0009) (remote check)

VMware ESX / ESXi Tools Update Privilege Escalation (VMSA-2010-0018) (remote check)

VMware ESX / ESXi Unsupported Version Detection

VMware ESX Java Runtime Environment (JRE) Multiple Vulnerabilities (VMSA-2010-0002) (remote check)

VMware ESX Multiple Vulnerabilities (VMSA-2010-0007) (remote check)

VMware ESX Multiple Vulnerabilities (VMSA-2010-0013) (remote check)

VMware ESX Multiple Vulnerabilities (VMSA-2010-0015) (remote check)

VMware ESX Multiple Vulnerabilities (VMSA-2010-0019) (remote check)

VMware ESX Privilege Escalation (VMSA-2010-0017) (remote check)

VMware ESX Third-Party Libraries and Components Multiple Vulnerabilities (VMSA-2010-0006) (remote check)

VMware ESX Third-Party Libraries Multiple Vulnerabilities (VMSA-2010-0001) (remote check)

VMware ESX Third-Party Libraries Multiple Vulnerabilities (VMSA-2010-0004) (remote check)

VMware ESX/ESXi CIM Services Multiple Vulnerabilities

VMware Inactive Virtual Machines

VMware vCenter Active Virtual Machines

VMware vCenter Data Collection

VMware vCenter Inactive Virtual Machines

VMware vSphere Installed Patches

VMware vSphere Installed VIBs

# Virtuozzo Local Security Checks

Virtuozzo 6 : 389-ds-base / 389-ds-base-devel / 389-ds-base-libs (VZLSA-2017-0893)

Virtuozzo 6 : autocorr-af / autocorr-bg / autocorr-ca / etc (VZLSA-2017-0979)

Virtuozzo 6 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-0063)

Virtuozzo 6 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-1105)

Virtuozzo 6 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-1202)

Virtuozzo 6 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-1679)

Virtuozzo 6 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2019-1492)

Virtuozzo 6 : bluez / bluez-alsa / bluez-compat / bluez-cups / etc (VZLSA-2017-2685)

Virtuozzo 6 : cpupools / cpupools-features / etc (VZA-2018-006)

Virtuozzo 6 : cpupools / cpupools-features / etc (VZA-2018-034)

Virtuozzo 6 : cpupools / cpupools-features / etc (VZA-2018-055)

Virtuozzo 6 : cpupools / cpupools-features / etc (VZA-2019-040)

Virtuozzo 6 : dbus / dbus-devel / dbus-doc / dbus-libs / etc (VZLSA-2019-1726)

Virtuozzo 6 : dnsmasq / dnsmasq-utils (VZLSA-2017-2838)

Virtuozzo 6 : emacs-git / emacs-git-el / git / git-all / git-cvs / etc (VZLSA-2017-2485)

Virtuozzo 6 : emacs-mercurial / emacs-mercurial-el / mercurial / etc (VZLSA-2017-1576)

Virtuozzo 6 : firefox (VZLSA-2017-0190)

Virtuozzo 6 : firefox (VZLSA-2017-0459)

Virtuozzo 6 : firefox (VZLSA-2017-1104)

Virtuozzo 6 : firefox (VZLSA-2017-2831)

Virtuozzo 6 : freeradius / freeradius-krb5 / freeradius-ldap / etc (VZLSA-2017-1759)

Virtuozzo 6 : ghostscript / ghostscript-devel / ghostscript-doc / etc (VZLSA-2017-0014)

Virtuozzo 6 : ghostscript / ghostscript-devel / ghostscript-doc / etc (VZLSA-2017-1230)

Virtuozzo 6 : glibc / glibc-common / glibc-devel / glibc-headers / etc (VZLSA-2017-1480)

Virtuozzo 6 : glusterfs / glusterfs-api / glusterfs-api-devel / etc (VZLSA-2018-2892)

Virtuozzo 6 : httpd / httpd-devel / httpd-manual / httpd-tools / etc (VZLSA-2017-1721)

Virtuozzo 6 : httpd / httpd-devel / httpd-manual / httpd-tools / etc (VZLSA-2017-2478)

Virtuozzo 6 : httpd / httpd-devel / httpd-manual / httpd-tools / etc (VZLSA-2017-2972)

Virtuozzo 6 : jasper / jasper-devel / jasper-libs / jasper-utils (VZLSA-2017-1208)

Virtuozzo 6 : java-1.7.0-openjdk / java-1.7.0-openjdk-demo / etc (VZLSA-2017-0269)

Virtuozzo 6 : java-1.7.0-openjdk / java-1.7.0-openjdk-demo / etc (VZLSA-2017-1204)

Virtuozzo 6 : java-1.7.0-openjdk / java-1.7.0-openjdk-demo / etc (VZLSA-2017-2424)

Virtuozzo 6 : java-1.7.0-openjdk / java-1.7.0-openjdk-demo / etc (VZLSA-2018-3409)

Virtuozzo 6 : java-1.7.0-openjdk / java-1.7.0-openjdk-demo / etc (VZLSA-2019-0462)

Virtuozzo 6 : java-1.7.0-openjdk / java-1.7.0-openjdk-demo / etc (VZLSA-2019-3158)

Virtuozzo 6 : java-1.8.0-openjdk / java-1.8.0-openjdk-debug / etc (VZLSA-2017-0180)

Virtuozzo 6 : java-1.8.0-openjdk / java-1.8.0-openjdk-debug / etc (VZLSA-2017-1109)

Virtuozzo 6 : java-1.8.0-openjdk / java-1.8.0-openjdk-debug / etc (VZLSA-2017-1789)

Virtuozzo 6 : java-1.8.0-openjdk / java-1.8.0-openjdk-debug / etc (VZLSA-2017-2998)

Virtuozzo 6 : java-1.8.0-openjdk / java-1.8.0-openjdk-debug / etc (VZLSA-2018-2943)

Virtuozzo 6 : java-1.8.0-openjdk / java-1.8.0-openjdk-debug / etc (VZLSA-2019-1811)

Virtuozzo 6 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0036)

Virtuozzo 6 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0293)

Virtuozzo 6 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0307)

Virtuozzo 6 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0892)

Virtuozzo 6 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-1372)

Virtuozzo 6 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-1486)

Virtuozzo 6 : libsmbclient / libsmbclient-devel / samba / etc (VZLSA-2017-1270)

Virtuozzo 6 : libsmbclient / libsmbclient-devel / samba / etc (VZLSA-2017-2789)

Virtuozzo 6 : libssh2 / libssh2-devel / libssh2-docs (VZLSA-2019-1652)

Virtuozzo 6 : libtirpc / libtirpc-devel (VZLSA-2017-1268)

Virtuozzo 6 : libvirt / libvirt-client / libvirt-devel / etc (VZLSA-2019-1180)

Virtuozzo 6 : libvirt / libvirt-client / libvirt-devel / etc (VZLSA-2019-1578)

Virtuozzo 6 : libvzctl / parallels-kernel-modules / etc (VZA-2017-005)

Virtuozzo 6 : mysql / mysql-bench / mysql-devel / mysql-embedded / etc (VZLSA-2017-0184)

Virtuozzo 6 : nss / nss-devel / nss-pkcs11-devel / nss-sysinit / etc (VZLSA-2017-1364)

Virtuozzo 6 : nss / nss-devel / nss-pkcs11-devel / nss-sysinit / etc (VZLSA-2017-2832)

Virtuozzo 6 : nss / nss-devel / nss-pkcs11-devel / nss-sysinit / etc (VZLSA-2018-2898)

Virtuozzo 6 : nss-util / nss-util-devel (VZLSA-2017-1100)

Virtuozzo 6 : ntp / ntp-doc / ntp-perl / ntpdate (VZLSA-2017-0252)

Virtuozzo 6 : ntp / ntp-doc / ntp-perl / ntpdate (VZLSA-2017-3071)

Virtuozzo 6 : openjpeg / openjpeg-devel / openjpeg-libs (VZLSA-2017-0559)

Virtuozzo 6 : openssl / openssl-devel / openssl-perl / etc (VZLSA-2017-0286)

Virtuozzo 6 : openssl / openssl-devel / openssl-perl / etc (VZLSA-2019-2471)

Virtuozzo 6 : parallels-kernel-modules / etc (VZA-2019-063)

Virtuozzo 6 : parallels-kernel-modules / etc (VZA-2019-093)

Virtuozzo 6 : parallels-server-bm-release / etc (VZA-2018-017)

Virtuozzo 6 : parallels-server-bm-release / pfcache / ploop / etc (VZA-2017-003)

Virtuozzo 6 : parallels-server-bm-release / shaman / vzkernel / etc (VZA-2019-033)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2016-104)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-001)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-009)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-019)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-025)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-031)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-037)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-047)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-055)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-061)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-076)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-085)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-090)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-096)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-107)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2017-114)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2018-002)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2018-029)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2018-033)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2018-041)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2018-048)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2018-075)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2018-086)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2019-037)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2019-052)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2019-067)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2019-089)

Virtuozzo 6 : parallels-server-bm-release / vzkernel / etc (VZA-2020-011)

Virtuozzo 6 : postgresql / postgresql-contrib / postgresql-devel / etc (VZLSA-2017-2860)

Virtuozzo 6 : python-paramiko (VZLSA-2018-3406)

Virtuozzo 6 : qemu-guest-agent / qemu-img / qemu-kvm / etc (VZLSA-2017-0309)

Virtuozzo 6 : qemu-guest-agent / qemu-img / qemu-kvm / etc (VZLSA-2017-0352)

Virtuozzo 6 : qemu-guest-agent / qemu-img / qemu-kvm / etc (VZLSA-2017-1206)

Virtuozzo 6 : rpcbind (VZLSA-2017-1267)

Virtuozzo 6 : samba4 / samba4-client / samba4-common / samba4-dc / etc (VZLSA-2017-1271)

Virtuozzo 6 : samba4 / samba4-client / samba4-common / samba4-dc / etc (VZLSA-2017-2791)

Virtuozzo 6 : spice-server / spice-server-devel (VZLSA-2017-0253)

Virtuozzo 6 : spice-server / spice-server-devel (VZLSA-2018-3522)

Virtuozzo 6 : squid34 (VZLSA-2017-0183)

Virtuozzo 6 : sudo / sudo-devel (VZLSA-2017-1382)

Virtuozzo 6 : sudo / sudo-devel (VZLSA-2017-1574)

Virtuozzo 6 : thunderbird (VZLSA-2017-0238)

Virtuozzo 6 : thunderbird (VZLSA-2017-0498)

Virtuozzo 6 : thunderbird (VZLSA-2017-1201)

Virtuozzo 6 : thunderbird (VZLSA-2017-1561)

Virtuozzo 6 : thunderbird (VZLSA-2017-2885)

Virtuozzo 6 : tomcat6 / tomcat6-admin-webapps / etc (VZLSA-2017-0527)

Virtuozzo 6 : tomcat6 / tomcat6-admin-webapps / etc (VZLSA-2017-3080)

Virtuozzo 6 : wpa\_supplicant (VZLSA-2017-2911)

Virtuozzo 7 : 389-ds-base / 389-ds-base-devel / 389-ds-base-libs / etc (VZLSA-2017-0920)

Virtuozzo 7 : 389-ds-base / 389-ds-base-devel / 389-ds-base-libs / etc (VZLSA-2019-3981)

Virtuozzo 7 : anaconda / anaconda-core / anaconda-dracut / etc (VZA-2017-012)

Virtuozzo 7 : anaconda / anaconda-core / anaconda-dracut / etc (VZA-2018-037)

Virtuozzo 7 : apr / apr-devel (VZLSA-2017-3270)

Virtuozzo 7 : autocorr-af / autocorr-bg / autocorr-ca / etc (VZLSA-2017-0914)

Virtuozzo 7 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-0062)

Virtuozzo 7 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-0276)

Virtuozzo 7 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-1095)

Virtuozzo 7 : bind / bind-chroot / bind-devel / bind-libs / etc (VZLSA-2017-1680)

Virtuozzo 7 : bind97 / bind97-chroot / bind97-devel / etc (VZLSA-2017-0064)

Virtuozzo 7 : bpftool / cpupools / cpupools-features / etc (VZA-2019-039)

Virtuozzo 7 : crit / criu / criu-devel / ksm-vz / libcompel / etc (VZA-2018-003)

Virtuozzo 7 : crit / criu / criu-devel / python-criu / vzkernel / etc (VZA-2017-056)

Virtuozzo 7 : ctdb / ctdb-tests / libsmbclient / etc (VZLSA-2017-1265)

Virtuozzo 7 : curl / libcurl / libcurl-devel (VZLSA-2017-3263)

Virtuozzo 7 : dovecot / dovecot-devel / dovecot-mysql / etc (VZLSA-2019-2836)

Virtuozzo 7 : emacs / emacs-common / emacs-el / emacs-filesystem / etc (VZLSA-2017-2771)

Virtuozzo 7 : firefox (VZLSA-2017-0461)

Virtuozzo 7 : firefox (VZLSA-2017-0558)

Virtuozzo 7 : firefox (VZLSA-2017-1106)

Virtuozzo 7 : firefox (VZLSA-2017-1440)

Virtuozzo 7 : firefox (VZLSA-2019-1763)

Virtuozzo 7 : flatpak / flatpak-builder / flatpak-devel / etc (VZLSA-2019-0375)

Virtuozzo 7 : freeradius / freeradius-devel / freeradius-doc / etc (VZLSA-2017-1581)

Virtuozzo 7 : ghostscript / ghostscript-cups / ghostscript-devel / etc (VZLSA-2017-0013)

Virtuozzo 7 : ghostscript / ghostscript-cups / ghostscript-devel / etc (VZLSA-2018-2918)

Virtuozzo 7 : ghostscript / ghostscript-cups / ghostscript-devel / etc (VZLSA-2019-0633)

Virtuozzo 7 : ghostscript / ghostscript-cups / ghostscript-devel / etc (VZLSA-2019-1017)

Virtuozzo 7 : glibc / glibc-common / glibc-devel / glibc-headers / etc (VZLSA-2017-1481)

Virtuozzo 7 : graphite2 / graphite2-devel (VZLSA-2017-1793)

Virtuozzo 7 : gstreamer-plugins-bad-free / etc (VZLSA-2017-0018)

Virtuozzo 7 : gstreamer-plugins-good / etc (VZLSA-2017-0019)

Virtuozzo 7 : gstreamer1-plugins-bad-free / etc (VZLSA-2017-0021)

Virtuozzo 7 : gstreamer1-plugins-good (VZLSA-2017-0020)

Virtuozzo 7 : httpd / httpd-devel / httpd-manual / httpd-tools / etc (VZLSA-2017-0906)

Virtuozzo 7 : icoutils (VZLSA-2017-0837)

Virtuozzo 7 : ipa-admintools / ipa-client / ipa-client-common / etc (VZLSA-2017-0001)

Virtuozzo 7 : ipa-admintools / ipa-client / ipa-client-common / etc (VZLSA-2017-0388)

Virtuozzo 7 : java-1.6.0-openjdk / java-1.6.0-openjdk-demo / etc (VZLSA-2017-0061)

Virtuozzo 7 : java-1.7.0-openjdk / etc (VZLSA-2017-3392)

Virtuozzo 7 : java-1.7.0-openjdk / etc (VZLSA-2019-0464)

Virtuozzo 7 : java-1.8.0-openjdk / etc (VZLSA-2017-1108)

Virtuozzo 7 : java-1.8.0-openjdk / etc (VZLSA-2018-2942)

Virtuozzo 7 : kdelibs / kdelibs-apidocs / kdelibs-common / etc (VZLSA-2017-1264)

Virtuozzo 7 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0086)

Virtuozzo 7 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0294)

Virtuozzo 7 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0386)

Virtuozzo 7 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-0933)

Virtuozzo 7 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-1308)

Virtuozzo 7 : kernel / kernel-abi-whitelists / kernel-debug / etc (VZLSA-2017-1484)

Virtuozzo 7 : kernel / kernel-PAE / kernel-PAE-devel / etc (VZLSA-2017-0323)

Virtuozzo 7 : kmod-kvm / kmod-kvm-debug / kvm / kvm-qemu-img / etc (VZLSA-2017-0454)

Virtuozzo 7 : ksm-vz / prl-disp-legacy / prl-disp-service / etc (VZA-2017-087)

Virtuozzo 7 : libblkid / libblkid-devel / libmount / etc (VZLSA-2017-0907)

Virtuozzo 7 : liblouis / liblouis-devel / liblouis-doc / etc (VZLSA-2017-3384)

Virtuozzo 7 : libtiff / libtiff-devel / libtiff-static / etc (VZLSA-2017-0225)

Virtuozzo 7 : libtirpc / libtirpc-devel (VZLSA-2017-1263)

Virtuozzo 7 : nss / nss-devel / nss-pkcs11-devel / nss-sysinit / etc (VZLSA-2017-1365)

Virtuozzo 7 : openjpeg / openjpeg-devel / openjpeg-libs (VZLSA-2017-0838)

Virtuozzo 7 : OVMF / am\_storage / anaconda / anaconda-core / etc (VZA-2017-103)

Virtuozzo 7 : OVMF / anaconda / anaconda-core / anaconda-dracut / etc (VZA-2017-033)

Virtuozzo 7 : OVMF / anaconda / anaconda-core / anaconda-dracut / etc (VZA-2017-066)

Virtuozzo 7 : OVMF / anaconda / anaconda-core / anaconda-dracut / etc (VZA-2019-013)

Virtuozzo 7 : OVMF / crit / criu / criu-devel / ksm-vz / etc (VZA-2018-063)

Virtuozzo 7 : php / php-bcmath / php-cli / php-common / php-dba / etc (VZLSA-2017-3221)

Virtuozzo 7 : php / php-bcmath / php-cli / php-common / php-dba / etc (VZLSA-2019-3286)

Virtuozzo 7 : procmail (VZLSA-2017-3269)

Virtuozzo 7 : qemu-img / qemu-kvm / qemu-kvm-common / etc (VZLSA-2017-0083)

Virtuozzo 7 : qemu-img / qemu-kvm / qemu-kvm-common / etc (VZLSA-2017-0396)

Virtuozzo 7 : qemu-img / qemu-kvm / qemu-kvm-common / etc (VZLSA-2017-0987)

Virtuozzo 7 : qemu-img / qemu-kvm / qemu-kvm-common / etc (VZLSA-2017-1430)

Virtuozzo 7 : readykernel-patch (VZA-2017-004)

Virtuozzo 7 : readykernel-patch (VZA-2017-006)

Virtuozzo 7 : readykernel-patch (VZA-2017-007)

Virtuozzo 7 : readykernel-patch (VZA-2017-008)

Virtuozzo 7 : readykernel-patch (VZA-2017-010)

Virtuozzo 7 : readykernel-patch (VZA-2017-017)

Virtuozzo 7 : readykernel-patch (VZA-2017-021)

Virtuozzo 7 : readykernel-patch (VZA-2017-026)

Virtuozzo 7 : readykernel-patch (VZA-2017-027)

Virtuozzo 7 : readykernel-patch (VZA-2017-028)

Virtuozzo 7 : readykernel-patch (VZA-2017-029)

Virtuozzo 7 : readykernel-patch (VZA-2017-032)

Virtuozzo 7 : readykernel-patch (VZA-2017-038)

Virtuozzo 7 : readykernel-patch (VZA-2017-042)

Virtuozzo 7 : readykernel-patch (VZA-2017-043)

Virtuozzo 7 : readykernel-patch (VZA-2017-044)

Virtuozzo 7 : readykernel-patch (VZA-2017-045)

Virtuozzo 7 : readykernel-patch (VZA-2017-052)

Virtuozzo 7 : readykernel-patch (VZA-2017-053)

Virtuozzo 7 : readykernel-patch (VZA-2017-057)

Virtuozzo 7 : readykernel-patch (VZA-2017-058)

Virtuozzo 7 : readykernel-patch (VZA-2017-062)

Virtuozzo 7 : readykernel-patch (VZA-2017-063)

Virtuozzo 7 : readykernel-patch (VZA-2017-065)

Virtuozzo 7 : readykernel-patch (VZA-2017-067)

Virtuozzo 7 : readykernel-patch (VZA-2017-068)

Virtuozzo 7 : readykernel-patch (VZA-2017-069)

Virtuozzo 7 : readykernel-patch (VZA-2017-070)

Virtuozzo 7 : readykernel-patch (VZA-2017-071)

Virtuozzo 7 : readykernel-patch (VZA-2017-072)

Virtuozzo 7 : readykernel-patch (VZA-2017-073)

Virtuozzo 7 : readykernel-patch (VZA-2017-077)

Virtuozzo 7 : readykernel-patch (VZA-2017-078)

Virtuozzo 7 : readykernel-patch (VZA-2017-079)

Virtuozzo 7 : readykernel-patch (VZA-2017-082)

Virtuozzo 7 : readykernel-patch (VZA-2017-083)

Virtuozzo 7 : readykernel-patch (VZA-2017-086)

Virtuozzo 7 : readykernel-patch (VZA-2017-091)

Virtuozzo 7 : readykernel-patch (VZA-2017-094)

Virtuozzo 7 : readykernel-patch (VZA-2017-097)

Virtuozzo 7 : readykernel-patch (VZA-2017-098)

Virtuozzo 7 : readykernel-patch (VZA-2017-099)

Virtuozzo 7 : readykernel-patch (VZA-2017-100)

Virtuozzo 7 : readykernel-patch (VZA-2017-101)

Virtuozzo 7 : readykernel-patch (VZA-2017-102)

Virtuozzo 7 : readykernel-patch (VZA-2017-109)

Virtuozzo 7 : readykernel-patch (VZA-2017-110)

Virtuozzo 7 : readykernel-patch (VZA-2017-111)

Virtuozzo 7 : readykernel-patch (VZA-2017-115)

Virtuozzo 7 : readykernel-patch (VZA-2017-116)

Virtuozzo 7 : readykernel-patch (VZA-2017-117)

Virtuozzo 7 : readykernel-patch (VZA-2017-120)

Virtuozzo 7 : readykernel-patch (VZA-2018-004)

Virtuozzo 7 : readykernel-patch (VZA-2018-005)

Virtuozzo 7 : readykernel-patch (VZA-2018-007)

Virtuozzo 7 : readykernel-patch (VZA-2018-014)

Virtuozzo 7 : readykernel-patch (VZA-2018-015)

Virtuozzo 7 : readykernel-patch (VZA-2018-024)

Virtuozzo 7 : readykernel-patch (VZA-2018-025)

Virtuozzo 7 : readykernel-patch (VZA-2018-026)

Virtuozzo 7 : readykernel-patch (VZA-2018-030)

Virtuozzo 7 : readykernel-patch (VZA-2018-035)

Virtuozzo 7 : readykernel-patch (VZA-2018-036)

Virtuozzo 7 : readykernel-patch (VZA-2018-038)

Virtuozzo 7 : readykernel-patch (VZA-2018-045)

Virtuozzo 7 : readykernel-patch (VZA-2018-046)

Virtuozzo 7 : readykernel-patch (VZA-2018-049)

Virtuozzo 7 : readykernel-patch (VZA-2018-050)

Virtuozzo 7 : readykernel-patch (VZA-2018-052)

Virtuozzo 7 : readykernel-patch (VZA-2018-072)

Virtuozzo 7 : readykernel-patch (VZA-2018-077)

Virtuozzo 7 : readykernel-patch (VZA-2018-080)

Virtuozzo 7 : readykernel-patch (VZA-2018-085)

Virtuozzo 7 : readykernel-patch (VZA-2018-088)

Virtuozzo 7 : readykernel-patch (VZA-2018-089)

Virtuozzo 7 : readykernel-patch (VZA-2019-001)

Virtuozzo 7 : readykernel-patch (VZA-2019-003)

Virtuozzo 7 : readykernel-patch (VZA-2019-004)

Virtuozzo 7 : readykernel-patch (VZA-2019-006)

Virtuozzo 7 : readykernel-patch (VZA-2019-008)

Virtuozzo 7 : readykernel-patch (VZA-2019-042)

Virtuozzo 7 : readykernel-patch (VZA-2019-043)

Virtuozzo 7 : readykernel-patch (VZA-2019-044)

Virtuozzo 7 : readykernel-patch (VZA-2019-045)

Virtuozzo 7 : readykernel-patch (VZA-2019-046)

Virtuozzo 7 : readykernel-patch (VZA-2019-050)

Virtuozzo 7 : readykernel-patch (VZA-2019-064)

Virtuozzo 7 : readykernel-patch (VZA-2019-068)

Virtuozzo 7 : readykernel-patch (VZA-2019-074)

Virtuozzo 7 : readykernel-patch (VZA-2019-076)

Virtuozzo 7 : readykernel-patch (VZA-2019-078)

Virtuozzo 7 : readykernel-patch (VZA-2019-081)

Virtuozzo 7 : readykernel-patch (VZA-2019-085)

Virtuozzo 7 : readykernel-patch (VZA-2019-086)

Virtuozzo 7 : readykernel-patch (VZA-2020-013)

Virtuozzo 7 : readykernel-patch (VZA-2020-015)

Virtuozzo 7 : rpcbind (VZLSA-2017-1262)

Virtuozzo 7 : spice-server / spice-server-devel (VZLSA-2017-0254)

Virtuozzo 7 : squid / squid-migration-script / squid-sysvinit (VZLSA-2017-0182)

Virtuozzo 7 : sudo / sudo-devel (VZLSA-2016-2872)

Virtuozzo 7 : tomcat / tomcat-admin-webapps / tomcat-docs-webapp / etc (VZLSA-2017-0935)

Virtuozzo 7 : vmauth (VZA-2017-018)

Virtuozzo 7 : wget (VZLSA-2017-3075)

Virtuozzo 7 : wpa\_supplicant (VZLSA-2017-2907)

# Ubuntu Local Security Checks

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : acpid vulnerabilities (USN-1296-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : ca-certificates-java vulnerability (USN-1197-7)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : clamav vulnerability (USN-1258-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : cvs vulnerability (USN-1371-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : empathy vulnerabilities (USN-1250-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : firefox vulnerabilities (USN-1355-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : firefox vulnerabilities (USN-1400-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : firefox vulnerability (USN-1360-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : firefox vulnerability (USN-1367-2)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : icedtea-web, openjdk-6, openjdk-6b18 vulnerabilities (USN-1263-1) (BEAST)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : icu vulnerability (USN-1348-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : jasper vulnerabilities (USN-1315-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : kdeutils vulnerability (USN-1276-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : krb5 vulnerabilities (USN-1233-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : libarchive vulnerabilities (USN-1310-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : libmodplug vulnerabilities (USN-1255-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : libvorbis vulnerability (USN-1370-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : mozvoikko update (USN-1355-2)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : openjdk-6 vulnerabilities (USN-1373-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : openjdk-6, openjdk-6b18 regression (USN-1263-2) (BEAST)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : openldap vulnerability (USN-1266-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : puppet vulnerabilities (USN-1372-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : puppet vulnerability (USN-1238-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : python-django vulnerabilities (USN-1297-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : python-httplib2 vulnerability (USN-1375-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : python-pam vulnerability (USN-1395-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : qemu-kvm vulnerability (USN-1339-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : quagga vulnerabilities (USN-1261-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : radvd vulnerabilities (USN-1257-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : ruby1.8 vulnerabilities (USN-1377-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : software-properties vulnerability (USN-1352-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : t1lib vulnerabilities (USN-1335-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : t1lib vulnerability (USN-1316-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : tomcat6 vulnerabilities (USN-1252-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : tomcat6 vulnerabilities (USN-1359-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : ubufox update (USN-1400-2)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : vsftpd vulnerability (USN-1288-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : xorg vulnerability (USN-1349-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 / 11.10 : xorg-server vulnerabilities (USN-1232-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : acpid vulnerability (USN-1234-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : apturl vulnerability (USN-1132-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : ca-certificates vulnerability (USN-1197-5)

Ubuntu 10.04 LTS / 10.10 / 11.04 : dovecot vulnerability (USN-1143-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : ecryptfs-utils vulnerabilities (USN-1188-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : ecryptfs-utils vulnerability (USN-1196-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : eucalyptus, rampart vulnerability (USN-1137-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : evince vulnerability (USN-1347-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : exim4 vulnerability (USN-1130-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : exim4 vulnerability (USN-1135-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : firefox, xulrunner-1.9.2 vulnerability (USN-1197-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : firefox, xulrunner-1.9.2 vulnerability (USN-1197-3)

Ubuntu 10.04 LTS / 10.10 / 11.04 : gdm-guest-session vulnerability (USN-1399-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : gimp vulnerability (USN-1147-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : gimp vulnerability (USN-1214-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : icedtea-web, openjdk-6, openjdk-6b18 vulnerabilities (USN-1178-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : kde4libs vulnerability (USN-1248-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : libmodplug vulnerabilities (USN-1148-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : librsvg vulnerability (USN-1206-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : libsndfile vulnerability (USN-1174-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : libsoup2.4 vulnerability (USN-1181-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : libvirt vulnerabilities (USN-1152-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : libvirt vulnerability (USN-1180-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : libxfont vulnerability (USN-1191-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : likewise-open vulnerability (USN-1171-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : mutt vulnerability (USN-1221-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : nagios3 vulnerabilities (USN-1151-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : nss vulnerability (USN-1197-4)

Ubuntu 10.04 LTS / 10.10 / 11.04 : openjdk-6, openjdk-6b18 vulnerabilities (USN-1154-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : openjdk-6b18 vulnerabilities (USN-1373-2)

Ubuntu 10.04 LTS / 10.10 / 11.04 : pidgin vulnerabilities (USN-1273-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : puppet vulnerabilities (USN-1223-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : puppet vulnerability (USN-1217-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : python3.1, python3.2 vulnerabilities (USN-1314-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : qemu-kvm vulnerabilities (USN-1145-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : qemu-kvm vulnerabilities (USN-1165-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : qemu-kvm vulnerability (USN-1177-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : qt4-x11 vulnerability (USN-1197-6)

Ubuntu 10.04 LTS / 10.10 / 11.04 : quassel vulnerability (USN-1200-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : quassel vulnerability (USN-1230-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : rdesktop vulnerability (USN-1136-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : subversion vulnerabilities (USN-1144-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerabilities (USN-1150-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerabilities (USN-1185-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerabilities (USN-1213-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerabilities (USN-1254-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerabilities (USN-1350-1)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerabilities (USN-1401-2)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerability (USN-1197-2)

Ubuntu 10.04 LTS / 10.10 / 11.04 : thunderbird vulnerability (USN-1367-3)

Ubuntu 10.04 LTS / 10.10 / 11.04 : usb-creator vulnerability (USN-1127-1)

Ubuntu 10.04 LTS / 10.10 : clamav vulnerabilities (USN-1031-1)

Ubuntu 10.04 LTS / 10.10 : dovecot vulnerabilities (USN-1059-1)

Ubuntu 10.04 LTS / 10.10 : ffmpeg vulnerabilities (USN-1209-1)

Ubuntu 10.04 LTS / 10.10 : ffmpeg vulnerabilities (USN-1320-1)

Ubuntu 10.04 LTS / 10.10 : firefox regression (USN-1149-2)

Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerabilities (USN-1149-1)

Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerabilities (USN-1184-1)

Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerabilities (USN-1210-1)

Ubuntu 10.04 LTS / 10.10 : firefox, xulrunner-1.9.2 vulnerabilities (USN-1251-1)

Ubuntu 10.04 LTS / 10.10 : ifupdown update (USN-1037-1)

Ubuntu 10.04 LTS / 10.10 : krb5 vulnerability (USN-999-1)

Ubuntu 10.04 LTS / 10.10 : linux vulnerabilities (USN-1090-1)

Ubuntu 10.04 LTS / 10.10 : linux, linux-ec2 vulnerabilities (USN-1054-1)

Ubuntu 10.04 LTS / 10.10 : linux-mvl-dove vulnerabilities (USN-1093-1)

Ubuntu 10.04 LTS / 10.10 : openssl vulnerability (USN-1064-1)

Ubuntu 10.04 LTS / 10.10 : tex-common vulnerability (USN-1103-1)

Ubuntu 10.04 LTS / 10.10 : thunderbird vulnerabilities (USN-1050-1)

Ubuntu 10.04 LTS / 10.10 : thunderbird vulnerabilities (USN-1122-1)

Ubuntu 10.04 LTS / 10.10 : thunderbird vulnerabilities (USN-998-1)

Ubuntu 10.04 LTS / 10.10 : thunderbird, thunderbird-locales vulnerabilities (USN-1020-1)

Ubuntu 10.04 LTS / 10.10 : tiff vulnerability (USN-1120-1)

Ubuntu 10.04 LTS / 10.10 : ubufox and webfav update (USN-1355-3)

Ubuntu 10.04 LTS / 10.10 : webkit vulnerabilities (USN-1195-1)

Ubuntu 10.04 LTS / 10.10 : xorg-server vulnerability (USN-1232-3)

Ubuntu 10.04 LTS / 10.10 : xulrunner-1.9.2 vulnerabilities (USN-1353-1)

Ubuntu 10.04 LTS / 10.10 : xulrunner-1.9.2 vulnerabilities (USN-1401-1)

Ubuntu 10.04 LTS / 10.10 : xulrunner-1.9.2 vulnerability (USN-1367-4)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS / 12.10 : exim4 vulnerability (USN-1618-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS / 12.10 : firefox vulnerabilities (USN-1620-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS / 12.10 : openjdk-6, openjdk-7 vulnerabilities (USN-1619-1) (ROBOT)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : apparmor update (USN-1430-4)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : bind9 vulnerability (USN-1518-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : clamav vulnerabilities (USN-1482-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : devscripts vulnerabilities (USN-1593-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : dhcp3, isc-dhcp vulnerability (USN-1571-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox regression (USN-1548-2)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox regressions (USN-1463-3)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox vulnerabilities (USN-1430-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox vulnerabilities (USN-1463-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox vulnerabilities (USN-1509-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox vulnerabilities (USN-1548-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox vulnerabilities (USN-1600-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : firefox vulnerabilities (USN-1608-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : gimp vulnerabilities (USN-1559-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : icedtea-web vulnerabilities (USN-1521-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : icedtea-web, openjdk-6 vulnerabilities (USN-1505-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : imagemagick vulnerabilities (USN-1435-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : imagemagick vulnerability (USN-1544-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : krb5 vulnerabilities (USN-1520-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libconfig-inifiles-perl vulnerability (USN-1543-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libgssglue vulnerability (USN-1612-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libotr vulnerability (USN-1541-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : moin vulnerabilities (USN-1604-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : mono vulnerabilities (USN-1517-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : nut vulnerability (USN-1456-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : nvidia-graphics-drivers, nvidia-graphics-drivers-173, nvidia-graphics-drivers-173-updates, nvidia-graphics-drivers-updates vulnerability (USN-1523-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : openjdk-6 vulnerabilities (USN-1553-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : pidgin vulnerabilities (USN-1500-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : puppet vulnerabilities (USN-1506-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : python-crypto vulnerability (USN-1484-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : python-django vulnerabilities (USN-1560-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : qemu-kvm vulnerability (USN-1522-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : qemu-kvm vulnerability (USN-1590-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : quagga vulnerabilities (USN-1441-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : quagga vulnerability (USN-1605-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : raptor vulnerability (USN-1480-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : ruby1.8 vulnerabilities (USN-1603-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : samba vulnerability (USN-1434-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : software-properties vulnerability (USN-1588-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : thunderbird regressions (USN-1551-2)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : thunderbird vulnerabilities (USN-1430-3)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : thunderbird vulnerabilities (USN-1510-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : thunderbird vulnerabilities (USN-1551-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : thunderbird vulnerabilities (USN-1611-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : ubufox update (USN-1509-2)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : ubuntuone-client vulnerability (USN-1465-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : ubuntuone-storage-protocol update (USN-1465-2)

Ubuntu 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : xmlrpc-c vulnerabilities (USN-1527-2)

Ubuntu 10.04 LTS / 11.04 / 11.10 : libgdata, evolution-data-server vulnerability (USN-1547-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 : network-manager vulnerability (USN-1483-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 : network-manager-applet vulnerability (USN-1483-2)

Ubuntu 10.04 LTS / 11.04 / 11.10 : nss vulnerability (USN-1540-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 : nvidia-graphics-drivers, nvidia-graphics-drivers-173, nvidia-graphics-drivers-173-updates, nvidia-graphics-drivers-updates vulnerability (USN-1420-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 : puppet vulnerabilities (USN-1419-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 : python2.6 vulnerabilities (USN-1596-1)

Ubuntu 10.04 LTS / 11.04 / 11.10 : ubufox update (USN-1430-2)

Ubuntu 10.04 LTS / 11.04 : jetty vulnerability (USN-1429-1)

Ubuntu 10.04 LTS / 11.04 : python3.1 vulnerabilities (USN-1616-1)

Ubuntu 10.04 LTS / 11.04 : qt4-x11 vulnerabilities (USN-1504-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 / 13.04 : clamav vulnerabilities (USN-1816-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : bind9 vulnerability (USN-1783-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : clamav vulnerabilities (USN-1773-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : dbus-glib vulnerability (USN-1753-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox regression (USN-1681-3)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox regression (USN-1681-4)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox regressions (USN-1638-3)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox vulnerabilities (USN-1638-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox vulnerabilities (USN-1681-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox vulnerabilities (USN-1729-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox vulnerabilities (USN-1786-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : firefox vulnerability (USN-1758-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : gimp vulnerability (USN-1659-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : icedtea-web vulnerabilities (USN-1804-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : icedtea-web vulnerability (USN-1625-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : inkscape vulnerabilities (USN-1712-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libssh vulnerabilities (USN-1640-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libssh vulnerability (USN-1707-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : lynx-cur vulnerabilities (USN-1642-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : moin vulnerabilities (USN-1680-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : munin vulnerabilities (USN-1622-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : mysql-5.1, mysql-5.5, mysql-dfsg-5.1 vulnerabilities (USN-1621-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : mysql-5.1, mysql-5.5, mysql-dfsg-5.1 vulnerabilities (USN-1703-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : mysql-5.1, mysql-5.5, mysql-dfsg-5.1 vulnerabilities (USN-1807-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : mysql-5.1, mysql-5.5, mysql-dfsg-5.1 vulnerability (USN-1658-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : nspr update (USN-1687-2)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : nspr update (USN-1763-2)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : nss vulnerability (USN-1687-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : nss vulnerability (USN-1763-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : openjdk-6, openjdk-7 vulnerabilities (USN-1724-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : openjdk-6, openjdk-7 vulnerabilities (USN-1735-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : pidgin vulnerabilities (USN-1746-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : python-django regression (USN-1632-2)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : python-django vulnerabilities (USN-1757-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : python-django vulnerability (USN-1632-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : qemu-kvm vulnerability (USN-1692-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : qt4-x11 vulnerabilities (USN-1723-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : ruby1.8, ruby1.9.1 vulnerability (USN-1780-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : squid, squid3 vulnerabilities (USN-1713-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : thunderbird vulnerabilities (USN-1620-2)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : thunderbird vulnerabilities (USN-1636-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : thunderbird vulnerabilities (USN-1681-2)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : thunderbird vulnerabilities (USN-1748-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : thunderbird vulnerabilities (USN-1791-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : thunderbird vulnerability (USN-1758-2)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : tomcat6, tomcat7 vulnerabilities (USN-1685-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : ubufox update (USN-1638-2)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : vino vulnerability (USN-1701-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : xorg-server, xorg-server-lts-quantal vulnerability (USN-1803-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : apport update (USN-1668-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : libproxy vulnerabilities (USN-1629-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : openjdk-6 vulnerabilities (USN-1755-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : openjdk-6 vulnerabilities (USN-1819-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : qt4-x11 vulnerability (USN-1628-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : rpm vulnerabilities (USN-1695-1)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : thunderbird vulnerabilities (USN-1463-4)

Ubuntu 10.04 LTS / 11.10 / 12.04 LTS : tomcat6 vulnerabilities (USN-1637-1)

Ubuntu 10.04 LTS / 11.10 : jquery vulnerability (USN-1722-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : bind9 vulnerability (USN-2081-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : curl vulnerability (USN-2048-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : devscripts vulnerability (USN-2084-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : gnupg vulnerability (USN-2059-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : graphviz vulnerabilities (USN-2083-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : libjpeg-turbo, libjpeg6b vulnerabilities (USN-2060-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : libxfont vulnerability (USN-2078-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : mysql-5.5, mysql-dfsg-5.1 vulnerabilities (USN-2006-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : nss vulnerabilities (USN-2030-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : nss vulnerability (USN-2063-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : php5 vulnerabilities (USN-2055-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 / 13.10 : samba vulnerabilities (USN-2054-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : apache2 vulnerabilities (USN-1903-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : bind9 vulnerability (USN-1910-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : curl vulnerability (USN-1894-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : eglibc vulnerabilities (USN-1991-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : gnupg, gnupg2 vulnerabilities (USN-1987-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : gnupg, libgcrypt11 vulnerability (USN-1923-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : gnutls26 vulnerability (USN-1843-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : hplip vulnerability (USN-1956-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libvirt vulnerabilities (USN-1954-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libx11 vulnerabilities (USN-1854-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxcb vulnerability (USN-1855-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxext vulnerability (USN-1857-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxi vulnerabilities (USN-1859-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxml2 regression (USN-1904-2)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxml2 vulnerabilities (USN-1904-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxrender vulnerability (USN-1863-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxt vulnerabilities (USN-1865-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxtst vulnerability (USN-1866-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : libxxf86vm vulnerability (USN-1870-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : mysql-5.5, mysql-dfsg-5.1 vulnerabilities (USN-1909-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : openssl vulnerability (USN-1898-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : php5 vulnerabilities (USN-1905-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : php5 vulnerability (USN-1937-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : policykit-1 vulnerability (USN-1953-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : pyopenssl vulnerability (USN-1965-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : python-django vulnerabilities (USN-1967-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : python-httplib2 vulnerability (USN-1948-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : samba vulnerability (USN-1966-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : tiff vulnerabilities (USN-1832-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.04 : tomcat6, tomcat7 vulnerabilities (USN-1841-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : dovecot vulnerability (USN-2213-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : dpkg vulnerability (USN-2183-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : dpkg vulnerability (USN-2183-2)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : libxfont vulnerabilities (USN-2211-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : libxml2 vulnerability (USN-2214-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : python-django regression (USN-2169-2)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : python-django vulnerabilities (USN-2169-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : python-django vulnerabilities (USN-2212-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : qemu, qemu-kvm vulnerabilities (USN-2182-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : tiff vulnerabilities (USN-2205-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : apache2 vulnerabilities (USN-2152-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : ca-certificates update (USN-2154-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : cups vulnerability (USN-2172-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : curl vulnerabilities (USN-2167-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : curl vulnerability (USN-2097-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerabilities (USN-2123-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : file vulnerability (USN-2162-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : freeradius vulnerabilities (USN-2122-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2127-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : hplip vulnerabilities (USN-2085-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : mutt vulnerability (USN-2147-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : mysql-5.5, mysql-dfsg-5.1 vulnerabilities (USN-2086-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : net-snmp vulnerabilities (USN-2166-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : nspr vulnerability (USN-2087-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : nss vulnerability (USN-2088-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : nss vulnerability (USN-2159-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2155-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : php5 vulnerabilities (USN-2126-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : php5 vulnerability (USN-2163-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : postgresql-8.4, postgresql-9.1 vulnerabilities (USN-2120-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python-imaging vulnerabilities (USN-2168-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : python2.6, python2.7, python3.2, python3.3 vulnerability (USN-2125-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : samba vulnerability (USN-2156-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : sudo vulnerabilities (USN-2146-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 / 13.10 : tomcat6, tomcat7 vulnerabilities (USN-2130-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 : curl regression (USN-2048-2)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 : hplip vulnerabilities (USN-1981-1)

Ubuntu 10.04 LTS / 12.04 LTS / 12.10 : perl vulnerability (USN-2099-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : apt vulnerability (USN-2246-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : chkrootkit vulnerability (USN-2230-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : dpkg vulnerabilities (USN-2242-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : file vulnerabilities (USN-2278-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : gnupg, gnupg2 vulnerability (USN-2258-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : gnutls26 vulnerability (USN-2229-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : libxml2 regression (USN-2214-2)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : libxml2 regression (USN-2214-3)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : nspr vulnerability (USN-2265-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : openssl regression (USN-2232-3)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : openssl vulnerabilities (USN-2232-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : php5 vulnerabilities (USN-2254-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : php5 vulnerabilities (USN-2276-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 / 14.04 LTS : samba vulnerabilities (USN-2257-1)

Ubuntu 10.04 LTS / 12.04 LTS / 13.10 : libxalan2-java vulnerability (USN-2218-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : apache2 vulnerabilities (USN-2523-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : bind9 vulnerability (USN-2437-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : binutils vulnerabilities (USN-2496-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : bsd-mailx vulnerability (USN-2455-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : ca-certificates update (USN-2509-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : cpio vulnerabilities (USN-2456-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : cups vulnerability (USN-2520-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : curl vulnerability (USN-2399-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : curl vulnerability (USN-2474-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : dpkg vulnerability (USN-2566-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : e2fsprogs vulnerabilities (USN-2507-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : ecryptfs-utils vulnerability (USN-2524-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : eglibc, glibc vulnerabilities (USN-2432-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : eglibc, glibc vulnerabilities (USN-2519-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : elfutils vulnerability (USN-2482-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : file vulnerabilities (USN-2494-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : flac vulnerabilities (USN-2426-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : freetype vulnerabilities (USN-2510-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : gnupg, gnupg2 vulnerabilities (USN-2554-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : gnutls26, gnutls28 vulnerabilities (USN-2540-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : graphviz vulnerability (USN-2435-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : krb5 vulnerabilities (USN-2498-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : libevent vulnerability (USN-2477-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : libgcrypt11, libgcrypt20 vulnerabilities (USN-2555-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : libtasn1-3, libtasn1-6 vulnerability (USN-2559-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : libxfont vulnerabilities (USN-2536-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : mime-support vulnerability (USN-2453-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : mutt vulnerability (USN-2440-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : nss update (USN-2504-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : nss vulnerability (USN-2452-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : ntp vulnerabilities (USN-2449-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : ntp vulnerabilities (USN-2497-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : openssl vulnerabilities (USN-2459-1) (FREAK)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : openssl vulnerabilities (USN-2537-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : php5 vulnerabilities (USN-2391-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : php5 vulnerabilities (USN-2535-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : php5 vulnerabilities (USN-2572-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : postgresql-8.4, postgresql-9.1, postgresql-9.3, postgresql-9.4 vulnerabilities (USN-2499-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : ppp vulnerability (USN-2429-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : python-django vulnerabilities (USN-2469-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : python-django vulnerabilities (USN-2539-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : qemu, qemu-kvm vulnerabilities (USN-2409-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : qemu, qemu-kvm vulnerabilities (USN-2439-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : sudo vulnerability (USN-2533-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : tcpdump vulnerabilities (USN-2433-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : tiff regression (USN-2553-2)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : tiff vulnerabilities (USN-2553-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : unzip vulnerabilities (USN-2472-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : unzip vulnerability (USN-2489-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS / 14.10 : wget vulnerability (USN-2393-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : apache2 vulnerabilities (USN-2299-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : apt vulnerabilities (USN-2348-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : apt vulnerability (USN-2353-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulnerabilities (USN-2364-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulnerabilities (USN-2380-1) (Shellshock)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulnerability (USN-2362-1) (Shellshock)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : bash vulnerability (USN-2363-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : coreutils vulnerabilities (USN-2473-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : cups vulnerabilities (USN-2341-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : cups vulnerability (USN-2293-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : curl vulnerabilities (USN-2346-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : dbus vulnerabilities (USN-2352-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : eglibc vulnerabilities (USN-2306-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : eglibc vulnerability (USN-2328-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : file vulnerability (USN-2369-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : gpgme1.0 vulnerability (USN-2307-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : krb5 vulnerabilities (USN-2310-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : libgcrypt11 vulnerability (USN-2339-2)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : libtasn1-3, libtasn1-6 vulnerabilities (USN-2294-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : libvirt vulnerabilities (USN-2366-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : libxml2 vulnerability (USN-2389-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : nss update (USN-2350-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : nss vulnerability (USN-2343-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : nss vulnerability (USN-2361-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : openssl vulnerabilities (USN-2308-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : openssl vulnerabilities (USN-2385-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : php5 vulnerabilities (USN-2344-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : procmail vulnerability (USN-2340-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : python-django vulnerabilities (USN-2347-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : qemu, qemu-kvm vulnerabilities (USN-2342-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : rsyslog vulnerabilities (USN-2381-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : tomcat6, tomcat7 vulnerabilities (USN-2302-1)

Ubuntu 10.04 LTS / 12.04 LTS / 14.04 LTS : wpa, wpasupplicant vulnerability (USN-2383-1)

Ubuntu 10.04 LTS / 12.04 LTS : eglibc vulnerability (USN-2485-1) (GHOST)

Ubuntu 10.04 LTS / 12.04 LTS : gnupg vulnerability (USN-2339-1)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 regression (USN-2124-2)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-1908-1)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-2033-1)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-2124-1)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-2191-1)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-2312-1)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-2386-1)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-2486-1) (POODLE)

Ubuntu 10.04 LTS / 12.04 LTS : openjdk-6 vulnerabilities (USN-2573-1)

Ubuntu 10.04 LTS / 12.04 LTS : python-django regression (USN-2469-2)

Ubuntu 10.04 LTS : bogofilter vulnerability (USN-1667-1)

Ubuntu 10.04 LTS : clamav vulnerability (USN-2488-2)

Ubuntu 10.04 LTS : cups vulnerabilities (USN-2144-1)

Ubuntu 10.04 LTS : eglibc regression (USN-2306-2)

Ubuntu 10.04 LTS : eglibc regression (USN-2306-3)

Ubuntu 10.04 LTS : ffmpeg vulnerabilities (USN-1479-1)

Ubuntu 10.04 LTS : ffmpeg vulnerabilities (USN-1675-1)

Ubuntu 10.04 LTS : ffmpeg vulnerabilities (USN-1706-1)

Ubuntu 10.04 LTS : ghostscript vulnerabilities (USN-2483-2)

Ubuntu 10.04 LTS : ghostscript vulnerability (USN-2434-2)

Ubuntu 10.04 LTS : krb5 vulnerability (USN-940-2)

Ubuntu 10.04 LTS : libcommons-fileupload-java vulnerability (USN-2029-1)

Ubuntu 10.04 LTS : libvirt regression (USN-1008-4)

Ubuntu 10.04 LTS : libvirt update (USN-1008-3)

Ubuntu 10.04 LTS : libxml-security-java vulnerability (USN-2028-1)

Ubuntu 10.04 LTS : likewise-open regression (USN-964-2)

Ubuntu 10.04 LTS : likewise-open vulnerability (USN-964-1)

Ubuntu 10.04 LTS : linux regression (USN-947-2)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1080-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1168-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1218-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1253-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1286-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1311-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1344-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1389-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1425-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1445-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1492-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1535-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1555-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1572-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1606-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1775-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1792-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1805-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1824-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1876-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1899-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1912-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1939-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-1976-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2015-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2036-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2064-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2107-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2128-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2173-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2219-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2233-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2251-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2282-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2332-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2354-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2374-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2441-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2462-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2490-1)

Ubuntu 10.04 LTS : linux vulnerabilities (USN-2511-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-1411-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-1468-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-1651-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-1661-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-1683-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-1725-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-1736-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-2196-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-2266-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-2415-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-2525-1)

Ubuntu 10.04 LTS : linux vulnerability (USN-2583-1)

Ubuntu 10.04 LTS : linux, linux-ec2 vulnerabilities (USN-1141-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1080-2)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1086-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1161-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1216-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1239-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1269-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1299-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1324-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1388-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1426-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1453-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1491-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1534-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1556-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1573-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1776-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1798-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1808-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1829-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1877-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1900-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1913-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1940-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-1977-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2016-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2037-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2065-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2108-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2129-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2174-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2220-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2234-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2252-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2281-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2333-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2355-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2375-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2416-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2442-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2491-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerabilities (USN-2512-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1410-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1469-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1597-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1653-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1664-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1684-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1728-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-1737-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-2197-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-2267-1)

Ubuntu 10.04 LTS : linux-ec2 vulnerability (USN-2584-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1083-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1187-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1205-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1219-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1242-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1278-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1292-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1332-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1387-1)

Ubuntu 10.04 LTS : linux-lts-backport-maverick vulnerabilities (USN-1421-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1256-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1279-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1301-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1337-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1386-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1440-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1470-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1490-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1538-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerabilities (USN-1574-1)

Ubuntu 10.04 LTS : linux-lts-backport-natty vulnerability (USN-1562-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1294-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1340-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1384-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1409-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1433-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1455-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1471-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1539-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1575-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1594-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1652-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1688-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1719-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1760-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerabilities (USN-1788-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerability (USN-1313-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerability (USN-1342-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerability (USN-1489-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerability (USN-1563-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerability (USN-1678-1)

Ubuntu 10.04 LTS : linux-lts-backport-oneiric vulnerability (USN-1738-1)

Ubuntu 10.04 LTS : linux-mvl-dove vulnerabilities (USN-1162-1)

Ubuntu 10.04 LTS : linux-mvl-dove vulnerabilities (USN-1203-1)

Ubuntu 10.04 LTS : linux-mvl-dove vulnerabilities (USN-1240-1)

Ubuntu 10.04 LTS : mako vulnerability (USN-996-1)

Ubuntu 10.04 LTS : mountall vulnerability (USN-985-1)

Ubuntu 10.04 LTS : mozilla-devscripts update (USN-1430-5)

Ubuntu 10.04 LTS : net-snmp vulnerability (USN-946-1)

Ubuntu 10.04 LTS : openoffice.org vulnerabilities (USN-1496-1)

Ubuntu 10.04 LTS : openoffice.org vulnerability (USN-1537-1)

Ubuntu 10.04 LTS : openssl vulnerabilities (USN-2232-4)

Ubuntu 10.04 LTS : oprofile vulnerabilities (USN-1166-1)

Ubuntu 10.04 LTS : paste vulnerability (USN-1026-1)

Ubuntu 10.04 LTS : puppet regression (USN-1223-2)

Ubuntu 10.04 LTS : python2.6 vulnerability (USN-1982-1)

Ubuntu 10.04 LTS : thunderbird regression (USN-978-2)

Ubuntu 10.04 LTS : thunderbird vulnerabilities (USN-943-1)

Ubuntu 10.04 LTS : thunderbird vulnerabilities (USN-958-1)

Ubuntu 10.04 LTS : thunderbird vulnerabilities (USN-978-1)

Ubuntu 10.04 LTS : ubuntuone-client regression (USN-1465-3)

Ubuntu 10.04 LTS : virtinst update (USN-1008-2)

Ubuntu 10.04 LTS : xorg-server regression (USN-1232-2)

Ubuntu 10.10 / 11.04 / 11.10 : curl vulnerability (USN-1346-1)

Ubuntu 10.10 / 11.04 / 11.10 : Puppet vulnerability (USN-1365-1)

Ubuntu 10.10 / 11.04 / 11.10 : software-center vulnerability (USN-1270-1)

Ubuntu 10.10 / 11.04 : cifs-utils vulnerabilities (USN-1226-2)

Ubuntu 10.10 / 11.04 : freetype vulnerability (USN-1173-1)

Ubuntu 10.10 / 11.04 : tgt vulnerabilities (USN-1156-1)

Ubuntu 10.10 : aptdaemon vulnerability (USN-1068-1)

Ubuntu 10.10 : bind9 vulnerability (USN-1070-1)

Ubuntu 10.10 : CUPS update (USN-1036-1)

Ubuntu 10.10 : eucalyptus vulnerability (USN-1033-1)

Ubuntu 10.10 : language-selector vulnerability (USN-1115-1)

Ubuntu 10.10 : libvpx vulnerability (USN-1015-1)

Ubuntu 10.10 : libvpx vulnerability (USN-1087-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1081-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1160-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1183-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1201-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1227-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1243-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1272-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1293-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1341-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1361-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1379-1)

Ubuntu 10.10 : linux vulnerabilities (USN-1407-1)

Ubuntu 10.10 : linux-mvl-dove vulnerabilities (USN-1159-1)

Ubuntu 10.10 : linux-mvl-dove vulnerabilities (USN-1208-1)

Ubuntu 10.10 : linux-mvl-dove vulnerabilities (USN-1245-1)

Ubuntu 10.10 : linux-mvl-dove vulnerabilities (USN-1274-1)

Ubuntu 10.10 : linux-mvl-dove vulnerabilities (USN-1303-1)

Ubuntu 10.10 : linux-mvl-dove vulnerabilities (USN-1328-1)

Ubuntu 10.10 : linux-mvl-dove vulnerability (USN-1391-1)

Ubuntu 10.10 : linux-mvl-dove vulnerability (USN-1415-1)

Ubuntu 10.10 : openjdk-6 regression (USN-1024-2)

Ubuntu 10.10 : openjdk-6b18 vulnerabilities (USN-1079-3)

Ubuntu 10.10 : pam vulnerability (USN-959-2)

Ubuntu 10.10 : postgresql-8.4 vulnerability (USN-1002-2)

Ubuntu 10.10 : python-django vulnerability (USN-1004-1)

Ubuntu 11.04 / 11.10 / 12.04 LTS / 12.10 : python3.2 vulnerabilities (USN-1615-1)

Ubuntu 11.04 / 11.10 / 12.04 LTS : clamav regression (USN-1482-2)

Ubuntu 11.04 / 11.10 / 12.04 LTS : clamav regression (USN-1482-3)

Ubuntu 11.04 / 11.10 / 12.04 LTS : freeradius vulnerability (USN-1585-1)

Ubuntu 11.04 / 11.10 / 12.04 LTS : isc-dhcp vulnerabilities (USN-1519-1)

Ubuntu 11.04 / 11.10 / 12.04 LTS : libav vulnerabilities (USN-1478-1)

Ubuntu 11.04 / 11.10 / 12.04 LTS : libreoffice vulnerability (USN-1536-1)

Ubuntu 11.04 / 11.10 / 12.04 LTS : unity-2d update (USN-1463-2)

Ubuntu 11.04 / 11.10 / 12.04 LTS : update-manager vulnerabilities (USN-1443-1)

Ubuntu 11.04 / 11.10 / 12.04 LTS : update-manager vulnerability (USN-1443-2)

Ubuntu 11.04 / 11.10 : apt vulnerability (USN-1385-1)

Ubuntu 11.04 / 11.10 : aptdaemon vulnerability (USN-1414-1)

Ubuntu 11.04 / 11.10 : commons-daemon vulnerability (USN-1298-1)

Ubuntu 11.04 / 11.10 : firefox vulnerabilities (USN-1277-1)

Ubuntu 11.04 / 11.10 : firefox vulnerabilities (USN-1306-1)

Ubuntu 11.04 / 11.10 : icedtea-web regression (USN-1505-2)

Ubuntu 11.04 / 11.10 : isc-dhcp vulnerability (USN-1309-1)

Ubuntu 11.04 / 11.10 : koffice vulnerability (USN-1526-1)

Ubuntu 11.04 / 11.10 : ldm vulnerability (USN-1398-1)

Ubuntu 11.04 / 11.10 : libav vulnerabilities (USN-1333-1)

Ubuntu 11.04 / 11.10 : libreoffice, libreoffice-l10n vulnerabilities (USN-1495-1)

Ubuntu 11.04 / 11.10 : mozvoikko, ubufox update (USN-1277-2)

Ubuntu 11.04 / 11.10 : mozvoikko, ubufox update (USN-1306-2)

Ubuntu 11.04 / 11.10 : python2.7 vulnerabilities (USN-1592-1)

Ubuntu 11.04 / 11.10 : system-config-printer vulnerability (USN-1265-1)

Ubuntu 11.04 / 11.10 : ubuntu-sso-client vulnerability (USN-1464-1)

Ubuntu 11.04 / 11.10 : usbmuxd vulnerability (USN-1354-1)

Ubuntu 11.04 : apt vulnerability (USN-1169-1)

Ubuntu 11.04 : clamav vulnerability (USN-1179-1)

Ubuntu 11.04 : firefox regression (USN-1157-3)

Ubuntu 11.04 : Firefox vulnerabilities (USN-1121-1)

Ubuntu 11.04 : firefox vulnerabilities (USN-1157-1)

Ubuntu 11.04 : firefox vulnerabilities (USN-1192-1)

Ubuntu 11.04 : Firefox vulnerabilities (USN-1222-1)

Ubuntu 11.04 : gdm vulnerability (USN-1142-1)

Ubuntu 11.04 : gsettings-desktop-schemas regression (USN-1400-5)

Ubuntu 11.04 : libav vulnerabilities (USN-1209-2)

Ubuntu 11.04 : libvoikko regression (USN-1192-3)

Ubuntu 11.04 : linux vulnerabilities (USN-1167-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1193-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1211-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1246-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1285-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1312-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1345-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1362-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1380-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1406-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1422-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1432-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1457-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1488-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1531-1)

Ubuntu 11.04 : linux vulnerabilities (USN-1567-1)

Ubuntu 11.04 : linux vulnerability (USN-1557-1)

Ubuntu 11.04 : mozvoikko update (USN-1192-2)

Ubuntu 11.04 : mozvoikko, ubufox, webfav update (USN-1157-2)

Ubuntu 11.04 : mozvoikko, ubufox, webfav update (USN-1222-2)

Ubuntu 11.04 : puppet regression (USN-1238-2)

Ubuntu 11.04 : rsyslog vulnerability (USN-1224-1)

Ubuntu 11.04 : rsyslog vulnerability (USN-1338-1)

Ubuntu 11.04 : thunderbird regression (USN-1122-3)

Ubuntu 11.04 : thunderbird vulnerabilities (USN-1122-2)

Ubuntu 11.04 : thunderbird vulnerabilities (USN-1463-6)

Ubuntu 11.04 : unity-2d update (USN-1463-5)

Ubuntu 11.10 / 12.04 LTS / 12.10 : apt vulnerability (USN-1662-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : apt vulnerability (USN-1762-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : firefox regression (USN-1729-2)

Ubuntu 11.10 / 12.04 LTS / 12.10 : glance vulnerability (USN-1710-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : gnome-online-accounts vulnerability (USN-1779-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : haproxy vulnerabilities (USN-1800-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : libav vulnerabilities (USN-1705-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : nova vulnerabilities (USN-1771-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : nova vulnerability (USN-1709-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : nova vulnerability (USN-1734-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : puppet vulnerabilities (USN-1759-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : python-keyring vulnerabilities (USN-1634-1)

Ubuntu 11.10 / 12.04 LTS / 12.10 : transmission vulnerability (USN-1747-1)

Ubuntu 11.10 / 12.04 LTS : accountsservice vulnerability (USN-1485-1)

Ubuntu 11.10 / 12.04 LTS : AppArmor update (USN-1676-1)

Ubuntu 11.10 / 12.04 LTS : aptdaemon vulnerability (USN-1666-1)

Ubuntu 11.10 / 12.04 LTS : emacs23 vulnerabilities (USN-1586-1)

Ubuntu 11.10 / 12.04 LTS : icedtea-web regression (USN-1804-2)

Ubuntu 11.10 / 12.04 LTS : kdepim vulnerability (USN-1512-1)

Ubuntu 11.10 / 12.04 LTS : nova regression (USN-1466-2)

Ubuntu 11.10 / 12.04 LTS : nova vulnerabilities (USN-1497-1)

Ubuntu 11.10 / 12.04 LTS : nova vulnerability (USN-1438-1)

Ubuntu 11.10 / 12.04 LTS : nova vulnerability (USN-1466-1)

Ubuntu 11.10 / 12.04 LTS : nova vulnerability (USN-1545-1)

Ubuntu 11.10 / 12.04 LTS : rhythmbox vulnerability (USN-1503-1)

Ubuntu 11.10 / 12.04 LTS : xserver-xorg-video-qxl vulnerability (USN-1714-1)

Ubuntu 11.10 : accountsservice vulnerability (USN-1351-1)

Ubuntu 11.10 : ca-certificates-java regression (USN-1197-8)

Ubuntu 11.10 : colord vulnerability (USN-1289-1)

Ubuntu 11.10 : dovecot vulnerability (USN-1295-1)

Ubuntu 11.10 : krb5 vulnerability (USN-1290-1)

Ubuntu 11.10 : libav vulnerabilities (USN-1674-1)

Ubuntu 11.10 : lightdm vulnerabilities (USN-1262-1)

Ubuntu 11.10 : lightdm vulnerability (USN-1382-1)

Ubuntu 11.10 : lightdm vulnerability (USN-1399-2)

Ubuntu 11.10 : linux vulnerabilities (USN-1363-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1405-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1431-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1452-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1472-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1533-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1568-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1607-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1648-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1689-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1720-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1756-1)

Ubuntu 11.10 : linux vulnerabilities (USN-1787-1)

Ubuntu 11.10 : linux vulnerability (USN-1275-1)

Ubuntu 11.10 : linux vulnerability (USN-1322-1)

Ubuntu 11.10 : linux vulnerability (USN-1336-1)

Ubuntu 11.10 : linux vulnerability (USN-1412-1)

Ubuntu 11.10 : linux vulnerability (USN-1487-1)

Ubuntu 11.10 : linux vulnerability (USN-1554-1)

Ubuntu 11.10 : linux vulnerability (USN-1677-1)

Ubuntu 11.10 : linux vulnerability (USN-1739-1)

Ubuntu 11.10 : nova vulnerability (USN-1247-1)

Ubuntu 11.10 : nova vulnerability (USN-1305-1)

Ubuntu 11.10 : nova vulnerability (USN-1326-1)

Ubuntu 11.10 : nova vulnerability (USN-1413-1)

Ubuntu 11.10 : thunderbird regressions (USN-1400-4)

Ubuntu 11.10 : thunderbird vulnerabilities (USN-1282-1)

Ubuntu 11.10 : thunderbird vulnerabilities (USN-1343-1)

Ubuntu 11.10 : thunderbird vulnerabilities (USN-1369-1)

Ubuntu 11.10 : thunderbird vulnerabilities (USN-1400-3)

Ubuntu 11.10 : ubuntuone-couch vulnerability (USN-1381-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : apport vulnerability (USN-2007-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : curl vulnerability (USN-2058-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : firefox vulnerabilities (USN-2009-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : firefox vulnerabilities (USN-2031-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : firefox vulnerabilities (USN-2052-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : gimp vulnerability (USN-2051-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : libav vulnerabilities (USN-2011-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : libav vulnerabilities (USN-2025-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : memcached vulnerabilities (USN-2080-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : openssl vulnerabilities (USN-2079-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : pixman vulnerability (USN-2047-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : puppet regression (USN-2077-2)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : puppet vulnerability (USN-2077-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : qt4-x11, qtbase-opensource-src vulnerability (USN-2057-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : ruby1.8, ruby1.9.1 vulnerabilities (USN-2035-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : thunderbird vulnerabilities (USN-2010-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : thunderbird vulnerabilities (USN-2032-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 / 13.10 : thunderbird vulnerabilities (USN-2053-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : apt-xapian-index vulnerability (USN-1955-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : dbus vulnerability (USN-1874-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : evolution-data-server vulnerability (USN-1922-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : firefox regression (USN-1890-2)

Ubuntu 12.04 LTS / 12.10 / 13.04 : firefox vulnerabilities (USN-1822-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : firefox vulnerabilities (USN-1890-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : firefox vulnerabilities (USN-1924-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : firefox vulnerabilities (USN-1951-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : haproxy vulnerability (USN-1889-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : icedtea-web update (USN-1907-2)

Ubuntu 12.04 LTS / 12.10 / 13.04 : icu vulnerabilities (USN-1989-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : kde4libs vulnerability (USN-1842-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : keystone vulnerability (USN-1830-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : language-selector vulnerability (USN-1958-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : lcms2 vulnerability (USN-1911-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libdmx vulnerability (USN-1852-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libfs vulnerability (USN-1853-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libmodule-signature-perl vulnerability (USN-1896-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libraw vulnerabilities (USN-1964-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libraw vulnerability (USN-1884-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxcursor vulnerability (USN-1856-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxfixes vulnerability (USN-1858-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxinerama vulnerability (USN-1860-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxp vulnerability (USN-1861-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxrandr, libxrandr-lts-quantal vulnerability (USN-1862-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxres vulnerability (USN-1864-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxv vulnerabilities (USN-1867-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxvmc vulnerabilities (USN-1868-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : libxxf86dga vulnerabilities (USN-1869-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : maas vulnerabilities (USN-2013-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : mesa, mesa-lts-quantal vulnerabilities (USN-1888-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : nas vulnerabilities (USN-1986-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : nova vulnerabilities (USN-2000-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : nova vulnerability (USN-1831-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : puppet vulnerabilities (USN-1928-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : puppet vulnerability (USN-1886-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : pymongo vulnerability (USN-1897-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : python2.7 vulnerabilities (USN-1983-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : rtkit vulnerability (USN-1959-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : ruby1.8, ruby1.9.1 vulnerability (USN-1902-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : software-properties vulnerability (USN-1960-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : subversion vulnerabilities (USN-1893-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : suds vulnerability (USN-2008-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : swift vulnerabilities (USN-1887-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : swift vulnerability (USN-2001-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : telepathy-gabble vulnerabilities (USN-1873-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : telepathy-idle vulnerability (USN-1821-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : thunderbird vulnerabilities (USN-1823-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : thunderbird vulnerabilities (USN-1891-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : thunderbird vulnerabilities (USN-1925-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : thunderbird vulnerabilities (USN-1952-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : txt2man vulnerability (USN-1979-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : ubufox, unity-firefox-extension update (USN-1924-2)

Ubuntu 12.04 LTS / 12.10 / 13.04 : ubuntu-system-service vulnerability (USN-1962-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : usb-creator vulnerability (USN-1963-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : vino vulnerability (USN-1980-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : xorg-server, xorg-server-lts-quantal, xorg-server-lts-raring vulnerabilities (USN-1990-1)

Ubuntu 12.04 LTS / 12.10 / 13.04 : xserver-xorg-video-openchrome, xserver-xorg-video-openchrome-lts-quantal vulnerability (USN-1871-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : firefox vulnerabilities (USN-2185-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : mysql-5.5 vulnerabilities (USN-2170-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : openssl vulnerabilities (USN-2192-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 / 14.04 LTS : thunderbird vulnerabilities (USN-2189-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : clamav update (USN-2157-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : cups-filters vulnerabilities (USN-2143-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : firefox regression (USN-2102-2)

Ubuntu 12.04 LTS / 12.10 / 13.10 : firefox vulnerabilities (USN-2102-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : firefox vulnerabilities (USN-2150-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : gnutls26 vulnerability (USN-2121-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : icedtea-web vulnerability (USN-2131-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : imagemagick vulnerabilities (USN-2132-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libav vulnerabilities (USN-2103-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libgadu vulnerability (USN-2101-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : librsvg vulnerability (USN-2149-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libssh vulnerability (USN-2145-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libvirt vulnerabilities (USN-2093-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libyaml regression (USN-2098-2)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libyaml vulnerability (USN-2098-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libyaml vulnerability (USN-2160-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : libyaml-libyaml-perl vulnerabilities (USN-2161-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : maas vulnerabilities (USN-2105-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : munin vulnerabilities (USN-2090-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : openssh vulnerability (USN-2164-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : openssl vulnerabilities (USN-2165-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : pidgin vulnerabilities (USN-2100-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : qemu, qemu-kvm vulnerabilities (USN-2092-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : swift vulnerability (USN-2207-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : thunderbird vulnerabilities (USN-2119-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : thunderbird vulnerabilities (USN-2151-1)

Ubuntu 12.04 LTS / 12.10 / 13.10 : udisks, udisks2 vulnerability (USN-2142-1)

Ubuntu 12.04 LTS / 12.10 : bind9 vulnerability (USN-1657-1)

Ubuntu 12.04 LTS / 12.10 : glance vulnerability (USN-1626-1)

Ubuntu 12.04 LTS / 12.10 : glance vulnerability (USN-1764-1)

Ubuntu 12.04 LTS / 12.10 : gtk+3.0 update (USN-2149-2)

Ubuntu 12.04 LTS / 12.10 : initramfs-tools vulnerability (USN-2153-1)

Ubuntu 12.04 LTS / 12.10 : keystone vulnerabilities (USN-1641-1)

Ubuntu 12.04 LTS / 12.10 : keystone vulnerabilities (USN-1730-1)

Ubuntu 12.04 LTS / 12.10 : keystone vulnerability (USN-1715-1)

Ubuntu 12.04 LTS / 12.10 : libav vulnerabilities (USN-1630-1)

Ubuntu 12.04 LTS / 12.10 : libav vulnerabilities (USN-1790-1)

Ubuntu 12.04 LTS / 12.10 : libvirt vulnerabilities (USN-1708-1)

Ubuntu 12.04 LTS / 12.10 : nvidia-graphics-drivers, nvidia-graphics-drivers-updates, nvidia-settings, nvidia-settings-updates vulnerability (USN-1799-1)

Ubuntu 12.04 LTS / 12.10 : openssl regression (USN-1732-2)

Ubuntu 12.04 LTS / 12.10 : openssl vulnerability (USN-1732-3)

Ubuntu 12.04 LTS / 12.10 : python3.2 vulnerabilities (USN-1984-1)

Ubuntu 12.04 LTS / 12.10 : ruby1.9.1 vulnerabilities (USN-1614-1)

Ubuntu 12.04 LTS / 12.10 : ruby1.9.1 vulnerabilities (USN-1733-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : dbus vulnerabilities (USN-2275-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : firefox vulnerabilities (USN-2243-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : json-c vulnerabilities (USN-2245-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : lxml vulnerability (USN-2217-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : miniupnpc vulnerability (USN-2280-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : mod-wsgi vulnerabilities (USN-2222-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : nova vulnerabilities (USN-2247-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : openssl regression (USN-2232-2)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : pidgin vulnerability (USN-2216-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : thunderbird vulnerabilities (USN-2250-1)

Ubuntu 12.04 LTS / 13.10 / 14.04 LTS : transmission vulnerability (USN-2279-1)

Ubuntu 12.04 LTS / 13.10 : libav vulnerabilities (USN-2277-1)

Ubuntu 12.04 LTS / 13.10 : libav vulnerability (USN-2244-1)

Ubuntu 12.04 LTS / 13.10 : libgadu vulnerability (USN-2215-1)

Ubuntu 12.04 LTS / 14.04 / 15.04 / 15.10 : nvidia-graphics-drivers vulnerability (USN-2814-1)

Ubuntu 12.04 LTS / 14.04 / 15.10 : firefox vulnerabilities (USN-2917-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : apport vulnerabilities (USN-2609-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : aptdaemon vulnerability (USN-2648-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : bind9 vulnerability (USN-2669-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : clamav vulnerabilities (USN-2594-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : cups vulnerabilities (USN-2629-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : cups-filters vulnerabilities (USN-2659-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : curl vulnerabilities (USN-2591-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : dnsmasq vulnerability (USN-2593-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : firefox vulnerabilities (USN-2602-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : firefox vulnerability (USN-2571-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : fuse vulnerability (USN-2617-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : libmodule-signature-perl vulnerabilities (USN-2607-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : libtasn1-3, libtasn1-6 vulnerability (USN-2604-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : libwmf vulnerabilities (USN-2670-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : libxml-libxml-perl vulnerability (USN-2592-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : mysql-5.5, mysql-5.6 vulnerabilities (USN-2674-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : nbd vulnerabilities (USN-2676-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : nss vulnerabilities (USN-2672-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : openldap vulnerabilities (USN-2622-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : openssl update (USN-2624-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : openssl vulnerabilities (USN-2639-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : php5 vulnerabilities (USN-2658-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : postgresql-9.1, postgresql-9.3, postgresql-9.4 vulnerabilities (USN-2621-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : python-django vulnerabilities (USN-2671-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : qemu, qemu-kvm vulnerabilities (USN-2608-1) (Venom)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : qemu, qemu-kvm vulnerabilities (USN-2630-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : qt4-x11, qtbase-opensource-src vulnerabilities (USN-2626-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : thunderbird vulnerabilities (USN-2603-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : thunderbird vulnerabilities (USN-2673-1) (Logjam)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : unattended-upgrades vulnerability (USN-2657-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 / 15.04 : wpa, wpasupplicant vulnerabilities (USN-2650-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : batik vulnerability (USN-2548-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : bind9 vulnerability (USN-2503-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : clamav vulnerabilities (USN-2423-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : clamav vulnerability (USN-2488-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : dbus vulnerability (USN-2425-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : devscripts vulnerability (USN-2649-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox regression (USN-2458-3)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox regression (USN-2505-2)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox vulnerabilities (USN-2424-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox vulnerabilities (USN-2458-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox vulnerabilities (USN-2505-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox vulnerabilities (USN-2538-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox vulnerabilities (USN-2550-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : firefox vulnerability (USN-2557-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : git vulnerability (USN-2470-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : icu vulnerabilities (USN-2522-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : jasper vulnerabilities (USN-2483-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : jasper vulnerability (USN-2434-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : libarchive vulnerabilities (USN-2549-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : libksba vulnerability (USN-2427-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : libreoffice vulnerabilities (USN-2578-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : libssh vulnerability (USN-2478-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : libx11, libxrender vulnerability (USN-2568-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : libyaml vulnerability (USN-2461-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : libyaml-libyaml-perl vulnerability (USN-2461-2)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : maas regression (USN-2431-2)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : mailman vulnerability (USN-2558-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : mod-wsgi vulnerability (USN-2431-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : mono vulnerabilities (USN-2547-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : mysql-5.5 vulnerabilities (USN-2480-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : mysql-5.5 vulnerabilities (USN-2575-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : ntp vulnerabilities (USN-2567-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : nvidia-graphics-drivers-304, nvidia-graphics-drivers-304-updates, nvidia-graphics-drivers-331, nvidia-graphics-drivers-331-updates vulnerabilities (USN-2438-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : openvpn vulnerability (USN-2430-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : patch vulnerabilities (USN-2651-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : php5 vulnerabilities (USN-2501-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : pidgin vulnerabilities (USN-2390-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : ppp vulnerability (USN-2595-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : python2.7, python3.2, python3.4 vulnerabilities (USN-2653-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : pyyaml vulnerability (USN-2461-3)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : rpm vulnerabilities (USN-2479-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : ruby1.8, ruby1.9.1, ruby2.0, ruby2.1 vulnerabilities (USN-2397-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : ruby1.8, ruby1.9.1, ruby2.0, ruby2.1 vulnerability (USN-2412-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : samba vulnerability (USN-2508-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : tcpdump vulnerabilities (USN-2580-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : thunderbird vulnerabilities (USN-2428-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : thunderbird vulnerabilities (USN-2460-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : thunderbird vulnerabilities (USN-2506-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : thunderbird vulnerabilities (USN-2552-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : ubufox update (USN-2458-2)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : unzip vulnerabilities (USN-2502-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : usb-creator vulnerability (USN-2576-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : xorg-server, xorg-server-lts-trusty vulnerabilities (USN-2436-1)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : xorg-server, xorg-server-lts-trusty vulnerabilities (USN-2436-2)

Ubuntu 12.04 LTS / 14.04 LTS / 14.10 : xorg-server, xorg-server-lts-trusty, xorg-server-lts-utopic vulnerabilities (USN-2500-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : apport vulnerability (USN-2782-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : audiofile vulnerability (USN-2787-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : bind9 vulnerability (USN-2837-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : bind9 vulnerability (USN-2874-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : curl vulnerability (USN-2882-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : dpkg vulnerability (USN-2820-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : ecryptfs-utils vulnerability (USN-2876-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : firefox vulnerabilities (USN-2785-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : firefox vulnerabilities (USN-2833-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : firefox vulnerabilities (USN-2880-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : firefox vulnerability (USN-2866-1) (SLOTH)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : git vulnerability (USN-2835-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : grub2 vulnerability (USN-2836-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : isc-dhcp vulnerability (USN-2868-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : krb5 vulnerabilities (USN-2810-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : ldb vulnerabilities (USN-2856-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : libpng vulnerabilities (USN-2815-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : libpng vulnerabilities (USN-2861-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : libsndfile vulnerabilities (USN-2832-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : libvirt vulnerabilities (USN-2867-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : libxml2 vulnerabilities (USN-2812-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : libxml2 vulnerabilities (USN-2834-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : libxml2 vulnerabilities (USN-2875-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : mysql-5.5, mysql-5.6 vulnerabilities (USN-2781-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : mysql-5.5, mysql-5.6 vulnerabilities (USN-2881-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : nspr vulnerability (USN-2790-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : nss vulnerabilities (USN-2791-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : nss vulnerability (USN-2864-1) (SLOTH)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : ntp vulnerabilities (USN-2783-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : openssh vulnerabilities (USN-2869-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : openssl vulnerabilities (USN-2830-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : php5 vulnerabilities (USN-2786-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : pygments vulnerability (USN-2862-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : python-django vulnerability (USN-2816-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : qemu, qemu-kvm vulnerabilities (USN-2828-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : rsync vulnerability (USN-2879-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : samba vulnerabilities (USN-2855-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : thunderbird vulnerabilities (USN-2819-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : thunderbird vulnerabilities (USN-2859-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : unzip regression (USN-2788-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 / 15.10 : unzip vulnerabilities (USN-2788-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : apache2 vulnerabilities (USN-2686-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : apport vulnerability (USN-2744-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : bind9 vulnerabilities (USN-2693-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : bind9 vulnerability (USN-2728-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : commons-httpclient vulnerabilities (USN-2769-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : expat vulnerability (USN-2726-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : firefox regression (USN-2702-3)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : firefox regression (USN-2743-4)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : firefox vulnerabilities (USN-2702-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : firefox vulnerabilities (USN-2723-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : firefox vulnerabilities (USN-2743-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : firefox vulnerability (USN-2707-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : firefox vulnerability (USN-2768-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : freetype vulnerabilities (USN-2739-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : gdk-pixbuf vulnerabilities (USN-2767-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : gdk-pixbuf vulnerability (USN-2722-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : ghostscript vulnerability (USN-2697-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : gnutls26, gnutls28 vulnerability (USN-2865-1) (SLOTH)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : hplip vulnerability (USN-2699-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : icu vulnerabilities (USN-2740-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : libreoffice vulnerabilities (USN-2793-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : libvdpau vulnerabilities (USN-2729-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : miniupnpc vulnerability (USN-2780-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : net-snmp vulnerabilities (USN-2711-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : nvidia-graphics-drivers-304, nvidia-graphics-drivers-304-updates, nvidia-graphics-drivers-340, nvidia-graphics-drivers-340-updates, nvidia-graphics-drivers-346, nvidia-graphics-drivers-346-updates, jockey vulnerability (USN-2747-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : openldap vulnerabilities (USN-2742-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : openslp-dfsg vulnerabilities (USN-2730-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : openssh regression (USN-2710-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : openssh vulnerabilities (USN-2710-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : pcre3 vulnerabilities (USN-2694-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : php5 vulnerabilities (USN-2758-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : postgresql-9.1, postgresql-9.3, postgresql-9.4 vulnerabilities (USN-2772-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : python-django vulnerability (USN-2720-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : qemu, qemu-kvm vulnerabilities (USN-2724-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : qemu, qemu-kvm vulnerabilities (USN-2745-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : rpcbind vulnerability (USN-2756-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : sqlite3 vulnerabilities (USN-2698-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : subversion vulnerabilities (USN-2721-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : swift vulnerabilities (USN-2704-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : thunderbird vulnerabilities (USN-2712-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : thunderbird vulnerabilities (USN-2754-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : tidy vulnerabilities (USN-2695-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : ubufox update (USN-2702-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.04 : ubufox update (USN-2743-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : apache2 vulnerability (USN-3038-1) (httpoxy)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : dosfstools vulnerabilities (USN-2986-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : expat vulnerabilities (USN-3010-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : expat vulnerability (USN-2983-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : firefox regression (USN-2936-3)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : firefox vulnerabilities (USN-2993-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : imagemagick vulnerabilities (USN-2990-1) (ImageTragick)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : libarchive vulnerabilities (USN-2981-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : libarchive vulnerabilities (USN-3033-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : libgd2 vulnerabilities (USN-2987-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : libgd2 vulnerabilities (USN-3030-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : libksba vulnerabilities (USN-2982-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : libxml2 vulnerabilities (USN-2994-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : mysql-5.5, mysql-5.6, mysql-5.7 vulnerabilities (USN-3040-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nspr vulnerability (USN-3028-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nss vulnerability (USN-3029-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : openssl vulnerabilities (USN-2959-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : php5, php7.0 vulnerabilities (USN-2984-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : qemu, qemu-kvm vulnerabilities (USN-2974-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : samba regressions (USN-2950-3) (Badlock)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : squid3 vulnerabilities (USN-2995-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : thunderbird vulnerabilities (USN-2934-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : thunderbird vulnerabilities (USN-2973-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : thunderbird vulnerabilities (USN-3023-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : tomcat6, tomcat7 vulnerabilities (USN-3024-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : wget vulnerability (USN-3012-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : bind9 vulnerabilities (USN-2925-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : bsh vulnerability (USN-2923-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : ca-certificates update (USN-2913-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : cpio vulnerabilities (USN-2906-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : eglibc, glibc regression (USN-2985-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : eglibc, glibc vulnerabilities (USN-2985-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : eglibc, glibc vulnerability (USN-2900-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : eog vulnerability (USN-2898-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : exim4 vulnerabilities (USN-2933-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : firefox regression (USN-2880-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : firefox regressions (USN-2917-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : firefox regressions (USN-2917-3)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : firefox vulnerability (USN-2893-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : gimp vulnerability (USN-3025-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : git vulnerabilities (USN-2938-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : glib-networking update (USN-2913-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : gtk+2.0, gtk+3.0 vulnerability (USN-2898-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : jasper vulnerabilities (USN-2919-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : kde4libs vulnerability (USN-3042-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : libgcrypt11, libgcrypt20 vulnerability (USN-2896-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : libreoffice vulnerabilities (USN-2899-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : libssh vulnerabilities (USN-2912-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : libtasn1-3, libtasn1-6 vulnerability (USN-2957-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : mysql-5.5, mysql-5.6 vulnerabilities (USN-2953-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : nss vulnerability (USN-2903-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : nss vulnerability (USN-2924-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : openssh vulnerabilities (USN-2966-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : openssl vulnerabilities (USN-2914-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : optipng vulnerabilities (USN-2951-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : pam regression (USN-2935-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : pam vulnerabilities (USN-2935-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : pcre3 vulnerabilities (USN-2943-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : perl vulnerabilities (USN-2916-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : php5 vulnerabilities (USN-2952-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : pidgin vulnerabilities (USN-3031-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : poppler vulnerabilities (USN-2958-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : postgresql-9.1, postgresql-9.3, postgresql-9.4 vulnerabilities (USN-2894-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : python-django vulnerabilities (USN-2915-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : qemu, qemu-kvm vulnerabilities (USN-2891-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : quagga vulnerabilities (USN-2941-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : samba regression (USN-2855-2)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : samba vulnerabilities (USN-2922-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : samba vulnerabilities (USN-2950-1) (Badlock)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : squid3 vulnerabilities (USN-2921-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : thunderbird vulnerabilities (USN-2904-1) (SLOTH)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : tiff vulnerabilities (USN-2939-1)

Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : xchat-gnome vulnerability (USN-2945-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : bind9 vulnerabilities (USN-3259-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : freetype vulnerability (USN-3263-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : ghostscript vulnerabilities (USN-3272-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : libxslt vulnerabilities (USN-3271-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : apparmor vulnerability (USN-3247-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : apport vulnerabilities (USN-3157-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : bind9 vulnerabilities (USN-3172-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : bind9 vulnerabilities (USN-3201-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : bind9 vulnerability (USN-3119-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : c-ares vulnerability (USN-3143-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : curl vulnerabilities (USN-3123-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : dbus vulnerabilities (USN-3116-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : eject vulnerability (USN-3246-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : exim4 vulnerability (USN-3164-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox regression (USN-3175-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox regression (USN-3216-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox vulnerabilities (USN-3111-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox vulnerabilities (USN-3124-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox vulnerabilities (USN-3140-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox vulnerabilities (USN-3155-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox vulnerabilities (USN-3175-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox vulnerabilities (USN-3216-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox vulnerability (USN-3238-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : freetype vulnerability (USN-3237-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : ghostscript vulnerabilities (USN-3148-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : gnutls26, gnutls28 vulnerabilities (USN-3183-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : gst-plugins-base0.10, gst-plugins-base1.0 vulnerabilities (USN-3244-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : gst-plugins-good0.10, gst-plugins-good1.0 vulnerabilities (USN-3245-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : gst-plugins-good0.10, gst-plugins-good1.0 vulnerability (USN-3135-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : gst-plugins-good0.10, gst-plugins-good1.0 vulnerability (USN-3135-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : icu vulnerabilities (USN-3227-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : imagemagick regression (USN-3142-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : imagemagick vulnerabilities (USN-3131-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : imagemagick vulnerabilities (USN-3142-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : imagemagick vulnerabilities (USN-3222-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : imagemagick vulnerabilities (USN-3232-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : irssi vulnerabilities (USN-3184-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libarchive vulnerabilities (USN-3225-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libevent vulnerabilities (USN-3228-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libgc vulnerability (USN-3197-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libgd2 vulnerabilities (USN-3117-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libgd2 vulnerabilities (USN-3213-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libvncserver vulnerabilities (USN-3171-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libxml2 vulnerabilities (USN-3235-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libxpm vulnerability (USN-3185-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon, linux-ti-omap4 vulnerability (USN-3256-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : mailman vulnerabilities (USN-3118-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : memcached vulnerabilities (USN-3120-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : moin vulnerabilities (USN-3137-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3109-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3174-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : nettle vulnerability (USN-3193-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : network-manager-applet vulnerability (USN-3217-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : nss vulnerabilities (USN-3163-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : nvidia-graphics-drivers-304 and nvidia-graphics-drivers-340 vulnerability (USN-3173-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : nvidia-graphics-drivers-304, nvidia-graphics-drivers-340, nvidia-graphics-drivers-375 vulnerability (USN-3240-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : openssl vulnerabilities (USN-3181-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : pcsc-lite vulnerability (USN-3176-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : python-django vulnerabilities (USN-3115-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : python-django vulnerabilities (USN-3254-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : qemu, qemu-kvm vulnerabilities (USN-3125-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : quagga vulnerability (USN-3110-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : samba regression (USN-3242-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : samba vulnerabilities (USN-3158-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : samba vulnerability (USN-3242-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : squid3 vulnerabilities (USN-3192-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : tar vulnerability (USN-3132-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : tcpdump vulnerabilities (USN-3205-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : thunderbird vulnerabilities (USN-3112-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : thunderbird vulnerabilities (USN-3141-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : thunderbird vulnerabilities (USN-3165-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : thunderbird vulnerabilities (USN-3233-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : tomcat6, tomcat7, tomcat8 vulnerabilities (USN-3177-1) (httpoxy)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : vim vulnerability (USN-3139-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : bind9 vulnerability (USN-3088-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : clamav vulnerabilities (USN-3093-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : curl vulnerabilities (USN-3048-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : eglibc, glibc regression (USN-3239-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : eglibc, glibc vulnerabilities (USN-3239-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : eog vulnerability (USN-3069-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : firefox vulnerabilities (USN-3044-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : firefox vulnerabilities (USN-3076-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : fontconfig vulnerability (USN-3063-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : gdk-pixbuf vulnerabilities (USN-3085-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : gnupg vulnerability (USN-3064-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : imlib2 vulnerabilities (USN-3075-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : libgcrypt11, libgcrypt20 vulnerability (USN-3065-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : libidn vulnerabilities (USN-3068-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : LibreOffice vulnerability (USN-3210-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : linux-hwe, linux-lts-trusty, linux-lts-xenial vulnerability (USN-3256-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : mysql-5.5, mysql-5.7 vulnerability (USN-3078-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : ntp vulnerabilities (USN-3096-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : nvidia-graphics-drivers-304, nvidia-graphics-drivers-340, nvidia-graphics-drivers-367 vulnerability (USN-3122-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : openssh vulnerabilities (USN-3061-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : openssl regression (USN-3087-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : openssl vulnerabilities (USN-3087-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : php5, php7.0 vulnerabilities (USN-3045-1) (httpoxy)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : php5, php7.0 vulnerabilities (USN-3095-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : postgresql-9.1, postgresql-9.3, postgresql-9.5 vulnerabilities (USN-3066-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : python-django vulnerability (USN-3089-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : python2.7, python3.2, python3.4, python3.5 vulnerabilities (USN-3134-1) (httpoxy)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : qemu, qemu-kvm regression (USN-3047-2)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : qemu, qemu-kvm vulnerabilities (USN-3047-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : quagga vulnerabilities (USN-3102-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : thunderbird vulnerabilities (USN-3073-1)

Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : tomcat6, tomcat7, tomcat8 vulnerability (USN-3081-1)

Ubuntu 12.04 LTS / 14.04 LTS : apt vulnerability (USN-2370-1)

Ubuntu 12.04 LTS / 14.04 LTS : audiofile vulnerabilities (USN-3241-1)

Ubuntu 12.04 LTS / 14.04 LTS : exuberant-ctags vulnerability (USN-2371-1)

Ubuntu 12.04 LTS / 14.04 LTS : firefox vulnerabilities (USN-2295-1)

Ubuntu 12.04 LTS / 14.04 LTS : firefox vulnerabilities (USN-2329-1)

Ubuntu 12.04 LTS / 14.04 LTS : firefox vulnerabilities (USN-2360-1)

Ubuntu 12.04 LTS / 14.04 LTS : firefox vulnerabilities (USN-2372-1)

Ubuntu 12.04 LTS / 14.04 LTS : gnutls26 update (USN-2913-4)

Ubuntu 12.04 LTS / 14.04 LTS : gnutls26 vulnerability (USN-2821-1)

Ubuntu 12.04 LTS / 14.04 LTS : gnutls26 vulnerability (USN-3183-2)

Ubuntu 12.04 LTS / 14.04 LTS : gtk-vnc vulnerabilities (USN-3203-1)

Ubuntu 12.04 LTS / 14.04 LTS : kde4libs vulnerability (USN-2304-1)

Ubuntu 12.04 LTS / 14.04 LTS : kde4libs vulnerability (USN-3223-1)

Ubuntu 12.04 LTS / 14.04 LTS : libdbd-mysql-perl vulnerabilities (USN-3103-1)

Ubuntu 12.04 LTS / 14.04 LTS : libvncserver vulnerabilities (USN-2365-1)

Ubuntu 12.04 LTS / 14.04 LTS : lua5.1 vulnerability (USN-2338-1)

Ubuntu 12.04 LTS / 14.04 LTS : lzo2 vulnerability (USN-2300-1)

Ubuntu 12.04 LTS / 14.04 LTS : mysql-5.5 vulnerabilities (USN-2291-1)

Ubuntu 12.04 LTS / 14.04 LTS : mysql-5.5 vulnerabilities (USN-2384-1)

Ubuntu 12.04 LTS / 14.04 LTS : openjdk-7 vulnerabilities (USN-3194-1)

Ubuntu 12.04 LTS / 14.04 LTS : openssl update (USN-2913-3)

Ubuntu 12.04 LTS / 14.04 LTS : php5 vulnerabilities (USN-3196-1)

Ubuntu 12.04 LTS / 14.04 LTS : pidgin vulnerability (USN-3231-1)

Ubuntu 12.04 LTS / 14.04 LTS : pixman vulnerability (USN-2918-1)

Ubuntu 12.04 LTS / 14.04 LTS : serf vulnerability (USN-2315-1)

Ubuntu 12.04 LTS / 14.04 LTS : squid3 vulnerability (USN-2327-1)

Ubuntu 12.04 LTS / 14.04 LTS : subversion vulnerabilities (USN-2316-1)

Ubuntu 12.04 LTS / 14.04 LTS : thunderbird vulnerabilities (USN-2296-1)

Ubuntu 12.04 LTS / 14.04 LTS : thunderbird vulnerabilities (USN-2330-1)

Ubuntu 12.04 LTS / 14.04 LTS : thunderbird vulnerabilities (USN-2360-2)

Ubuntu 12.04 LTS / 14.04 LTS : thunderbird vulnerabilities (USN-2373-1)

Ubuntu 12.04 LTS / 14.04 LTS : tomcat6, tomcat7 regression (USN-3177-2) (httpoxy)

Ubuntu 12.04 LTS / 14.04 LTS : tomcat6, tomcat7 vulnerability (USN-3204-1)

Ubuntu 12.04 LTS / 14.04 LTS : w3m vulnerabilities (USN-3214-1)

Ubuntu 12.04 LTS / 15.10 / 16.04 LTS : libreoffice vulnerability (USN-3022-1)

Ubuntu 12.04 LTS : acpi-support vulnerability (USN-2297-1)

Ubuntu 12.04 LTS : apache2 update (USN-2625-1)

Ubuntu 12.04 LTS : bind9 vulnerability (USN-3108-1)

Ubuntu 12.04 LTS : calligra vulnerability (USN-1525-1)

Ubuntu 12.04 LTS : djvulibre vulnerability (USN-2056-1)

Ubuntu 12.04 LTS : eglibc regression (USN-3239-3)

Ubuntu 12.04 LTS : eglibc vulnerability (USN-3323-2) (Stack Clash)

Ubuntu 12.04 LTS : feedparser vulnerability (USN-1449-1)

Ubuntu 12.04 LTS : firefox vulnerabilities (USN-2656-2) (Logjam)

Ubuntu 12.04 LTS : foomatic-filters vulnerability (USN-2831-2)

Ubuntu 12.04 LTS : foomatic-filters vulnerability (USN-2838-2)

Ubuntu 12.04 LTS : FreeType vulnerabilities (USN-3282-2)

Ubuntu 12.04 LTS : gparted vulnerability (USN-2471-1)

Ubuntu 12.04 LTS : gpsd vulnerability (USN-1820-1)

Ubuntu 12.04 LTS : horizon vulnerabilities (USN-1439-1)

Ubuntu 12.04 LTS : horizon vulnerability (USN-1565-1)

Ubuntu 12.04 LTS : icoutils vulnerabilities (USN-3178-1)

Ubuntu 12.04 LTS : icoutils vulnerabilities (USN-3226-1)

Ubuntu 12.04 LTS : icu regression (USN-2522-2)

Ubuntu 12.04 LTS : icu vulnerabilities (USN-2522-3)

Ubuntu 12.04 LTS : ipsec-tools vulnerability (USN-2623-1)

Ubuntu 12.04 LTS : jinja2 vulnerabilities (USN-2301-1)

Ubuntu 12.04 LTS : jockey vulnerability (USN-1957-1)

Ubuntu 12.04 LTS : kde-runtime vulnerability (USN-2414-1)

Ubuntu 12.04 LTS : kde-workspace vulnerabilities (USN-2402-1)

Ubuntu 12.04 LTS : kdepimlibs vulnerability (USN-3100-1)

Ubuntu 12.04 LTS : keystone vulnerabilities (USN-1552-1)

Ubuntu 12.04 LTS : keystone vulnerability (USN-1564-1)

Ubuntu 12.04 LTS : konversation vulnerability (USN-2401-1)

Ubuntu 12.04 LTS : libav vulnerabilities (USN-2309-1)

Ubuntu 12.04 LTS : libav vulnerabilities (USN-2349-1)

Ubuntu 12.04 LTS : libav vulnerabilities (USN-2534-1)

Ubuntu 12.04 LTS : libav vulnerabilities (USN-2944-1)

Ubuntu 12.04 LTS : libkdcraw vulnerabilities (USN-1978-1)

Ubuntu 12.04 LTS : libkdcraw vulnerability (USN-1885-1)

Ubuntu 12.04 LTS : libnl3 vulnerability (USN-3311-2)

Ubuntu 12.04 LTS : libotr vulnerabilities (USN-2091-1)

Ubuntu 12.04 LTS : libotr vulnerability (USN-2926-1)

Ubuntu 12.04 LTS : libreoffice vulnerability (USN-2400-1)

Ubuntu 12.04 LTS : libreoffice vulnerability (USN-3046-1)

Ubuntu 12.04 LTS : linux regression (USN-1696-2)

Ubuntu 12.04 LTS : linux regression (USN-2640-2)

Ubuntu 12.04 LTS : linux regression (USN-3338-2) (Stack Clash)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1448-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1473-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1529-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1579-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1644-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1696-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1767-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1793-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1809-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1833-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1878-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1941-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-1968-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2017-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2038-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2066-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2109-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2133-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2221-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2235-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2259-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2283-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2334-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2356-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2376-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2417-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2443-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2463-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2492-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2513-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2541-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2560-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2631-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2678-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2713-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2759-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2773-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2792-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2840-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2846-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2886-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2967-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-2996-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3021-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3049-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3072-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3097-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3126-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3167-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3187-1)

Ubuntu 12.04 LTS : linux vulnerabilities (USN-3338-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1486-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1515-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1610-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1669-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1741-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1825-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1844-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1914-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1929-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-1992-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2198-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2268-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2526-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2585-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2596-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2611-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2640-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2660-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2731-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2800-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2911-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-2928-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-3082-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-3104-1) (Dirty COW)

Ubuntu 12.04 LTS : linux vulnerability (USN-3144-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-3150-1)

Ubuntu 12.04 LTS : linux vulnerability (USN-3159-1)

Ubuntu 12.04 LTS : linux, linux-ti-omap4 vulnerabilities (USN-3206-1)

Ubuntu 12.04 LTS : linux, linux-ti-omap4 vulnerability (USN-3218-1)

Ubuntu 12.04 LTS : linux, linux-ti-omap4 vulnerability (USN-3248-1)

Ubuntu 12.04 LTS : linux-lts-quantal - Linux kernel hardware enablement from Quantal regression (USN-1704-2)

Ubuntu 12.04 LTS : linux-lts-quantal - Linux kernel hardware enablement from Quantal vulnerabilities (USN-1704-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1768-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1795-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1812-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1834-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1880-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1931-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1947-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-1970-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2019-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2040-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2068-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2111-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2135-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2175-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2223-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2262-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerabilities (USN-2285-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-1743-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-1749-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-1828-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-1845-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-1915-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-1994-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-2199-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-2237-1)

Ubuntu 12.04 LTS : linux-lts-quantal vulnerability (USN-2269-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-1936-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-1943-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-1971-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-1995-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2020-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2041-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2069-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2112-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2136-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2158-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2176-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2224-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2238-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerabilities (USN-2286-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerability (USN-1849-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerability (USN-1916-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerability (USN-2094-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerability (USN-2200-1)

Ubuntu 12.04 LTS : linux-lts-raring vulnerability (USN-2270-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2042-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2070-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2113-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2137-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2177-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2225-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2239-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2261-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerabilities (USN-2287-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerability (USN-2095-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerability (USN-2201-1)

Ubuntu 12.04 LTS : linux-lts-saucy vulnerability (USN-2271-1)

Ubuntu 12.04 LTS : linux-lts-trusty regression (USN-2642-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2260-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2288-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2317-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2336-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2358-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2378-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2394-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2419-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2445-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2465-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2515-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2515-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2543-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2562-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2587-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2613-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2633-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2662-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2680-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2687-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2701-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2749-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2775-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2795-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2826-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2841-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2847-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2887-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2907-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2929-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2946-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2968-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-2998-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3018-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3051-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3071-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3083-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3098-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3127-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3145-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3160-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3168-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3207-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerabilities (USN-3343-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2272-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2313-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2527-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2597-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2597-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2619-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2642-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2715-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2733-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2763-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2804-1)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2870-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-2975-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3034-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3105-2) (Dirty COW)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3149-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3188-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3219-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3250-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3264-2)

Ubuntu 12.04 LTS : linux-lts-trusty vulnerability (USN-3335-2)

Ubuntu 12.04 LTS : mesa vulnerability (USN-1623-1)

Ubuntu 12.04 LTS : mesa vulnerability (USN-1818-1)

Ubuntu 12.04 LTS : nova vulnerability (USN-1501-1)

Ubuntu 12.04 LTS : nss regression (USN-2903-2)

Ubuntu 12.04 LTS : nss vulnerability (USN-1540-2)

Ubuntu 12.04 LTS : openjdk-6 vulnerabilities (USN-2706-1) (Bar Mitzvah) (Logjam)

Ubuntu 12.04 LTS : openjdk-6 vulnerabilities (USN-2827-1)

Ubuntu 12.04 LTS : openjdk-6 vulnerabilities (USN-2885-1)

Ubuntu 12.04 LTS : openjdk-6 vulnerabilities (USN-2972-1)

Ubuntu 12.04 LTS : openjdk-6 vulnerabilities (USN-3077-1)

Ubuntu 12.04 LTS : openjdk-6 vulnerabilities (USN-3154-1)

Ubuntu 12.04 LTS : openjdk-6 vulnerabilities (USN-3198-1)

Ubuntu 12.04 LTS : openssl update (USN-2367-1)

Ubuntu 12.04 LTS : openssl update (USN-2606-1)

Ubuntu 12.04 LTS : openssl vulnerability (USN-1516-1)

Ubuntu 12.04 LTS : openssl vulnerability (USN-2863-1) (SLOTH)

Ubuntu 12.04 LTS : openvpn vulnerability (USN-2368-1)

Ubuntu 12.04 LTS : oxygen-gtk3 update (USN-2936-2)

Ubuntu 12.04 LTS : pam regression (USN-2935-3)

Ubuntu 12.04 LTS : php5 vulnerability (USN-1702-1)

Ubuntu 12.04 LTS : python-crypto vulnerability (USN-3199-3)

Ubuntu 12.04 LTS : python-imaging vulnerabilities (USN-3080-1)

Ubuntu 12.04 LTS : python-imaging vulnerabilities (USN-3229-1)

Ubuntu 12.04 LTS : raptor2 vulnerability (USN-1901-1)

Ubuntu 12.04 LTS : rtmpdump vulnerabilities (USN-3283-2)

Ubuntu 12.04 LTS : ruby1.9.1 vulnerabilities (USN-1583-1)

Ubuntu 12.04 LTS : ruby1.9.1 vulnerabilities (USN-1602-1)

Ubuntu 12.04 LTS : rubygems vulnerabilities (USN-1582-1)

Ubuntu 12.04 LTS : samba regressions (USN-2950-4) (Badlock)

Ubuntu 12.04 LTS : samba vulnerability (USN-1802-1)

Ubuntu 12.04 LTS : samba vulnerability (USN-3296-2) (SambaCry)

Ubuntu 12.04 LTS : tiff vulnerabilities (USN-3212-3)

Ubuntu 12.04 LTS : tiff vulnerabilities (USN-3212-4)

Ubuntu 12.04 LTS : tomcat6 vulnerabilities (USN-2655-1)

Ubuntu 12.04 LTS : transmission vulnerability (USN-1584-1)

Ubuntu 12.04 LTS : ubiquity-slideshow-ubuntu vulnerability (USN-1561-1)

Ubuntu 12.04 LTS : webkit vulnerabilities (USN-1524-1)

Ubuntu 12.04 LTS : webkit vulnerabilities (USN-1617-1)

Ubuntu 12.04 LTS : xdiagnose update (USN-1591-1)

Ubuntu 12.04 LTS : xmlrpc-c vulnerabilities (USN-3013-1)

Ubuntu 12.04 LTS : xorg-server vulnerability (USN-1502-1)

Ubuntu 12.04 LTS : xscreensaver vulnerability (USN-2789-1)

Ubuntu 12.10 / 13.04 / 13.10 : cups vulnerability (USN-2082-1)

Ubuntu 12.10 / 13.04 / 13.10 : horizon vulnerability (USN-2062-1)

Ubuntu 12.10 / 13.04 / 13.10 : keystone vulnerability (USN-2034-1)

Ubuntu 12.10 / 13.04 / 13.10 : openjdk-7 vulnerabilities (USN-2089-1)

Ubuntu 12.10 / 13.04 : file-roller vulnerability (USN-1906-1)

Ubuntu 12.10 / 13.04 : glance vulnerability (USN-2003-1)

Ubuntu 12.10 / 13.04 : imagemagick vulnerability (USN-1949-1)

Ubuntu 12.10 / 13.04 : keystone vulnerabilities (USN-1875-1)

Ubuntu 12.10 / 13.04 : keystone vulnerabilities (USN-2002-1)

Ubuntu 12.10 / 13.04 : libimobiledevice vulnerability (USN-1927-1)

Ubuntu 12.10 / 13.04 : openjdk-7 vulnerabilities (USN-1907-1)

Ubuntu 12.10 / 13.04 : python3.3 vulnerabilities (USN-1985-1)

Ubuntu 12.10 / 13.10 / 14.04 LTS : elfutils vulnerability (USN-2188-1)

Ubuntu 12.10 / 13.10 / 14.04 LTS : jbigkit vulnerability (USN-2190-1)

Ubuntu 12.10 / 13.10 / 14.04 LTS : openjdk-7 vulnerabilities (USN-2187-1)

Ubuntu 12.10 : boost1.49 vulnerability (USN-1727-1)

Ubuntu 12.10 : cinder vulnerability (USN-1731-1)

Ubuntu 12.10 : cinder vulnerability (USN-2208-1)

Ubuntu 12.10 : curl vulnerability (USN-1721-1)

Ubuntu 12.10 : glance vulnerability (USN-1626-2)

Ubuntu 12.10 : gnome-screensaver vulnerability (USN-1716-1)

Ubuntu 12.10 : keystone vulnerability (USN-1772-1)

Ubuntu 12.10 : libunity-webapps vulnerability (USN-1635-1)

Ubuntu 12.10 : linux regression (USN-1699-2)

Ubuntu 12.10 : linux vulnerabilities (USN-1646-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1699-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1750-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1769-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1796-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1813-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1835-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1881-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1932-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1944-1)

Ubuntu 12.10 : linux vulnerabilities (USN-1972-1)

Ubuntu 12.10 : linux vulnerabilities (USN-2021-1)

Ubuntu 12.10 : linux vulnerabilities (USN-2043-1)

Ubuntu 12.10 : linux vulnerabilities (USN-2071-1)

Ubuntu 12.10 : linux vulnerabilities (USN-2114-1)

Ubuntu 12.10 : linux vulnerabilities (USN-2138-1)

Ubuntu 12.10 : linux vulnerabilities (USN-2178-1)

Ubuntu 12.10 : linux vulnerability (USN-1671-1)

Ubuntu 12.10 : linux vulnerability (USN-1744-1)

Ubuntu 12.10 : linux vulnerability (USN-1826-1)

Ubuntu 12.10 : linux vulnerability (USN-1846-1)

Ubuntu 12.10 : linux vulnerability (USN-1917-1)

Ubuntu 12.10 : linux vulnerability (USN-1996-1)

Ubuntu 12.10 : linux vulnerability (USN-2202-1)

Ubuntu 12.10 : nova regression (USN-1831-2)

Ubuntu 12.10 : nova vulnerability (USN-1663-1)

Ubuntu 12.10 : openjdk-7 vulnerabilities (USN-1693-1)

Ubuntu 12.10 : openjdk-7 vulnerabilities (USN-1755-2)

Ubuntu 12.10 : openjdk-7 vulnerabilities (USN-1806-1)

Ubuntu 12.10 : pam-xdg-support vulnerability (USN-1766-1)

Ubuntu 12.10 : quantum vulnerability (USN-2208-2)

Ubuntu 12.10 : remote-login-service vulnerability (USN-1624-1)

Ubuntu 12.10 : rpm vulnerability (USN-1694-1)

Ubuntu 12.10 : ruby1.8 vulnerabilities (USN-1603-2)

Ubuntu 12.10 : ubuntu-release-upgrader vulnerability (USN-1892-1)

Ubuntu 12.10 : unity-firefox-extension update (USN-1786-2)

Ubuntu 12.10 : unity-firefox-extension vulnerability (USN-1639-1)

Ubuntu 12.10 : unity-firefox-extension vulnerability (USN-1665-1)

Ubuntu 13.04 / 13.10 : spice vulnerability (USN-2027-1)

Ubuntu 13.04 : cinder vulnerabilities (USN-2005-1)

Ubuntu 13.04 : cyrus-sasl2 vulnerability (USN-1988-1)

Ubuntu 13.04 : ghostscript vulnerability (USN-1911-2)

Ubuntu 13.04 : libvirt vulnerability (USN-1895-1)

Ubuntu 13.04 : libxml2 vulnerability (USN-1817-1)

Ubuntu 13.04 : lightdm vulnerability (USN-1950-1)

Ubuntu 13.04 : linux vulnerabilities (USN-1815-1)

Ubuntu 13.04 : linux vulnerabilities (USN-1837-1)

Ubuntu 13.04 : linux vulnerabilities (USN-1935-1)

Ubuntu 13.04 : linux vulnerabilities (USN-1938-1)

Ubuntu 13.04 : linux vulnerabilities (USN-1974-1)

Ubuntu 13.04 : linux vulnerabilities (USN-1998-1)

Ubuntu 13.04 : linux vulnerabilities (USN-2023-1)

Ubuntu 13.04 : linux vulnerabilities (USN-2045-1)

Ubuntu 13.04 : linux vulnerabilities (USN-2073-1)

Ubuntu 13.04 : linux vulnerability (USN-1827-1)

Ubuntu 13.04 : linux vulnerability (USN-1847-1)

Ubuntu 13.04 : linux vulnerability (USN-1919-1)

Ubuntu 13.04 : mysql-5.5 vulnerabilities (USN-1807-2)

Ubuntu 13.04 : php5 vulnerability (USN-1872-1)

Ubuntu 13.04 : python-glanceclient vulnerability (USN-2004-1)

Ubuntu 13.04 : python-keystoneclient vulnerability (USN-1851-1)

Ubuntu 13.04 : spice vulnerability (USN-1926-1)

Ubuntu 13.04 : systemd vulnerability (USN-1961-1)

Ubuntu 13.10 / 14.04 LTS : cinder vulnerability (USN-2248-1)

Ubuntu 13.10 / 14.04 LTS : neutron vulnerabilities (USN-2255-1)

Ubuntu 13.10 / 14.04 LTS : php5 updates (USN-2254-2)

Ubuntu 13.10 : freetype vulnerabilities (USN-2148-1)

Ubuntu 13.10 : glance vulnerability (USN-2193-1)

Ubuntu 13.10 : horizon vulnerability (USN-2206-1)

Ubuntu 13.10 : indicator-datetime vulnerability (USN-2186-1)

Ubuntu 13.10 : keystone vulnerability (USN-2061-1)

Ubuntu 13.10 : libvirt vulnerabilities (USN-2209-1)

Ubuntu 13.10 : libvirt vulnerability (USN-2026-1)

Ubuntu 13.10 : lightdm vulnerability (USN-2012-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2049-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2075-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2117-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2140-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2179-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2228-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2241-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2264-1)

Ubuntu 13.10 : linux vulnerabilities (USN-2289-1)

Ubuntu 13.10 : linux vulnerability (USN-2096-1)

Ubuntu 13.10 : linux vulnerability (USN-2203-1)

Ubuntu 13.10 : linux vulnerability (USN-2273-1)

Ubuntu 13.10 : lxc vulnerability (USN-2104-1)

Ubuntu 13.10 : neutron vulnerability (USN-2194-1)

Ubuntu 13.10 : openssh vulnerability (USN-2014-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : firefox vulnerabilities (USN-2656-1) (Logjam)

Ubuntu 14.04 LTS / 14.10 / 15.04 : icu vulnerabilities (USN-2605-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : lxc vulnerabilities (USN-2675-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : network-manager vulnerability (USN-2581-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : oxide-qt vulnerabilities (USN-2570-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : oxide-qt vulnerabilities (USN-2582-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : oxide-qt vulnerabilities (USN-2610-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : oxide-qt vulnerabilities (USN-2652-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : python-dbusmock vulnerability (USN-2618-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : strongswan vulnerability (USN-2628-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : tomcat7 vulnerabilities (USN-2654-1)

Ubuntu 14.04 LTS / 14.10 / 15.04 : wpa vulnerability (USN-2577-1)

Ubuntu 14.04 LTS / 14.10 : apport vulnerability (USN-2569-1)

Ubuntu 14.04 LTS / 14.10 : apport vulnerability (USN-2569-2)

Ubuntu 14.04 LTS / 14.10 : cgmanager vulnerability (USN-2451-1)

Ubuntu 14.04 LTS / 14.10 : cups-filters vulnerability (USN-2532-1)

Ubuntu 14.04 LTS / 14.10 : jakarta-taglibs-standard vulnerability (USN-2551-1)

Ubuntu 14.04 LTS / 14.10 : libreoffice vulnerability (USN-2398-1)

Ubuntu 14.04 LTS / 14.10 : libvirt vulnerabilities (USN-2404-1)

Ubuntu 14.04 LTS / 14.10 : openjdk-7 vulnerabilities (USN-2487-1) (POODLE)

Ubuntu 14.04 LTS / 14.10 : openjdk-7 vulnerabilities (USN-2574-1)

Ubuntu 14.04 LTS / 14.10 : oxide-qt vulnerabilities (USN-2410-1)

Ubuntu 14.04 LTS / 14.10 : oxide-qt vulnerabilities (USN-2476-1)

Ubuntu 14.04 LTS / 14.10 : oxide-qt vulnerabilities (USN-2495-1)

Ubuntu 14.04 LTS / 14.10 : oxide-qt vulnerabilities (USN-2521-1)

Ubuntu 14.04 LTS / 14.10 : oxide-qt vulnerabilities (USN-2556-1)

Ubuntu 14.04 LTS / 14.10 : requests vulnerability (USN-2531-1)

Ubuntu 14.04 LTS / 14.10 : samba vulnerability (USN-2481-1)

Ubuntu 14.04 LTS / 14.10 : squid3 vulnerabilities (USN-2422-1)

Ubuntu 14.04 LTS / 14.10 : strongswan vulnerability (USN-2450-1)

Ubuntu 14.04 LTS / 14.10 : t1utils vulnerability (USN-2627-1)

Ubuntu 14.04 LTS / 14.10 : unbound vulnerability (USN-2484-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : cups-filters vulnerability (USN-2831-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : cups-filters vulnerability (USN-2838-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : icedtea-web vulnerabilities (USN-2817-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : openjdk-7 vulnerabilities (USN-2784-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : openjdk-7 vulnerabilities (USN-2884-1) (SLOTH)

Ubuntu 14.04 LTS / 15.04 / 15.10 : openjdk-7 vulnerability (USN-2818-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : oxide-qt vulnerabilities (USN-2825-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : oxide-qt vulnerabilities (USN-2860-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : oxide-qt vulnerabilities (USN-2877-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : sosreport vulnerabilities (USN-2845-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : strongswan vulnerability (USN-2811-1)

Ubuntu 14.04 LTS / 15.04 / 15.10 : wpa vulnerabilities (USN-2808-1)

Ubuntu 14.04 LTS / 15.04 : click vulnerability (USN-2771-1)

Ubuntu 14.04 LTS / 15.04 : lxc vulnerability (USN-2753-1)

Ubuntu 14.04 LTS / 15.04 : openjdk-7 vulnerabilities (USN-2696-1) (Bar Mitzvah) (Logjam)

Ubuntu 14.04 LTS / 15.04 : oxide-qt vulnerabilities (USN-2677-1)

Ubuntu 14.04 LTS / 15.04 : oxide-qt vulnerabilities (USN-2735-1)

Ubuntu 14.04 LTS / 15.04 : oxide-qt vulnerabilities (USN-2757-1)

Ubuntu 14.04 LTS / 15.04 : oxide-qt vulnerabilities (USN-2770-1)

Ubuntu 14.04 LTS / 15.04 : pollinate update (USN-2709-1)

Ubuntu 14.04 LTS / 15.04 : pollinate update (USN-2709-2)

Ubuntu 14.04 LTS / 15.04 : python-keystoneclient, python-keystonemiddleware vulnerabilities (USN-2705-1)

Ubuntu 14.04 LTS / 15.04 : qemu vulnerabilities (USN-2692-1)

Ubuntu 14.04 LTS / 15.04 : simplestreams regression (USN-2746-2)

Ubuntu 14.04 LTS / 15.04 : simplestreams vulnerability (USN-2746-1)

Ubuntu 14.04 LTS / 15.04 : spice vulnerabilities (USN-2766-1)

Ubuntu 14.04 LTS / 15.04 : spice vulnerability (USN-2736-1)

Ubuntu 14.04 LTS / 15.04 : unity-firefox-extension, webapps-greasemonkey, webaccounts-browser-extension update (USN-2743-3)

Ubuntu 14.04 LTS / 15.04 : unity-settings-daemon vulnerability (USN-2741-1)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : libimobiledevice vulnerability (USN-3026-1)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : libsoup2.4 update (USN-2950-2) (Badlock)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : nginx vulnerability (USN-2991-1)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : oxide-qt vulnerabilities (USN-2955-1)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : oxide-qt vulnerabilities (USN-2960-1)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : oxide-qt vulnerabilities (USN-2992-1)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : oxide-qt vulnerabilities (USN-3015-1)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : samba regression (USN-2950-5) (Badlock)

Ubuntu 14.04 LTS / 15.10 / 16.04 LTS : spice vulnerabilities (USN-3014-1)

Ubuntu 14.04 LTS / 15.10 : graphite2 vulnerabilities (USN-2902-1)

Ubuntu 14.04 LTS / 15.10 : graphite2 vulnerabilities (USN-2927-1)

Ubuntu 14.04 LTS / 15.10 : nettle vulnerabilities (USN-2897-1)

Ubuntu 14.04 LTS / 15.10 : nginx vulnerabilities (USN-2892-1)

Ubuntu 14.04 LTS / 15.10 : openjdk-7 vulnerabilities (USN-2964-1)

Ubuntu 14.04 LTS / 15.10 : openjdk-7 vulnerability (USN-2942-1)

Ubuntu 14.04 LTS / 15.10 : oxide-qt vulnerabilities (USN-2895-1)

Ubuntu 14.04 LTS / 15.10 : oxide-qt vulnerabilities (USN-2920-1)

Ubuntu 14.04 LTS / 15.10 : oxide-qt vulnerability (USN-2905-1)

Ubuntu 14.04 LTS / 15.10 : python-django regression (USN-2915-2)

Ubuntu 14.04 LTS / 15.10 : python-django regression (USN-2915-3)

Ubuntu 14.04 LTS / 15.10 : webkitgtk vulnerabilities (USN-2937-1)

Ubuntu 14.04 LTS / 15.10 : xdelta3 vulnerability (USN-2901-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : apache2 vulnerabilities (USN-3340-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : apport vulnerability (USN-3354-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : bash vulnerabilities (USN-3294-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : bind9 vulnerabilities (USN-3346-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : eglibc, glibc vulnerability (USN-3323-1) (Stack Clash)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : evince vulnerability (USN-3351-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : exim4 vulnerability (USN-3322-1) (Stack Clash)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : expat vulnerability (USN-3356-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : firefox regression (USN-3260-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : firefox update (USN-3299-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : firefox vulnerabilities (USN-3260-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : firefox vulnerabilities (USN-3315-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : freetype vulnerabilities (USN-3282-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : ghostscript regression (USN-3272-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : git vulnerability (USN-3287-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : gnutls26, gnutls28 vulnerabilities (USN-3318-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : heimdal vulnerability (USN-3353-1) (Orpheus' Lyre)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : icu vulnerabilities (USN-3274-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : imagemagick vulnerabilities (USN-3302-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : irssi vulnerabilities (USN-3317-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : jbig2dec vulnerabilities (USN-3297-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : juju-core vulnerability (USN-3300-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : libgcrypt11, libgcrypt20 vulnerabilities (USN-3347-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : libmwaw vulnerability (USN-3319-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : libnl3 vulnerability (USN-3311-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : libsndfile vulnerabilities (USN-3306-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : libtasn1-6 vulnerability (USN-3309-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3269-1) (Riddle)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : nagios3 regression (USN-3253-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : nginx vulnerability (USN-3352-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : nss vulnerabilities (USN-3270-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : nss vulnerability (USN-3336-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : ntp vulnerabilities (USN-3349-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : nvidia-graphics-drivers-375 vulnerabilities (USN-3305-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : openldap vulnerability (USN-3307-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : openvpn vulnerabilities (USN-3339-1) (SWEET32)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : poppler vulnerabilities (USN-3350-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : qemu vulnerabilities (USN-3289-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : samba vulnerability (USN-3296-1) (SambaCry)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : samba vulnerability (USN-3348-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : samba vulnerability (USN-3353-2) (Orpheus' Lyre)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : shadow regression (USN-3276-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : shadow vulnerabilities (USN-3276-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : strongswan vulnerabilities (USN-3301-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : sudo vulnerability (USN-3304-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : thunderbird vulnerabilities (USN-3278-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : thunderbird vulnerabilities (USN-3321-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : valgrind vulnerabilities (USN-3337-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 / 17.04 : zziplib vulnerabilities (USN-3320-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : apache2 vulnerabilities (USN-3279-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : apt vulnerability (USN-3156-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : libreoffice vulnerabilities (USN-3273-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : lxc vulnerability (USN-3136-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : lxc vulnerability (USN-3224-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : miniupnpc vulnerability (USN-3298-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : nagios3 vulnerabilities (USN-3253-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : nginx regression (USN-3114-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : nginx vulnerability (USN-3114-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : nvidia-graphics-drivers-375 vulnerability (USN-3173-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : oxide-qt vulnerabilities (USN-3113-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : oxide-qt vulnerabilities (USN-3133-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : oxide-qt vulnerabilities (USN-3153-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : oxide-qt vulnerabilities (USN-3180-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : oxide-qt vulnerabilities (USN-3236-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : pillow vulnerabilities (USN-3230-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : Python Crypto regression (USN-3199-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : Python Crypto vulnerability (USN-3199-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : qemu vulnerabilities (USN-3261-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : spice vulnerabilities (USN-3202-1)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : tiff regression (USN-3212-2)

Ubuntu 14.04 LTS / 16.04 LTS / 16.10 : tiff vulnerabilities (USN-3212-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : apport vulnerabilities (USN-3480-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : awstats vulnerability (USN-3518-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : curl vulnerabilities (USN-3498-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : curl vulnerability (USN-3457-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : firefox regression (USN-3477-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : firefox regression (USN-3477-4)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : firefox regressions (USN-3477-3)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : firefox vulnerabilities (USN-3477-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : firefox vulnerabilities (USN-3516-1) (Meltdown) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : icu vulnerability (USN-3458-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : intel-microcode update (USN-3531-1) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : irssi vulnerabilities (USN-3465-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : irssi vulnerabilities (USN-3527-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : ldns vulnerabilities (USN-3491-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : libraw vulnerabilities (USN-3492-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : libxcursor vulnerability (USN-3501-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : libxfont, libxfont1, libxfont2 vulnerability (USN-3500-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : libxml-libxml-perl vulnerability (USN-3494-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : libxml2 vulnerability (USN-3504-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : libxml2 vulnerability (USN-3513-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : linux-firmware vulnerabilities (USN-3505-1) (KRACK)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3459-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : nvidia-graphics-drivers-384 vulnerability (USN-3521-1) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : openssl vulnerabilities (USN-3475-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : optipng vulnerability (USN-3495-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : poppler vulnerabilities (USN-3517-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : poppler vulnerability (USN-3467-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : postgresql-9.3, postgresql-9.5, postgresql-9.6 vulnerabilities (USN-3479-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : postgresql-common vulnerabilities (USN-3476-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : procmail vulnerability (USN-3483-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : quagga vulnerabilities (USN-3471-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : rsync vulnerabilities (USN-3506-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : ruby1.9.1, ruby2.0, ruby2.3 vulnerability (USN-3515-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : samba vulnerabilities (USN-3486-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : thunderbird vulnerabilities (USN-3490-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 / 17.10 : wget vulnerabilities (USN-3464-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : apache2 vulnerability (USN-3370-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : apache2 vulnerability (USN-3425-1) (Optionsbleed)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : augeas vulnerability (USN-3400-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : bind9 regression (USN-3346-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : bluez vulnerability (USN-3413-1) (BlueBorne)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : bzr vulnerability (USN-3411-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : c-ares vulnerability (USN-3395-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : ca-certificates update (USN-3432-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : clamav vulnerabilities (USN-3393-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : curl vulnerabilities (USN-3441-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : cvs vulnerability (USN-3399-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : db5.3 vulnerability (USN-3489-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : dnsmasq vulnerabilities (USN-3430-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : evince vulnerability (USN-3503-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : firefox regression (USN-3391-3)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : firefox regression (USN-3435-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : firefox vulnerabilities (USN-3391-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : firefox vulnerabilities (USN-3435-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : freeradius vulnerabilities (USN-3369-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : freerdp vulnerabilities (USN-3380-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : gdb vulnerabilities (USN-3367-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : gdk-pixbuf vulnerabilities (USN-3418-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : ghostscript vulnerabilities (USN-3403-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : git vulnerability (USN-3387-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : git vulnerability (USN-3438-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : graphite2 vulnerabilities (USN-3398-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : imagemagick vulnerabilities (USN-3363-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libgd2 vulnerability (USN-3389-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libgd2 vulnerability (USN-3410-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libiberty vulnerabilities (USN-3368-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libidn vulnerability (USN-3434-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : liblouis vulnerabilities (USN-3408-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libplist vulnerability (USN-3429-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libsoup2.4 vulnerability (USN-3383-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libxfont, libxfont1, libxfont2 vulnerabilities (USN-3442-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : libxml2 vulnerabilities (USN-3424-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3357-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : nss vulnerability (USN-3431-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : nvidia-graphics-drivers-384 vulnerabilities (USN-3461-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : perl vulnerabilities (USN-3478-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : php5, php7.0 vulnerabilities (USN-3382-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : poppler vulnerabilities (USN-3433-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : poppler vulnerabilities (USN-3440-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : postgresql-9.3, postgresql-9.5, postgresql-9.6 vulnerabilities (USN-3390-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : python2.7 vulnerability (USN-3496-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : python3.4, python3.5 vulnerability (USN-3496-3)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : qemu regression (USN-3414-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : qemu vulnerabilities (USN-3414-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : ruby1.9.1, ruby2.0, ruby2.3 vulnerabilities (USN-3365-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : samba vulnerabilities (USN-3426-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : shotwell vulnerability (USN-3379-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : spice vulnerability (USN-3355-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : strongswan vulnerability (USN-3397-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : subversion vulnerabilities (USN-3388-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : tcpdump vulnerabilities (USN-3415-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : thunderbird vulnerabilities (USN-3416-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : thunderbird vulnerabilities (USN-3436-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : tomcat7, tomcat8 vulnerabilities (USN-3519-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : ubufox update (USN-3391-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : wpa vulnerabilities (USN-3455-1) (KRACK)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : xorg-server, xorg-server-hwe-16.04, xorg-server-lts-xenial vulnerabilities (USN-3362-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : xorg-server, xorg-server-hwe-16.04, xorg-server-lts-xenial vulnerabilities (USN-3453-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.04 : xorg-server, xorg-server-hwe-16.04, xorg-server-lts-xenial vulnerabilities (USN-3456-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : amd64-microcode update (USN-3690-1) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : cups vulnerabilities (USN-3713-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : curl vulnerabilities (USN-3648-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : exiv2 vulnerabilities (USN-3700-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : file vulnerabilities (USN-3686-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : firefox regression (USN-3645-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : firefox regressions (USN-3705-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : firefox vulnerabilities (USN-3645-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : firefox vulnerabilities (USN-3705-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : firefox vulnerability (USN-3682-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : git vulnerabilities (USN-3671-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : gnupg, gnupg2 vulnerabilities (USN-3675-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : imagemagick vulnerabilities (USN-3681-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : imagemagick vulnerabilities (USN-3711-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : libarchive-zip-perl vulnerability (USN-3703-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : libgcrypt11, libgcrypt20 vulnerability (USN-3689-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : libjpeg-turbo vulnerabilities (USN-3706-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : liblouis vulnerabilities (USN-3669-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : libpng, libpng1.6 vulnerabilities (USN-3712-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : libsoup2.4 vulnerability (USN-3701-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : libvirt vulnerability and update (USN-3680-1) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : ntp vulnerabilities (USN-3707-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : openssl, openssl1.0 vulnerabilities (USN-3692-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : perl vulnerability (USN-3684-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : php5, php7.0, php7.1, php7.2 vulnerabilities (USN-3646-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : policykit-1 vulnerabilities (USN-3717-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : poppler vulnerabilities (USN-3647-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : procps vulnerabilities (USN-3658-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : qemu update (USN-3679-1) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : qemu vulnerabilities (USN-3649-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : spice, spice-protocol vulnerability (USN-3659-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : thunderbird vulnerabilities (USN-3660-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : thunderbird vulnerabilities (USN-3714-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : tomcat7, tomcat8 vulnerabilities (USN-3665-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : unbound vulnerability (USN-3673-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : wget vulnerability (USN-3643-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : xdg-utils vulnerability (USN-3650-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 / 18.04 LTS : zziplib vulnerabilities (USN-3699-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : advancecomp vulnerability (USN-3570-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : apache2 vulnerabilities (USN-3627-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : bind9 vulnerability (USN-3535-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : clamav vulnerabilities (USN-3550-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : clamav vulnerabilities (USN-3592-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : curl vulnerabilities (USN-3554-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : curl vulnerabilities (USN-3598-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : dovecot vulnerabilities (USN-3587-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : dovecot vulnerability (USN-3556-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : eglibc, glibc vulnerabilities (USN-3534-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : erlang vulnerabilities (USN-3571-1) (ROBOT)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : exempi vulnerabilities (USN-3668-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : exim4 vulnerability (USN-3565-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : firefox regressions (USN-3544-2)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : firefox vulnerabilities (USN-3544-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : firefox vulnerabilities (USN-3596-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : firefox vulnerability (USN-3552-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : firefox vulnerability (USN-3599-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : firefox vulnerability (USN-3609-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : gdk-pixbuf vulnerabilities (USN-3532-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : icu vulnerability (USN-3610-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : intel-microcode regression (USN-3531-2) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : intel-microcode update (USN-3531-3) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : irssi vulnerabilities (USN-3590-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : isc-dhcp vulnerabilities (USN-3586-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libraw vulnerabilities (USN-3615-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libreoffice vulnerability (USN-3579-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libtasn1-6 vulnerabilities (USN-3547-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libvirt update (USN-3561-1) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libvirt vulnerabilities (USN-3576-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libvncserver vulnerability (USN-3618-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libvorbis vulnerabilities (USN-3569-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : libvorbis vulnerability (USN-3604-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : linux, linux-aws, linux-azure, linux-euclid, linux-gcp, linux-hwe, (USN-3641-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : mailman vulnerability (USN-3563-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : memcached vulnerabilities (USN-3588-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : memcached vulnerability (USN-3601-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : miniupnpc vulnerabilities (USN-3562-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3537-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3629-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : nvidia-graphics-drivers-384 vulnerabilities (USN-3662-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : openssh vulnerabilities (USN-3538-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : openssl vulnerability (USN-3611-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : openssl vulnerability (USN-3628-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : paramiko vulnerability (USN-3603-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : patch vulnerabilities (USN-3624-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : perl vulnerabilities (USN-3625-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : php5, php7.0, php7.1 vulnerabilities (USN-3600-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : postgresql-9.3, postgresql-9.5, postgresql-9.6 vulnerability (USN-3564-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : postgresql-9.3, postgresql-9.5, postgresql-9.6 vulnerability (USN-3589-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : python-crypto vulnerability (USN-3616-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : python-django vulnerabilities (USN-3591-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : qemu update (USN-3560-1) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : qemu vulnerabilities (USN-3575-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : qpdf vulnerabilities (USN-3638-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : quagga vulnerabilities (USN-3573-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : rsync vulnerabilities (USN-3543-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : ruby1.9.1, ruby2.0, ruby2.3 vulnerabilities (USN-3621-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : ruby1.9.1, ruby2.0, ruby2.3 vulnerabilities (USN-3685-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : ruby1.9.1, ruby2.3 vulnerabilities (USN-3528-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : samba vulnerabilities (USN-3595-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : screen-resolution-extra vulnerability (USN-3607-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : sensible-utils vulnerability (USN-3584-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : sharutils vulnerability (USN-3605-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : squid3 vulnerabilities (USN-3557-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : thunderbird vulnerabilities (USN-3529-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : thunderbird vulnerabilities (USN-3545-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : tiff vulnerabilities (USN-3606-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : transmission vulnerability (USN-3533-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : ubuntu-release-upgrader vulnerability (USN-3623-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : w3m vulnerabilities (USN-3555-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : wavpack vulnerabilities (USN-3568-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : wayland vulnerability (USN-3622-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : zsh vulnerabilities (USN-3593-1)

Ubuntu 14.04 LTS / 16.04 LTS / 17.10 : zsh vulnerabilities (USN-3608-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : advancecomp vulnerability (USN-3936-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : apache2 vulnerabilities (USN-3937-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : apt vulnerability (USN-3863-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : bind9 vulnerabilities (USN-3893-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : busybox vulnerabilities (USN-3935-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : clamav vulnerabilities (USN-3940-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : cups vulnerability (USN-3842-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : curl vulnerabilities (USN-3805-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : curl vulnerabilities (USN-3882-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : dovecot vulnerability (USN-3881-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : dovecot vulnerability (USN-3928-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : firefox regression (USN-3918-3)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : firefox regressions (USN-3801-2)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : firefox regressions (USN-3918-4)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : firefox vulnerabilities (USN-3801-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : firefox vulnerabilities (USN-3844-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : firefox vulnerabilities (USN-3874-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : gettext vulnerability (USN-3815-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ghostscript regression (USN-3831-2)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ghostscript regression (USN-3866-2)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ghostscript regression (USN-3866-3)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ghostscript vulnerabilities (USN-3803-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ghostscript vulnerabilities (USN-3831-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ghostscript vulnerabilities (USN-3915-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ghostscript vulnerability (USN-3866-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : git vulnerabilities (USN-3829-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : irssi vulnerability (USN-3862-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : ldb vulnerability (USN-3895-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libapache2-mod-perl2 vulnerability (USN-3825-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libarchive vulnerabilities (USN-3859-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libarchive vulnerabilities (USN-3884-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libcaca vulnerabilities (USN-3860-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libgd2 vulnerabilities (USN-3900-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libssh regression (USN-3795-3)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libvncserver vulnerabilities (USN-3877-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : libxslt vulnerability (USN-3947-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : mysql-5.5, mysql-5.7 vulnerabilities (USN-3799-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : nginx vulnerabilities (USN-3812-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : nss vulnerabilities (USN-3850-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : nss vulnerability (USN-3898-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : openssh vulnerabilities (USN-3885-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : openssh vulnerability (USN-3885-2)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : openssl, openssl1.0 vulnerabilities (USN-3840-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : perl vulnerabilities (USN-3834-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : policykit-1 vulnerability (USN-3861-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : policykit-1 vulnerability (USN-3934-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : poppler regression (USN-3837-2)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : poppler vulnerabilities (USN-3837-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : python-django vulnerability (USN-3851-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : qemu vulnerabilities (USN-3826-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : qemu vulnerabilities (USN-3923-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : rssh vulnerabilities (USN-3946-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : samba vulnerabilities (USN-3827-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : samba vulnerability (USN-3939-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : snapd vulnerability (USN-3887-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : snapd vulnerability (USN-3917-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : spice vulnerability (USN-3870-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : systemd vulnerability (USN-3938-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : thunderbird vulnerabilities (USN-3868-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : thunderbird vulnerabilities (USN-3897-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : thunderbird vulnerabilities (USN-3927-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : tiff vulnerabilities (USN-3864-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : tiff vulnerabilities (USN-3906-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : walinuxagent vulnerability (USN-3907-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : wget vulnerabilities (USN-3943-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : wpa vulnerabilities (USN-3944-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 18.10 : XMLTooling vulnerability (USN-3921-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : AppArmor update (USN-3784-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : bind9 vulnerability (USN-3769-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : clamav regression (USN-3722-3)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : clamav regression (USN-3722-5)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : clamav vulnerabilities (USN-3722-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : clamav vulnerability (USN-3789-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : firefox regressions (USN-3761-2)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : firefox regressions (USN-3761-3)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : firefox vulnerabilities (USN-3761-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : firefox vulnerabilities (USN-3778-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ghostscript vulnerabilities (USN-3768-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ghostscript vulnerabilities (USN-3773-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : git vulnerability (USN-3791-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : imagemagick vulnerabilities (USN-3785-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : intel-microcode vulnerabilities (USN-3756-1) (Foreshadow) (Spectre)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : lcms2 vulnerabilities (USN-3770-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : lftp vulnerability (USN-3731-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libarchive vulnerabilities (USN-3736-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libgd2 vulnerabilities (USN-3755-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : liblouis vulnerabilities (USN-3782-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libraw vulnerabilities (USN-3838-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libssh vulnerability (USN-3795-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libtirpc vulnerabilities (USN-3759-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : libx11 vulnerabilities (USN-3758-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : linux-azure vulnerabilities (USN-3871-5)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : lxml vulnerability (USN-3841-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : moin vulnerability (USN-3794-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : mutt vulnerabilities (USN-3719-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : mysql-5.5, mysql-5.7 vulnerabilities (USN-3725-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : net-snmp vulnerability (USN-3792-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : openssh vulnerabilities (USN-3809-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : paramiko vulnerability (USN-3796-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : php5, php7.0, php7.2 vulnerabilities (USN-3766-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : poppler vulnerability (USN-3757-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : postgresql-10, postgresql-9.3, postgresql-9.5 vulnerabilities (USN-3744-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : ppp vulnerability (USN-3810-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : python2.7, python3.4, python3.5 vulnerabilities (USN-3817-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : requests vulnerability (USN-3790-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : samba vulnerabilities (USN-3738-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : spamassassin vulnerabilities (USN-3811-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : spice, spice-protocol vulnerability (USN-3751-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : strongswan vulnerabilities (USN-3771-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : strongswan vulnerability (USN-3774-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : texlive-bin vulnerabilities (USN-3788-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : thunderbird vulnerabilities (USN-3793-1)

Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : zsh vulnerabilities (USN-3764-1)

Ubuntu 14.04 LTS / 16.04 LTS : cups vulnerability (USN-3577-1)

Ubuntu 14.04 LTS / 16.04 LTS : elfutils vulnerabilities (USN-3670-1)

Ubuntu 14.04 LTS / 16.04 LTS : emacs24 vulnerability (USN-3427-1)

Ubuntu 14.04 LTS / 16.04 LTS : evolution-data-server vulnerability (USN-3724-1)

Ubuntu 14.04 LTS / 16.04 LTS : file-roller vulnerability (USN-3074-1)

Ubuntu 14.04 LTS / 16.04 LTS : firefox regression (USN-3596-2)

Ubuntu 14.04 LTS / 16.04 LTS : freeimage vulnerability (USN-3925-1)

Ubuntu 14.04 LTS / 16.04 LTS : gnome-keyring vulnerability (USN-3894-1)

Ubuntu 14.04 LTS / 16.04 LTS : gnupg vulnerability (USN-3733-1)

Ubuntu 14.04 LTS / 16.04 LTS : gnupg2 vulnerability (USN-3675-2)

Ubuntu 14.04 LTS / 16.04 LTS : harfbuzz vulnerabilities (USN-3067-1)

Ubuntu 14.04 LTS / 16.04 LTS : imagemagick regression (USN-3363-2)

Ubuntu 14.04 LTS / 16.04 LTS : jasper vulnerabilities (USN-3295-1)

Ubuntu 14.04 LTS / 16.04 LTS : jasper vulnerabilities (USN-3693-1)

Ubuntu 14.04 LTS / 16.04 LTS : libgd2 vulnerabilities (USN-3060-1)

Ubuntu 14.04 LTS / 16.04 LTS : libreoffice vulnerabilities (USN-3883-1)

Ubuntu 14.04 LTS / 16.04 LTS : libxcursor vulnerability (USN-3729-1)

Ubuntu 14.04 LTS / 16.04 LTS : libxkbcommon vulnerabilities (USN-3786-1)

Ubuntu 14.04 LTS / 16.04 LTS : linux-hwe, linux-aws-hwe, linux-azure, linux-gcp, linux-oracle (USN-3931-2)

Ubuntu 14.04 LTS / 16.04 LTS : linux-hwe, linux-aws-hwe, linux-azure, linux-gcp, linux-oracle vulnerabilities (USN-3901-2)

Ubuntu 14.04 LTS / 16.04 LTS : openslp-dfsg vulnerabilities (USN-3708-1)

Ubuntu 14.04 LTS / 16.04 LTS : oxide-qt vulnerabilities (USN-3041-1)

Ubuntu 14.04 LTS / 16.04 LTS : oxide-qt vulnerabilities (USN-3058-1)

Ubuntu 14.04 LTS / 16.04 LTS : oxide-qt vulnerabilities (USN-3091-1)

Ubuntu 14.04 LTS / 16.04 LTS : pacemaker vulnerabilities (USN-3462-1)

Ubuntu 14.04 LTS / 16.04 LTS : php5, php7.0 vulnerabilities (USN-3902-1)

Ubuntu 14.04 LTS / 16.04 LTS : python-werkzeug vulnerability (USN-3463-1)

Ubuntu 14.04 LTS / 16.04 LTS : qemu regression (USN-3575-2)

Ubuntu 14.04 LTS / 16.04 LTS : rabbitmq-server vulnerability (USN-3374-1)

Ubuntu 14.04 LTS / 16.04 LTS : rtmpdump vulnerabilities (USN-3283-1)

Ubuntu 14.04 LTS / 16.04 LTS : samba vulnerability (USN-3092-1)

Ubuntu 14.04 LTS / 16.04 LTS : systemd vulnerabilities (USN-3558-1)

Ubuntu 14.04 LTS / 16.04 LTS : texlive-base vulnerability (USN-3401-1)

Ubuntu 14.04 LTS / 16.04 LTS : tiff vulnerabilities (USN-3602-1)

Ubuntu 14.04 LTS / 16.04 LTS : tomcat7, tomcat8 vulnerabilities (USN-3723-1)

Ubuntu 14.04 LTS / 16.04 LTS : tomcat7, tomcat8 vulnerability (USN-3787-1)

Ubuntu 14.04 LTS / 16.04 LTS : transfig vulnerability (USN-3760-1)

Ubuntu 14.04 LTS / 16.04 LTS : twisted vulnerability (USN-3585-1)

Ubuntu 14.04 LTS : amd64-microcode regression (USN-3690-2) (Spectre)

Ubuntu 14.04 LTS : ant vulnerability (USN-3721-1)

Ubuntu 14.04 LTS : apparmor vulnerability (USN-2413-1)

Ubuntu 14.04 LTS : apport vulnerability (USN-3664-2)

Ubuntu 14.04 LTS : audiofile vulnerabilities (USN-3800-1)

Ubuntu 14.04 LTS : bash vulnerability (USN-2363-2)

Ubuntu 14.04 LTS : batik vulnerability (USN-3280-1)

Ubuntu 14.04 LTS : batik vulnerability (USN-3661-1)

Ubuntu 14.04 LTS : bind9 vulnerability (USN-3956-2)

Ubuntu 14.04 LTS : bouncycastle vulnerabilities (USN-3727-1)

Ubuntu 14.04 LTS : ceilometer vulnerability (USN-2311-2)

Ubuntu 14.04 LTS : ceph vulnerabilities (USN-3452-1)

Ubuntu 14.04 LTS : cinder vulnerabilities (USN-2405-1)

Ubuntu 14.04 LTS : clamav vulnerabilities (USN-3728-2)

Ubuntu 14.04 LTS : clamav vulnerabilities (USN-3814-2)

Ubuntu 14.04 LTS : cups update (USN-2839-1)

Ubuntu 14.04 LTS : cups-filters vulnerability (USN-2210-1)

Ubuntu 14.04 LTS : db5.3 vulnerability (USN-4004-2)

Ubuntu 14.04 LTS : firebird2.5 vulnerabilities (USN-3929-1)

Ubuntu 14.04 LTS : firefox vulnerabilities (USN-3918-2)

Ubuntu 14.04 LTS : fontforge vulnerabilities (USN-3409-1)

Ubuntu 14.04 LTS : fop vulnerability (USN-3281-1)

Ubuntu 14.04 LTS : freerdp, freerdp2 vulnerabilities (USN-3845-1)

Ubuntu 14.04 LTS : gimp vulnerabilities (USN-3539-1)

Ubuntu 14.04 LTS : git vulnerability (USN-3243-1)

Ubuntu 14.04 LTS : glance vulnerabilities (USN-3446-1)

Ubuntu 14.04 LTS : glance vulnerability (USN-2322-1)

Ubuntu 14.04 LTS : glib2.0 vulnerability (USN-4014-2)

Ubuntu 14.04 LTS : GNU Screen vulnerability (USN-3996-1)

Ubuntu 14.04 LTS : gtk+3.0 update (USN-2475-1)

Ubuntu 14.04 LTS : heat vulnerability (USN-2249-1)

Ubuntu 14.04 LTS : horizon vulnerabilities (USN-2323-1)

Ubuntu 14.04 LTS : horizon vulnerability (USN-3447-1)

Ubuntu 14.04 LTS : jinja2 vulnerabilities (USN-4011-2)

Ubuntu 14.04 LTS : kde4libs vulnerability (USN-3286-1)

Ubuntu 14.04 LTS : keepalived vulnerability (USN-3995-2)

Ubuntu 14.04 LTS : keystone vulnerabilities (USN-2324-1)

Ubuntu 14.04 LTS : keystone vulnerability (USN-2406-1)

Ubuntu 14.04 LTS : lcms2 vulnerability (USN-2961-1)

Ubuntu 14.04 LTS : libffi vulnerability (USN-3454-1) (Stack Clash)

Ubuntu 14.04 LTS : liblouis vulnerability (USN-3474-1)

Ubuntu 14.04 LTS : liblwp-protocol-https-perl vulnerability (USN-2292-1)

Ubuntu 14.04 LTS : librelp vulnerability (USN-3612-1)

Ubuntu 14.04 LTS : libreoffice vulnerabilities (USN-3472-1)

Ubuntu 14.04 LTS : libreoffice vulnerability (USN-2253-1)

Ubuntu 14.04 LTS : libreoffice vulnerability (USN-2331-1)

Ubuntu 14.04 LTS : libseccomp vulnerability (USN-4001-2)

Ubuntu 14.04 LTS : libvirt update (USN-3985-2) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 14.04 LTS : libytnef vulnerabilities (USN-3288-1)

Ubuntu 14.04 LTS : libytnef vulnerabilities (USN-3667-1)

Ubuntu 14.04 LTS : linux regression (USN-2643-2)

Ubuntu 14.04 LTS : linux regressions (USN-3741-3) (Foreshadow)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2226-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2240-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2290-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2318-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2337-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2359-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2379-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2395-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2420-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2446-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2466-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2516-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2516-3)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2544-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2563-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2588-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2614-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2634-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2663-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2681-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2688-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2700-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2748-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2776-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2794-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2823-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2841-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2848-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2887-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2907-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2929-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2946-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2968-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-2989-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3018-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3052-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3071-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3083-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3098-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3127-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3145-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3160-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3168-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3207-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3343-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3360-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3381-1) (Stack Clash)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3386-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3406-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3422-1) (BlueBorne)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3445-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3470-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3510-1) (Dirty COW)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3542-1) (Spectre)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3583-1) (Meltdown)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3620-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3655-1) (Spectre)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3674-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3698-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3742-1) (Foreshadow)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3754-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3775-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3798-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3822-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3849-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3880-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3933-1)

Ubuntu 14.04 LTS : linux vulnerabilities (USN-3983-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 14.04 LTS : linux vulnerability (USN-2204-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2274-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2314-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2516-2)

Ubuntu 14.04 LTS : linux vulnerability (USN-2528-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2598-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2598-2)

Ubuntu 14.04 LTS : linux vulnerability (USN-2620-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2643-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2716-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2734-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2761-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2801-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2870-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2975-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-2999-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3034-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3105-1) (Dirty COW)

Ubuntu 14.04 LTS : linux vulnerability (USN-3149-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3188-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3219-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3250-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3264-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3290-1)

Ubuntu 14.04 LTS : linux vulnerability (USN-3524-1) (Meltdown)

Ubuntu 14.04 LTS : linux vulnerability (USN-3594-1) (Spectre)

Ubuntu 14.04 LTS : linux vulnerability (USN-3908-1)

Ubuntu 14.04 LTS : linux, linux-meta vulnerabilities (USN-3335-1) (Stack Clash)

Ubuntu 14.04 LTS : linux-aws vulnerabilities (USN-3485-3)

Ubuntu 14.04 LTS : linux-azure vulnerabilities (USN-3820-3)

Ubuntu 14.04 LTS : linux-azure vulnerabilities (USN-3847-3)

Ubuntu 14.04 LTS : linux-lts-utopic regression (USN-2447-2)

Ubuntu 14.04 LTS : linux-lts-utopic regression (USN-2644-2)

Ubuntu 14.04 LTS : linux-lts-utopic regression (USN-2909-2)

Ubuntu 14.04 LTS : linux-lts-utopic regression (USN-2948-2)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2447-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2467-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2517-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2545-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2564-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2589-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2615-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2635-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2664-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2682-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2689-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2777-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2797-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2844-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2849-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2888-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2909-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2931-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2948-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-2969-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-3000-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerabilities (USN-3019-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2529-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2599-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2599-2)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2644-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2717-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2750-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2764-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2805-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2824-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2873-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-2976-1)

Ubuntu 14.04 LTS : linux-lts-utopic vulnerability (USN-3036-1)

Ubuntu 14.04 LTS : linux-lts-vivid regression (USN-2910-2)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2636-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2665-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2683-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2690-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2751-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2778-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2798-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2829-2)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2842-2)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2854-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2889-2)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2910-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2932-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2949-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-2970-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-3001-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-3020-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerabilities (USN-3053-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2645-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2718-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2737-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2765-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2806-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2857-2)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2871-2)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-2977-1)

Ubuntu 14.04 LTS : linux-lts-vivid vulnerability (USN-3037-1)

Ubuntu 14.04 LTS : linux-lts-wily regression (USN-2908-5)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2843-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2853-1)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2890-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2908-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2930-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2947-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2971-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-2978-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-3002-1)

Ubuntu 14.04 LTS : linux-lts-wily vulnerabilities (USN-3017-3)

Ubuntu 14.04 LTS : linux-lts-wily vulnerability (USN-2807-1)

Ubuntu 14.04 LTS : linux-lts-wily vulnerability (USN-2858-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerability (USN-2872-2)

Ubuntu 14.04 LTS : linux-lts-wily vulnerability (USN-3035-3)

Ubuntu 14.04 LTS : linux-lts-xenial regression (USN-3392-2) (Stack Clash)

Ubuntu 14.04 LTS : linux-lts-xenial regression (USN-3522-4) (Meltdown)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-2965-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-2979-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3005-1)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3016-4)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3054-1)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3070-4)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3084-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3099-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3146-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3161-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3169-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3189-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3208-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3234-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3265-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3291-3)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3312-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3344-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3364-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3378-2) (Stack Clash)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3385-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3405-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3420-2) (BlueBorne)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3444-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3469-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3485-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerabilities (USN-3982-2) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerability (USN-3106-2) (Dirty COW)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerability (USN-3128-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerability (USN-3151-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerability (USN-3220-2)

Ubuntu 14.04 LTS : linux-lts-xenial vulnerability (USN-3249-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws regression (USN-3509-4) (Dirty COW)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3509-2) (Dirty COW)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3540-2) (Meltdown) (Spectre)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3582-2) (Spectre)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3619-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3631-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3654-2) (Spectre)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3676-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3696-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3741-2) (Foreshadow)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3753-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3776-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3797-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3821-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3848-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3879-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3910-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-3932-2)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerabilities (USN-4008-3)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-aws vulnerability (USN-3522-2) (Meltdown)

Ubuntu 14.04 LTS : linux-lts-xenial, linux-meta-lts-xenial vulnerabilities (USN-3334-1) (Stack Clash)

Ubuntu 14.04 LTS : lxc regression (USN-2753-2)

Ubuntu 14.04 LTS : lxc regression (USN-2753-3)

Ubuntu 14.04 LTS : lxc vulnerability (USN-3375-1)

Ubuntu 14.04 LTS : MariaDB vulnerabilities (USN-3957-2)

Ubuntu 14.04 LTS : munin regression (USN-3215-2)

Ubuntu 14.04 LTS : munin vulnerability (USN-3215-1)

Ubuntu 14.04 LTS : nasm vulnerabilities (USN-3694-1)

Ubuntu 14.04 LTS : neutron vulnerabilities (USN-2321-1)

Ubuntu 14.04 LTS : neutron vulnerability (USN-2408-1)

Ubuntu 14.04 LTS : nginx vulnerability (USN-2351-1)

Ubuntu 14.04 LTS : nova vulnerabilities (USN-2407-1)

Ubuntu 14.04 LTS : nova vulnerabilities (USN-3449-1)

Ubuntu 14.04 LTS : nova vulnerability (USN-2325-1)

Ubuntu 14.04 LTS : ocaml vulnerability (USN-3437-1)

Ubuntu 14.04 LTS : openjdk-7 regression (USN-2319-2)

Ubuntu 14.04 LTS : openjdk-7 regression (USN-3275-3)

Ubuntu 14.04 LTS : openjdk-7 update (USN-2319-3)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-2319-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-2388-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3062-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3130-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3275-2)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3396-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3497-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3614-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3691-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3824-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerability (USN-3735-1)

Ubuntu 14.04 LTS : openjdk-7 vulnerability (USN-3942-1)

Ubuntu 14.04 LTS : oxide-qt vulnerabilities (USN-2298-1)

Ubuntu 14.04 LTS : oxide-qt vulnerabilities (USN-2320-1)

Ubuntu 14.04 LTS : oxide-qt vulnerabilities (USN-2326-1)

Ubuntu 14.04 LTS : oxide-qt vulnerabilities (USN-2345-1)

Ubuntu 14.04 LTS : php5 vulnerabilities (USN-3566-1)

Ubuntu 14.04 LTS : php5 vulnerabilities (USN-3566-2)

Ubuntu 14.04 LTS : php5 vulnerabilities (USN-3922-2)

Ubuntu 14.04 LTS : Pillow regression (USN-3090-2)

Ubuntu 14.04 LTS : Pillow vulnerabilities (USN-3090-1)

Ubuntu 14.04 LTS : pixman vulnerability (USN-3843-1)

Ubuntu 14.04 LTS : pollinate update (USN-2387-1)

Ubuntu 14.04 LTS : puppet vulnerabilities (USN-3308-1)

Ubuntu 14.04 LTS : puppet vulnerability (USN-3567-1)

Ubuntu 14.04 LTS : python-pycadf vulnerability (USN-2311-1)

Ubuntu 14.04 LTS : requests vulnerabilities (USN-2382-1)

Ubuntu 14.04 LTS : rsync vulnerability (USN-2171-1)

Ubuntu 14.04 LTS : ruby1.9.1 vulnerabilities (USN-3439-1)

Ubuntu 14.04 LTS : ruby1.9.1, ruby2.0 regression (USN-3621-2)

Ubuntu 14.04 LTS : samba vulnerability (USN-2305-1)

Ubuntu 14.04 LTS : samba vulnerability (USN-3976-2)

Ubuntu 14.04 LTS : samba vulnerability (USN-3976-4)

Ubuntu 14.04 LTS : sudo vulnerability (USN-3968-2)

Ubuntu 14.04 LTS : swift vulnerabilities (USN-3451-1)

Ubuntu 14.04 LTS : swift vulnerability (USN-2256-1)

Ubuntu 14.04 LTS : unity vulnerabilities (USN-2184-1)

Ubuntu 14.04 LTS : unity vulnerabilities (USN-2184-2)

Ubuntu 14.04 LTS : unity vulnerability (USN-2303-1)

Ubuntu 14.04 LTS : wpa vulnerability (USN-3969-2)

Ubuntu 14.10 / 15.04 : haproxy vulnerability (USN-2668-1)

Ubuntu 14.10 : autofs vulnerability (USN-2579-1)

Ubuntu 14.10 : exiv2 vulnerability (USN-2454-1)

Ubuntu 14.10 : gnutls28 vulnerability (USN-2403-1)

Ubuntu 14.10 : linux regression (USN-2448-2)

Ubuntu 14.10 : linux regression (USN-2600-2)

Ubuntu 14.10 : linux regression (USN-2646-2)

Ubuntu 14.10 : linux vulnerabilities (USN-2396-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2421-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2448-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2468-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2518-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2546-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2565-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2590-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2616-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2637-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2666-1)

Ubuntu 14.10 : linux vulnerabilities (USN-2685-1)

Ubuntu 14.10 : linux vulnerability (USN-2530-1)

Ubuntu 14.10 : linux vulnerability (USN-2600-1)

Ubuntu 14.10 : linux vulnerability (USN-2646-1)

Ubuntu 14.10 : mountall vulnerability (USN-2411-1)

Ubuntu 14.10 : openjdk-7 vulnerabilities (USN-2388-2)

Ubuntu 14.10 : systemd-shim vulnerability (USN-2392-1)

Ubuntu 15.04 / 15.10 : lxcfs vulnerabilities (USN-2813-1)

Ubuntu 15.04 / 15.10 : perl vulnerability (USN-2878-1)

Ubuntu 15.04 : cinder vulnerability (USN-2703-1)

Ubuntu 15.04 : cups-filters vulnerability (USN-2725-1)

Ubuntu 15.04 : cyrus-sasl2 vulnerability (USN-2755-1)

Ubuntu 15.04 : gnutls28 vulnerabilities (USN-2727-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2638-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2667-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2684-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2691-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2752-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2779-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2799-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2829-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2842-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2850-1)

Ubuntu 15.04 : linux vulnerabilities (USN-2889-1)

Ubuntu 15.04 : linux vulnerability (USN-2601-1)

Ubuntu 15.04 : linux vulnerability (USN-2647-1)

Ubuntu 15.04 : linux vulnerability (USN-2719-1)

Ubuntu 15.04 : linux vulnerability (USN-2738-1)

Ubuntu 15.04 : linux vulnerability (USN-2762-1)

Ubuntu 15.04 : linux vulnerability (USN-2802-1)

Ubuntu 15.04 : linux vulnerability (USN-2857-1)

Ubuntu 15.04 : linux vulnerability (USN-2871-1)

Ubuntu 15.04 : ntfs-3g vulnerability (USN-2617-2)

Ubuntu 15.04 : ntfs-3g vulnerability (USN-2617-3)

Ubuntu 15.04 : usb-creator vulnerability (USN-2576-2)

Ubuntu 15.10 / 16.04 LTS : dnsmasq vulnerability (USN-3009-1)

Ubuntu 15.10 / 16.04 LTS : ecryptfs-utils vulnerability (USN-3032-1)

Ubuntu 15.10 / 16.04 LTS : libndp vulnerability (USN-2980-1)

Ubuntu 15.10 / 16.04 LTS : libusbmuxd vulnerability (USN-3026-2)

Ubuntu 15.10 / 16.04 LTS : lxd vulnerabilities (USN-2988-1)

Ubuntu 15.10 : linux regression (USN-2908-4)

Ubuntu 15.10 : linux vulnerabilities (USN-2843-1)

Ubuntu 15.10 : linux vulnerabilities (USN-2851-1)

Ubuntu 15.10 : linux vulnerabilities (USN-2890-1)

Ubuntu 15.10 : linux vulnerabilities (USN-2908-1)

Ubuntu 15.10 : linux vulnerabilities (USN-2930-1)

Ubuntu 15.10 : linux vulnerabilities (USN-2947-1)

Ubuntu 15.10 : linux vulnerabilities (USN-2971-1)

Ubuntu 15.10 : linux vulnerabilities (USN-2978-1)

Ubuntu 15.10 : linux vulnerabilities (USN-3003-1)

Ubuntu 15.10 : linux vulnerabilities (USN-3017-1)

Ubuntu 15.10 : linux vulnerability (USN-2803-1)

Ubuntu 15.10 : linux vulnerability (USN-2858-1)

Ubuntu 15.10 : linux vulnerability (USN-2872-1)

Ubuntu 15.10 : linux vulnerability (USN-3035-1)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-2843-3)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-2890-3)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-2908-3)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-2930-3)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-2947-3)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-2971-3)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-3004-1)

Ubuntu 15.10 : linux-raspi2 vulnerabilities (USN-3017-2)

Ubuntu 15.10 : linux-raspi2 vulnerability (USN-2852-1)

Ubuntu 15.10 : linux-raspi2 vulnerability (USN-2858-3)

Ubuntu 15.10 : linux-raspi2 vulnerability (USN-2872-3)

Ubuntu 15.10 : linux-raspi2 vulnerability (USN-2978-3)

Ubuntu 15.10 : linux-raspi2 vulnerability (USN-3035-2)

Ubuntu 15.10 : lxd vulnerability (USN-2809-1)

Ubuntu 15.10 : miniupnpc vulnerability (USN-2780-2)

Ubuntu 15.10 : openssl vulnerability (USN-2883-1)

Ubuntu 15.10 : oxide-qt vulnerabilities (USN-2770-2)

Ubuntu 15.10 : php5 regression (USN-2952-2)

Ubuntu 16.04 LTS / 16.10 / 17.04 : lintian vulnerability (USN-3310-1)

Ubuntu 16.04 LTS / 16.10 / 17.04 : openjdk-8 vulnerabilities (USN-3275-1)

Ubuntu 16.04 LTS / 16.10 / 17.04 : webkit2gtk vulnerabilities (USN-3303-1)

Ubuntu 16.04 LTS / 16.10 : dovecot regression (USN-3258-2)

Ubuntu 16.04 LTS / 16.10 : dovecot vulnerability (USN-3258-1)

Ubuntu 16.04 LTS / 16.10 : iucode-tool vulnerability (USN-3186-1)

Ubuntu 16.04 LTS / 16.10 : lightdm vulnerability (USN-3255-1)

Ubuntu 16.04 LTS / 16.10 : ntfs-3g vulnerability (USN-3182-1)

Ubuntu 16.04 LTS / 16.10 : openjdk-8 vulnerabilities (USN-3121-1)

Ubuntu 16.04 LTS / 16.10 : openjdk-8 vulnerabilities (USN-3179-1)

Ubuntu 16.04 LTS / 16.10 : php7.0 regression (USN-3211-2)

Ubuntu 16.04 LTS / 16.10 : php7.0 vulnerabilities (USN-3211-1)

Ubuntu 16.04 LTS / 16.10 : python-cryptography vulnerability (USN-3138-1)

Ubuntu 16.04 LTS / 16.10 : webkit2gtk vulnerabilities (USN-3191-1)

Ubuntu 16.04 LTS / 16.10 : webkit2gtk vulnerabilities (USN-3200-1)

Ubuntu 16.04 LTS / 16.10 : webkit2gtk vulnerabilities (USN-3257-1)

Ubuntu 16.04 LTS / 17.04 / 17.10 : apport regression (USN-3480-3)

Ubuntu 16.04 LTS / 17.04 / 17.10 : apport regressions (USN-3480-2)

Ubuntu 16.04 LTS / 17.04 / 17.10 : openjdk-8 vulnerabilities (USN-3473-1)

Ubuntu 16.04 LTS / 17.04 / 17.10 : openssl vulnerabilities (USN-3512-1)

Ubuntu 16.04 LTS / 17.04 / 17.10 : python-pysaml2 vulnerability (USN-3520-1)

Ubuntu 16.04 LTS / 17.04 / 17.10 : webkit2gtk vulnerabilities (USN-3481-1)

Ubuntu 16.04 LTS / 17.04 / 17.10 : webkit2gtk vulnerabilities (USN-3514-1)

Ubuntu 16.04 LTS / 17.04 / 17.10 : webkit2gtk vulnerabilities (USN-3530-1) (Spectre)

Ubuntu 16.04 LTS / 17.04 : libmspack vulnerabilities (USN-3394-1)

Ubuntu 16.04 LTS / 17.04 : openjdk-8 regression (USN-3366-2)

Ubuntu 16.04 LTS / 17.04 : openjdk-8 vulnerabilities (USN-3366-1)

Ubuntu 16.04 LTS / 17.04 : openvswitch vulnerabilities (USN-3450-1)

Ubuntu 16.04 LTS / 17.04 : pyjwt vulnerability (USN-3407-1)

Ubuntu 16.04 LTS / 17.04 : python-pysaml2 vulnerability (USN-3402-1)

Ubuntu 16.04 LTS / 17.04 : sssd vulnerability (USN-3526-1)

Ubuntu 16.04 LTS / 17.04 : webkit2gtk vulnerabilities (USN-3376-1)

Ubuntu 16.04 LTS / 17.04 : webkit2gtk vulnerabilities (USN-3460-1)

Ubuntu 16.04 LTS / 17.10 / 18.04 LTS : apport vulnerability (USN-3664-1)

Ubuntu 16.04 LTS / 17.10 / 18.04 LTS : libraw vulnerabilities (USN-3639-1)

Ubuntu 16.04 LTS / 17.10 / 18.04 LTS : webkit2gtk vulnerabilities (USN-3687-1)

Ubuntu 16.04 LTS / 17.10 / 18.04 LTS : webkit2gtk vulnerability (USN-3640-1)

Ubuntu 16.04 LTS / 17.10 : dns-root-data update (USN-3715-1)

Ubuntu 16.04 LTS / 17.10 : gcab vulnerability (USN-3546-1)

Ubuntu 16.04 LTS / 17.10 : openjdk-8 vulnerabilities (USN-3613-1)

Ubuntu 16.04 LTS / 17.10 : openjdk-8 vulnerabilities (USN-3644-1)

Ubuntu 16.04 LTS / 17.10 : ruby2.3 vulnerabilities (USN-3553-1)

Ubuntu 16.04 LTS / 17.10 : webkit2gtk vulnerabilities (USN-3551-1)

Ubuntu 16.04 LTS / 17.10 : webkit2gtk vulnerabilities (USN-3635-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : apport vulnerability (USN-4051-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : bind9 vulnerability (USN-3956-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : bzip2 regression (USN-4038-3)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : bzip2 vulnerabilities (USN-4038-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : curl vulnerabilities (USN-3993-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : dbus vulnerability (USN-4015-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : Docker vulnerabilities (USN-4048-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : exiv2 vulnerabilities (USN-4056-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : expat vulnerability (USN-4040-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : firefox regression (USN-3991-2)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : firefox regression (USN-3991-3)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : firefox vulnerabilities (USN-3991-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : firefox vulnerabilities (USN-4054-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : flightcrew vulnerabilities (USN-4055-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : ghostscript vulnerability (USN-3970-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : glib2.0 vulnerability (USN-4014-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : gnutls28 vulnerabilities (USN-3999-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : gvfs vulnerabilities (USN-4053-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : imagemagick vulnerabilities (USN-4034-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : intel-microcode update (USN-3977-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : intel-microcode update (USN-3977-2) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : intel-microcode update (USN-3977-3) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : irssi vulnerabilities (USN-4046-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : jinja2 vulnerabilities (USN-4011-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : libseccomp vulnerability (USN-4001-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : libvirt update (USN-3985-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : libvirt vulnerabilities (USN-4047-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-gke-4.15, linux-hwe, linux-kvm, linux-oem, linux-oracle, linux-raspi2, linux-snapdragon update (USN-4041-1) (SACK Slowness)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-hwe, (USN-4017-1) (SACK Panic) (SACK Slowness)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : mysql-5.7 vulnerabilities (USN-3957-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : openjdk-8, openjdk-lts vulnerabilities (USN-3975-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : pacemaker vulnerabilities (USN-3952-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : php7.0, php7.2 vulnerabilities (USN-3953-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : php7.0, php7.2 vulnerabilities (USN-4009-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : policykit-desktop-privileges update (USN-4037-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : poppler vulnerabilities (USN-4042-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : postgresql-10, postgresql-11, postgresql-9.5 vulnerabilities (USN-3972-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : python-django vulnerabilities (USN-4043-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : python-urllib3 vulnerabilities (USN-3990-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : qemu update (USN-3978-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : samba vulnerability (USN-3976-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : sqlite3 vulnerabilities (USN-4019-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : thunderbird vulnerabilities (USN-3997-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : thunderbird vulnerabilities (USN-4028-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : thunderbird vulnerabilities (USN-4045-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : thunderbird vulnerabilities (USN-4064-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : vim vulnerabilities (USN-4016-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : whoopsie vulnerability (USN-4052-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : wpa vulnerability (USN-3969-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : zeromq3 vulnerability (USN-4050-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : Zipios vulnerability (USN-4057-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : znc vulnerability (USN-4044-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : elfutils vulnerabilities (USN-4012-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : file vulnerabilities (USN-3911-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : firefox vulnerabilities (USN-3918-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : glib2.0 vulnerability (USN-4049-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : gpac vulnerabilities (USN-3926-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : gst-plugins-base0.10, gst-plugins-base1.0 vulnerability (USN-3958-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : haproxy vulnerabilities (USN-3858-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : keepalived vulnerability (USN-3995-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : libmspack vulnerabilities (USN-3814-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : libraw vulnerabilities (USN-3989-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : libsndfile vulnerabilities (USN-4013-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : libvirt vulnerability (USN-3909-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : lua5.3 vulnerability (USN-3941-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : mosquitto vulnerabilities (USN-4023-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : mysql-5.7 vulnerabilities (USN-3867-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : network-manager vulnerability (USN-3807-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : ntfs-3g update (USN-3914-2)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : openjdk-8, openjdk-lts vulnerabilities (USN-3804-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : openssl, openssl1.0 vulnerability (USN-3899-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : php-pear vulnerability (USN-3857-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : python-django vulnerability (USN-3890-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : qtbase-opensource-src vulnerabilities (USN-4003-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : systemd vulnerabilities (USN-3816-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : systemd vulnerabilities (USN-3855-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : systemd vulnerability (USN-3806-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : systemd vulnerability (USN-3816-2)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : systemd vulnerability (USN-3891-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : tcpflow vulnerabilities (USN-3955-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : Wireshark vulnerabilities (USN-3986-1)

Ubuntu 16.04 LTS / 18.04 LTS / 18.10 : xorg-server, xorg-server-hwe-16.04 vulnerability (USN-3802-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : apport regression (USN-4171-3)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : apport vulnerabilities (USN-4171-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : clamav vulnerability (USN-4230-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : cpio vulnerability (USN-4176-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : djvulibre vulnerabilities (USN-4198-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : e2fsprogs vulnerability (USN-4249-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : exiv2 vulnerability (USN-4159-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : file vulnerability (USN-4172-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : firefox regressions (USN-4165-2)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : firefox vulnerabilities (USN-4165-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : firefox vulnerabilities (USN-4234-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : ghostscript vulnerability (USN-4193-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : git vulnerabilities (USN-4220-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : haproxy vulnerability (USN-4174-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : imagemagick vulnerabilities (USN-4192-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : intel-microcode regression (USN-4182-3)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : intel-microcode update (USN-4182-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : libssh vulnerability (USN-4219-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : libxslt vulnerabilities (USN-4164-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : mysql-5.7, mysql-8.0 vulnerabilities (USN-4195-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : nginx vulnerability (USN-4235-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : nss vulnerability (USN-4203-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : nss vulnerability (USN-4231-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : openjdk-8, openjdk-lts vulnerabilities (USN-4223-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : php5, php7.0, php7.2, php7.3 vulnerabilities (USN-4239-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : php7.0, php7.2, php7.3 vulnerability (USN-4166-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : postgresql-common vulnerability (USN-4194-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : python-apt regression (USN-4247-2)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : python-apt vulnerabilities (USN-4247-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : python-django vulnerability (USN-4224-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : python-ecdsa vulnerabilities (USN-4196-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : python-psutil vulnerability (USN-4204-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : python-pysaml2 vulnerability (USN-4245-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : qemu vulnerabilities (USN-4191-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : ruby-nokogiri vulnerability (USN-4175-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : ruby2.3, ruby2.5 vulnerabilities (USN-4201-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : samba vulnerabilities (USN-4167-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : samba vulnerabilities (USN-4217-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : samba vulnerabilities (USN-4244-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : spamassassin vulnerabilities (USN-4237-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : sqlite3 vulnerabilities (USN-4205-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : squid, squid3 vulnerabilities (USN-4213-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : sysstat vulnerabilities (USN-4242-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : whoopsie regression (USN-4170-2)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : whoopsie regression (USN-4170-3)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 / 19.10 : whoopsie vulnerability (USN-4170-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : ansible vulnerabilities (USN-4072-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : apache2 regression (USN-4113-2) (Internal Data Buffering)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : apache2 vulnerabilities (USN-4113-1) (Internal Data Buffering)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : aspell vulnerability (USN-4155-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : clamav vulnerabilities (USN-4146-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : cups vulnerabilities (USN-4105-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : curl vulnerabilities (USN-4129-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : Docker vulnerability (USN-4103-2)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : Dovecot regression (USN-4110-3)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : dovecot vulnerability (USN-4110-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : e2fsprogs vulnerability (USN-4142-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : exim4 vulnerability (USN-4075-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : exim4 vulnerability (USN-4124-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : expat vulnerability (USN-4132-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : firefox regressions (USN-4054-2)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : firefox vulnerabilities (USN-4122-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : firefox vulnerability (USN-4101-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : firefox vulnerability (USN-4140-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : ghostscript vulnerabilities (USN-4111-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : ghostscript vulnerability (USN-4092-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : giflib vulnerabilities (USN-4107-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : ibus regression (USN-4134-2)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : ibus vulnerability (USN-4134-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : kconfig, kde4libs vulnerabilities (USN-4100-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libarchive vulnerability (USN-4169-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libbsd vulnerabilities (USN-4243-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libjpeg-turbo vulnerabilities (USN-4190-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libpcap vulnerability (USN-4221-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libreoffice vulnerabilities (USN-4063-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libreoffice vulnerabilities (USN-4102-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libreoffice vulnerability (USN-4138-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : libvpx vulnerabilities (USN-4199-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, (USN-4135-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : linux-aws, linux-aws-hwe vulnerability (USN-4096-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : memcached vulnerability (USN-4125-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : mysql-5.7 vulnerabilities (USN-4070-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : nginx vulnerabilities (USN-4099-1) (0-Length Headers Leak) (Data Dribble) (Resource Loop)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : NLTK vulnerability (USN-4106-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : nova vulnerability (USN-4104-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : nss vulnerabilities (USN-4060-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : nss vulnerability (USN-4215-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : openexr vulnerabilities (USN-4148-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : openldap vulnerabilities (USN-4078-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : patch vulnerabilities (USN-4071-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : php7.0, php7.2 vulnerabilities (USN-4097-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : postgresql-10, postgresql-11, postgresql-9.5 vulnerabilities (USN-4090-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : python-django vulnerabilities (USN-4084-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : python2.7, python3.5, python3.6, python3.7 vulnerabilities (USN-4127-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : python2.7, python3.5, python3.6, python3.7 vulnerabilities (USN-4151-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : redis vulnerabilities (USN-4061-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : redmine vulnerabilities (USN-4200-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : SDL 2.0 vulnerabilities (USN-4143-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : Sigil vulnerability (USN-4085-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : squid, squid3 vulnerabilities (USN-4059-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : squid, squid3 vulnerabilities (USN-4065-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : sudo vulnerability (USN-4154-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : tiff vulnerabilities (USN-4158-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : uw-imap vulnerability (USN-4160-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : Wireshark vulnerabilities (USN-4133-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : wpa vulnerability (USN-4136-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : apport regression (USN-4171-5)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : apport vulnerabilities (USN-4315-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : bluez vulnerabilities (USN-4311-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : clamav vulnerability (USN-4280-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : cyrus-sasl2 vulnerability (USN-4256-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : exiv2 vulnerability (USN-4270-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : firefox vulnerabilities (USN-4299-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : firefox vulnerabilities (USN-4317-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : firefox vulnerabilities (USN-4323-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : git vulnerability (USN-4329-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : ibus vulnerability (USN-4134-3)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : icu vulnerability (USN-4305-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : libarchive vulnerabilities (USN-4293-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : libexif vulnerabilities (USN-4277-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : libpam-krb5 vulnerability (USN-4314-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : libpam-radius-auth vulnerability (USN-4290-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : libxml2 vulnerabilities (USN-4274-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : mysql-5.7, mysql-8.0 vulnerabilities (USN-4250-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : openjdk-8, openjdk-lts vulnerabilities (USN-4257-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : php5, php7.0, php7.2, php7.3 vulnerabilities (USN-4279-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : php5, php7.0, php7.2, php7.3 vulnerabilities (USN-4330-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : pillow vulnerabilities (USN-4272-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : ppp vulnerability (USN-4288-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : python-django vulnerability (USN-4296-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : python-reportlab vulnerability (USN-4273-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : qemu vulnerabilities (USN-4283-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : qtbase-opensource-src vulnerabilities (USN-4275-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : rake vulnerability (USN-4295-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : spamassassin vulnerabilities (USN-4265-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : sqlite3 vulnerabilities (USN-4298-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : squid, squid3 vulnerabilities (USN-4289-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : sudo vulnerability (USN-4263-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : systemd vulnerabilities (USN-4269-1)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : twisted vulnerabilities (USN-4308-1) (Ping Flood) (Reset Flood) (Settings Flood)

Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : vim vulnerabilities (USN-4309-1)

Ubuntu 16.04 LTS / 18.04 LTS : corosync vulnerability (USN-4000-1)

Ubuntu 16.04 LTS / 18.04 LTS : evince update (USN-4024-1)

Ubuntu 16.04 LTS / 18.04 LTS : evolution-data-server vulnerability (USN-3998-1)

Ubuntu 16.04 LTS / 18.04 LTS : file-roller vulnerability (USN-4139-1)

Ubuntu 16.04 LTS / 18.04 LTS : gnutls28 update (USN-4233-1)

Ubuntu 16.04 LTS / 18.04 LTS : gnutls28 update (USN-4233-2)

Ubuntu 16.04 LTS / 18.04 LTS : libebml vulnerability (USN-4073-1)

Ubuntu 16.04 LTS / 18.04 LTS : libiberty vulnerabilities (USN-4326-1)

Ubuntu 16.04 LTS / 18.04 LTS : libmspack vulnerabilities (USN-3728-1)

Ubuntu 16.04 LTS / 18.04 LTS : libmspack vulnerability (USN-4066-1)

Ubuntu 16.04 LTS / 18.04 LTS : librabbitmq vulnerability (USN-4214-2)

Ubuntu 16.04 LTS / 18.04 LTS : libsdl1.2 vulnerabilities (USN-4156-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-gke-4.15, (USN-4115-2)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-gke-4.15, (USN-4162-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-gke-4.15, (USN-4185-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-gke-4.15, (USN-4227-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-gke-4.15, (USN-4287-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-azure, linux-hwe, linux-kvm, (USN-4144-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-gcp, linux-gke-4.15, linux-hwe, (USN-4210-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-aws, linux-aws-hwe, linux-gcp, linux-gke-4.15, linux-hwe, (USN-4302-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-azure, linux-gcp, linux-gke-4.15, linux-hwe, linux-kvm, (USN-4115-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-hwe vulnerabilities (USN-4318-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-hwe, linux-azure, linux-gcp, linux-gke-4.15, linux-kvm, (USN-4094-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux, linux-hwe, linux-oem vulnerability and regression (USN-4185-3)

Ubuntu 16.04 LTS / 18.04 LTS : linux-aws vulnerabilities (USN-4118-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux-aws, linux-aws-hwe, linux-azure, linux-gcp, linux-gke-4.15, (USN-4324-1)

Ubuntu 16.04 LTS / 18.04 LTS : linux-azure vulnerabilities (USN-3777-3) (Spectre)

Ubuntu 16.04 LTS / 18.04 LTS : linux-azure, linux-oem, linux-gcp vulnerabilities (USN-3752-3)

Ubuntu 16.04 LTS / 18.04 LTS : openjdk-8, openjdk-lts regression (USN-3830-1)

Ubuntu 16.04 LTS / 18.04 LTS : openvswitch vulnerabilities (USN-3873-1)

Ubuntu 16.04 LTS / 18.04 LTS : rsync vulnerabilities (USN-4292-1)

Ubuntu 16.04 LTS / 18.04 LTS : ruby-rack vulnerability (USN-4089-1)

Ubuntu 16.04 LTS / 18.04 LTS : samba regression (USN-3976-3)

Ubuntu 16.04 LTS / 18.04 LTS : sdl-image1.2 vulnerabilities (USN-4238-1)

Ubuntu 16.04 LTS / 18.04 LTS : tcpdump vulnerabilities (USN-4252-1)

Ubuntu 16.04 LTS / 18.04 LTS : tmpreaper vulnerability (USN-4077-1)

Ubuntu 16.04 LTS / 18.04 LTS : Tomcat vulnerabilities (USN-4128-1)

Ubuntu 16.04 LTS / 18.04 LTS : webkit2gtk vulnerabilities (USN-3743-1)

Ubuntu 16.04 LTS / 18.10 / 19.04 : ceph vulnerabilities (USN-4035-1)

Ubuntu 16.04 LTS / 18.10 : neutron vulnerability (USN-4036-1)

Ubuntu 16.04 LTS / 18.10 : openjdk-8, openjdk-lts vulnerability (USN-3875-1)

Ubuntu 16.04 LTS : Apache Solr vulnerability (USN-4259-1)

Ubuntu 16.04 LTS : apparmor update (USN-4008-2)

Ubuntu 16.04 LTS : bash vulnerability (USN-4058-1)

Ubuntu 16.04 LTS : dnsmasq update (USN-3716-1)

Ubuntu 16.04 LTS : doxygen vulnerability (USN-4002-1)

Ubuntu 16.04 LTS : evince vulnerability (USN-4067-1)

Ubuntu 16.04 LTS : freetype vulnerability (USN-4126-1)

Ubuntu 16.04 LTS : gdk-pixbuf vulnerability (USN-3912-1)

Ubuntu 16.04 LTS : glib2.0 regression (USN-4049-3)

Ubuntu 16.04 LTS : graphicsmagick vulnerabilities (USN-4206-1)

Ubuntu 16.04 LTS : graphicsmagick vulnerabilities (USN-4222-1)

Ubuntu 16.04 LTS : graphicsmagick vulnerabilities (USN-4232-1)

Ubuntu 16.04 LTS : graphicsmagick vulnerabilities (USN-4248-1)

Ubuntu 16.04 LTS : graphicsmagick vulnerabilities (USN-4266-1)

Ubuntu 16.04 LTS : Gunicorn vulnerability (USN-4022-1)

Ubuntu 16.04 LTS : haproxy vulnerability (USN-3011-1)

Ubuntu 16.04 LTS : irssi vulnerabilities (USN-3086-1)

Ubuntu 16.04 LTS : kamailio vulnerability (USN-4240-1)

Ubuntu 16.04 LTS : keystone vulnerability (USN-3448-1)

Ubuntu 16.04 LTS : libgcrypt20 vulnerability (USN-4236-2)

Ubuntu 16.04 LTS : libtasn1-6 vulnerability (USN-2957-2)

Ubuntu 16.04 LTS : linux regression (USN-3522-3) (Meltdown)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-2965-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-2979-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3006-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3016-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3055-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3070-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3084-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3099-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3146-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3161-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3169-1)

Ubuntu 16.04 LTS : linux vulnerabilities (USN-3291-1)

Ubuntu 16.04 LTS : linux vulnerability (USN-3106-1) (Dirty COW)

Ubuntu 16.04 LTS : linux vulnerability (USN-3128-1)

Ubuntu 16.04 LTS : linux vulnerability (USN-3151-1)

Ubuntu 16.04 LTS : linux vulnerability (USN-4186-3)

Ubuntu 16.04 LTS : linux, linux-aws, linux-euclid vulnerabilities (USN-3540-1) (Meltdown) (Spectre)

Ubuntu 16.04 LTS : linux, linux-aws, linux-euclid, linux-kvm vulnerability (USN-3522-1) (Meltdown)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3420-1) (BlueBorne)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3444-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3469-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3485-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon regression (USN-3392-1) (Stack Clash)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3234-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3265-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3312-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3344-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3378-1) (Stack Clash)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3385-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3405-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerability (USN-3249-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm vulnerabilities (USN-4186-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm vulnerability (USN-4303-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2 regression (USN-3509-3) (Dirty COW)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2 vulnerabilities (USN-4076-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon (USN-4211-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon (USN-4228-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon (USN-4254-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon (USN-4286-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3509-1) (Dirty COW)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3582-1) (Spectre)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3619-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3631-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3676-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3696-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3741-1) (Foreshadow)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3753-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3776-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3797-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3821-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3848-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3879-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3910-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3932-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-3982-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-4008-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-4095-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-4116-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-4145-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-4163-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, linux-raspi2, linux-snapdragon vulnerability (USN-4320-1)

Ubuntu 16.04 LTS : linux, linux-aws, linux-kvm, vulnerabilities (USN-3654-1) (Spectre)

Ubuntu 16.04 LTS : linux, linux-gke, linux-raspi2, linux-snapdragon vulnerability (USN-3220-1)

Ubuntu 16.04 LTS : linux, linux-meta vulnerabilities (USN-3328-1) (Stack Clash)

Ubuntu 16.04 LTS : linux, linux-raspi2, linux-snapdragon vulnerabilities (USN-3189-1)

Ubuntu 16.04 LTS : linux, linux-raspi2, linux-snapdragon vulnerabilities (USN-3364-1)

Ubuntu 16.04 LTS : linux, linux-snapdragon vulnerabilities (USN-3208-1)

Ubuntu 16.04 LTS : linux-aws vulnerability (USN-3220-3)

Ubuntu 16.04 LTS : linux-aws, linux-gke vulnerabilities (USN-3364-3)

Ubuntu 16.04 LTS : linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3291-2)

Ubuntu 16.04 LTS : linux-aws, linux-meta-aws vulnerabilities (USN-3331-1) (Stack Clash)

Ubuntu 16.04 LTS : linux-aws-hwe, linux-hwe, linux-oracle vulnerability (USN-4007-2)

Ubuntu 16.04 LTS : linux-azure vulnerabilities (USN-3511-1) (Dirty COW)

Ubuntu 16.04 LTS : linux-azure vulnerabilities (USN-3632-1)

Ubuntu 16.04 LTS : linux-azure vulnerabilities (USN-3678-2)

Ubuntu 16.04 LTS : linux-azure vulnerability (USN-3488-1)

Ubuntu 16.04 LTS : linux-euclid vulnerability (USN-3633-1)

Ubuntu 16.04 LTS : linux-gcp vulnerabilities (USN-3468-3)

Ubuntu 16.04 LTS : linux-gcp vulnerabilities (USN-3507-2) (Dirty COW)

Ubuntu 16.04 LTS : linux-gcp vulnerability (USN-3443-3)

Ubuntu 16.04 LTS : linux-gcp vulnerability (USN-3484-3)

Ubuntu 16.04 LTS : linux-gke, linux-meta-gke vulnerabilities (USN-3329-1) (Stack Clash)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3342-2)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3361-1)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3371-1)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3377-2) (Stack Clash)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3384-2)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3419-2) (BlueBorne)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3443-2)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3468-2)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3508-2) (Dirty COW)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3597-2) (Meltdown) (Spectre)

Ubuntu 16.04 LTS : linux-hwe vulnerabilities (USN-3752-2)

Ubuntu 16.04 LTS : linux-hwe vulnerability (USN-3221-2)

Ubuntu 16.04 LTS : linux-hwe vulnerability (USN-3251-2)

Ubuntu 16.04 LTS : linux-hwe vulnerability (USN-3266-2)

Ubuntu 16.04 LTS : linux-hwe vulnerability (USN-3292-2)

Ubuntu 16.04 LTS : linux-hwe vulnerability (USN-3313-2) (deprecated)

Ubuntu 16.04 LTS : linux-hwe vulnerability (USN-3404-2)

Ubuntu 16.04 LTS : linux-hwe vulnerability (USN-3484-2)

Ubuntu 16.04 LTS : linux-hwe, linux-aws-hwe vulnerabilities (USN-4255-2)

Ubuntu 16.04 LTS : linux-hwe, linux-aws-hwe, linux-azure, linux-gcp vulnerabilities (USN-3847-2)

Ubuntu 16.04 LTS : linux-hwe, linux-aws-hwe, linux-gcp vulnerabilities (USN-3871-4)

Ubuntu 16.04 LTS : linux-hwe, linux-azure vulnerabilities (USN-3695-2)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp regression (USN-3718-2)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp vulnerabilities (USN-3740-2) (Foreshadow)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp vulnerabilities (USN-3762-2)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp vulnerabilities (USN-3820-2)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp vulnerability (USN-3732-2)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp, linux-oem vulnerabilities (USN-3523-2) (Meltdown)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp, linux-oem vulnerabilities (USN-3541-2) (Meltdown) (Spectre)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp, linux-oem vulnerabilities (USN-3581-2) (Spectre)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp, linux-oem vulnerabilities (USN-3653-2) (Spectre)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp, linux-oem vulnerability (USN-3548-2)

Ubuntu 16.04 LTS : linux-hwe, linux-azure, linux-gcp, linux-oracle vulnerabilities (USN-3981-2) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 16.04 LTS : linux-hwe, linux-gcp vulnerabilities (USN-3777-2)

Ubuntu 16.04 LTS : linux-hwe, linux-gcp vulnerabilities (USN-3836-2)

Ubuntu 16.04 LTS : linux-hwe, linux-gcp vulnerabilities (USN-4068-2)

Ubuntu 16.04 LTS : linux-hwe, linux-gcp, linux-oem vulnerabilities (USN-3617-2)

Ubuntu 16.04 LTS : linux-hwe, linux-gcp, linux-oem vulnerabilities (USN-3677-2)

Ubuntu 16.04 LTS : linux-hwe, linux-gcp, linux-oem vulnerability (USN-3630-2)

Ubuntu 16.04 LTS : linux-hwe, linux-meta-hwe vulnerabilities (USN-3333-1) (Stack Clash)

Ubuntu 16.04 LTS : linux-kvm vulnerabilities (USN-3549-1) (Spectre)

Ubuntu 16.04 LTS : linux-meta-raspi2, linux-raspi2 vulnerabilities (USN-3332-1) (Stack Clash)

Ubuntu 16.04 LTS : linux-meta-snapdragon, linux-snapdragon vulnerabilities (USN-3330-1) (Stack Clash)

Ubuntu 16.04 LTS : linux-oem vulnerabilities (USN-3697-2)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-2965-3)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3007-1)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3016-2)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3056-1)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3070-2)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3084-3)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3099-3)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3161-3)

Ubuntu 16.04 LTS : linux-raspi2 vulnerabilities (USN-3169-3)

Ubuntu 16.04 LTS : linux-raspi2 vulnerability (USN-2979-3)

Ubuntu 16.04 LTS : linux-raspi2 vulnerability (USN-3106-3) (Dirty COW)

Ubuntu 16.04 LTS : linux-raspi2 vulnerability (USN-3151-4)

Ubuntu 16.04 LTS : linux-raspi2, linux-snapdragon vulnerabilities (USN-3656-1)

Ubuntu 16.04 LTS : linux-snapdragon vulnerabilities (USN-3016-3)

Ubuntu 16.04 LTS : linux-snapdragon vulnerabilities (USN-3057-1)

Ubuntu 16.04 LTS : linux-snapdragon vulnerabilities (USN-3070-3)

Ubuntu 16.04 LTS : linux-snapdragon vulnerabilities (USN-3084-4)

Ubuntu 16.04 LTS : linux-snapdragon vulnerabilities (USN-3099-4)

Ubuntu 16.04 LTS : linux-snapdragon vulnerabilities (USN-3161-4)

Ubuntu 16.04 LTS : linux-snapdragon vulnerabilities (USN-3169-4)

Ubuntu 16.04 LTS : linux-snapdragon vulnerability (USN-2965-4)

Ubuntu 16.04 LTS : linux-snapdragon vulnerability (USN-2979-4)

Ubuntu 16.04 LTS : linux-snapdragon vulnerability (USN-3008-1)

Ubuntu 16.04 LTS : linux-snapdragon vulnerability (USN-3106-4) (Dirty COW)

Ubuntu 16.04 LTS : linux-snapdragon vulnerability (USN-3128-3)

Ubuntu 16.04 LTS : linux-snapdragon vulnerability (USN-3151-3)

Ubuntu 16.04 LTS : mbedtls vulnerabilities (USN-4267-1)

Ubuntu 16.04 LTS : mutt vulnerabilities (USN-3719-3)

Ubuntu 16.04 LTS : mysql-5.7 vulnerabilities (USN-2954-1)

Ubuntu 16.04 LTS : nova-lxd vulnerability (USN-3195-1)

Ubuntu 16.04 LTS : openjdk-8 vulnerabilities (USN-2963-1)

Ubuntu 16.04 LTS : openjdk-8 vulnerabilities (USN-3043-1)

Ubuntu 16.04 LTS : openjdk-8 vulnerabilities (USN-4080-1)

Ubuntu 16.04 LTS : openjdk-8 vulnerability (USN-3734-1)

Ubuntu 16.04 LTS : p7zip vulnerabilities (USN-3913-1)

Ubuntu 16.04 LTS : php7.0 regression (USN-4279-2)

Ubuntu 16.04 LTS : pyopenssl vulnerabilities (USN-3813-1)

Ubuntu 16.04 LTS : python-django vulnerability (USN-3039-1)

Ubuntu 16.04 LTS : python-oslo.middleware vulnerability (USN-3666-1)

Ubuntu 16.04 LTS : sox vulnerabilities (USN-4079-1)

Ubuntu 16.04 LTS : subversion vulnerabilities (USN-4082-1)

Ubuntu 16.04 LTS : sudo vulnerabilities (USN-3968-1)

Ubuntu 16.04 LTS : systemd regression (USN-3816-3)

Ubuntu 16.04 LTS : systemd vulnerability (USN-3094-1)

Ubuntu 16.04 LTS : tomcat8 vulnerabilities (USN-4251-1)

Ubuntu 16.04 LTS : tomcat8 vulnerability (USN-3027-1)

Ubuntu 16.04 LTS : tracker vulnerability (USN-3101-1)

Ubuntu 16.04 LTS : ubuntu-core-launcher vulnerability (USN-2956-1)

Ubuntu 16.04 LTS : VCFtools vulnerabilities (USN-3974-1)

Ubuntu 16.04 LTS : web2py vulnerabilities (USN-4030-1)

Ubuntu 16.04 LTS : webkit2gtk vulnerabilities (USN-3079-1)

Ubuntu 16.04 LTS : webkit2gtk vulnerabilities (USN-3166-1)

Ubuntu 16.04 LTS : xmlrpc-epi vulnerability (USN-3059-1)

Ubuntu 16.04 LTS : zlib vulnerabilities (USN-4246-1)

Ubuntu 16.10 / 17.04 : lightdm vulnerability (USN-3285-1)

Ubuntu 16.10 / 17.04 : systemd vulnerability (USN-3341-1)

Ubuntu 16.10 : apt regression (USN-3156-2)

Ubuntu 16.10 : linux vulnerabilities (USN-3147-1)

Ubuntu 16.10 : linux vulnerabilities (USN-3162-1)

Ubuntu 16.10 : linux vulnerabilities (USN-3170-1)

Ubuntu 16.10 : linux vulnerabilities (USN-3190-1)

Ubuntu 16.10 : linux vulnerability (USN-3107-1) (Dirty COW)

Ubuntu 16.10 : linux vulnerability (USN-3129-1)

Ubuntu 16.10 : linux vulnerability (USN-3152-1)

Ubuntu 16.10 : linux, linux-meta vulnerabilities (USN-3326-1) (Stack Clash)

Ubuntu 16.10 : linux, linux-raspi2 vulnerabilities (USN-3209-1)

Ubuntu 16.10 : linux, linux-raspi2 vulnerabilities (USN-3342-1)

Ubuntu 16.10 : linux, linux-raspi2 vulnerabilities (USN-3359-1)

Ubuntu 16.10 : linux, linux-raspi2 vulnerability (USN-3221-1)

Ubuntu 16.10 : linux, linux-raspi2 vulnerability (USN-3251-1)

Ubuntu 16.10 : linux, linux-raspi2 vulnerability (USN-3266-1)

Ubuntu 16.10 : linux, linux-raspi2 vulnerability (USN-3292-1)

Ubuntu 16.10 : linux, linux-raspi2 vulnerability (USN-3313-1) (deprecated)

Ubuntu 16.10 : linux-meta-raspi2, linux-raspi2 vulnerabilities (USN-3327-1) (Stack Clash)

Ubuntu 16.10 : linux-raspi2 vulnerabilities (USN-3129-2)

Ubuntu 16.10 : linux-raspi2 vulnerabilities (USN-3152-2)

Ubuntu 16.10 : linux-raspi2 vulnerabilities (USN-3162-2)

Ubuntu 16.10 : linux-raspi2 vulnerabilities (USN-3170-2)

Ubuntu 16.10 : linux-raspi2 vulnerabilities (USN-3190-2)

Ubuntu 16.10 : linux-raspi2 vulnerability (USN-3107-2) (Dirty COW)

Ubuntu 17.04 / 17.10 : exim4 vulnerability (USN-3493-1)

Ubuntu 17.04 / 17.10 : exim4 vulnerability (USN-3499-1)

Ubuntu 17.04 / 17.10 : systemd vulnerability (USN-3466-1)

Ubuntu 17.04 : curl vulnerability (USN-3262-1)

Ubuntu 17.04 : emacs25 vulnerability (USN-3428-1)

Ubuntu 17.04 : file vulnerability (USN-3412-1)

Ubuntu 17.04 : freeradius vulnerability (USN-3316-1)

Ubuntu 17.04 : libgcrypt20 vulnerability (USN-3417-1)

Ubuntu 17.04 : libidn2-0 vulnerability (USN-3421-1)

Ubuntu 17.04 : linux, linux-meta vulnerabilities (USN-3324-1) (Stack Clash)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3293-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3314-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3345-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3358-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3377-1) (Stack Clash)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3384-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3419-1) (BlueBorne)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3443-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3468-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerabilities (USN-3508-1) (Dirty COW)

Ubuntu 17.04 : linux, linux-raspi2 vulnerability (USN-3404-1)

Ubuntu 17.04 : linux, linux-raspi2 vulnerability (USN-3484-1)

Ubuntu 17.04 : linux-meta-raspi2, linux-raspi2 vulnerabilities (USN-3325-1) (Stack Clash)

Ubuntu 17.04 : miniupnpc vulnerability (USN-3298-2)

Ubuntu 17.04 : openvpn vulnerabilities (USN-3284-1)

Ubuntu 17.04 : qemu vulnerabilities (USN-3268-1)

Ubuntu 17.04 : samba vulnerability (USN-3267-1)

Ubuntu 17.10 / 18.04 LTS : curl vulnerability (USN-3710-1)

Ubuntu 17.10 / 18.04 LTS : devscripts vulnerability (USN-3704-1)

Ubuntu 17.10 / 18.04 LTS : mozjs52 vulnerabilities (USN-3688-1)

Ubuntu 17.10 / 18.04 LTS : wavpack vulnerabilities (USN-3637-1)

Ubuntu 17.10 / 18.04 LTS : xapian-core vulnerability (USN-3709-1)

Ubuntu 17.10 : dpdk vulnerability (USN-3642-2)

Ubuntu 17.10 : freetype vulnerability (USN-3572-1)

Ubuntu 17.10 : libreoffice regression (USN-3579-2)

Ubuntu 17.10 : libreoffice regression (USN-3579-3)

Ubuntu 17.10 : linux vulnerabilities (USN-3523-1) (Meltdown)

Ubuntu 17.10 : linux vulnerabilities (USN-3541-1) (Meltdown) (Spectre)

Ubuntu 17.10 : linux vulnerabilities (USN-3581-1) (Spectre)

Ubuntu 17.10 : linux vulnerabilities (USN-3617-1)

Ubuntu 17.10 : linux vulnerabilities (USN-3653-1) (Spectre)

Ubuntu 17.10 : linux vulnerability (USN-3548-1)

Ubuntu 17.10 : linux, linux-raspi2 vulnerabilities (USN-3487-1)

Ubuntu 17.10 : linux, linux-raspi2 vulnerabilities (USN-3507-1) (Dirty COW)

Ubuntu 17.10 : linux, linux-raspi2 vulnerabilities (USN-3597-1) (Meltdown) (Spectre)

Ubuntu 17.10 : linux, linux-raspi2 vulnerabilities (USN-3677-1)

Ubuntu 17.10 : linux, linux-raspi2 vulnerabilities (USN-3697-1)

Ubuntu 17.10 : linux, linux-raspi2 vulnerability (USN-3630-1)

Ubuntu 17.10 : linux-raspi2 vulnerabilities (USN-3523-3)

Ubuntu 17.10 : linux-raspi2 vulnerabilities (USN-3581-3)

Ubuntu 17.10 : linux-raspi2 vulnerabilities (USN-3617-3)

Ubuntu 17.10 : linux-raspi2 vulnerabilities (USN-3657-1)

Ubuntu 17.10 : packagekit vulnerability (USN-3634-1)

Ubuntu 17.10 : python-django vulnerabilities (USN-3559-1)

Ubuntu 17.10 : wavpack vulnerabilities (USN-3578-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : bind9 vulnerability (USN-4026-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : FFmpeg vulnerabilities (USN-3967-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : freeradius vulnerabilities (USN-3954-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : gnome-desktop3 vulnerability (USN-3994-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : libmysofa vulnerability (USN-4033-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : linux, linux-hwe vulnerability (USN-4031-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : MediaInfo vulnerabilities (USN-3988-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : memcached vulnerability (USN-3963-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : postgresql-10, postgresql-11 vulnerability (USN-4027-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : python-gnupg vulnerabilities (USN-3964-1)

Ubuntu 18.04 LTS / 18.10 / 19.04 : webkit2gtk vulnerabilities (USN-3992-1)

Ubuntu 18.04 LTS / 18.10 : exim4 vulnerability (USN-4010-1)

Ubuntu 18.04 LTS / 18.10 : FreeRDP vulnerabilities (USN-3845-2)

Ubuntu 18.04 LTS / 18.10 : gdm3 vulnerability (USN-3892-1)

Ubuntu 18.04 LTS / 18.10 : gnome-shell vulnerability (USN-3966-1)

Ubuntu 18.04 LTS / 18.10 : gnupg2 vulnerability (USN-3853-1)

Ubuntu 18.04 LTS / 18.10 : gvfs vulnerability (USN-3888-1)

Ubuntu 18.04 LTS / 18.10 : isc-dhcp vulnerability (USN-3973-1)

Ubuntu 18.04 LTS / 18.10 : libapache2-mod-auth-mellon vulnerabilities (USN-3924-1)

Ubuntu 18.04 LTS / 18.10 : libpng1.6 vulnerability (USN-3962-1)

Ubuntu 18.04 LTS / 18.10 : nvidia-graphics-drivers-390 vulnerability (USN-3904-1)

Ubuntu 18.04 LTS / 18.10 : postgresql-10 vulnerability (USN-3818-1)

Ubuntu 18.04 LTS / 18.10 : webkit2gtk vulnerabilities (USN-3828-1)

Ubuntu 18.04 LTS / 18.10 : webkit2gtk vulnerabilities (USN-3854-1)

Ubuntu 18.04 LTS / 18.10 : webkit2gtk vulnerabilities (USN-3889-1)

Ubuntu 18.04 LTS / 18.10 : webkit2gtk vulnerabilities (USN-3948-1)

Ubuntu 18.04 LTS / 19.04 / 19.10 : bind9 vulnerability (USN-4197-1)

Ubuntu 18.04 LTS / 19.04 / 19.10 : dpdk regression (USN-4189-2)

Ubuntu 18.04 LTS / 19.04 / 19.10 : dpdk vulnerability (USN-4189-1)

Ubuntu 18.04 LTS / 19.04 / 19.10 : firefox vulnerabilities (USN-4216-1)

Ubuntu 18.04 LTS / 19.04 / 19.10 : freetds vulnerability (USN-4173-1)

Ubuntu 18.04 LTS / 19.04 / 19.10 : haproxy vulnerability (USN-4212-1)

Ubuntu 18.04 LTS / 19.04 / 19.10 : libgcrypt20 vulnerability (USN-4236-1)

Ubuntu 18.04 LTS / 19.04 / 19.10 : mariadb vulnerabilities (USN-4195-2)

Ubuntu 18.04 LTS / 19.04 / 19.10 : webkit2gtk vulnerabilities (USN-4181-1)

Ubuntu 18.04 LTS / 19.04 : BWA vulnerability (USN-4087-1)

Ubuntu 18.04 LTS / 19.04 : ceph vulnerability (USN-4112-1)

Ubuntu 18.04 LTS / 19.04 : libidn2 vulnerabilities (USN-4168-1)

Ubuntu 18.04 LTS / 19.04 : libsoup2.4 vulnerability (USN-4152-1)

Ubuntu 18.04 LTS / 19.04 : linux, linux-aws, linux-aws-5.0, linux-azure, linux-gcp, linux-gke-5.0, (USN-4226-1)

Ubuntu 18.04 LTS / 19.04 : linux, linux-aws, linux-aws-5.0, linux-gcp, linux-gke-5.0, linux-hwe, (USN-4209-1)

Ubuntu 18.04 LTS / 19.04 : linux, linux-aws, linux-azure, linux-gcp, linux-gke-5.0, linux-hwe, (USN-4147-1)

Ubuntu 18.04 LTS / 19.04 : linux, linux-aws, linux-azure, linux-gcp, linux-gke-5.0, linux-hwe, (USN-4184-1)

Ubuntu 18.04 LTS / 19.04 : linux, linux-azure, linux-gcp, linux-gke-5.0, linux-hwe, linux-kvm, (USN-4114-1)

Ubuntu 18.04 LTS / 19.04 : linux, linux-hwe, linux-azure, linux-gcp, linux-kvm, linux-raspi2, (USN-4093-1)

Ubuntu 18.04 LTS / 19.04 : linux, linux-hwe, linux-oem-osp1 vulnerability and regression (USN-4184-2)

Ubuntu 18.04 LTS / 19.04 : npm/fstream vulnerability (USN-4123-1)

Ubuntu 18.04 LTS / 19.04 : openjdk-lts vulnerabilities (USN-4083-1)

Ubuntu 18.04 LTS / 19.04 : poppler vulnerability (USN-4091-1)

Ubuntu 18.04 LTS / 19.04 : sox vulnerabilities (USN-4079-2)

Ubuntu 18.04 LTS / 19.04 : systemd regression (USN-4120-2)

Ubuntu 18.04 LTS / 19.04 : systemd vulnerability (USN-4120-1)

Ubuntu 18.04 LTS / 19.04 : Tomcat vulnerabilities (USN-4128-2)

Ubuntu 18.04 LTS / 19.04 : vlc vulnerabilities (USN-4074-1)

Ubuntu 18.04 LTS / 19.04 : vlc vulnerabilities (USN-4131-1)

Ubuntu 18.04 LTS / 19.04 : wavpack vulnerabilities (USN-4062-1)

Ubuntu 18.04 LTS / 19.04 : webkit2gtk vulnerabilities (USN-4130-1)

Ubuntu 18.04 LTS / 19.04 : webkit2gtk vulnerabilities (USN-4178-1)

Ubuntu 18.04 LTS / 19.04 : wpa vulnerability (USN-4098-1)

Ubuntu 18.04 LTS / 19.10 : ceph vulnerability (USN-4304-1)

Ubuntu 18.04 LTS / 19.10 : firefox vulnerabilities (USN-4278-1)

Ubuntu 18.04 LTS / 19.10 : haproxy vulnerability (USN-4321-1)

Ubuntu 18.04 LTS / 19.10 : libapache2-mod-auth-mellon vulnerability (USN-4291-1)

Ubuntu 18.04 LTS / 19.10 : libssh vulnerability (USN-4327-1)

Ubuntu 18.04 LTS / 19.10 : linux, linux-aws, linux-azure, linux-azure-5.3, linux-gcp, linux-gcp-5.3, (USN-4225-1)

Ubuntu 18.04 LTS / 19.10 : linux, linux-aws, linux-azure, linux-azure-5.3, linux-gcp, linux-gcp-5.3, (USN-4313-1)

Ubuntu 18.04 LTS / 19.10 : linux, linux-aws, linux-azure-5.3, linux-gcp, linux-gcp-5.3, linux-hwe, (USN-4284-1)

Ubuntu 18.04 LTS / 19.10 : linux, linux-aws, linux-gcp, linux-gcp-5.3, linux-gke-5.3, linux-hwe, (USN-4300-1)

Ubuntu 18.04 LTS / 19.10 : linux, linux-aws, linux-gcp, linux-gcp-5.3, linux-hwe, linux-kvm, (USN-4319-1)

Ubuntu 18.04 LTS / 19.10 : linux, linux-aws, linux-gcp, linux-gcp-5.3, linux-kvm, linux-oracle (USN-4208-1)

Ubuntu 18.04 LTS / 19.10 : mariadb-10.1, mariadb-10.3 vulnerability (USN-4250-2)

Ubuntu 18.04 LTS / 19.10 : mesa vulnerability (USN-4271-1)

Ubuntu 18.04 LTS / 19.10 : OpenSMTPD vulnerabilities (USN-4294-1)

Ubuntu 18.04 LTS / 19.10 : OpenSMTPD vulnerability (USN-4268-1)

Ubuntu 18.04 LTS / 19.10 : postgresql-10, postgresql-11 vulnerability (USN-4282-1)

Ubuntu 18.04 LTS / 19.10 : python-django vulnerability (USN-4264-1)

Ubuntu 18.04 LTS / 19.10 : runc vulnerabilities (USN-4297-1)

Ubuntu 18.04 LTS / 19.10 : thunderbird regression (USN-4202-2)

Ubuntu 18.04 LTS / 19.10 : thunderbird vulnerabilities (USN-4241-1)

Ubuntu 18.04 LTS / 19.10 : thunderbird vulnerabilities (USN-4328-1)

Ubuntu 18.04 LTS / 19.10 : webkit2gtk vulnerabilities (USN-4261-1)

Ubuntu 18.04 LTS / 19.10 : webkit2gtk vulnerabilities (USN-4281-1)

Ubuntu 18.04 LTS / 19.10 : webkit2gtk vulnerability (USN-4310-1)

Ubuntu 18.04 LTS : apache2 update (USN-4307-1)

Ubuntu 18.04 LTS : apache2 vulnerabilities (USN-3627-2)

Ubuntu 18.04 LTS : apache2 vulnerabilities (USN-3783-1)

Ubuntu 18.04 LTS : apt vulnerability (USN-3746-1)

Ubuntu 18.04 LTS : base-files vulnerability (USN-3748-1)

Ubuntu 18.04 LTS : bind9 vulnerability (USN-3683-1)

Ubuntu 18.04 LTS : dino-im vulnerabilities (USN-4306-1)

Ubuntu 18.04 LTS : dpdk vulnerability (USN-3642-1)

Ubuntu 18.04 LTS : gdm3 vulnerability (USN-3737-1)

Ubuntu 18.04 LTS : gnome-bluetooth vulnerability (USN-3856-1)

Ubuntu 18.04 LTS : graphicsmagick vulnerabilities (USN-4207-1)

Ubuntu 18.04 LTS : haproxy vulnerability (USN-3663-1)

Ubuntu 18.04 LTS : haproxy vulnerability (USN-3780-1)

Ubuntu 18.04 LTS : libxkbcommon vulnerabilities (USN-3786-2)

Ubuntu 18.04 LTS : libzstd vulnerability (USN-4108-1)

Ubuntu 18.04 LTS : linux regression (USN-3871-2)

Ubuntu 18.04 LTS : linux vulnerabilities (USN-3871-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oem regression (USN-3718-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oem vulnerability (USN-3652-1) (Spectre)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oem, (USN-3732-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oem, (USN-3847-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oem, and (USN-3740-1) (Foreshadow)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oem, linux-raspi2 vulnerabilities (USN-3695-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oem, linux-raspi2 vulnerabilities (USN-3820-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2 (USN-3762-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm vulnerabilities (USN-3678-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm, linux-oem, linux-oracle, (USN-3931-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm, linux-oem, linux-oracle, (USN-3981-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm, linux-oem, linux-oracle, (USN-4007-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm, linux-oem, linux-oracle, linux-raspi2 vulnerabilities (USN-3901-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm, linux-oem, linux-raspi2 vulnerabilities (USN-3777-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm, linux-oracle, linux-raspi2, (USN-4068-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-gcp, linux-kvm, linux-raspi2 vulnerabilities (USN-3752-1)

Ubuntu 18.04 LTS : linux, linux-aws, linux-oem vulnerabilities (USN-4255-1)

Ubuntu 18.04 LTS : linux, linux-gcp, linux-kvm, linux-raspi2 vulnerabilities (USN-3836-1)

Ubuntu 18.04 LTS : linux-aws vulnerabilities (USN-3833-1)

Ubuntu 18.04 LTS : linux-aws, linux-gcp, linux-kvm, linux-oem, linux-raspi2 vulnerabilities (USN-3871-3)

Ubuntu 18.04 LTS : linux-aws-5.0, linux-azure, linux-gcp, linux-gke-5.0, linux-oracle-5.0 (USN-4285-1)

Ubuntu 18.04 LTS : linux-aws-5.0, linux-gcp, linux-gke-5.0, linux-oracle-5.0 vulnerabilities (USN-4258-1)

Ubuntu 18.04 LTS : linux-aws-5.0, linux-gcp, linux-gke-5.0, linux-oracle-5.0 vulnerabilities (USN-4301-1)

Ubuntu 18.04 LTS : linux-azure vulnerabilities (USN-3678-3)

Ubuntu 18.04 LTS : linux-azure, linux-gcp, linux-gke-5.0, linux-oem-osp1, linux-oracle-5.0 (USN-4325-1)

Ubuntu 18.04 LTS : linux-hwe vulnerabilities (USN-3872-1)

Ubuntu 18.04 LTS : linux-hwe vulnerabilities (USN-4069-2)

Ubuntu 18.04 LTS : linux-hwe vulnerabilities (USN-4225-2)

Ubuntu 18.04 LTS : linux-hwe vulnerability (USN-4006-2)

Ubuntu 18.04 LTS : linux-hwe vulnerability (USN-4253-2)

Ubuntu 18.04 LTS : linux-hwe, linux-azure vulnerabilities (USN-3903-2)

Ubuntu 18.04 LTS : linux-hwe, linux-azure vulnerabilities (USN-3930-2)

Ubuntu 18.04 LTS : linux-hwe, linux-azure vulnerabilities (USN-3980-2) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 18.04 LTS : linux-hwe, linux-azure, linux-gcp, linux-gke-5.0 vulnerabilities (USN-4157-2)

Ubuntu 18.04 LTS : linux-raspi2 vulnerabilities (USN-3678-4)

Ubuntu 18.04 LTS : lxc vulnerability (USN-3730-1)

Ubuntu 18.04 LTS : MariaDB vulnerabilities (USN-4070-2)

Ubuntu 18.04 LTS : mariadb-10.1 vulnerabilities (USN-3957-3)

Ubuntu 18.04 LTS : mozjs52 vulnerabilities (USN-3749-1)

Ubuntu 18.04 LTS : mysql-5.7 vulnerabilities (USN-3629-3)

Ubuntu 18.04 LTS : openjdk-lts regression (USN-3747-2)

Ubuntu 18.04 LTS : openjdk-lts vulnerabilities (USN-3747-1)

Ubuntu 18.04 LTS : openjdk-lts vulnerability (USN-3949-1)

Ubuntu 18.04 LTS : openjpeg2 vulnerabilities (USN-4109-1)

Ubuntu 18.04 LTS : pango1.0 vulnerability (USN-3750-1)

Ubuntu 18.04 LTS : php7.2 vulnerability (USN-3702-1)

Ubuntu 18.04 LTS : php7.2 vulnerability (USN-3702-2)

Ubuntu 18.04 LTS : python-cryptography vulnerability (USN-3720-1)

Ubuntu 18.04 LTS : python-django vulnerability (USN-3726-1)

Ubuntu 18.04 LTS : udisks2 vulnerability (USN-3772-1)

Ubuntu 18.04 LTS : webkit2gtk regression (USN-3781-2)

Ubuntu 18.04 LTS : webkit2gtk vulnerabilities (USN-3781-1)

Ubuntu 18.04 LTS : Yubico PIV Tool vulnerabilities (USN-4276-1)

Ubuntu 18.10 / 19.04 : aria2 vulnerability (USN-3965-1)

Ubuntu 18.10 / 19.04 : dovecot vulnerabilities (USN-3961-1)

Ubuntu 18.10 / 19.04 : dovecot vulnerability (USN-3951-1)

Ubuntu 18.10 / 19.04 : libvirt vulnerabilities (USN-4021-1)

Ubuntu 18.10 / 19.04 : Monit vulnerabilities (USN-3971-1)

Ubuntu 18.10 / 19.04 : Neovim vulnerability (USN-4016-2)

Ubuntu 18.10 : libsolv vulnerabilities (USN-3916-1)

Ubuntu 18.10 : libssh vulnerability (USN-3795-2)

Ubuntu 18.10 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2 (USN-3930-1)

Ubuntu 18.10 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2 vulnerabilities (USN-3980-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 18.10 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2 vulnerability (USN-3846-1)

Ubuntu 18.10 : linux, linux-aws, linux-gcp, linux-kvm, linux-raspi2 vulnerabilities (USN-3878-1)

Ubuntu 18.10 : linux, linux-aws, linux-gcp, linux-kvm, linux-raspi2 vulnerability (USN-3819-1)

Ubuntu 18.10 : linux, linux-aws, linux-gcp, linux-kvm, linux-raspi2 vulnerability (USN-4006-1)

Ubuntu 18.10 : linux, linux-azure, linux-gcp, linux-kvm, linux-raspi2 vulnerabilities (USN-3903-1)

Ubuntu 18.10 : linux, linux-gcp, linux-kvm, linux-raspi2 vulnerabilities (USN-3835-1)

Ubuntu 18.10 : linux-aws vulnerabilities (USN-3832-1)

Ubuntu 18.10 : linux-azure vulnerabilities (USN-3878-2)

Ubuntu 18.10 : net-snmp vulnerability (USN-3792-3)

Ubuntu 18.10 : paramiko vulnerability (USN-3796-3)

Ubuntu 18.10 : requests vulnerability (USN-3790-2)

Ubuntu 18.10 : subversion vulnerability (USN-3869-1)

Ubuntu 18.10 : texlive-bin vulnerability (USN-3788-2)

Ubuntu 18.10 : znc vulnerability (USN-3950-1)

Ubuntu 19.04 / 19.10 : fribidi vulnerability (USN-4179-1)

Ubuntu 19.04 / 19.10 : librabbitmq vulnerability (USN-4214-1)

Ubuntu 19.04 : advancecomp vulnerability (USN-3936-2)

Ubuntu 19.04 : docker-credential-helpers vulnerability (USN-4103-1)

Ubuntu 19.04 : exim4 vulnerability (USN-4141-1)

Ubuntu 19.04 : irssi vulnerability (USN-4119-1)

Ubuntu 19.04 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2 vulnerabilities (USN-3979-1) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Ubuntu 19.04 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2, (USN-4069-1)

Ubuntu 19.04 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2, linux-snapdragon vulnerabilities (USN-4157-1)

Ubuntu 19.04 : linux, linux-aws, linux-gcp, linux-kvm, linux-raspi2, linux-snapdragon (USN-4005-1)

Ubuntu 19.04 : linux-aws vulnerabilities (USN-4117-1)

Ubuntu 19.04 : MariaDB vulnerabilities (USN-4070-3)

Ubuntu 19.04 : Mercurial vulnerability (USN-4086-1)

Ubuntu 19.04 : Mosquitto vulnerability (USN-4137-1)

Ubuntu 19.04 : octavia vulnerability (USN-4153-1)

Ubuntu 19.04 : pango1.0 vulnerability (USN-4081-1)

Ubuntu 19.04 : samba vulnerabilities (USN-4018-1)

Ubuntu 19.04 : samba vulnerability (USN-4121-1)

Ubuntu 19.04 : unbound vulnerability (USN-4149-1)

Ubuntu 19.10 : aspell vulnerability (USN-4155-2)

Ubuntu 19.10 : gnutls28 vulnerability (USN-4322-1)

Ubuntu 19.10 : keystone vulnerability (USN-4262-1)

Ubuntu 19.10 : linux vulnerability (USN-4183-2)

Ubuntu 19.10 : linux, linux-aws vulnerability (USN-4253-1)

Ubuntu 19.10 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-oracle, (USN-4183-1)

Ubuntu 19.10 : linux, linux-aws, linux-azure, linux-gcp, linux-kvm, linux-raspi2 (USN-4161-1)

Ubuntu 19.10 : rygel vulnerability (USN-4177-1)

Ubuntu 19.10 : Timeshift vulnerability (USN-4312-1)

Ubuntu 4.10 / 5.04 / 5.10 : aide vulnerabilities (USN-151-3)

Ubuntu 4.10 / 5.04 / 5.10 : apache2 vulnerability (USN-225-1)

Ubuntu 4.10 / 5.04 / 5.10 : apache2, apache vulnerabilities (USN-241-1)

Ubuntu 4.10 / 5.04 / 5.10 : bluez-hcidump vulnerability (USN-256-1)

Ubuntu 4.10 / 5.04 / 5.10 : courier vulnerability (USN-226-1)

Ubuntu 4.10 / 5.04 / 5.10 : cpio vulnerability (USN-234-1)

Ubuntu 4.10 / 5.04 / 5.10 : curl vulnerability (USN-228-1)

Ubuntu 4.10 / 5.04 / 5.10 : curl, wget vulnerabilities (USN-205-1)

Ubuntu 4.10 / 5.04 / 5.10 : cyrus-sasl2 vulnerability (USN-272-1)

Ubuntu 4.10 / 5.04 / 5.10 : dia vulnerabilities (USN-266-1)

Ubuntu 4.10 / 5.04 / 5.10 : enigmail vulnerability (USN-211-1)

Ubuntu 4.10 / 5.04 / 5.10 : fetchmail vulnerability (USN-215-1)

Ubuntu 4.10 / 5.04 / 5.10 : fetchmail vulnerability (USN-233-1)

Ubuntu 4.10 / 5.04 / 5.10 : flex vulnerability (USN-260-1)

Ubuntu 4.10 / 5.04 / 5.10 : gnupg vulnerability (USN-252-1)

Ubuntu 4.10 / 5.04 / 5.10 : gnupg vulnerability (USN-264-1)

Ubuntu 4.10 / 5.04 / 5.10 : gtk+2.0, gdk-pixbuf vulnerabilities (USN-216-1)

Ubuntu 4.10 / 5.04 / 5.10 : heimdal vulnerability (USN-247-1)

Ubuntu 4.10 / 5.04 / 5.10 : heimdal vulnerability (USN-253-1)

Ubuntu 4.10 / 5.04 / 5.10 : imagemagick vulnerabilities (USN-246-1)

Ubuntu 4.10 / 5.04 / 5.10 : ipsec-tools vulnerability (USN-221-1)

Ubuntu 4.10 / 5.04 / 5.10 : kdegraphics, koffice, xpdf, cupsys, poppler, tetex-bin vulnerabilities (USN-270-1)

Ubuntu 4.10 / 5.04 / 5.10 : libapache2-mod-auth-pgsql vulnerability (USN-239-1)

Ubuntu 4.10 / 5.04 / 5.10 : libgda2 vulnerability (USN-212-1)

Ubuntu 4.10 / 5.04 / 5.10 : libtasn1-2 vulnerability (USN-251-1)

Ubuntu 4.10 / 5.04 / 5.10 : libungif4 vulnerabilities (USN-214-1)

Ubuntu 4.10 / 5.04 / 5.10 : linux-source-2.6.8.1/-2.6.10/-2.6.12 vulnerabilities (USN-231-1)

Ubuntu 4.10 / 5.04 / 5.10 : linux-source-2.6.8.1/-2.6.10/-2.6.12 vulnerabilities (USN-244-1)

Ubuntu 4.10 / 5.04 / 5.10 : linux-source-2.6.8.1/-2.6.10/-2.6.12 vulnerabilities (USN-263-1)

Ubuntu 4.10 / 5.04 / 5.10 : lynx regression fix (USN-206-2)

Ubuntu 4.10 / 5.04 / 5.10 : lynx vulnerability (USN-206-1)

Ubuntu 4.10 / 5.04 / 5.10 : mailman vulnerabilities (USN-242-1)

Ubuntu 4.10 / 5.04 / 5.10 : mailman vulnerability (USN-267-1)

Ubuntu 4.10 / 5.04 / 5.10 : mozilla vulnerabilities (USN-275-1)

Ubuntu 4.10 / 5.04 / 5.10 : mozilla-firefox, firefox vulnerabilities (USN-271-1)

Ubuntu 4.10 / 5.04 / 5.10 : mysql-dfsg vulnerability (USN-274-1)

Ubuntu 4.10 / 5.04 / 5.10 : netpbm-free vulnerabilities (USN-218-1)

Ubuntu 4.10 / 5.04 / 5.10 : netpbm-free vulnerability (USN-210-1)

Ubuntu 4.10 / 5.04 / 5.10 : noweb vulnerability (USN-254-1)

Ubuntu 4.10 / 5.04 / 5.10 : openssh vulnerability (USN-255-1)

Ubuntu 4.10 / 5.04 / 5.10 : openssl vulnerability (USN-204-1)

Ubuntu 4.10 / 5.04 / 5.10 : perl vulnerability (USN-222-1)

Ubuntu 4.10 / 5.04 / 5.10 : perl vulnerability (USN-222-2)

Ubuntu 4.10 / 5.04 / 5.10 : php4, php5 vulnerabilities (USN-232-1)

Ubuntu 4.10 / 5.04 / 5.10 : php4, php5 vulnerabilities (USN-261-1)

Ubuntu 4.10 / 5.04 / 5.10 : postgresql-7.4, postgresql-8.0, postgresql vulnerability (USN-258-1)

Ubuntu 4.10 / 5.04 / 5.10 : rpm vulnerability (USN-151-4)

Ubuntu 4.10 / 5.04 / 5.10 : ruby1.8 vulnerability (USN-273-1)

Ubuntu 4.10 / 5.04 / 5.10 : sudo vulnerability (USN-213-1)

Ubuntu 4.10 / 5.04 / 5.10 : sudo vulnerability (USN-235-1)

Ubuntu 4.10 / 5.04 / 5.10 : sudo vulnerability (USN-235-2)

Ubuntu 4.10 / 5.04 / 5.10 : ucd-snmp vulnerability (USN-190-2)

Ubuntu 4.10 / 5.04 / 5.10 : unzip regression fix (USN-248-2)

Ubuntu 4.10 / 5.04 / 5.10 : unzip vulnerability (USN-248-1)

Ubuntu 4.10 / 5.04 / 5.10 : w3c-libwww vulnerability (USN-220-1)

Ubuntu 4.10 / 5.04 / 5.10 : xine-lib vulnerability (USN-230-2)

Ubuntu 4.10 / 5.04 / 5.10 : xpdf, poppler, cupsys, tetex-bin vulnerabilities (USN-236-1)

Ubuntu 4.10 / 5.04 / 5.10 : xpdf, poppler, kdegraphics vulnerabilities (USN-249-1)

Ubuntu 4.10 / 5.04 / 5.10 : xpdf/cupsys/tetex-bin/kdegraphics/koffice vulnerabilities (USN-227-1)

Ubuntu 4.10 / 5.04 : abiword vulnerabilities (USN-203-1)

Ubuntu 4.10 / 5.04 : abiword vulnerability (USN-188-1)

Ubuntu 4.10 / 5.04 : apache vulnerability (USN-160-2)

Ubuntu 4.10 / 5.04 : apache2 vulnerabilities (USN-160-1)

Ubuntu 4.10 / 5.04 : apache2 vulnerability (USN-120-1)

Ubuntu 4.10 / 5.04 : apache2, libapache-mod-ssl vulnerabilities (USN-177-1)

Ubuntu 4.10 / 5.04 : binutils regression (USN-136-2)

Ubuntu 4.10 / 5.04 : binutils vulnerability (USN-136-1)

Ubuntu 4.10 / 5.04 : bzip2 vulnerabilities (USN-127-1)

Ubuntu 4.10 / 5.04 : bzip2 vulnerability (USN-161-1)

Ubuntu 4.10 / 5.04 : cfengine vulnerabilities (USN-198-1)

Ubuntu 4.10 / 5.04 : courier vulnerabilities (USN-201-1)

Ubuntu 4.10 / 5.04 : cpio vulnerabilities (USN-189-1)

Ubuntu 4.10 / 5.04 : cvs vulnerability (USN-117-1)

Ubuntu 4.10 / 5.04 : dpkg, ia32-libs, amd64-libs vulnerabilities (USN-151-2)

Ubuntu 4.10 / 5.04 : evolution vulnerabilities (USN-166-1)

Ubuntu 4.10 / 5.04 : fetchmail vulnerability (USN-153-1)

Ubuntu 4.10 / 5.04 : gaim vulnerabilities (USN-125-1)

Ubuntu 4.10 / 5.04 : gaim vulnerabilities (USN-168-1)

Ubuntu 4.10 / 5.04 : gaim vulnerability (USN-139-1)

Ubuntu 4.10 / 5.04 : gaim vulnerability (USN-140-1)

Ubuntu 4.10 / 5.04 : gdb vulnerabilities (USN-135-1)

Ubuntu 4.10 / 5.04 : gedit vulnerability (USN-138-1)

Ubuntu 4.10 / 5.04 : gnupg vulnerability (USN-170-1)

Ubuntu 4.10 / 5.04 : gnutls11, gnutls10 vulnerability (USN-126-1)

Ubuntu 4.10 / 5.04 : gzip vulnerabilities (USN-116-1)

Ubuntu 4.10 / 5.04 : gzip vulnerability (USN-158-1)

Ubuntu 4.10 / 5.04 : heartbeat vulnerability (USN-165-1)

Ubuntu 4.10 / 5.04 : imagemagick vulnerabilities (USN-132-1)

Ubuntu 4.10 / 5.04 : krb4, krb5 vulnerabilities (USN-224-1)

Ubuntu 4.10 / 5.04 : linux-source-2.6.10, linux-source-2.6.8.1 vulnerabilities (USN-137-1)

Ubuntu 4.10 / 5.04 : linux-source-2.6.10, linux-source-2.6.8.1 vulnerabilities (USN-143-1)

Ubuntu 4.10 / 5.04 : linux-source-2.6.10, linux-source-2.6.8.1 vulnerabilities (USN-178-1)

Ubuntu 4.10 / 5.04 : linux-source-2.6.10, linux-source-2.6.8.1 vulnerabilities (USN-187-1)

Ubuntu 4.10 / 5.04 : linux-source-2.6.10, linux-source-2.6.8.1 vulnerabilities (USN-199-1)

Ubuntu 4.10 / 5.04 : linux-source-2.6.8.1, linux-source-2.6.10 vulnerabilities (USN-131-1)

Ubuntu 4.10 / 5.04 : linux-source-2.6.8.1, linux-source-2.6.10 vulnerabilities (USN-169-1)

Ubuntu 4.10 / 5.04 : mozilla vulnerabilities (USN-155-1)

Ubuntu 4.10 / 5.04 : mozilla, mozilla-firefox vulnerabilities (USN-186-1)

Ubuntu 4.10 / 5.04 : mozilla, mozilla-thunderbird, mozilla-firefox vulnerabilities (USN-181-1)

Ubuntu 4.10 / 5.04 : mozilla-thunderbird vulnerabilities (USN-157-1)

Ubuntu 4.10 / 5.04 : mozilla-thunderbird vulnerabilities (USN-200-1)

Ubuntu 4.10 / 5.04 : mysql-dfsg vulnerability (USN-180-1)

Ubuntu 4.10 / 5.04 : nasm vulnerability (USN-128-1)

Ubuntu 4.10 / 5.04 : net-snmp vulnerability (USN-190-1)

Ubuntu 4.10 / 5.04 : netpbm-free vulnerability (USN-164-1)

Ubuntu 4.10 / 5.04 : openldap2, libpam-ldap, libnss-ldap vulnerabilities (USN-152-1)

Ubuntu 4.10 / 5.04 : openoffice.org vulnerability (USN-121-1)

Ubuntu 4.10 / 5.04 : openssh vulnerability (USN-209-1)

Ubuntu 4.10 / 5.04 : openssl weak default configuration (USN-179-1)

Ubuntu 4.10 / 5.04 : pcre3 vulnerability (USN-173-1)

Ubuntu 4.10 / 5.04 : pcre3, apache2 vulnerabilities (USN-173-2)

Ubuntu 4.10 / 5.04 : php4 vulnerabilities (USN-171-1)

Ubuntu 4.10 / 5.04 : php4 vulnerability (USN-207-1)

Ubuntu 4.10 / 5.04 : php4, php4-universe fixed packages (USN-147-2)

Ubuntu 4.10 / 5.04 : php4, php4-universe vulnerability (USN-147-1)

Ubuntu 4.10 / 5.04 : postgresql vulnerabilities (USN-118-1)

Ubuntu 4.10 / 5.04 : python2.1, python2.2, python2.3, gnumeric vulnerabilities (USN-173-4)

Ubuntu 4.10 / 5.04 : ruby1.8 vulnerability (USN-146-1)

Ubuntu 4.10 / 5.04 : ruby1.8 vulnerability (USN-195-1)

Ubuntu 4.10 / 5.04 : shorewall vulnerability (USN-197-1)

Ubuntu 4.10 / 5.04 : squid vulnerabilities (USN-183-1)

Ubuntu 4.10 / 5.04 : squid vulnerability (USN-122-1)

Ubuntu 4.10 / 5.04 : squid vulnerability (USN-129-1)

Ubuntu 4.10 / 5.04 : squid vulnerability (USN-192-1)

Ubuntu 4.10 / 5.04 : sudo vulnerability (USN-142-1)

Ubuntu 4.10 / 5.04 : tcpdump vulnerabilities (USN-119-1)

Ubuntu 4.10 / 5.04 : tcpdump vulnerability (USN-141-1)

Ubuntu 4.10 / 5.04 : texinfo vulnerability (USN-194-1)

Ubuntu 4.10 / 5.04 : tiff vulnerability (USN-130-1)

Ubuntu 4.10 / 5.04 : tiff vulnerability (USN-156-1)

Ubuntu 4.10 / 5.04 : unzip vulnerability (USN-159-1)

Ubuntu 4.10 / 5.04 : unzip vulnerability (USN-191-1)

Ubuntu 4.10 / 5.04 : util-linux vulnerability (USN-184-1)

Ubuntu 4.10 / 5.04 : vim vulnerability (USN-154-1)

Ubuntu 4.10 / 5.04 : wget vulnerabilities (USN-145-1)

Ubuntu 4.10 / 5.04 : xine-lib vulnerabilities (USN-123-1)

Ubuntu 4.10 / 5.04 : xine-lib vulnerability (USN-196-1)

Ubuntu 4.10 / 5.04 : xorg, xfree86 vulnerabilities (USN-182-1)

Ubuntu 4.10 / 5.04 : xpdf vulnerability (USN-163-1)

Ubuntu 4.10 / 5.04 : xscreensaver vulnerability (USN-269-1)

Ubuntu 4.10 / 5.04 : zlib vulnerability (USN-148-1)

Ubuntu 4.10 / 5.04 : zlib vulnerability (USN-151-1)

Ubuntu 4.10 / 5.10 : linux-source-2.6.8.1/-2.6.10/-2.6.12 vulnerabilities (USN-219-1)

Ubuntu 4.10 : apache vulnerabilities (USN-65-1)

Ubuntu 4.10 : apache vulnerability (USN-133-1)

Ubuntu 4.10 : apache2 bug fix (USN-173-3)

Ubuntu 4.10 : apache2 vulnerability (USN-23-1)

Ubuntu 4.10 : bogofilter vulnerability (USN-26-1)

Ubuntu 4.10 : cdrtools vulnerability (USN-100-1)

Ubuntu 4.10 : cpio vulnerability (USN-75-1)

Ubuntu 4.10 : cupsys vulnerabilities (USN-50-1)

Ubuntu 4.10 : cupsys vulnerability (USN-185-1)

Ubuntu 4.10 : curl vulnerability (USN-86-1)

Ubuntu 4.10 : cyrus21-imapd vulnerabilities (USN-31-1)

Ubuntu 4.10 : cyrus21-imapd vulnerability (USN-37-1)

Ubuntu 4.10 : cyrus21-imapd vulnerability (USN-87-1)

Ubuntu 4.10 : dbus vulnerability (USN-144-1)

Ubuntu 4.10 : debmake vulnerability (USN-49-1)

Ubuntu 4.10 : emacs21 vulnerability (USN-76-1)

Ubuntu 4.10 : enscript vulnerabilities (USN-68-1)

Ubuntu 4.10 : epiphany-browser regressions (USN-155-2)

Ubuntu 4.10 : evolution vulnerability (USN-69-1)

Ubuntu 4.10 : exim4 vulnerabilities (USN-56-1)

Ubuntu 4.10 : gaim vulnerabilities (USN-106-1)

Ubuntu 4.10 : gaim vulnerabilities (USN-8-1)

Ubuntu 4.10 : gaim vulnerabilities (USN-85-1)

Ubuntu 4.10 : gettext vulnerabilities (USN-5-1)

Ubuntu 4.10 : GhostScript utility script vulnerabilities (USN-3-1)

Ubuntu 4.10 : groff utility vulnerability (USN-13-1)

Ubuntu 4.10 : groff vulnerabilities (USN-43-1)

Ubuntu 4.10 : gtk+2.0, gdk-pixbuf vulnerabilities (USN-108-1)

Ubuntu 4.10 : imagemagick vulnerabilities (USN-35-1)

Ubuntu 4.10 : imagemagick vulnerability (USN-62-1)

Ubuntu 4.10 : imagemagick vulnerability (USN-7-1)

Ubuntu 4.10 : imagemagick vulnerability (USN-90-1)

Ubuntu 4.10 : imlib+png2 vulnerabilities (USN-53-1)

Ubuntu 4.10 : imlib2 vulnerabilities (USN-55-1)

Ubuntu 4.10 : ipsec-tools vulnerability (USN-107-1)

Ubuntu 4.10 : iptables vulnerability (USN-81-1)

Ubuntu 4.10 : krb5 vulnerability (USN-58-1)

Ubuntu 4.10 : lesstif1-1 vulnerabilities (USN-83-1)

Ubuntu 4.10 : lesstif1-1 vulnerabilities (USN-83-2)

Ubuntu 4.10 : lesstif1-1 vulnerabilities (USN-92-1)

Ubuntu 4.10 : libapache2-mod-python vulnerabilities (USN-80-1)

Ubuntu 4.10 : libdbi-perl vulnerabilities (USN-70-1)

Ubuntu 4.10 : libexif vulnerabilities (USN-91-1)

Ubuntu 4.10 : libgd vulnerabilities (USN-21-1)

Ubuntu 4.10 : libgd vulnerabilities (USN-33-1)

Ubuntu 4.10 : libgd2 vulnerabilities (USN-11-1)

Ubuntu 4.10 : libgd2 vulnerability (USN-25-1)

Ubuntu 4.10 : libxml vulnerabilities (USN-89-1)

Ubuntu 4.10 : libxpm4 vulnerability (USN-27-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-103-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-110-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-30-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-38-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-47-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-57-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-60-0)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-82-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerabilities (USN-95-1)

Ubuntu 4.10 : linux-source-2.6.8.1 vulnerability (USN-39-1)

Ubuntu 4.10 : lvm10 vulnerability (USN-15-1)

Ubuntu 4.10 : mailman vulnerabilities (USN-59-1)

Ubuntu 4.10 : mailman vulnerabilities (USN-78-1)

Ubuntu 4.10 : mailman vulnerabilities (USN-78-2)

Ubuntu 4.10 : mozilla-firefox vulnerabilities (USN-149-3)

Ubuntu 4.10 : mozilla-firefox vulnerabilities (USN-186-2)

Ubuntu 4.10 : mysql-dfsg vulnerabilities (USN-32-1)

Ubuntu 4.10 : mysql-dfsg vulnerabilities (USN-96-1)

Ubuntu 4.10 : mysql-dfsg vulnerability (USN-109-1)

Ubuntu 4.10 : mysql-dfsg vulnerability (USN-63-1)

Ubuntu 4.10 : nasm vulnerability (USN-45-1)

Ubuntu 4.10 : netkit-telnet vulnerabilities (USN-101-1)

Ubuntu 4.10 : nfs-utils vulnerability (USN-36-1)

Ubuntu 4.10 : ntp vulnerability (USN-175-1)

Ubuntu 4.10 : openslp vulnerabilities (USN-98-1)

Ubuntu 4.10 : openssh information leakage (USN-34-1)

Ubuntu 4.10 : openssl script vulnerability (USN-24-1)

Ubuntu 4.10 : passwd vulnerabilities (USN-17-1)

Ubuntu 4.10 : perl vulnerabilities (USN-16-1)

Ubuntu 4.10 : perl vulnerabilities (USN-44-1)

Ubuntu 4.10 : perl vulnerabilities (USN-72-1)

Ubuntu 4.10 : perl vulnerability (USN-94-1)

Ubuntu 4.10 : php4 vulnerabilities (USN-105-1)

Ubuntu 4.10 : php4 vulnerabilities (USN-112-1)

Ubuntu 4.10 : php4 vulnerabilities (USN-40-1)

Ubuntu 4.10 : php4 vulnerabilities (USN-66-1)

Ubuntu 4.10 : php4 vulnerabilities (USN-99-1)

Ubuntu 4.10 : php4 vulnerabilities (USN-99-2)

Ubuntu 4.10 : php4 vulnerability (USN-66-2)

Ubuntu 4.10 : PNG library vulnerabilities (USN-1-1)

Ubuntu 4.10 : postfix vulnerability (USN-74-1)

Ubuntu 4.10 : postfix vulnerability (USN-74-2)

Ubuntu 4.10 : postgresql contributed script vulnerability (USN-6-1)

Ubuntu 4.10 : postgresql vulnerabilities (USN-79-1)

Ubuntu 4.10 : postgresql vulnerability (USN-71-1)

Ubuntu 4.10 : ppp Denial of Service (USN-12-1)

Ubuntu 4.10 : python2.2, python2.3 vulnerability (USN-73-1)

Ubuntu 4.10 : reportbug information disclosure (USN-88-1)

Ubuntu 4.10 : ruby1.8 vulnerability (USN-20-1)

Ubuntu 4.10 : samba vulnerability (USN-22-1)

Ubuntu 4.10 : samba vulnerability (USN-29-1)

Ubuntu 4.10 : samba vulnerability (USN-41-1)

Ubuntu 4.10 : sharutils vulnerabilities (USN-102-1)

Ubuntu 4.10 : sharutils vulnerability (USN-104-1)

Ubuntu 4.10 : squid vulnerabilities (USN-19-1)

Ubuntu 4.10 : squid vulnerabilities (USN-67-1)

Ubuntu 4.10 : squid vulnerabilities (USN-77-1)

Ubuntu 4.10 : squid vulnerabilities (USN-84-1)

Ubuntu 4.10 : squid vulnerability (USN-111-1)

Ubuntu 4.10 : squid vulnerability (USN-93-1)

Ubuntu 4.10 : Standard C library script vulnerabilities (USN-4-1)

Ubuntu 4.10 : sudo vulnerability (USN-28-1)

Ubuntu 4.10 : tetex-bin vulnerabilities (USN-9-1)

Ubuntu 4.10 : tetex-bin vulnerability (USN-51-1)

Ubuntu 4.10 : tiff vulnerability (USN-46-1)

Ubuntu 4.10 : tiff vulnerability (USN-54-1)

Ubuntu 4.10 : updated enigmail (USN-157-2)

Ubuntu 4.10 : vim vulnerabilities (USN-61-1)

Ubuntu 4.10 : vim vulnerability (USN-52-1)

Ubuntu 4.10 : xfree86 vulnerability (USN-97-1)

Ubuntu 4.10 : xine-lib vulnerabilities (USN-42-1)

Ubuntu 4.10 : XML library vulnerabilities (USN-10-1)

Ubuntu 4.10 : xpdf vulnerabilities (USN-14-1)

Ubuntu 4.10 : xpdf vulnerabilities (USN-2-1)

Ubuntu 4.10 : xpdf, cupsys vulnerabilities (USN-64-1)

Ubuntu 4.10 : xpdf, tetex-bin vulnerabilities (USN-48-1)

Ubuntu 4.10 : zip vulnerability (USN-18-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS / 6.10 : imagemagick vulnerability (USN-372-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS / 6.10 : ruby1.8 vulnerability (USN-371-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS / 6.10 : screen vulnerability (USN-370-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : apache2 vulnerability (USN-328-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : awstats vulnerabilities (USN-360-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : awstats vulnerability (USN-290-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : bind9 vulnerabilities (USN-343-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : binutils vulnerability (USN-292-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : courier vulnerability (USN-294-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : dovecot, exim4, postfix vulnerabilities (USN-288-3)

Ubuntu 5.04 / 5.10 / 6.06 LTS : ffmpeg, xine-lib vulnerabilities (USN-358-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : freetype vulnerabilities (USN-291-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : freetype vulnerability (USN-324-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : gdb vulnerability (USN-356-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : gimp vulnerability (USN-312-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : gnupg vulnerability (USN-304-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : gnupg vulnerability (USN-332-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : gnutls11, gnutls12 vulnerability (USN-348-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : gzip vulnerabilities (USN-349-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : heartbeat vulnerability (USN-326-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : heartbeat vulnerability (USN-335-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : imagemagick vulnerabilities (USN-340-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : imagemagick vulnerability (USN-337-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : kdebase vulnerability (USN-301-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : kdelibs vulnerability (USN-322-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : krb5 vulnerabilities (USN-334-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : libgd2 vulnerability (USN-298-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : libmms, xine-lib vulnerabilities (USN-315-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : libmusicbrainz-2.0, libmusicbrainz-2.1 vulnerability (USN-363-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : libtunepimp vulnerability (USN-318-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : libwmf vulnerability (USN-333-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : libxfont, xorg vulnerabilities (USN-344-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : libxfont, xorg vulnerability (USN-341-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : linux-source-2.6.10/-2.6.12/-2.6.15 vulnerabilities (USN-311-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : linux-source-2.6.10/-2.6.12/-2.6.15 vulnerabilities (USN-346-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : linux-source-2.6.10/-2.6.12/-2.6.15 vulnerabilities (USN-347-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : linux-source-2.6.10/2.6.12/2.6.15 vulnerabilities (USN-302-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : mailman vulnerabilities (USN-345-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : mutt vulnerability (USN-307-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : openldap2, openldap2.2 vulnerability (USN-305-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : openssh vulnerabilities (USN-355-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : openssl vulnerabilities (USN-353-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : openssl vulnerability (USN-339-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : openssl vulnerability (USN-353-2)

Ubuntu 5.04 / 5.10 / 6.06 LTS : php4, php5 vulnerabilities (USN-320-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : php4, php5 vulnerabilities (USN-342-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : php4, php5 vulnerabilities (USN-362-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : python2.3, python2.4 vulnerability (USN-359-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : qt-x11-free vulnerability (USN-368-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : ruby1.8 vulnerability (USN-325-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : samba vulnerability (USN-314-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : shadow vulnerability (USN-308-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : tiff vulnerabilities (USN-289-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : tiff vulnerabilities (USN-330-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : wv2 vulnerability (USN-300-1)

Ubuntu 5.04 / 5.10 / 6.06 LTS : xine-lib vulnerability (USN-295-1)

Ubuntu 5.04 / 5.10 : awstats vulnerability (USN-285-1)

Ubuntu 5.04 / 5.10 : binutils vulnerability (USN-336-1)

Ubuntu 5.04 / 5.10 : dia vulnerabilities (USN-286-1)

Ubuntu 5.04 / 5.10 : firefox, mozilla-firefox vulnerabilities (USN-296-2)

Ubuntu 5.04 / 5.10 : gdm vulnerabilitiy (USN-278-1)

Ubuntu 5.04 / 5.10 : kaffeine vulnerability (USN-268-1)

Ubuntu 5.04 / 5.10 : kdegraphics, koffice vulnerabilities (USN-236-2)

Ubuntu 5.04 / 5.10 : kdelibs vulnerability (USN-245-1)

Ubuntu 5.04 / 5.10 : libnasl vulnerability (USN-279-1)

Ubuntu 5.04 / 5.10 : linux-source-2.6.10, linux-source-2.6.12 vulnerabilities (USN-281-1)

Ubuntu 5.04 / 5.10 : linux-source-2.6.10, linux-source-2.6.12 vulnerability (USN-319-2)

Ubuntu 5.04 / 5.10 : mozilla vulnerabilities (USN-323-1)

Ubuntu 5.04 / 5.10 : mozilla vulnerabilities (USN-361-1)

Ubuntu 5.04 / 5.10 : mozilla-thunderbird vulnerabilities (USN-276-1)

Ubuntu 5.04 / 5.10 : mozilla-thunderbird vulnerabilities (USN-297-3)

Ubuntu 5.04 / 5.10 : mysql-dfsg vulnerability (USN-274-2)

Ubuntu 5.04 / 5.10 : mysql-dfsg-4.1, mysql-dfsg vulnerabilities (USN-283-1)

Ubuntu 5.04 / 5.10 : nagios vulnerability (USN-282-1)

Ubuntu 5.04 / 5.10 : nagios vulnerability (USN-287-1)

Ubuntu 5.04 / 5.10 : postgresql-7.4/-8.0, postgresql, psycopg, (USN-288-1)

Ubuntu 5.04 / 5.10 : quagga vulnerabilities (USN-284-1)

Ubuntu 5.04 / 5.10 : tar vulnerability (USN-257-1)

Ubuntu 5.04 / 5.10 : texinfo regression bug fix (USN-194-2)

Ubuntu 5.04 / 5.10 : tiff vulnerabilities (USN-277-1)

Ubuntu 5.04 / 5.10 : xorg vulnerability (USN-280-1)

Ubuntu 5.04 / 6.06 LTS : openoffice.org-amd64, openoffice.org vulnerabilities (USN-313-1)

Ubuntu 5.04 : awstats vulnerability (USN-167-1)

Ubuntu 5.04 : courier vulnerability (USN-174-1)

Ubuntu 5.04 : dia vulnerability (USN-193-1)

Ubuntu 5.04 : ekg vulnerabilities (USN-162-1)

Ubuntu 5.04 : ffmpeg vulnerability (USN-230-1)

Ubuntu 5.04 : graphviz vulnerability (USN-208-1)

Ubuntu 5.04 : inkscape vulnerability (USN-223-1)

Ubuntu 5.04 : kdebase vulnerability (USN-176-1)

Ubuntu 5.04 : kdelibs fixed packages (USN-114-2)

Ubuntu 5.04 : kdelibs vulnerability (USN-114-1)

Ubuntu 5.04 : kdelibs vulnerability (USN-150-1)

Ubuntu 5.04 : kdewebdev vulnerability (USN-115-1)

Ubuntu 5.04 : koffice vulnerability (USN-202-1)

Ubuntu 5.04 : libksba vulnerability (USN-365-1)

Ubuntu 5.04 : libnet-ssleay-perl vulnerability (USN-113-1)

Ubuntu 5.04 : lm-sensors vulnerabilities (USN-172-1)

Ubuntu 5.04 : mozilla-firefox bug fix (USN-124-2)

Ubuntu 5.04 : mozilla-firefox regressions (USN-149-2)

Ubuntu 5.04 : mozilla-firefox vulnerabilities (USN-134-1)

Ubuntu 5.04 : mozilla-firefox vulnerabilities (USN-149-1)

Ubuntu 5.04 : mozilla-firefox, mozilla vulnerabilities (USN-124-1)

Ubuntu 5.04 : mozilla-locale-... updates (USN-155-3)

Ubuntu 5.04 : php4 regression (USN-320-2)

Ubuntu 5.04 : pike7.6 vulnerability (USN-367-1)

Ubuntu 5.04 : wget bug fix (USN-145-2)

Ubuntu 5.10 / 6.06 LTS / 6.10 : avahi regression (USN-380-2)

Ubuntu 5.10 / 6.06 LTS / 6.10 : avahi vulnerability (USN-380-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : avahi vulnerability (USN-402-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : bind9 vulnerabilities (USN-418-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : dbus vulnerability (USN-401-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : ekiga, gnomemeeting vulnerabilities (USN-426-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : ekiga, gnomemeeting vulnerability (USN-434-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : enigmail vulnerability (USN-427-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : evince vulnerability (USN-390-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : evince vulnerability (USN-390-2)

Ubuntu 5.10 / 6.06 LTS / 6.10 : fetchmail vulnerability (USN-405-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : file vulnerability (USN-439-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : firefox vulnerabilities (USN-428-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : firefox vulnerability (USN-443-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : freetype, libxfont, xorg, xorg-server vulnerabilities (USN-448-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : geoip vulnerability (USN-412-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (USN-389-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (USN-393-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : gnupg vulnerability (USN-432-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : gtk+2.0 vulnerability (USN-415-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : imagemagick vulnerabilities (USN-422-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : imlib2 regression fix (USN-376-2)

Ubuntu 5.10 / 6.06 LTS / 6.10 : imlib2 vulnerabilities (USN-376-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : inkscape vulnerability (USN-438-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : ipsec-tools vulnerability (USN-450-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : kdegraphics, koffice, poppler vulnerability (USN-410-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : kdelibs vulnerabilities (USN-447-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : kdelibs vulnerability (USN-420-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : kdelibs, qt-x11-free vulnerability (USN-452-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : kdenetwork vulnerability (USN-409-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : krb5 vulnerabilities (USN-449-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : libgsf vulnerability (USN-391-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : libgtop2 vulnerability (USN-407-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : libpng vulnerability (USN-383-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : libsoup vulnerability (USN-411-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : libwpd vulnerability (USN-437-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : linux-source-2.6.12/-2.6.15/-2.6.17 vulnerabilities (USN-395-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : linux-source-2.6.12/2.6.15/2.6.17 vulnerabilities (USN-416-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : moin, moin1.3 vulnerabilities (USN-423-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : moin, moin1.3 vulnerability (USN-421-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : mozilla-thunderbird vulnerabilities (USN-382-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : mozilla-thunderbird vulnerabilities (USN-400-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : mozilla-thunderbird vulnerabilities (USN-431-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : mutt vulnerabilities (USN-373-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : nas vulnerabilities (USN-446-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : openldap2.2 vulnerability (USN-384-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : openoffice.org(2)/-amd64, ia32-libs-openoffice.org vulnerabilities (USN-444-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 regression (USN-424-2)

Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 vulnerabilities (USN-424-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : php5 vulnerability (USN-375-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : postgresql-7.4/-8.0/-8.1 vulnerabilities (USN-417-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : ruby1.8 vulnerability (USN-394-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : samba vulnerabilities (USN-419-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : tar vulnerability (USN-385-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : tcpdump vulnerability (USN-429-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : texinfo vulnerability (USN-379-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : w3m vulnerabilities (USN-399-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : xine-lib vulnerability (USN-392-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : xine-lib vulnerability (USN-433-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : xine-lib vulnerability (USN-435-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : xmms vulnerabilities (USN-445-1)

Ubuntu 5.10 / 6.06 LTS / 6.10 : xorg, xorg-server vulnerabilities (USN-403-1)

Ubuntu 5.10 / 6.06 LTS : firefox regression (USN-398-4)

Ubuntu 5.10 / 6.06 LTS : firefox vulnerabilities (USN-381-1)

Ubuntu 5.10 / 6.06 LTS : firefox vulnerabilities (USN-398-2)

Ubuntu 5.10 / 6.06 LTS : gdm vulnerability (USN-293-1)

Ubuntu 5.10 / 6.06 LTS : imagemagick vulnerability (USN-386-1)

Ubuntu 5.10 / 6.06 LTS : libapache2-mod-python vulnerability (USN-430-1)

Ubuntu 5.10 / 6.06 LTS : mono vulnerability (USN-357-1)

Ubuntu 5.10 / 6.06 LTS : mysql-dfsg-4.1, mysql-dfsg-5.0 vulnerability (USN-303-1)

Ubuntu 5.10 / 6.06 LTS : openoffice.org/-amd64, openoffice.org2/-amd64 vulnerability (USN-406-1)

Ubuntu 5.10 / 6.06 LTS : ppp vulnerability (USN-310-1)

Ubuntu 5.10 / 6.06 LTS : xinit vulnerability (USN-364-1)

Ubuntu 5.10 : binutils vulnerability (USN-366-1)

Ubuntu 5.10 : blender vulnerability (USN-238-1)

Ubuntu 5.10 : blender vulnerability (USN-238-2)

Ubuntu 5.10 : bluez-utils vulnerability (USN-413-1)

Ubuntu 5.10 : bogofilter vulnerability (USN-240-1)

Ubuntu 5.10 : inkscape vulnerability (USN-217-1)

Ubuntu 5.10 : irssi-text vulnerability (USN-259-1)

Ubuntu 5.10 : koffice vulnerability (USN-388-1)

Ubuntu 5.10 : libcairo vulnerability (USN-265-1)

Ubuntu 5.10 : libmms vulnerability (USN-309-1)

Ubuntu 5.10 : linux-source-2.6.12 vulnerability (USN-250-1)

Ubuntu 5.10 : mozilla-thunderbird vulnerabilities (USN-350-1)

Ubuntu 5.10 : mysql-dfsg-4.1 vulnerability (USN-180-2)

Ubuntu 5.10 : mysql-dfsg-4.1 vulnerability (USN-306-1)

Ubuntu 5.10 : mysql-dfsg-4.1 vulnerability (USN-321-1)

Ubuntu 5.10 : nbd vulnerability (USN-237-1)

Ubuntu 5.10 : openoffice.org2-amd64, openoffice.org2 vulnerabilities (USN-313-2)

Ubuntu 5.10 : tetex-bin vulnerability (USN-410-2)

Ubuntu 5.10 : tuxpaint vulnerability (USN-243-1)

Ubuntu 5.10 : Ubuntu 5.10 installer vulnerability (USN-262-1)

Ubuntu 5.10 : zope2.8 vulnerability (USN-229-1)

Ubuntu 5.10 : zope2.8 vulnerability (USN-317-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : apache2 vulnerabilities (USN-575-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : boost vulnerabilities (USN-570-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : bzip2 vulnerability (USN-590-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : cupsys vulnerabilities (USN-563-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : cupsys vulnerabilities (USN-598-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : cupsys vulnerability (USN-539-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : dhcp vulnerability (USN-531-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : dhcp vulnerability (USN-531-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : dovecot vulnerabilities (USN-593-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : e2fsprogs vulnerability (USN-555-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : evolution vulnerability (USN-583-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : firefox vulnerabilities (USN-535-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : firefox vulnerabilities (USN-546-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : firefox vulnerabilities (USN-576-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : firefox vulnerabilities (USN-592-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : firefox vulnerabilities (USN-602-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : flac vulnerability (USN-540-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : ghostscript, gs-esp, gs-gpl vulnerability (USN-599-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : gnumeric vulnerability (USN-604-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : icu vulnerabilities (USN-591-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : koffice vulnerabilities (USN-542-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : koffice vulnerability (USN-603-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : krb5 vulnerabilities (USN-587-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : libcairo regression (USN-550-3)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : libcairo vulnerability (USN-550-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : libcdio vulnerability (USN-580-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : libgd2 vulnerability (USN-557-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : libpng vulnerabilities (USN-538-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : libxfont, xorg-server vulnerabilities (USN-571-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : libxml2 vulnerability (USN-569-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : mailman vulnerability (USN-586-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : mono vulnerability (USN-553-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : mozilla-thunderbird, thunderbird vulnerabilities (USN-536-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : mozilla-thunderbird, thunderbird vulnerabilities (USN-582-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : mysql-dfsg-5.0 vulnerabilities (USN-559-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : mysql-dfsg-5.0 vulnerabilities (USN-588-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : net-snmp vulnerability (USN-564-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : openldap vulnerabilities (USN-551-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : openldap2.2, openldap2.3 vulnerabilities (USN-584-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : openssh vulnerability (USN-566-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : openssh vulnerability (USN-597-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : openssl vulnerability (USN-534-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : pcre3 vulnerabilities (USN-547-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : pcre3 vulnerability (USN-581-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : perl vulnerability (USN-552-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : php5 vulnerabilities (USN-549-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : poppler vulnerabilities (USN-542-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : poppler vulnerability (USN-603-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : postgresql vulnerabilities (USN-568-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : pwlib vulnerability (USN-561-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : python2.4/2.5 vulnerabilities (USN-585-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : ruby1.8 vulnerabilities (USN-596-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : samba regression (USN-544-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : samba vulnerabilities (USN-544-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : samba vulnerability (USN-556-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : sdl-image1.2 vulnerabilities (USN-595-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : squid vulnerability (USN-565-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : squid vulnerability (USN-601-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : tetex-bin, texlive-bin vulnerabilities (USN-554-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : tomboy vulnerability (USN-560-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : unzip vulnerability (USN-589-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 / 7.10 : xorg-server regression (USN-571-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 : apache2 vulnerabilities (USN-499-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : bind9 vulnerability (USN-491-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : curl vulnerability (USN-484-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : debian-goodies vulnerability (USN-526-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : dovecot vulnerability (USN-487-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : elinks vulnerability (USN-457-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : elinks vulnerability (USN-519-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : emacs21 vulnerability (USN-504-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : enigmail regression (USN-469-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 : evolution-data-server vulnerability (USN-475-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : fetchmail vulnerabilities (USN-520-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : file vulnerability (USN-439-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 : firefox vulnerabilities (USN-468-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : firefox vulnerabilities (USN-490-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : firefox vulnerabilities (USN-493-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : freetype vulnerability (USN-466-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : gimp vulnerability (USN-467-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : gimp vulnerability (USN-480-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : gimp vulnerability (USN-494-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : imagemagick vulnerabilities (USN-481-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : imagemagick vulnerabilities (USN-523-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : jasper vulnerability (USN-501-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : kdebase vulnerability (USN-517-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : kdebase, kdelibs vulnerabilities (USN-502-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : koffice vulnerability (USN-496-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : krb5 vulnerabilities (USN-477-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : krb5, librpcsecgss vulnerability (USN-511-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : krb5, librpcsecgss vulnerability (USN-511-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 : ktorrent vulnerability (USN-436-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 : libapache2-mod-perl2 vulnerability (USN-488-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : libexif vulnerability (USN-471-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : libexif vulnerability (USN-478-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : libgd2 vulnerabilities (USN-473-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : libpng vulnerability (USN-472-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : libsndfile vulnerability (USN-525-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : libvorbis vulnerabilities (USN-498-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : linux-restricted-modules-2.6.15/.17/.20 vulnerabilities (USN-479-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : linux-restricted-modules-2.6.17/20, vmware-player-kernel-2.6.15 vulnerabilities (USN-543-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : linux-source-2.6.15, linux-source-2.6.17, linux-source-2.6.20 vulnerabilities (USN-518-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : linux-source-2.6.15/2.6.17/2.6.20 vulnerabilities (USN-464-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : moin vulnerabilities (USN-458-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : mozilla-thunderbird (USN-582-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 : mozilla-thunderbird vulnerabilities (USN-469-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : mozilla-thunderbird vulnerabilities (USN-503-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : mysql-dfsg-5.0 vulnerabilities (USN-528-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : opal vulnerability (USN-562-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : openoffice.org(2)/-amd64 vulnerability (USN-482-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : openoffice.org/-amd64 vulnerability (USN-524-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : openssl vulnerabilities (USN-522-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : php5 vulnerabilities (USN-455-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : php5 vulnerabilities (USN-462-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : php5 vulnerabilities (USN-485-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : poppler vulnerability (USN-496-2)

Ubuntu 6.06 LTS / 6.10 / 7.04 : postgresql-8.1, postgresql-8.2 vulnerability (USN-454-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : pptpd vulnerability (USN-459-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : qt-x11-free vulnerability (USN-495-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : qt-x11-free vulnerability (USN-513-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : quagga vulnerability (USN-461-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : quagga vulnerability (USN-512-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : rsync vulnerability (USN-500-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : samba vulnerabilities (USN-460-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : t1lib vulnerability (USN-515-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : tar vulnerability (USN-506-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : tcpdump vulnerability (USN-492-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : tk8.3, tk8.4 vulnerability (USN-529-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : util-linux vulnerability (USN-533-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : vim vulnerability (USN-505-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : xfce4-terminal vulnerability (USN-497-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : xfsdump vulnerability (USN-516-1)

Ubuntu 6.06 LTS / 6.10 / 7.04 : xscreensaver vulnerability (USN-474-1)

Ubuntu 6.06 LTS / 6.10 : dovecot vulnerability (USN-387-1)

Ubuntu 6.06 LTS / 6.10 : evince-gtk vulnerability (USN-390-3)

Ubuntu 6.06 LTS / 6.10 : evolution vulnerability (USN-442-1)

Ubuntu 6.06 LTS / 6.10 : gdm vulnerability (USN-396-1)

Ubuntu 6.06 LTS / 6.10 : gnupg2, gpgme1.0 vulnerability (USN-432-2)

Ubuntu 6.06 LTS / 6.10 : krb5 vulnerability (USN-408-1)

Ubuntu 6.06 LTS / 6.10 : ktorrent vulnerabilities (USN-436-1)

Ubuntu 6.06 LTS / 6.10 : libmodplug vulnerability (USN-521-1)

Ubuntu 6.06 LTS / 6.10 : libnet-dns-perl vulnerabilities (USN-483-1)

Ubuntu 6.06 LTS / 6.10 : libnet-dns-perl vulnerability (USN-594-1)

Ubuntu 6.06 LTS / 6.10 : libx11 vulnerability (USN-453-1)

Ubuntu 6.06 LTS / 6.10 : linux-restricted-modules-2.6.15, linux-restricted-modules-2.6.17 vulnerability (USN-377-1)

Ubuntu 6.06 LTS / 6.10 : linux-source-2.6.15/2.6.17 vulnerabilities (USN-451-1)

Ubuntu 6.06 LTS / 6.10 : mono vulnerability (USN-397-1)

Ubuntu 6.06 LTS / 6.10 : mysql-dfsg-5.0 vulnerability (USN-440-1)

Ubuntu 6.06 LTS / 6.10 : postgresql-8.1 regression (USN-417-2)

Ubuntu 6.06 LTS / 6.10 : postgresql-8.1 regression (USN-417-3)

Ubuntu 6.06 LTS / 6.10 : rdesktop regression (USN-453-2)

Ubuntu 6.06 LTS / 6.10 : rpm vulnerability (USN-378-1)

Ubuntu 6.06 LTS / 6.10 : slocate vulnerability (USN-425-1)

Ubuntu 6.06 LTS / 6.10 : squid vulnerabilities (USN-414-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : bind9 vulnerability (USN-622-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : cupsys vulnerabilities (USN-656-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : dbus vulnerabilities (USN-653-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : emacs21, emacs22 vulnerabilities (USN-607-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : evolution vulnerabilities (USN-615-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : freetype vulnerabilities (USN-643-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gnutls12, gnutls13 vulnerabilities (USN-613-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : gst-plugins-good0.10 vulnerability (USN-611-3)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : ipsec-tools vulnerabilities (USN-641-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerabilities (USN-644-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxml2 vulnerability (USN-640-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : libxslt vulnerabilities (USN-633-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-625-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/20/22 vulnerabilities (USN-637-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : mozilla-thunderbird, thunderbird vulnerabilities (USN-605-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : mozilla-thunderbird, thunderbird vulnerabilities (USN-629-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : mozilla-thunderbird, thunderbird vulnerabilities (USN-647-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : openldap2.2, openldap2.3 vulnerability (USN-634-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : openssl-blacklist update (USN-612-11)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : openssl-blacklist update (USN-612-8)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : openssl-blacklist update (USN-612-9)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : pcre3 vulnerability (USN-624-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : php5 vulnerabilities (USN-628-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : postfix vulnerability (USN-636-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : python2.4, python2.5 vulnerabilities (USN-632-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : rdesktop vulnerabilities (USN-646-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : ruby1.8 vulnerabilities (USN-621-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : ruby1.8 vulnerabilities (USN-651-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : samba regression (USN-617-2)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : samba vulnerabilities (USN-617-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : speex vulnerability (USN-611-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : tiff vulnerability (USN-639-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : vorbis-tools vulnerability (USN-611-2)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : xine-lib vulnerabilities (USN-635-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 / 8.04 LTS : xorg-server vulnerabilities (USN-616-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : cpio vulnerability (USN-650-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : cupsys vulnerability (USN-606-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : firefox vulnerabilities (USN-619-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : firefox vulnerabilities (USN-623-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : hsqldb, openoffice.org/-amd64 vulnerabilities (USN-609-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : libexif vulnerabilities (USN-654-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : linux-source-2.6.15/20/22 vulnerabilities (USN-618-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : ltsp vulnerability (USN-610-1)

Ubuntu 6.06 LTS / 7.04 / 7.10 : openssh vulnerabilities (USN-649-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : avahi vulnerabilities (USN-696-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : awstats vulnerability (USN-686-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : bind9 vulnerability (USN-706-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : cups, cupsys vulnerabilities (USN-707-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : cups, cupsys vulnerability (USN-760-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : curl vulnerability (USN-726-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : ekg, libgadu vulnerability (USN-692-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : enscript vulnerability (USN-660-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : firefox, firefox-3.0, xulrunner-1.9 vulnerabilities (USN-667-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : firefox, firefox-3.0, xulrunner-1.9 vulnerabilities (USN-745-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : ghostscript, gs-gpl vulnerabilities (USN-743-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : git-core vulnerabilities (USN-723-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : gnutls12, gnutls13, gnutls26 regression (USN-678-2)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : gnutls12, gnutls13, gnutls26 vulnerability (USN-678-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : icu vulnerability (USN-747-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : imlib2 vulnerability (USN-683-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : jasper vulnerabilities (USN-742-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : kdepim vulnerability (USN-725-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : krb5 vulnerabilities (USN-755-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : lcms vulnerabilities (USN-744-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libarchive-tar-perl, perl vulnerabilities (USN-700-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libpng vulnerabilities (USN-730-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libsndfile vulnerability (USN-749-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : libxml2 vulnerabilities (USN-673-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.15/22 vulnerabilities (USN-679-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : moin vulnerabilities (USN-716-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : mozilla-thunderbird, thunderbird vulnerabilities (USN-668-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : mozilla-thunderbird, thunderbird vulnerabilities (USN-741-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : net-snmp vulnerabilities (USN-685-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : nfs-utils vulnerability (USN-687-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : nss, firefox vulnerability (USN-740-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : ntp vulnerability (USN-705-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : openoffice.org, openoffice.org-amd64 vulnerabilities (USN-677-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : openssl vulnerability (USN-704-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : openssl vulnerability (USN-750-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : php5 vulnerabilities (USN-720-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : python-crypto vulnerability (USN-729-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : shadow vulnerability (USN-695-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : udev vulnerabilities (USN-758-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : vim vulnerabilities (USN-712-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : vm-builder vulnerability (USN-670-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : xine-lib vulnerabilities (USN-710-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : xine-lib vulnerability (USN-746-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS / 8.10 : xterm vulnerabilities (USN-703-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : apache2 vulnerabilities (USN-731-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : hplip vulnerabilities (USN-674-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : imlib2 vulnerability (USN-697-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : libvorbis vulnerabilities (USN-682-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux, linux-source-2.6.15/22 vulnerabilities (USN-659-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : linux-source-2.6.15/22, linux vulnerabilities (USN-714-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : mysql-dfsg-5.0 vulnerabilities (USN-671-1)

Ubuntu 6.06 LTS / 7.10 / 8.04 LTS : tk8.0, tk8.3, tk8.4 vulnerability (USN-664-1)

Ubuntu 6.06 LTS / 7.10 : evolution-data-server vulnerability (USN-733-1)

Ubuntu 6.06 LTS / 7.10 : gnome-screensaver vulnerabilities (USN-669-1)

Ubuntu 6.06 LTS / 7.10 : imagemagick vulnerability (USN-681-1)

Ubuntu 6.06 LTS / 7.10 : libsoup vulnerability (USN-737-1)

Ubuntu 6.06 LTS / 7.10 : netpbm-free vulnerability (USN-665-1)

Ubuntu 6.06 LTS / 7.10 : tar vulnerability (USN-709-1)

Ubuntu 6.06 LTS / 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apache2, apr vulnerabilities (USN-1134-1)

Ubuntu 6.06 LTS / 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : perl vulnerabilities (USN-1129-1)

Ubuntu 6.06 LTS / 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : postfix vulnerability (USN-1131-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : apache2 vulnerabilities (USN-860-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : apache2 vulnerabilities (USN-908-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : audiofile vulnerability (USN-912-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : bind9 vulnerabilities (USN-888-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : bind9 vulnerability (USN-865-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : cups, cupsys vulnerabilities (USN-906-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : cups, cupsys vulnerability (USN-856-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : dpkg vulnerability (USN-909-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : expat vulnerabilities (USN-890-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : fuse vulnerability (USN-892-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : gzip vulnerabilities (USN-889-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : krb5 vulnerability (USN-881-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : libgd2 vulnerabilities (USN-854-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : libhtml-parser-perl vulnerability (USN-855-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : libpng vulnerabilities (USN-913-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : lintian vulnerabilities (USN-891-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-864-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-894-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : linux, linux-source-2.6.15 vulnerabilities (USN-914-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : moin vulnerabilities (USN-911-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : moin vulnerabilities (USN-925-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-897-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : ntp vulnerability (USN-867-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : openssl vulnerability (USN-884-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : php5 vulnerabilities (USN-862-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : php5 vulnerabilities (USN-882-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerabilities (USN-876-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : python2.4 vulnerabilities (USN-890-3)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : samba vulnerability (USN-893-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : samba vulnerability (USN-918-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : squid vulnerabilities (USN-901-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : sudo vulnerabilities (USN-905-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 / 9.10 : sudo vulnerability (USN-928-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : acpid vulnerability (USN-766-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 regression (USN-802-2)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 vulnerabilities (USN-787-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : apache2 vulnerabilities (USN-802-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : bind9 vulnerability (USN-808-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : cron vulnerability (USN-778-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : cups, cupsys vulnerability (USN-780-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : curl vulnerability (USN-818-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : cyrus-sasl2 vulnerability (USN-790-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dbus vulnerability (USN-799-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : dhcp3 vulnerability (USN-803-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : fetchmail vulnerability (USN-816-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : freetype vulnerability (USN-767-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : gnutls12, gnutls13, gnutls26 vulnerabilities (USN-809-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : gst-plugins-good0.10 vulnerability (USN-789-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : imagemagick vulnerability (USN-784-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : ipsec-tools vulnerabilities (USN-785-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : irssi vulnerability (USN-800-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libmodplug vulnerabilities (USN-771-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libwmf vulnerability (USN-769-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : libxml2 vulnerabilities (USN-815-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-793-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-807-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerabilities (USN-852-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : linux, linux-source-2.6.15 vulnerability (USN-819-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : neon, neon27 vulnerabilities (USN-835-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : newt vulnerability (USN-837-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : ntp vulnerabilities (USN-777-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : openssl vulnerabilities (USN-792-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : openssl vulnerability (USN-830-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : php5 vulnerability (USN-824-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : poppler regression (USN-850-2)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : poppler vulnerabilities (USN-850-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : postgresql-8.1, postgresql-8.3 vulnerabilities (USN-834-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : quagga vulnerability (USN-775-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : ruby1.8, ruby1.9 vulnerabilities (USN-805-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : samba vulnerabilities (USN-839-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : subversion vulnerability (USN-812-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : tiff vulnerability (USN-797-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : tiff vulnerability (USN-801-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : wget vulnerability (USN-842-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 / 9.04 : zope3 vulnerabilities (USN-848-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : apt vulnerabilities (USN-762-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : ghostscript, gs-esp, gs-gpl vulnerabilities (USN-757-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : pango1.0 vulnerability (USN-773-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : php5 vulnerabilities (USN-761-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : poppler vulnerabilities (USN-759-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : postgresql-8.1, postgresql-8.3 vulnerability (USN-753-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : python2.4, python2.5 vulnerabilities (USN-806-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : quagga regression (USN-775-2)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : redhat-cluster, redhat-cluster-suite vulnerabilities (USN-875-1)

Ubuntu 6.06 LTS / 8.04 LTS / 8.10 : xine-lib vulnerabilities (USN-763-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : linux, linux-ec2, linux-source-2.6.15 vulnerabilities (USN-1000-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : openssl vulnerabilities (USN-1003-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : poppler vulnerabilities (USN-1005-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : apache2 vulnerability (USN-990-2)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : bzip2 vulnerability (USN-986-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : cups, cupsys vulnerabilities (USN-952-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : dpkg vulnerability (USN-986-3)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : freetype vulnerabilities (USN-963-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : freetype vulnerabilities (USN-972-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : glibc, eglibc vulnerabilities (USN-944-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libpng vulnerabilities (USN-960-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libwww-perl vulnerability (USN-981-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15 vulnerabilities (USN-947-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-source-2.6.15 vulnerabilities (USN-988-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-{ec2,fsl-imx51,mvl-dove,source-2.6.15,ti-omap} vulnerabilities (USN-974-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : linux, linux-{source-2.6.15,ec2,mvl-dove,ti-omap} vulnerabilities (USN-966-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : lvm2 vulnerability (USN-1001-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : moin vulnerabilities (USN-977-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-950-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : openldap, openldap2.2, openldap2.3 vulnerabilities (USN-965-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : openssl vulnerability (USN-990-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : php5 vulnerabilities (USN-989-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerabilities (USN-942-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-1002-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : samba vulnerability (USN-987-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : sudo vulnerability (USN-956-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : tiff vulnerabilities (USN-954-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : w3m vulnerability (USN-967-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : wget vulnerability (USN-982-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 : krb5 vulnerabilities (USN-940-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-933-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.04 : samba vulnerability (USN-951-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 / 11.04 : php5 regressions (USN-1126-2)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 / 11.04 : php5 vulnerabilities (USN-1126-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : apache2 vulnerabilities (USN-1021-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : awstats vulnerability (USN-1047-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : bind9 vulnerabilities (USN-1025-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : cups, cupsys vulnerability (USN-1012-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : dhcp3 vulnerability (USN-1108-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : exim4 vulnerabilities (USN-1060-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : freetype vulnerabilities (USN-1013-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : krb5 vulnerabilities (USN-1030-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : libxml2 vulnerability (USN-1016-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : linux, linux-{ec2,source-2.6.15} vulnerabilities (USN-1023-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : mailman vulnerabilities (USN-1069-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1017-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openslp, openslp-dfsg vulnerability (USN-1118-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openssl vulnerabilities (USN-1029-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : php5 regression (USN-1042-2)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : php5 vulnerabilities (USN-1042-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : postfix vulnerabilities (USN-1113-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : postgresql-8.1, postgresql-8.3, postgresql-8.4 vulnerability (USN-1058-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : quagga vulnerabilities (USN-1095-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : samba vulnerability (USN-1075-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : subversion vulnerabilities (USN-1053-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : subversion vulnerability (USN-1096-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff regression (USN-1085-2)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff vulnerabilities (USN-1085-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : tiff vulnerability (USN-1102-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : vsftpd vulnerability (USN-1098-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 / 10.04 LTS : quagga vulnerabilities (USN-1027-1)

Ubuntu 6.06 LTS / 8.04 LTS / 9.10 : exim4 vulnerability (USN-1032-1)

Ubuntu 6.06 LTS / 8.10 : network-manager vulnerability (USN-727-2)

Ubuntu 6.06 LTS : apache2 vulnerability (USN-813-2)

Ubuntu 6.06 LTS : blender vulnerabilities (USN-699-1)

Ubuntu 6.06 LTS : devscripts vulnerability (USN-847-2)

Ubuntu 6.06 LTS : dhcdbd vulnerability (USN-299-1)

Ubuntu 6.06 LTS : dovecot regression (USN-288-4)

Ubuntu 6.06 LTS : elinks vulnerabilities (USN-851-1)

Ubuntu 6.06 LTS : firefox regression (USN-327-2)

Ubuntu 6.06 LTS : firefox regression (USN-428-2)

Ubuntu 6.06 LTS : firefox vulnerabilities (USN-296-1)

Ubuntu 6.06 LTS : firefox vulnerabilities (USN-327-1)

Ubuntu 6.06 LTS : firefox vulnerabilities (USN-351-1)

Ubuntu 6.06 LTS : firefox vulnerabilities (USN-645-2)

Ubuntu 6.06 LTS : firefox vulnerabilities (USN-690-3)

Ubuntu 6.06 LTS : firefox vulnerabilities (USN-717-3)

Ubuntu 6.06 LTS : firefox vulnerabilities (USN-728-3)

Ubuntu 6.06 LTS : gaim vulnerabilities (USN-781-2)

Ubuntu 6.06 LTS : gaim vulnerability (USN-675-2)

Ubuntu 6.06 LTS : gnutls12 vulnerability (USN-948-1)

Ubuntu 6.06 LTS : Installer vulnerability (USN-316-1)

Ubuntu 6.06 LTS : lcms vulnerability (USN-652-1)

Ubuntu 6.06 LTS : linux-restricted-modules-2.6.15 regression fix (USN-346-2)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-1057-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-1071-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-1092-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-1111-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-331-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-508-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-578-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerabilities (USN-752-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerability (USN-319-1)

Ubuntu 6.06 LTS : linux-source-2.6.15 vulnerability (USN-489-1)

Ubuntu 6.06 LTS : mozilla-thunderbird vulnerabilities (USN-297-1)

Ubuntu 6.06 LTS : mozilla-thunderbird vulnerabilities (USN-329-1)

Ubuntu 6.06 LTS : mozilla-thunderbird vulnerabilities (USN-352-1)

Ubuntu 6.06 LTS : mozilla-thunderbird vulnerabilities (USN-701-2)

Ubuntu 6.06 LTS : mozilla-thunderbird, thunderbird-quickfile updates (USN-297-2)

Ubuntu 6.06 LTS : mysql-dfsg-5.0 regression (USN-588-2)

Ubuntu 6.06 LTS : mysql-dfsg-5.0 vulnerabilities (USN-338-1)

Ubuntu 6.06 LTS : nagios vulnerability (USN-698-1)

Ubuntu 6.06 LTS : nagios-plugins vulnerability (USN-532-1)

Ubuntu 6.06 LTS : net-snmp vulnerability (USN-456-1)

Ubuntu 6.06 LTS : openldap2.2 vulnerability (USN-858-1)

Ubuntu 6.06 LTS : openssh update (USN-612-7)

Ubuntu 6.06 LTS : postgresql-8.1 vulnerabilities (USN-288-2)

Ubuntu 6.06 LTS : postgresql-8.1 vulnerabilities (USN-369-1)

Ubuntu 6.06 LTS : pptpd vulnerabilities (USN-459-2)

Ubuntu 6.06 LTS : python-xml vulnerabilities (USN-890-4)

Ubuntu 6.06 LTS : redhat-cluster-suite vulnerability (USN-489-2)

Ubuntu 6.06 LTS : xorg-server vulnerability (USN-514-1)

Ubuntu 6.10 / 7.04 / 7.10 : firefox regression (USN-546-2)

Ubuntu 6.10 / 7.04 / 7.10 : ghostscript, gs-gpl vulnerability (USN-501-2)

Ubuntu 6.10 / 7.04 / 7.10 : linux-source-2.6.17/20/22 vulnerabilities (USN-558-1)

Ubuntu 6.10 / 7.04 / 7.10 : linux-source-2.6.17/20/22 vulnerabilities (USN-574-1)

Ubuntu 6.10 / 7.04 / 7.10 : linux-source-2.6.17/20/22 vulnerability (USN-577-1)

Ubuntu 6.10 / 7.04 : hplip vulnerability (USN-530-1)

Ubuntu 6.10 / 7.04 : vim vulnerability (USN-463-1)

Ubuntu 6.10 : firefox vulnerabilities (USN-398-1)

Ubuntu 6.10 : firefox-themes-ubuntu regression (USN-398-3)

Ubuntu 6.10 : gnupg2 vulnerabilities (USN-393-2)

Ubuntu 6.10 : linux-restricted-modules-2.6.17 regression (USN-416-2)

Ubuntu 6.10 : linux-restricted-modules-2.6.17 vulnerability (USN-404-1)

Ubuntu 6.10 : linux-source-2.6.17 vulnerabilities (USN-486-1)

Ubuntu 6.10 : linux-source-2.6.17 vulnerabilities (USN-509-1)

Ubuntu 6.10 : postgresql-8.1 vulnerabilities (USN-369-2)

Ubuntu 6.10 : squid vulnerability (USN-441-1)

Ubuntu 6.10 : wv vulnerability (USN-374-1)

Ubuntu 7.04 / 7.10 / 8.04 LTS : exiv2 vulnerabilities (USN-655-1)

Ubuntu 7.04 / 7.10 / 8.04 LTS : firefox, firefox-3.0, xulrunner-1.9 vulnerabilities (USN-645-1)

Ubuntu 7.04 / 7.10 / 8.04 LTS : kdelibs vulnerability (USN-608-1)

Ubuntu 7.04 / 7.10 / 8.04 LTS : openssh update (USN-612-5)

Ubuntu 7.04 / 7.10 / 8.04 LTS : openssh vulnerability (USN-612-2)

Ubuntu 7.04 / 7.10 / 8.04 LTS : openssl vulnerability (USN-612-1)

Ubuntu 7.04 / 7.10 / 8.04 LTS : openvpn regression (USN-612-10)

Ubuntu 7.04 / 7.10 / 8.04 LTS : openvpn regression (USN-612-6)

Ubuntu 7.04 / 7.10 / 8.04 LTS : openvpn vulnerability (USN-612-3)

Ubuntu 7.04 / 7.10 / 8.04 LTS : ssl-cert vulnerability (USN-612-4)

Ubuntu 7.04 / 7.10 : apt-listchanges vulnerability (USN-572-1)

Ubuntu 7.04 / 7.10 : dovecot vulnerability (USN-567-1)

Ubuntu 7.04 / 7.10 : libcairo regression (USN-550-2)

Ubuntu 7.04 / 7.10 : pulseaudio vulnerability (USN-573-1)

Ubuntu 7.04 / 7.10 : rsync vulnerability (USN-600-1)

Ubuntu 7.04 : linux-source-2.6.20 vulnerabilities (USN-470-1)

Ubuntu 7.04 : linux-source-2.6.20 vulnerabilities (USN-510-1)

Ubuntu 7.04 : pulseaudio vulnerability (USN-465-1)

Ubuntu 7.04 : redhat-cluster-suite vulnerability (USN-476-1)

Ubuntu 7.04 : samba regression (USN-460-2)

Ubuntu 7.04 : tcp-wrappers vulnerability (USN-507-1)

Ubuntu 7.04 : xen-3.0 vulnerability (USN-527-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : amarok vulnerabilities (USN-739-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : compiz-fusion-plugins-main vulnerability (USN-688-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : ffmpeg, ffmpeg-debian vulnerabilities (USN-734-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : glib2.0 vulnerability (USN-738-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : gst-plugins-good0.10 vulnerabilities (USN-736-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : ktorrent vulnerabilities (USN-711-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : libvirt vulnerability (USN-694-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : linux, linux-source-2.6.22 vulnerabilities (USN-751-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : LittleCMS vulnerability (USN-693-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : network-manager-applet vulnerabilities (USN-727-1)

Ubuntu 7.10 / 8.04 LTS / 8.10 : thunderbird vulnerabilities (USN-701-1)

Ubuntu 7.10 / 8.04 LTS : amarok vulnerability (USN-657-1)

Ubuntu 7.10 / 8.04 LTS : ffmpeg vulnerability (USN-630-1)

Ubuntu 7.10 / 8.04 LTS : linux-ubuntu-modules-2.6.22/24 vulnerability (USN-662-2)

Ubuntu 7.10 / 8.04 LTS : moodle vulnerability (USN-658-1)

Ubuntu 7.10 / 8.04 LTS : pidgin vulnerabilities (USN-675-1)

Ubuntu 7.10 / 8.04 LTS : poppler vulnerability (USN-631-1)

Ubuntu 7.10 / 8.04 LTS : postfix vulnerability (USN-642-1)

Ubuntu 7.10 / 8.04 LTS : yelp vulnerability (USN-638-1)

Ubuntu 7.10 : compiz vulnerability (USN-537-2)

Ubuntu 7.10 : emacs22 vulnerability (USN-541-1)

Ubuntu 7.10 : firefox vulnerabilities (USN-690-2)

Ubuntu 7.10 : firefox vulnerabilities (USN-728-2)

Ubuntu 7.10 : firefox-3.0 vulnerabilities (USN-717-2)

Ubuntu 7.10 : gnome-screensaver vulnerability (USN-537-1)

Ubuntu 7.10 : hplip vulnerabilities (USN-674-2)

Ubuntu 7.10 : hplip vulnerability (USN-708-1)

Ubuntu 7.10 : link-grammar vulnerability (USN-545-1)

Ubuntu 7.10 : php5 regression (USN-549-2)

Ubuntu 7.10 : pidgin vulnerability (USN-548-1)

Ubuntu 7.10 : qt4-x11 vulnerability (USN-579-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : apache2 vulnerabilities (USN-1368-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : apache2, apache2-mpm-itk vulnerabilities (USN-1259-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : backuppc vulnerabilites (USN-1249-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : bind9 vulnerability (USN-1264-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : bzip2 vulnerability (USN-1308-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : devscripts vulnerabilities (USN-1366-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : eglibc, glibc vulnerabilities (USN-1396-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : freetype vulnerabilities (USN-1267-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : freetype vulnerabilities (USN-1403-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : gnutls13, gnutls26 vulnerabilities (USN-1418-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerabilities (USN-1367-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerability (USN-1402-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libpng vulnerability (USN-1417-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libxml2 vulnerabilities (USN-1334-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : libxml2 vulnerability (USN-1376-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1397-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : openssl vulnerabilities (USN-1357-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : pam vulnerabilities (USN-1237-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 regression (USN-1358-2)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerabilities (USN-1231-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerabilities (USN-1358-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : php5 vulnerability (USN-1307-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1378-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : tiff vulnerabilities (USN-1416-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : update-manager regression (USN-1284-2)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 / 11.10 : update-manager vulnerabilities (USN-1284-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apache2 vulnerability (USN-1199-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apt vulnerabilities (USN-1215-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : apt vulnerability (USN-1283-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : bind9 vulnerabilities (USN-1139-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : bind9 vulnerability (USN-1163-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : cups, cupsys vulnerabilities (USN-1207-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : curl vulnerabilities (USN-1158-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : dbus vulnerability (USN-1176-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : dhcp3, isc-dhcp vulnerabilities (USN-1190-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : foomatic-filters vulnerabilities (USN-1194-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : libpng vulnerabilities (USN-1175-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : libxml2 vulnerability (USN-1153-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : logrotate vulnerabilities (USN-1172-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : pam regression (USN-1140-2)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : pam vulnerabilities (USN-1140-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : postgresql-8.3, postgresql-8.4 vulnerability (USN-1229-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : samba vulnerabilities (USN-1182-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 / 11.04 : vino vulnerabilities (USN-1128-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 : ghostscript vulnerabilities (USN-1317-1)

Ubuntu 8.04 LTS / 10.04 LTS / 10.10 : nbd vulnerability (USN-1155-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : apt update (USN-1475-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : apt vulnerability (USN-1477-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : backuppc vulnerability (USN-1444-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : bind9 vulnerabilities (USN-1462-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : bind9 vulnerability (USN-1566-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : bind9 vulnerability (USN-1601-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : dbus regressions (USN-1576-2)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : dbus vulnerability (USN-1576-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : eglibc, glibc vulnerabilities (USN-1589-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : expat vulnerabilities (USN-1527-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : gnupg, gnupg2 vulnerability (USN-1570-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libexif vulnerabilities (USN-1513-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libgc vulnerability (USN-1546-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libtasn1-3 vulnerability (USN-1436-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libxml2 vulnerability (USN-1447-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libxml2 vulnerability (USN-1587-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : libxslt vulnerabilities (USN-1595-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : mysql-5.1, mysql-5.5, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1467-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : net-snmp vulnerability (USN-1450-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : openssl vulnerabilities (USN-1451-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : php5 vulnerabilities (USN-1481-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : php5 vulnerabilities (USN-1569-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : php5 vulnerability (USN-1437-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1461-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1542-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : sudo vulnerability (USN-1442-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : tiff vulnerabilities (USN-1498-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 / 12.04 LTS : tiff vulnerability (USN-1511-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities (USN-1427-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : openssl vulnerabilities (USN-1424-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : openssl vulnerability (USN-1428-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.04 / 11.10 : samba vulnerability (USN-1423-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache2 vulnerabilities (USN-1627-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : apache2 vulnerabilities (USN-1765-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : cups, cupsys vulnerability (USN-1654-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : curl vulnerability (USN-1801-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : freetype vulnerabilities (USN-1686-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : gnupg, gnupg2 vulnerability (USN-1682-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : gnutls13, gnutls26 vulnerability (USN-1752-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libxml2 vulnerability (USN-1656-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libxml2 vulnerability (USN-1782-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : libxslt vulnerability (USN-1784-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : openssl vulnerabilities (USN-1732-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : perl vulnerabilities (USN-1643-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : perl vulnerability (USN-1770-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : php5 vulnerability (USN-1761-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : poppler vulnerabilities (USN-1785-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities (USN-1789-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerability (USN-1717-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : sudo vulnerability (USN-1754-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS / 12.10 : tiff vulnerabilities (USN-1631-1)

Ubuntu 8.04 LTS / 10.04 LTS / 11.10 / 12.04 LTS : tiff vulnerability (USN-1655-1)

Ubuntu 8.04 LTS / 10.04 LTS : dbus-glib vulnerability (USN-1138-1)

Ubuntu 8.04 LTS / 10.04 LTS : firefox, firefox-3.0, xulrunner-1.9.2 vulnerabilities (USN-930-1)

Ubuntu 8.04 LTS / 10.04 LTS : firefox, firefox-3.0, xulrunner-1.9.2 vulnerabilities (USN-957-1)

Ubuntu 8.04 LTS / 10.04 LTS : firefox, firefox-3.0, xulrunner-1.9.2 vulnerability (USN-957-2)

Ubuntu 8.04 LTS / 10.04 LTS : ghostscript vulnerability (USN-1581-1)

Ubuntu 8.04 LTS / 10.04 LTS : network-manager, modemmanger update (USN-1138-2)

Ubuntu 8.04 LTS / 10.04 LTS : samba vulnerabilities (USN-1226-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : emacs22, emacs23 vulnerability (USN-919-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : ffmpeg, ffmpeg-debian regression (USN-931-2)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : ffmpeg, ffmpeg-debian vulnerabilities (USN-931-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : firefox-3.0, firefox-3.5, xulrunner-1.9, xulrunner-1.9.1 vulnerabilities (USN-853-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : gimp vulnerabilities (USN-880-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : irssi regression (USN-929-2)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : irssi vulnerabilities (USN-929-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : kdelibs vulnerabilities (USN-871-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : libnss-db vulnerability (USN-922-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : libthai vulnerability (USN-887-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : libvorbis vulnerabilities (USN-861-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : openjdk-6 vulnerabilities (USN-923-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : openoffice.org vulnerabilities (USN-903-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : pidgin vulnerabilities (USN-886-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : pidgin vulnerabilities (USN-902-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : python2.5 vulnerabilities (USN-890-2)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : squid vulnerability (USN-904-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : thunderbird vulnerabilities (USN-915-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 / 9.10 : transmission vulnerabilities (USN-885-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : Apport vulnerability (USN-768-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : apr vulnerability (USN-813-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : apr-util vulnerabilities (USN-786-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : apr-util vulnerability (USN-813-3)

Ubuntu 8.04 LTS / 8.10 / 9.04 : backuppc vulnerability (USN-843-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : cmake vulnerabilities (USN-890-6)

Ubuntu 8.04 LTS / 8.10 / 9.04 : devscripts vulnerability (USN-847-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : dnsmasq vulnerabilities (USN-827-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : dovecot vulnerabilities (USN-838-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 regression (USN-877-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-764-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-765-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-779-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-798-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-821-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-873-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-895-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-920-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : firefox-3.0, xulrunner-1.9 vulnerability (USN-811-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : glib2.0 vulnerability (USN-841-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : icu vulnerability (USN-846-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : kde4libs, kdelibs vulnerabilities (USN-822-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : kde4libs, kdelibs vulnerability (USN-833-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : krb5 vulnerabilities (USN-924-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : libcompress-raw-zlib-perl, perl vulnerability (USN-794-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : libsndfile vulnerabilities (USN-849-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : libvorbis vulnerability (USN-825-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : mimetex vulnerabilities (USN-844-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : mono vulnerabilities (USN-826-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : nagios2, nagios3 vulnerability (USN-795-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : nspr update (USN-810-2)

Ubuntu 8.04 LTS / 8.10 / 9.04 : nss regression (USN-810-3)

Ubuntu 8.04 LTS / 8.10 / 9.04 : nss vulnerabilities (USN-810-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : openexr vulnerabilities (USN-831-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : openoffice.org vulnerabilities (USN-840-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : pidgin vulnerabilities (USN-781-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : pidgin vulnerability (USN-796-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : pidgin vulnerability (USN-820-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : pulseaudio vulnerability (USN-804-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : qt4-x11 vulnerability (USN-829-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : thunderbird vulnerabilities (USN-782-1)

Ubuntu 8.04 LTS / 8.10 / 9.04 : thunderbird vulnerabilities (USN-817-1)

Ubuntu 8.04 LTS / 8.10 : dash vulnerability (USN-732-1)

Ubuntu 8.04 LTS / 8.10 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-690-1)

Ubuntu 8.04 LTS / 8.10 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-717-1)

Ubuntu 8.04 LTS / 8.10 : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-728-1)

Ubuntu 8.04 LTS / 8.10 : kvm vulnerabilities (USN-776-1)

Ubuntu 8.04 LTS / 8.10 : libpam-krb5 vulnerabilities (USN-719-1)

Ubuntu 8.04 LTS / 8.10 : moodle vulnerabilities (USN-791-1)

Ubuntu 8.04 LTS / 8.10 : pygresql vulnerability (USN-870-1)

Ubuntu 8.04 LTS / 8.10 : sudo vulnerability (USN-722-1)

Ubuntu 8.04 LTS / 8.10 : vinagre vulnerability (USN-689-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-3.0, firefox-3.5, xulrunner-1.9.1, xulrunner-1.9.2 vulnerabilities (USN-997-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : glibc, eglibc vulnerabilities (USN-1009-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10 : nss vulnerabilities (USN-1007-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : avahi vulnerabilities (USN-992-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : bogofilter vulnerability (USN-980-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : fastjar vulnerability (USN-953-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : firefox, firefox-3.0, firefox-3.5, xulrunner-1.9.1, xulrunner-1.9.2 regression (USN-975-2)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : firefox, firefox-3.0, firefox-3.5, xulrunner-1.9.1, xulrunner-1.9.2 vulnerabilities (USN-975-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : ghostscript vulnerabilities (USN-961-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : gnupg2 vulnerability (USN-970-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : lftp vulnerability (USN-984-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libgdiplus vulnerability (USN-993-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libhx vulnerability (USN-994-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : libvirt vulnerabilities (USN-1008-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : openoffice.org vulnerability (USN-949-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 / 10.04 LTS : texlive-bin vulnerabilities (USN-937-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 : libmikmod vulnerabilities (USN-995-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 : netpbm-free vulnerability (USN-934-1)

Ubuntu 8.04 LTS / 9.04 / 9.10 : xorg-server vulnerabilities (USN-939-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : apr-util vulnerability (USN-1022-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : avahi vulnerability (USN-1084-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : dbus vulnerability (USN-1044-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : eglibc, glibc vulnerability (USN-1009-2)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : evince vulnerabilities (USN-1035-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : ffmpeg vulnerabilities (USN-1104-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-3.0, firefox-3.5 vulnerability (USN-1011-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-3.0, firefox-3.5, xulrunner-1.9.2 vulnerabilities (USN-1112-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-{3.0,3.5}, xulrunner-1.9.2 regression (USN-1049-2)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-{3.0,3.5}, xulrunner-1.9.2 vulnerabilities (USN-1049-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-{3.0,3.5}, xulrunner-1.9.2 vulnerabilities (USN-1091-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : firefox, firefox-{3.0,3.5}, xulrunner-1.9.{1,2} vulnerabilities (USN-1019-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : fuse vulnerabilities (USN-1077-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : fuse vulnerability (USN-1045-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : gimp vulnerabilities (USN-1109-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : hplip vulnerability (USN-1051-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : imagemagick vulnerability (USN-1028-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : krb5 vulnerabilities (USN-1062-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : lcms vulnerability (USN-1043-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : logwatch vulnerability (USN-1078-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : nss vulnerabilities (USN-1106-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openjdk-6 vulnerability (USN-1024-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openjdk-6, openjdk-6b18 vulnerabilities (USN-1010-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openldap, openldap2.3 vulnerabilities (USN-1100-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openoffice.org vulnerabilities (USN-1056-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : openssl vulnerability (USN-1018-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : pango1.0 vulnerabilities (USN-1082-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : pidgin vulnerabilities (USN-1014-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : qt4-x11 vulnerabilities (USN-1101-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : thunderbird vulnerability (USN-1011-2)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : util-linux update (USN-1045-2)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : x11-xserver-utils vulnerability (USN-1107-1)

Ubuntu 8.04 LTS / 9.10 / 10.04 LTS / 10.10 : xulrunner-1.9.1, xulrunner-1.9.2 vulnerability (USN-1011-3)

Ubuntu 8.04 LTS : apturl, epiphany-browser, gecko-sharp, gnome-python-extras, liferea, rhythmbox, totem, ubufox, yelp update (USN-930-2)

Ubuntu 8.04 LTS : devhelp, epiphany-browser, midbrowser, yelp update (USN-626-2)

Ubuntu 8.04 LTS : dnsmasq vulnerability (USN-627-1)

Ubuntu 8.04 LTS : firefox regression (USN-930-3)

Ubuntu 8.04 LTS : firefox-3.0, xulrunner-1.9 regression (USN-645-3)

Ubuntu 8.04 LTS : firefox-3.0, xulrunner-1.9 vulnerabilities (USN-626-1)

Ubuntu 8.04 LTS : freeradius vulnerability (USN-832-1)

Ubuntu 8.04 LTS : glibc regression (USN-1589-2)

Ubuntu 8.04 LTS : kdegraphics vulnerabilities (USN-823-1)

Ubuntu 8.04 LTS : kvm regression (USN-776-2)

Ubuntu 8.04 LTS : linux regression (USN-974-2)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1072-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1105-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1133-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1146-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1170-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1186-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1189-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1225-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1236-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1268-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1291-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1323-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1390-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1493-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-1507-1)

Ubuntu 8.04 LTS : linux vulnerabilities (USN-614-1)

Ubuntu 8.04 LTS : linux vulnerability (USN-1454-1)

Ubuntu 8.04 LTS : linux vulnerability (USN-1598-1)

Ubuntu 8.04 LTS : linux vulnerability (USN-1650-1)

Ubuntu 8.04 LTS : linux vulnerability (USN-1660-1)

Ubuntu 8.04 LTS : nagios2 vulnerabilities (USN-698-3)

Ubuntu 8.04 LTS : nasm vulnerability (USN-648-1)

Ubuntu 8.04 LTS : nspr update (USN-927-5)

Ubuntu 8.04 LTS : nss vulnerability (USN-927-4)

Ubuntu 8.04 LTS : open-iscsi vulnerability (USN-1235-1)

Ubuntu 8.04 LTS : openoffice.org-l10n update (USN-677-2)

Ubuntu 8.04 LTS : openssl vulnerabilities (USN-620-1)

Ubuntu 8.04 LTS : pan vulnerability (USN-845-1)

Ubuntu 8.04 LTS : perl regression (USN-700-2)

Ubuntu 8.04 LTS : python2.4 vulnerabilities (USN-1613-2)

Ubuntu 8.04 LTS : python2.5 vulnerabilities (USN-1613-1)

Ubuntu 8.04 LTS : samba vulnerability (USN-1374-1)

Ubuntu 8.10 / 9.04 / 9.10 : clamav vulnerabilities (USN-926-1)

Ubuntu 8.10 / 9.04 / 9.10 : dhcp3 vulnerability (USN-803-2)

Ubuntu 8.10 / 9.04 / 9.10 : gnome-screensaver vulnerabilities (USN-907-1)

Ubuntu 8.10 / 9.04 / 9.10 : kde4libs vulnerabilities (USN-871-2)

Ubuntu 8.10 / 9.04 / 9.10 : kdebase-runtime vulnerabilities (USN-872-1)

Ubuntu 8.10 / 9.04 / 9.10 : kdebase-workspace vulnerability (USN-932-1)

Ubuntu 8.10 / 9.04 / 9.10 : openjdk-6 vulnerabilities (USN-859-1)

Ubuntu 8.10 / 9.04 / 9.10 : ruby1.9 vulnerabilities (USN-900-1)

Ubuntu 8.10 / 9.04 / 9.10 : tomcat6 vulnerabilities (USN-899-1)

Ubuntu 8.10 / 9.04 : moin vulnerability (USN-774-1)

Ubuntu 8.10 / 9.04 : network-manager-applet vulnerabilities (USN-883-1)

Ubuntu 8.10 / 9.04 : openjdk-6 vulnerabilities (USN-814-1)

Ubuntu 8.10 / 9.04 : pam vulnerability (USN-828-1)

Ubuntu 8.10 / 9.04 : qt4-x11 vulnerabilities (USN-857-1)

Ubuntu 8.10 / 9.04 : tomcat6 vulnerabilities (USN-788-1)

Ubuntu 8.10 / 9.04 : webkit vulnerabilities (USN-836-1)

Ubuntu 8.10 : clamav vulnerabilities (USN-754-1)

Ubuntu 8.10 : clamav vulnerability (USN-672-1)

Ubuntu 8.10 : clamav vulnerability (USN-684-1)

Ubuntu 8.10 : clamav vulnerability (USN-756-1)

Ubuntu 8.10 : curl regression (USN-726-2)

Ubuntu 8.10 : dovecot vulnerability (USN-666-1)

Ubuntu 8.10 : fglrx-installer vulnerability (USN-721-1)

Ubuntu 8.10 : gst-plugins-base0.10 vulnerability (USN-735-1)

Ubuntu 8.10 : linux regression (USN-661-1)

Ubuntu 8.10 : linux vulnerabilities (USN-715-1)

Ubuntu 8.10 : linux vulnerability (USN-662-1)

Ubuntu 8.10 : nagios3 vulnerabilities (USN-698-2)

Ubuntu 8.10 : OpenJDK vulnerabilities (USN-713-1)

Ubuntu 8.10 : openjdk-6 vulnerabilities (USN-748-1)

Ubuntu 8.10 : ruby1.9 vulnerability (USN-691-1)

Ubuntu 8.10 : samba vulnerability (USN-680-1)

Ubuntu 8.10 : samba vulnerability (USN-702-1)

Ubuntu 8.10 : squid vulnerability (USN-724-1)

Ubuntu 8.10 : system-tools-backends regression (USN-663-1)

Ubuntu 8.10 : webkit vulnerability (USN-676-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : clamav vulnerabilities (USN-945-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : clamav vulnerability (USN-986-2)

Ubuntu 9.04 / 9.10 / 10.04 LTS : dvipng vulnerability (USN-936-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : kdegraphics vulnerability (USN-979-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : kdenetwork vulnerabilities (USN-938-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : libpam-opie vulnerability (USN-955-2)

Ubuntu 9.04 / 9.10 / 10.04 LTS : openjdk-6 vulnerabilities (USN-971-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : opie vulnerability (USN-955-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : pcsc-lite vulnerability (USN-969-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : quassel vulnerability (USN-991-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : tomcat6 vulnerability (USN-976-1)

Ubuntu 9.04 / 9.10 / 10.04 LTS : vte vulnerability (USN-962-1)

Ubuntu 9.04 / 9.10 : ant, apturl, epiphany-browser, gluezilla, gnome-python-extras, liferea, mozvoikko, openjdk-6, packagekit, ubufox, webfav, yelp update (USN-930-5)

Ubuntu 9.04 / 9.10 : firefox, firefox-3.0, xulrunner-1.9.2 vulnerability (USN-930-6)

Ubuntu 9.04 / 9.10 : firefox-3.0, firefox-3.5, xulrunner-1.9.2 vulnerabilities (USN-930-4)

Ubuntu 9.04 : clamav vulnerability (USN-770-1)

Ubuntu 9.04 : ecryptfs-utils vulnerability (USN-783-1)

Ubuntu 9.04 : koffice vulnerabilities (USN-973-1)

Ubuntu 9.04 : moin vulnerability (USN-941-1)

Ubuntu 9.04 : moodle vulnerability (USN-791-2)

Ubuntu 9.04 : mpfr vulnerability (USN-772-1)

Ubuntu 9.04 : nspr update (USN-927-7)

Ubuntu 9.04 : nss vulnerability (USN-927-6)

Ubuntu 9.04 : php5 vulnerabilities (USN-761-2)

Ubuntu 9.04 : smarty vulnerability (USN-791-3)

Ubuntu 9.04 : thunderbird update (USN-927-8)

Ubuntu 9.10 / 10.04 LTS / 10.10 : apparmor update (USN-1039-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : clamav vulnerability (USN-1076-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : dhcp3 vulnerability (USN-1108-2)

Ubuntu 9.10 / 10.04 LTS / 10.10 : dpkg vulnerability (USN-1038-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : gdm vulnerability (USN-1099-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : italc vulnerability (USN-1061-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : kde4libs vulnerabilities (USN-1110-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : kdenetwork vulnerability (USN-1114-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : krb5 vulnerability (USN-1088-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : krb5 vulnerability (USN-1116-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : libvirt vulnerability (USN-1094-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : linux, linux-ec2 vulnerabilities (USN-1041-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : openjdk-6 vulnerabilities (USN-1079-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : openjdk-6, openjdk-6b18 vulnerabilities (USN-1055-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : openjdk-6, openjdk-6b18 vulnerability (USN-1052-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : pcsc-lite vulnerability (USN-1125-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : policykit-1 vulnerability (USN-1117-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : python-django vulnerabilities (USN-1040-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : python-django vulnerabilities (USN-1066-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : qemu-kvm vulnerability (USN-1063-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : rsync vulnerability (USN-1124-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : shadow vulnerability (USN-1065-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : sudo vulnerability (USN-1046-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : telepathy-gabble vulnerability (USN-1067-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : tomcat6 vulnerabilities (USN-1097-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : tomcat6 vulnerability (USN-1048-1)

Ubuntu 9.10 / 10.04 LTS / 10.10 : webkit vulnerabilities (USN-1006-1)

Ubuntu 9.10 / 10.04 LTS : base-files vulnerability (USN-968-1)

Ubuntu 9.10 / 10.04 LTS : openjdk-6b18 vulnerabilities (USN-1079-2)

Ubuntu 9.10 / 10.04 LTS : pam vulnerability (USN-959-1)

Ubuntu 9.10 / 10.04 LTS : sudo vulnerability (USN-983-1)

Ubuntu 9.10 : erlang vulnerability (USN-624-2)

Ubuntu 9.10 : firefox-3.5, xulrunner-1.9.1 regression (USN-853-2)

Ubuntu 9.10 : firefox-3.5, xulrunner-1.9.1 regression (USN-878-1)

Ubuntu 9.10 : firefox-3.5, xulrunner-1.9.1 vulnerabilities (USN-874-1)

Ubuntu 9.10 : firefox-3.5, xulrunner-1.9.1 vulnerabilities (USN-896-1)

Ubuntu 9.10 : firefox-3.5, xulrunner-1.9.1 vulnerabilities (USN-921-1)

Ubuntu 9.10 : gnome-screensaver vulnerability (USN-866-1)

Ubuntu 9.10 : gnome-screensaver vulnerability (USN-898-1)

Ubuntu 9.10 : grub2 vulnerability (USN-868-1)

Ubuntu 9.10 : krb5 vulnerabilities (USN-916-1)

Ubuntu 9.10 : krb5 vulnerability (USN-879-1)

Ubuntu 9.10 : linux vulnerability (USN-869-1)

Ubuntu 9.10 : linux, linux-ec2 vulnerabilities (USN-1073-1)

Ubuntu 9.10 : linux, linux-ec2 vulnerabilities (USN-1089-1)

Ubuntu 9.10 : Multiple Xulrunner 1.9.1 vulnerabilities (USN-1123-1)

Ubuntu 9.10 : nss regression (USN-927-2)

Ubuntu 9.10 : nss vulnerability (USN-927-1)

Ubuntu 9.10 : poppler vulnerabilities (USN-850-3)

Ubuntu 9.10 : puppet vulnerabilities (USN-917-1)

Ubuntu 9.10 : qemu-kvm vulnerability (USN-863-1)

Ubuntu 9.10 : thunderbird regression (USN-927-3)

Ubuntu 9.10 : xmlrpc-c vulnerabilities (USN-890-5)

USN-1119-1 : linux-ti-omap4 vulnerabilities

USN-1164-1 : linux-fsl-imx51 vulnerabilities

USN-1202-1 : linux-ti-omap4 vulnerabilities

USN-1204-1 : linux-fsl-imx51 vulnerabilities

USN-1212-1 : linux-ti-omap4 vulnerabilities

USN-1220-1 : linux-ti-omap4 vulnerabilities

USN-1228-1 : linux-ti-omap4 vulnerabilities

USN-1241-1 : linux-fsl-imx51 vulnerabilities

USN-1244-1 : linux-ti-omap4 vulnerabilities

USN-1260-1 : linux-ti-omap4 vulnerability

USN-1271-1 : linux-fsl-imx51 vulnerabilities

USN-1280-1 : linux-ti-omap4 vulnerabilities

USN-1281-1 : linux-ti-omap4 vulnerabilities

USN-1287-1 : linux-ti-omap4 vulnerability

USN-1300-1 : linux-fsl-imx51 vulnerabilities

USN-1302-1 : linux-ti-omap4 vulnerabilities

USN-1304-1 : linux-ti-omap4 vulnerabilities

USN-1318-1 : linux-fsl-imx51 vulnerabilities

USN-1319-1 : linux-ti-omap4 vulnerabilities

USN-1325-1 : linux-ti-omap4 vulnerabilities

USN-1329-1 : linux-ti-omap4 vulnerability

USN-1330-1 : linux-ti-omap4 vulnerabilities

USN-1356-1 : linux-ti-omap4 vulnerabilities

USN-1364-1 : linux-ti-omap4 vulnerabilities

USN-1383-1 : linux-ti-omap4 vulnerabilities

USN-1392-1 : linux-fsl-imx51 vulnerability

USN-1394-1 : Linux kernel (OMAP4) vulnerabilities

USN-1404-1 : linux-ti-omap4 vulnerability

USN-1408-1 : linux-fsl-imx51 vulnerability

USN-1458-1 : linux-ti-omap4 vulnerabilities

USN-1459-1 : linux-ti-omap4 vulnerabilities

USN-1460-1 : linux-ti-omap4 vulnerabilities

USN-1474-1 : linux-ti-omap4 vulnerabilities

USN-1476-1 : linux-ti-omap4 vulnerabilities

USN-1494-1 : linux-ti-omap4 vulnerability

USN-1499-1 : linux-ti-omap4 vulnerability

USN-1508-1 : linux-ti-omap4 vulnerability

USN-1514-1 : linux-ti-omap4 vulnerabilities

USN-1530-1 : linux-ti-omap4 vulnerabilities

USN-1532-1 : linux-ti-omap4 vulnerabilities

USN-1558-1 : linux-ti-omap4 vulnerability

USN-1577-1 : linux-ti-omap4 vulnerabilities

USN-1578-1 : linux-ti-omap4 vulnerabilities

USN-1580-1 : linux-ti-omap4 vulnerabilities

USN-1599-1 : linux-ti-omap4 vulnerability

USN-1609-1 : linux-ti-omap4 vulnerability

USN-1645-1 : linux-ti-omap4 vulnerabilities

USN-1647-1 : linux-ti-omap4 vulnerabilities

USN-1649-1 : linux-ti-omap4 vulnerabilities

USN-1670-1 : linux-ti-omap4 vulnerability

USN-1673-1 : linux-ti-omap4 vulnerability

USN-1679-1 : linux-ti-omap4 vulnerability

USN-1691-1 : linux-ti-omap4 vulnerability

USN-1698-1 : linux-ti-omap4 vulnerabilities

USN-1698-2 : linux-ti-omap4 regression

USN-1700-1 : linux-ti-omap4 vulnerabilities

USN-1700-2 : linux-ti-omap4 regression

USN-1726-1 : linux-ti-omap4 vulnerabilities

USN-1740-1 : linux-ti-omap4 vulnerability

USN-1742-1 : linux-ti-omap4 vulnerability

USN-1745-1 : linux-ti-omap4 vulnerability

USN-1751-1 : linux-ti-omap4 vulnerability

# SuSE Local Security Checks

# Solaris Local Security Checks

Oracle Solaris Critical Patch Update : apr2012\_SRU3

Oracle Solaris Critical Patch Update : apr2012\_SRU4

Oracle Solaris Critical Patch Update : apr2013\_SRU0

Oracle Solaris Critical Patch Update : apr2013\_SRU3

Oracle Solaris Critical Patch Update : apr2013\_SRU4\_5

Oracle Solaris Critical Patch Update : apr2013\_SRU4a

Oracle Solaris Critical Patch Update : apr2013\_SRU5

Oracle Solaris Critical Patch Update : apr2013\_SRU5\_5

Oracle Solaris Critical Patch Update : apr2014\_SRU11\_1\_17\_5\_0

Oracle Solaris Critical Patch Update : apr2015\_SRU11\_2\_8\_5\_0

Oracle Solaris Critical Patch Update : apr2015\_SRU11\_2\_9\_5\_0

Oracle Solaris Critical Patch Update : apr2016\_SRU11\_3\_4\_5\_0

Oracle Solaris Critical Patch Update : apr2016\_SRU11\_3\_5\_6\_0

Oracle Solaris Critical Patch Update : apr2016\_SRU11\_3\_6\_5\_0

Oracle Solaris Critical Patch Update : apr2016\_SRU11\_3\_7\_5\_0

Oracle Solaris Critical Patch Update : apr2017\_SRU11\_3\_17\_5\_0

Oracle Solaris Critical Patch Update : apr2017\_SRU11\_3\_18\_6\_0

Oracle Solaris Critical Patch Update : apr2017\_SRU11\_3\_19\_5\_0

Oracle Solaris Critical Patch Update : apr2018\_SRU11\_3\_27\_4\_0

Oracle Solaris Critical Patch Update : apr2018\_SRU11\_3\_28\_4\_0

Oracle Solaris Critical Patch Update : apr2018\_SRU11\_3\_29\_5\_0

Oracle Solaris Critical Patch Update : apr2018\_SRU11\_3\_30\_5\_0

Oracle Solaris Critical Patch Update : apr2018\_SRU11\_3\_31\_6\_0 (Spectre)

Oracle Solaris Critical Patch Update : apr2019\_SRU11\_4\_6\_4\_0

Oracle Solaris Critical Patch Update : apr2019\_SRU11\_4\_8\_5\_0

Oracle Solaris Critical Patch Update : apr2020\_SRU11\_3\_36\_20\_0

Oracle Solaris Critical Patch Update : apr2020\_SRU11\_4\_15\_5\_0

Oracle Solaris Critical Patch Update : apr2020\_SRU11\_4\_19\_3\_0

Oracle Solaris Critical Patch Update : jan2013\_SRU11\_1\_2\_5\_0

Oracle Solaris Critical Patch Update : jan2013\_SRU12\_4

Oracle Solaris Critical Patch Update : jan2013\_SRU13\_4

Oracle Solaris Critical Patch Update : jan2013\_SRU2\_5

Oracle Solaris Critical Patch Update : jan2014\_SRU11\_1\_13\_6\_0

Oracle Solaris Critical Patch Update : jan2014\_SRU11\_1\_15\_4\_0

Oracle Solaris Critical Patch Update : jan2014\_SRU11\_1\_16\_5\_0

Oracle Solaris Critical Patch Update : jan2014\_SRU1\_4

Oracle Solaris Critical Patch Update : jan2015\_SRU10\_5a

Oracle Solaris Critical Patch Update : jan2015\_SRU11\_1\_11\_4\_0

Oracle Solaris Critical Patch Update : jan2015\_SRU11\_1\_15\_4\_0

Oracle Solaris Critical Patch Update : jan2015\_SRU11\_1\_16\_5\_0

Oracle Solaris Critical Patch Update : jan2015\_SRU11\_2\_3\_5\_0

Oracle Solaris Critical Patch Update : jan2015\_SRU11\_2\_4\_6\_0

Oracle Solaris Critical Patch Update : jan2015\_SRU11\_2\_6\_4\_0

Oracle Solaris Critical Patch Update : jan2015\_SRU9\_5

Oracle Solaris Critical Patch Update : jan2016\_SRU11\_3\_0\_0\_0

Oracle Solaris Critical Patch Update : jan2016\_SRU11\_3\_3\_6\_0

Oracle Solaris Critical Patch Update : jan2016\_SRU11\_3\_4\_5\_0

Oracle Solaris Critical Patch Update : jan2017\_SRU11\_3\_15\_4\_0

Oracle Solaris Critical Patch Update : jan2017\_SRU11\_3\_16\_3\_0

Oracle Solaris Critical Patch Update : jan2018\_SRU11\_1\_12\_5\_0

Oracle Solaris Critical Patch Update : jan2018\_SRU11\_3\_27\_4\_0

Oracle Solaris Critical Patch Update : jan2019\_SRU11\_1\_19\_6\_0

Oracle Solaris Critical Patch Update : jan2019\_SRU11\_4\_0\_0\_0

Oracle Solaris Critical Patch Update : jan2019\_SRU11\_4\_3\_5\_0 (Foreshadow) (Spectre)

Oracle Solaris Critical Patch Update : jan2020\_SRU11\_4\_15\_5\_0

Oracle Solaris Critical Patch Update : jan2020\_SRU11\_4\_16\_4\_0

Oracle Solaris Critical Patch Update : jan2020\_SRU11\_4\_17\_3\_0

Oracle Solaris Critical Patch Update : jul2012\_SRU7\_5

Oracle Solaris Critical Patch Update : jul2012\_SRU8\_5

Oracle Solaris Critical Patch Update : jul2012\_SRU9\_5

Oracle Solaris Critical Patch Update : jul2014\_SRU11\_1\_17\_5\_0

Oracle Solaris Critical Patch Update : jul2014\_SRU11\_1\_18\_5\_0

Oracle Solaris Critical Patch Update : jul2014\_SRU11\_1\_19\_6\_0

Oracle Solaris Critical Patch Update : jul2015\_SRU11\_2\_10\_5\_0

Oracle Solaris Critical Patch Update : jul2015\_SRU11\_2\_11\_5\_0

Oracle Solaris Critical Patch Update : jul2016\_SRU11\_2\_14\_5\_0

Oracle Solaris Critical Patch Update : jul2016\_SRU11\_3\_10\_5\_0

Oracle Solaris Critical Patch Update : jul2016\_SRU11\_3\_8\_7\_0

Oracle Solaris Critical Patch Update : jul2016\_SRU11\_3\_9\_4\_0

Oracle Solaris Critical Patch Update : jul2017\_SRU11\_3\_0\_0\_0

Oracle Solaris Critical Patch Update : jul2017\_SRU11\_3\_20\_6\_0

Oracle Solaris Critical Patch Update : jul2017\_SRU11\_3\_21\_5\_0

Oracle Solaris Critical Patch Update : jul2017\_SRU11\_3\_22\_3\_0

Oracle Solaris Critical Patch Update : jul2017\_SRU11\_3\_2\_4\_0

Oracle Solaris Critical Patch Update : jul2017\_SRU11\_3\_9\_4\_0

Oracle Solaris Critical Patch Update : jul2018\_SRU11\_2\_11\_5\_0

Oracle Solaris Critical Patch Update : jul2018\_SRU11\_3\_12\_4\_0

Oracle Solaris Critical Patch Update : jul2018\_SRU11\_3\_31\_6\_0

Oracle Solaris Critical Patch Update : jul2018\_SRU11\_3\_32\_4\_0

Oracle Solaris Critical Patch Update : jul2018\_SRU11\_3\_33\_5\_0

Oracle Solaris Critical Patch Update : jul2018\_SRU11\_3\_34\_4\_0

Oracle Solaris Critical Patch Update : jul2019\_SRU11\_3\_36\_13\_0

Oracle Solaris Critical Patch Update : jul2019\_SRU11\_4\_10\_3\_0

Oracle Solaris Critical Patch Update : jul2019\_SRU11\_4\_11\_4\_0

Oracle Solaris Critical Patch Update : jul2019\_SRU11\_4\_7\_5\_0

Oracle Solaris Critical Patch Update : jul2019\_SRU11\_4\_8\_5\_0

Oracle Solaris Critical Patch Update : jul2019\_SRU11\_4\_9\_5\_0

Oracle Solaris Critical Patch Update : july2013\_SRU0

Oracle Solaris Critical Patch Update : july2013\_SRU11\_1\_6\_4\_0

Oracle Solaris Critical Patch Update : july2013\_SRU11\_1\_7\_5\_0

Oracle Solaris Critical Patch Update : july2013\_SRU11\_1\_9\_5\_1

Oracle Solaris Critical Patch Update : july2013\_SRU1\_4

Oracle Solaris Critical Patch Update : july2013\_SRU5\_5

Oracle Solaris Critical Patch Update : july2013\_SRU6\_6

Oracle Solaris Critical Patch Update : ldoms (SRU11\_2\_11\_5\_0)

Oracle Solaris Critical Patch Update : oct2012\_SRU10\_5

Oracle Solaris Critical Patch Update : oct2012\_SRU11\_4

Oracle Solaris Critical Patch Update : oct2012\_SRU12\_4

Oracle Solaris Critical Patch Update : oct2012\_SRU8\_5

Oracle Solaris Critical Patch Update : oct2012\_SRU9\_5

Oracle Solaris Critical Patch Update : oct2013\_SRU11\_1\_11\_4\_0

Oracle Solaris Critical Patch Update : oct2013\_SRU11\_1\_12\_5\_0

Oracle Solaris Critical Patch Update : oct2013\_SRU11\_1\_9\_5\_1

Oracle Solaris Critical Patch Update : oct2014\_11\_2SRU0

Oracle Solaris Critical Patch Update : oct2014\_SRU11\_1\_20\_5\_0

Oracle Solaris Critical Patch Update : oct2015\_SRU11\_1\_15\_4\_0

Oracle Solaris Critical Patch Update : oct2015\_SRU11\_2\_12\_5\_0

Oracle Solaris Critical Patch Update : oct2015\_SRU11\_2\_13\_6\_0

Oracle Solaris Critical Patch Update : oct2015\_SRU11\_2\_14\_5\_0

Oracle Solaris Critical Patch Update : oct2015\_SRU11\_2\_15\_4\_0

Oracle Solaris Critical Patch Update : oct2016\_SRU11\_2\_9\_5\_0

Oracle Solaris Critical Patch Update : oct2016\_SRU11\_3\_11\_6\_0

Oracle Solaris Critical Patch Update : oct2016\_SRU11\_3\_12\_4\_0

Oracle Solaris Critical Patch Update : oct2016\_SRU11\_3\_13\_4\_0

Oracle Solaris Critical Patch Update : oct2018\_SRU11\_3\_35\_6\_0

Oracle Solaris Critical Patch Update : oct2018\_SRU11\_4\_0\_0\_0

Oracle Solaris Critical Patch Update : oct2018\_SRU11\_4\_1\_4\_0

Oracle Solaris Critical Patch Update : oct2019\_SRU11\_3\_36\_15\_0

Oracle Solaris Critical Patch Update : oct2019\_SRU11\_4\_12\_5\_0

Oracle Solaris Critical Patch Update : oct2019\_SRU11\_4\_13\_4\_0

Oracle Solaris Critical Patch Update : oct2019\_SRU11\_4\_14\_5\_0

Oracle Solaris Third-Party Patch Update : ant (algorithmic\_complexity\_vulnerability\_in\_apache)

Oracle Solaris Third-Party Patch Update : apache (cve\_2011\_3607\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : apache (cve\_2012\_0021\_improper\_input)

Oracle Solaris Third-Party Patch Update : apache (cve\_2013\_1896\_denial\_of)

Oracle Solaris Third-Party Patch Update : apache (cve\_2013\_2765\_denial\_of)

Oracle Solaris Third-Party Patch Update : apache (cve\_2013\_4365\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : apache (multiple\_cross\_site\_scripting\_vulnerabilities)

Oracle Solaris Third-Party Patch Update : apache (multiple\_denial\_of\_service\_dos5)

Oracle Solaris Third-Party Patch Update : apache (multiple\_input\_validation\_vulnerabilities\_in1)

Oracle Solaris Third-Party Patch Update : apache (multiple\_vulnerabilities\_in\_apache\_http2)

Oracle Solaris Third-Party Patch Update : bash (cve\_2012\_3410\_stack\_based)

Oracle Solaris Third-Party Patch Update : bash (multiple\_vulnerabilities\_in\_bash) (Shellshock)

Oracle Solaris Third-Party Patch Update : bash (multiple\_vulnerabilities\_in\_bash1) (Shellshock)

Oracle Solaris Third-Party Patch Update : bind (cve\_2011\_4313\_denial\_of)

Oracle Solaris Third-Party Patch Update : bind (cve\_2012\_1667\_denial\_of)

Oracle Solaris Third-Party Patch Update : bind (cve\_2012\_3817\_denial\_of)

Oracle Solaris Third-Party Patch Update : bind (cve\_2012\_4244\_denial\_of)

Oracle Solaris Third-Party Patch Update : bind (cve\_2012\_5166\_denial\_of)

Oracle Solaris Third-Party Patch Update : cups (cve\_2014\_2856\_cross\_site)

Oracle Solaris Third-Party Patch Update : cvs (cve\_2012\_0804\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : dbus (cve\_2013\_2168\_input\_validation)

Oracle Solaris Third-Party Patch Update : django (multiple\_vulnerabilities\_in\_django)

Oracle Solaris Third-Party Patch Update : ejabberd (cve\_2013\_6169\_cryptographic\_issues)

Oracle Solaris Third-Party Patch Update : ekiga (cve\_2012\_5621\_denial\_of)

Oracle Solaris Third-Party Patch Update : emacs (cve\_2012\_3479\_arbitrary\_code)

Oracle Solaris Third-Party Patch Update : facter (cve\_2014\_3248\_untrusted\_search)

Oracle Solaris Third-Party Patch Update : fetchmail (multiple\_vulnerabilities\_in\_fetchmail) (BEAST)

Oracle Solaris Third-Party Patch Update : firefox (multiple\_vulnerabilities\_fixed\_in\_firefox1)

Oracle Solaris Third-Party Patch Update : firefox (multiple\_vulnerabilities\_in\_firefox)

Oracle Solaris Third-Party Patch Update : firefox (multiple\_vulnerabilities\_in\_firefox\_web)

Oracle Solaris Third-Party Patch Update : firefox (multiple\_vulnerabilities\_in\_firefox\_web1)

Oracle Solaris Third-Party Patch Update : firefox (multiple\_vulnerabilities\_in\_mozilla\_firefox1)

Oracle Solaris Third-Party Patch Update : flash (multiple\_vulnerabilities\_in\_adobe\_flashplayer4)

Oracle Solaris Third-Party Patch Update : flash (multiple\_vulnerabilities\_in\_adobe\_flashplayer6)

Oracle Solaris Third-Party Patch Update : foomatic (multiple\_vulnerabilities\_in\_foomatic)

Oracle Solaris Third-Party Patch Update : freetype (cve\_2011\_3439\_denial\_of)

Oracle Solaris Third-Party Patch Update : freetype (multiple\_buffer\_errors\_vulnerabilities\_in)

Oracle Solaris Third-Party Patch Update : freetype (multiple\_denial\_of\_service\_dos1)

Oracle Solaris Third-Party Patch Update : gegl (multiple\_integer\_overflow\_vulnerabilities\_in)

Oracle Solaris Third-Party Patch Update : ghostscript (multiple\_denial\_of\_service\_vulnerabilities7)

Oracle Solaris Third-Party Patch Update : gimp (cve\_2012\_2763\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : gimp (cve\_2012\_3236\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : gimp (cve\_2012\_4245\_arbitrary\_code)

Oracle Solaris Third-Party Patch Update : gimp (cve\_2012\_4564\_design\_error)

Oracle Solaris Third-Party Patch Update : gimp (multiple\_vulnerabilities\_in\_gimp)

Oracle Solaris Third-Party Patch Update : glance (cve\_2014\_5356\_permissions\_privileges)

Oracle Solaris Third-Party Patch Update : gnome (cve\_2007\_4460\_symlink\_attack)

Oracle Solaris Third-Party Patch Update : gnu-patch (multiple\_vulnerabilities\_in\_gnu\_patch)

Oracle Solaris Third-Party Patch Update : gnupg (cve\_2013\_4351\_cryptographic\_issues)

Oracle Solaris Third-Party Patch Update : gnutls (cve\_2011\_4128\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : gnutls (cve\_2012\_1573\_denial\_of)

Oracle Solaris Third-Party Patch Update : gnutls (cve\_2013\_1619\_cryptographic\_issues)

Oracle Solaris Third-Party Patch Update : gnutls (cve\_2014\_0092\_cryptographic\_issues)

Oracle Solaris Third-Party Patch Update : gnutls (multiple\_vulnerabilities\_in\_gnutls)

Oracle Solaris Third-Party Patch Update : grails (cve\_2012\_1833\_permissions\_privileges)

Oracle Solaris Third-Party Patch Update : grep (cve\_2012\_5667\_heap\_buffer)

Oracle Solaris Third-Party Patch Update : gtk (cve\_2012\_2370\_denial\_of)

Oracle Solaris Third-Party Patch Update : gzip (cve\_2009\_2624\_denial\_of)

Oracle Solaris Third-Party Patch Update : horizon (cve\_2014\_3594\_cross\_site)

Oracle Solaris Third-Party Patch Update : horizon (multiple\_cross\_site\_scripting\_xss1)

Oracle Solaris Third-Party Patch Update : hplip (cve\_2013\_0200\_link\_following)

Oracle Solaris Third-Party Patch Update : ibutils (cve\_2013\_2561\_link\_following)

Oracle Solaris Third-Party Patch Update : icu (cve\_2013\_0900\_race\_conditions)

Oracle Solaris Third-Party Patch Update : icu (multiple\_vulnerabilities\_in\_international\_components)

Oracle Solaris Third-Party Patch Update : imagemagick (multiple\_buffer\_errors\_vulnerabilities\_in2)

Oracle Solaris Third-Party Patch Update : imagemagick (multiple\_vulnerabilities\_in\_imagemagick2)

Oracle Solaris Third-Party Patch Update : ipmitool (cve\_2011\_4339\_access\_controls)

Oracle Solaris Third-Party Patch Update : isc-dhcp (cve\_2011\_4539\_denial\_of)

Oracle Solaris Third-Party Patch Update : isc-dhcp (cve\_2012\_3955\_denial\_of)

Oracle Solaris Third-Party Patch Update : isc-dhcp (multiple\_denial\_of\_service\_dos4)

Oracle Solaris Third-Party Patch Update : jinja2 (multiple\_vulnerabilities\_in\_jinja2)

Oracle Solaris Third-Party Patch Update : kerberos (cve\_2002\_2443\_denial\_of)

Oracle Solaris Third-Party Patch Update : kerberos (cve\_2010\_1322\_improper\_input)

Oracle Solaris Third-Party Patch Update : kerberos (cve\_2013\_1416\_denial\_of)

Oracle Solaris Third-Party Patch Update : kerberos (cve\_2014\_4345\_numeric\_errors)

Oracle Solaris Third-Party Patch Update : kerberos (multiple\_buffer\_errors\_vulnerabilities\_in4)

Oracle Solaris Third-Party Patch Update : kerberos (multiple\_input\_validation\_vulnerabilities\_in)

Oracle Solaris Third-Party Patch Update : kerberos (multiple\_vulnerabilities\_in\_kerberos1)

Oracle Solaris Third-Party Patch Update : keystone (cve\_2014\_2828\_authentication\_issues)

Oracle Solaris Third-Party Patch Update : keystone (cve\_2014\_3520\_privilege\_escalation)

Oracle Solaris Third-Party Patch Update : keystone (cve\_2014\_3621\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : keystone (cve\_2014\_7144\_cryptographic\_issues)

Oracle Solaris Third-Party Patch Update : lcms (cve\_2013\_4276\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : libcurl (cve\_2013\_1944\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : libcurl (cve\_2014\_3613\_cookie\_leak)

Oracle Solaris Third-Party Patch Update : libcurl (cve\_2014\_3707\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : libdbus (cve\_2012\_3524\_permissions\_privileges)

Oracle Solaris Third-Party Patch Update : libdrm (cve\_2012\_0044\_integer\_overflow)

Oracle Solaris Third-Party Patch Update : libdrm (cve\_2013\_0913\_numeric\_errors)

Oracle Solaris Third-Party Patch Update : libexif (multiple\_vulnerabilities\_in\_libexif1)

Oracle Solaris Third-Party Patch Update : libexpat (multiple\_resource\_management\_error\_vulnerabilities)

Oracle Solaris Third-Party Patch Update : libfxt (cve\_2011\_3256\_denial\_of)

Oracle Solaris Third-Party Patch Update : libgcrypt (cve\_2013\_4242\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : libmikmod (cve\_2009\_0179\_denial\_of)

Oracle Solaris Third-Party Patch Update : libotr (cve\_2012\_3461\_denial\_of)

Oracle Solaris Third-Party Patch Update : libpng (multiple\_vulnerabilities\_in\_libpng2)

Oracle Solaris Third-Party Patch Update : libproxy (multiple\_buffer\_errors\_vulnerability\_in1)

Oracle Solaris Third-Party Patch Update : librsvg (cve\_2011\_3146\_denial\_of)

Oracle Solaris Third-Party Patch Update : libsoup (cve\_2011\_2524\_directory\_traversal)

Oracle Solaris Third-Party Patch Update : libtasn1 (multiple\_vulnerabilities\_in\_gnu\_libtasn1)

Oracle Solaris Third-Party Patch Update : libtiff (cve\_2012\_1173\_numeric\_errors)

Oracle Solaris Third-Party Patch Update : libtiff (cve\_2012\_2088\_denial\_of)

Oracle Solaris Third-Party Patch Update : libtiff (cve\_2012\_3401\_denial\_of)

Oracle Solaris Third-Party Patch Update : libtiff (cve\_2012\_4564\_design\_error1)

Oracle Solaris Third-Party Patch Update : libtiff (cve\_2012\_5581\_denial\_of)

Oracle Solaris Third-Party Patch Update : libtiff (cve\_2013\_4231\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : libtiff (cve\_2013\_4243\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : libvorbis (cve\_2012\_0444\_memory\_corruption)

Oracle Solaris Third-Party Patch Update : libxml2 (cve\_2010\_4008\_denial\_of)

Oracle Solaris Third-Party Patch Update : libxml2 (cve\_2011\_0216\_denial\_of)

Oracle Solaris Third-Party Patch Update : libxml2 (cve\_2012\_5134\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : libxml2 (cve\_2013\_0338\_denial\_of)

Oracle Solaris Third-Party Patch Update : libxml2 (cve\_2013\_1969\_resource\_management)

Oracle Solaris Third-Party Patch Update : libxml2 (cve\_2014\_0191\_denial\_of)

Oracle Solaris Third-Party Patch Update : libxslt (cve\_2012\_2807\_numeric\_errors)

Oracle Solaris Third-Party Patch Update : libxslt (cve\_2012\_5581\_denial\_of1)

Oracle Solaris Third-Party Patch Update : libxslt (multiple\_vulnerabilities\_in\_libxslt)

Oracle Solaris Third-Party Patch Update : libxtsol (cve\_2014\_0397\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : lighttpd (cve\_2011\_4362\_denial\_of)

Oracle Solaris Third-Party Patch Update : lighttpd (cve\_2014\_2469\_denial\_of)

Oracle Solaris Third-Party Patch Update : lighttpd (multiple\_vulnerabilities\_in\_lighttpd)

Oracle Solaris Third-Party Patch Update : logilab-common (multiple\_symlink\_attack\_vulnerabilities\_in)

Oracle Solaris Third-Party Patch Update : lua (cve\_2014\_5461\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : memcached (cve\_2013\_0179\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : memcached (multiple\_vulnerabilities\_in\_memcached)

Oracle Solaris Third-Party Patch Update : modsecurity (cve\_2012\_2751\_improper\_input)

Oracle Solaris Third-Party Patch Update : mysql (multiple\_vulnerabilities\_in\_mysql)

Oracle Solaris Third-Party Patch Update : net-snmp (cve\_2012\_2141\_denial\_of)

Oracle Solaris Third-Party Patch Update : net-snmp (cve\_2012\_6151\_resource\_management)

Oracle Solaris Third-Party Patch Update : net-snmp (multiple\_vulnerabilities\_in\_net\_snmp)

Oracle Solaris Third-Party Patch Update : neutron (cve\_2014\_6414\_unauthenticated\_access)

Oracle Solaris Third-Party Patch Update : nmap (cve\_2013\_4885\_unrestricted\_file)

Oracle Solaris Third-Party Patch Update : nova (cve\_2014\_3517\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : nova (multiple\_vulnerabilities\_in\_nova)

Oracle Solaris Third-Party Patch Update : nss (cve\_2013\_1620\_lucky\_thirteen)

Oracle Solaris Third-Party Patch Update : ntp (cve\_2013\_5211\_input\_validation)

Oracle Solaris Third-Party Patch Update : ntp (multiple\_vulnerabilities\_in\_ntp)

Oracle Solaris Third-Party Patch Update : openssl (cve\_2010\_5298\_race\_conditions)

Oracle Solaris Third-Party Patch Update : openssl (cve\_2012\_0050\_denial\_of)

Oracle Solaris Third-Party Patch Update : openssl (cve\_2012\_0884\_cryptographic\_issue1)

Oracle Solaris Third-Party Patch Update : openssl (cve\_2012\_2333\_denial\_of)

Oracle Solaris Third-Party Patch Update : openssl (cve\_2014\_0224\_cryptographic\_issues1)

Oracle Solaris Third-Party Patch Update : openssl (cve\_2014\_3505\_denial\_of)

Oracle Solaris Third-Party Patch Update : openssl (cve\_2014\_3508\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : openssl (lucky\_thirteen\_vulnerability\_in\_solaris)

Oracle Solaris Third-Party Patch Update : openssl (multiple\_vulnerabilities\_in\_openssl1)

Oracle Solaris Third-Party Patch Update : openssl (multiple\_vulnerabilities\_in\_openssl4) (Heartbleed)

Oracle Solaris Third-Party Patch Update : openssl (multiple\_vulnerabilities\_in\_openssl6) (POODLE)

Oracle Solaris Third-Party Patch Update : perl (cve\_2014\_4330\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : perl-512 (cve\_2012\_5195\_heap\_buffer)

Oracle Solaris Third-Party Patch Update : perl-512 (cve\_2013\_1667\_denial\_of1)

Oracle Solaris Third-Party Patch Update : perl-516 (cve\_2013\_1667\_denial\_of2)

Oracle Solaris Third-Party Patch Update : perl-58 (cve\_2011\_2728\_denial\_of)

Oracle Solaris Third-Party Patch Update : perl-58 (cve\_2011\_3597\_improper\_input)

Oracle Solaris Third-Party Patch Update : perl-58 (cve\_2012\_5195\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : perl-58 (cve\_2012\_5526\_configuration\_vulnerability1)

Oracle Solaris Third-Party Patch Update : perl-58 (cve\_2012\_6329\_code\_injection1)

Oracle Solaris Third-Party Patch Update : perl-58 (cve\_2013\_1667\_denial\_of)

Oracle Solaris Third-Party Patch Update : php (cve\_2013\_4113\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : php (cve\_2013\_4248\_input\_validation)

Oracle Solaris Third-Party Patch Update : pidgin (cve\_2012\_3374\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : pidgin (multiple\_vulnerabilities\_in\_pidgin)

Oracle Solaris Third-Party Patch Update : pidgin (multiple\_vulnerabilities\_in\_pidgin2)

Oracle Solaris Third-Party Patch Update : procmail (cve\_2014\_3618\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : proftpd (cve\_2011\_4130\_use\_after)

Oracle Solaris Third-Party Patch Update : proftpd (cve\_2012\_6095\_race\_conditions)

Oracle Solaris Third-Party Patch Update : puppet (multiple\_vulnerabilities\_in\_puppet)

Oracle Solaris Third-Party Patch Update : puppet (multiple\_vulnerabilities\_in\_puppet1)

Oracle Solaris Third-Party Patch Update : py\_pil (cve\_2014\_3589\_input\_validation)

Oracle Solaris Third-Party Patch Update : py\_pil (multiple\_vulnerabilities\_in\_python\_image)

Oracle Solaris Third-Party Patch Update : python (cve\_2010\_1634\_integer\_overflow)

Oracle Solaris Third-Party Patch Update : python (cve\_2014\_7185\_integer\_overflow)

Oracle Solaris Third-Party Patch Update : python (multiple\_vulnerabilities\_in\_python) (BEAST)

Oracle Solaris Third-Party Patch Update : quagga (cve\_2012\_1820\_denial\_of)

Oracle Solaris Third-Party Patch Update : quagga (cve\_2013\_2236\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : quagga (multiple\_denial\_of\_service\_vulnerabilities4)

Oracle Solaris Third-Party Patch Update : ruby (cve\_2011\_4815\_denial\_of)

Oracle Solaris Third-Party Patch Update : ruby (cve\_2013\_4073\_cryptographic\_issues)

Oracle Solaris Third-Party Patch Update : ruby (cve\_2013\_4164\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : ruby (multiple\_cryptographic\_issues\_vulnerabilities\_in)

Oracle Solaris Third-Party Patch Update : ruby (multiple\_vulnerabilities\_in\_ruby1)

Oracle Solaris Third-Party Patch Update : rubygems (cve\_2012\_2125\_https\_to)

Oracle Solaris Third-Party Patch Update : rubygems (multiple\_cryptographic\_issues\_vulnerabilities\_in1)

Oracle Solaris Third-Party Patch Update : samba (cve\_2012\_1182\_arbitrary\_code)

Oracle Solaris Third-Party Patch Update : samba (cve\_2012\_2111\_access\_controls)

Oracle Solaris Third-Party Patch Update : samba (cve\_2012\_6150\_input\_validation)

Oracle Solaris Third-Party Patch Update : samba (cve\_2013\_4124\_denial\_of)

Oracle Solaris Third-Party Patch Update : samba (cve\_2013\_4475\_access\_control)

Oracle Solaris Third-Party Patch Update : samba (cve\_2013\_4496\_credentials\_management)

Oracle Solaris Third-Party Patch Update : samba (cve\_2014\_0178\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : samba (multiple\_vulnerabilities\_in\_samba1)

Oracle Solaris Third-Party Patch Update : samba (multiple\_vulnerabilities\_in\_samba\_web)

Oracle Solaris Third-Party Patch Update : sendmail (cve\_2014\_3956\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : slocate (cve\_2007\_0227\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : squid (cve\_2011\_3205\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : squid (cve\_2013\_4123\_input\_validation)

Oracle Solaris Third-Party Patch Update : squid (multiple\_vulnerabilities\_in\_squid)

Oracle Solaris Third-Party Patch Update : ssh (cve\_2010\_5107\_denial\_of)

Oracle Solaris Third-Party Patch Update : stardict (cve\_2009\_2260\_information\_exposure)

Oracle Solaris Third-Party Patch Update : subversion (cve\_2009\_0179\_denial\_of1)

Oracle Solaris Third-Party Patch Update : sudo (cve\_2012\_2337\_restriction\_bypass)

Oracle Solaris Third-Party Patch Update : sudo (multiple\_permissions\_privileges\_and\_access)

Oracle Solaris Third-Party Patch Update : tcsd (cve\_2012\_0698\_denial\_of)

Oracle Solaris Third-Party Patch Update : telnet (cve\_2011\_4862\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : texinfo (cve\_2006\_4810\_buffer\_overflow)

Oracle Solaris Third-Party Patch Update : thunderbird (multiple\_vulnerabilities\_in\_thunderbird2)

Oracle Solaris Third-Party Patch Update : thunderbird (multiple\_vulnerabilities\_in\_thunderbird3)

Oracle Solaris Third-Party Patch Update : thunderbird (multiple\_vulnerabilities\_in\_thunderbird4)

Oracle Solaris Third-Party Patch Update : thunderbird (multiple\_vulnerabilities\_in\_thunderbird5)

Oracle Solaris Third-Party Patch Update : thunderbird (multiple\_vulnerabilities\_in\_thunderbird6)

Oracle Solaris Third-Party Patch Update : thunderbird (multiple\_vulnerabilities\_in\_thunderbird7)

Oracle Solaris Third-Party Patch Update : tomcat (cve\_2011\_3375\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : tomcat (cve\_2013\_0346\_permissions\_privileges)

Oracle Solaris Third-Party Patch Update : tomcat (cve\_2014\_0075\_numeric\_errors)

Oracle Solaris Third-Party Patch Update : tomcat (multiple\_denial\_of\_service\_dos)

Oracle Solaris Third-Party Patch Update : tomcat (multiple\_vulnerabilities\_in\_apache\_tomcat3)

Oracle Solaris Third-Party Patch Update : tomcat (multiple\_vulnerabilities\_in\_apache\_tomcat4)

Oracle Solaris Third-Party Patch Update : tomcat (multiple\_vulnerabilities\_in\_tomcat)

Oracle Solaris Third-Party Patch Update : transmission (cve\_2012\_4037\_xss\_vulnerability)

Oracle Solaris Third-Party Patch Update : vino (cve\_2012\_4429\_information\_leak)

Oracle Solaris Third-Party Patch Update : vino (cve\_2013\_5745\_input\_validation)

Oracle Solaris Third-Party Patch Update : wanboot (cve\_2014\_0224\_cryptographic\_issues)

Oracle Solaris Third-Party Patch Update : wireshark (cve\_2014\_2907\_denial\_of)

Oracle Solaris Third-Party Patch Update : wireshark (cve\_2014\_4020\_numeric\_errors)

Oracle Solaris Third-Party Patch Update : wireshark (denial\_of\_service\_vulnerability\_in)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_buffer\_errors\_vulnerabilities\_in3)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_denial\_of\_service\_vulnerabilities2)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_fixed\_in\_wireshark)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark1)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark10)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark11)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark3)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark4)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark5)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark6)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark7)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark8)

Oracle Solaris Third-Party Patch Update : wireshark (multiple\_vulnerabilities\_in\_wireshark9)

Oracle Solaris Third-Party Patch Update : xdg-utils (cve\_2008\_0386\_improper\_input)

Oracle Solaris Third-Party Patch Update : xorg (cve\_2011\_4028\_information\_disclosure)

Oracle Solaris Third-Party Patch Update : xorg (cve\_2013\_4396\_use\_after)

Oracle Solaris Third-Party Patch Update : xorg (cve\_2013\_6462\_buffer\_errors)

Oracle Solaris Third-Party Patch Update : xorg (multiple\_vulnerabilities\_in\_x\_org)

Oracle Solaris Third-Party Patch Update : xorg (multiple\_vulnerabilities\_in\_x\_org1)

Oracle Solaris Third-Party Patch Update : xorg (multiple\_vulnerabilities\_in\_x\_org2)

Oracle Solaris Third-Party Patch Update : xpdf (cve\_2012\_2142\_arbitrary\_code)

Oracle third party patch update : bash\_2014\_10\_07

Solaris 10 (i386) : 116578-42

Solaris 10 (i386) : 117550-12

Solaris 10 (i386) : 117846-19

Solaris 10 (i386) : 122608-07

Solaris 10 (i386) : 124615-01

Solaris 10 (i386) : 124721-02

Solaris 10 (i386) : 125672-01

Solaris 10 (sparc) : 108669-21 (deprecated)

Solaris 10 (sparc) : 112760-18

Solaris 10 (sparc) : 113859-04

Solaris 10 (sparc) : 113859-04 (deprecated)

Solaris 10 (sparc) : 115610-25 (deprecated)

Solaris 10 (sparc) : 115614-28 (deprecated)

Solaris 10 (sparc) : 116264-09 (deprecated)

Solaris 10 (sparc) : 116271-10 (deprecated)

Solaris 10 (sparc) : 116577-42

Solaris 10 (sparc) : 116648-25

Solaris 10 (sparc) : 116648-25 (deprecated)

Solaris 10 (sparc) : 116831-04 (deprecated)

Solaris 10 (sparc) : 116832-04 (deprecated)

Solaris 10 (sparc) : 116834-04 (deprecated)

Solaris 10 (sparc) : 116837-03

Solaris 10 (sparc) : 117461-08

Solaris 10 (sparc) : 117654-67 (deprecated)

Solaris 10 (sparc) : 118207-63 (deprecated)

Solaris 10 (sparc) : 118371-10

Solaris 10 (sparc) : 118540-42 (deprecated)

Solaris 10 (sparc) : 118560-02

Solaris 10 (sparc) : 118562-14

Solaris 10 (sparc) : 118666-19

Solaris 10 (sparc) : 118666-61

Solaris 10 (sparc) : 118666-86 (deprecated)

Solaris 10 (sparc) : 118667-61

Solaris 10 (sparc) : 118667-86 (deprecated)

Solaris 10 (sparc) : 118777-18 (deprecated)

Solaris 10 (sparc) : 118822-30

Solaris 10 (sparc) : 118833-36 (deprecated)

Solaris 10 (sparc) : 118918-24 (deprecated)

Solaris 10 (sparc) : 119008-01 (deprecated)

Solaris 10 (sparc) : 119009-11 (deprecated)

Solaris 10 (sparc) : 119010-01 (deprecated)

Solaris 10 (sparc) : 119011-01 (deprecated)

Solaris 10 (sparc) : 119059-46

Solaris 10 (sparc) : 119059-65

Solaris 10 (sparc) : 119059-66

Solaris 10 (sparc) : 119059-69

Solaris 10 (sparc) : 119059-70

Solaris 10 (sparc) : 119059-71

Solaris 10 (sparc) : 119059-72

Solaris 10 (sparc) : 119059-73 (deprecated)

Solaris 10 (sparc) : 119059-74

Solaris 10 (sparc) : 119063-01

Solaris 10 (sparc) : 119063-02

Solaris 10 (sparc) : 119063-02 (deprecated)

Solaris 10 (sparc) : 119075-14

Solaris 10 (sparc) : 119090-33

Solaris 10 (sparc) : 119107-06

Solaris 10 (sparc) : 119115-36 (deprecated)

Solaris 10 (sparc) : 119117-52

Solaris 10 (sparc) : 119117-54 (deprecated)

Solaris 10 (sparc) : 119166-43 (deprecated)

Solaris 10 (sparc) : 119213-27 (BEAST)

Solaris 10 (sparc) : 119213-30

Solaris 10 (sparc) : 119213-31

Solaris 10 (sparc) : 119213-32

Solaris 10 (sparc) : 119213-33

Solaris 10 (sparc) : 119213-36

Solaris 10 (sparc) : 119213-36 (deprecated)

Solaris 10 (sparc) : 119213-37

Solaris 10 (sparc) : 119213-38

Solaris 10 (sparc) : 119252-29

Solaris 10 (sparc) : 119252-29 (deprecated)

Solaris 10 (sparc) : 119254-91

Solaris 10 (sparc) : 119254-92

Solaris 10 (sparc) : 119254-93 (deprecated)

Solaris 10 (sparc) : 119280-25 (deprecated)

Solaris 10 (sparc) : 119313-42 (deprecated)

Solaris 10 (sparc) : 119315-19 (deprecated)

Solaris 10 (sparc) : 119410-10

Solaris 10 (sparc) : 119410-10 (deprecated)

Solaris 10 (sparc) : 119465-17

Solaris 10 (sparc) : 119465-17 (deprecated)

Solaris 10 (sparc) : 119466-17 (deprecated)

Solaris 10 (sparc) : 119534-29 (deprecated)

Solaris 10 (sparc) : 119548-14

Solaris 10 (sparc) : 119548-14 (deprecated)

Solaris 10 (sparc) : 119593-01

Solaris 10 (sparc) : 119593-01

Solaris 10 (sparc) : 119596-03

Solaris 10 (sparc) : 119689-07

Solaris 10 (sparc) : 119719-01

Solaris 10 (sparc) : 119719-01

Solaris 10 (sparc) : 119725-06 (deprecated)

Solaris 10 (sparc) : 119757-30

Solaris 10 (sparc) : 119757-31

Solaris 10 (sparc) : 119757-32

Solaris 10 (sparc) : 119757-33

Solaris 10 (sparc) : 119757-34

Solaris 10 (sparc) : 119757-36

Solaris 10 (sparc) : 119757-37

Solaris 10 (sparc) : 119757-38

Solaris 10 (sparc) : 119757-43

Solaris 10 (sparc) : 119757-43 (deprecated)

Solaris 10 (sparc) : 119757-44

Solaris 10 (sparc) : 119764-07

Solaris 10 (sparc) : 119764-07 (deprecated)

Solaris 10 (sparc) : 119777-19 (deprecated)

Solaris 10 (sparc) : 119783-25

Solaris 10 (sparc) : 119783-29

Solaris 10 (sparc) : 119783-30

Solaris 10 (sparc) : 119783-31

Solaris 10 (sparc) : 119783-32

Solaris 10 (sparc) : 119783-33

Solaris 10 (sparc) : 119783-36

Solaris 10 (sparc) : 119783-37

Solaris 10 (sparc) : 119783-38

Solaris 10 (sparc) : 119783-39

Solaris 10 (sparc) : 119783-40

Solaris 10 (sparc) : 119783-40 (deprecated)

Solaris 10 (sparc) : 119783-41

Solaris 10 (sparc) : 119783-42

Solaris 10 (sparc) : 119783-43

Solaris 10 (sparc) : 119783-44

Solaris 10 (sparc) : 119810-07

Solaris 10 (sparc) : 119810-08

Solaris 10 (sparc) : 119810-08 (deprecated)

Solaris 10 (sparc) : 119812-16

Solaris 10 (sparc) : 119812-18

Solaris 10 (sparc) : 119812-20

Solaris 10 (sparc) : 119812-22 (deprecated)

Solaris 10 (sparc) : 119900-16

Solaris 10 (sparc) : 119900-17

Solaris 10 (sparc) : 119900-18

Solaris 10 (sparc) : 119900-18 (deprecated)

Solaris 10 (sparc) : 119903-02 (deprecated)

Solaris 10 (sparc) : 119906-18

Solaris 10 (sparc) : 119906-22 (deprecated)

Solaris 10 (sparc) : 119985-02

Solaris 10 (sparc) : 119985-02

Solaris 10 (sparc) : 119998-02

Solaris 10 (sparc) : 120011-14 (deprecated)

Solaris 10 (sparc) : 120036-07

Solaris 10 (sparc) : 120050-06

Solaris 10 (sparc) : 120068-03

Solaris 10 (sparc) : 120085-02

Solaris 10 (sparc) : 120094-35

Solaris 10 (sparc) : 120094-36

Solaris 10 (sparc) : 120094-36 (deprecated)

Solaris 10 (sparc) : 120185-23

Solaris 10 (sparc) : 120189-23

Solaris 10 (sparc) : 120201-06

Solaris 10 (sparc) : 120201-07

Solaris 10 (sparc) : 120201-07 (deprecated)

Solaris 10 (sparc) : 120201-08

Solaris 10 (sparc) : 120228-45 (deprecated)

Solaris 10 (sparc) : 120272-31

Solaris 10 (sparc) : 120272-40 (deprecated)

Solaris 10 (sparc) : 120286-03

Solaris 10 (sparc) : 120286-04 (deprecated)

Solaris 10 (sparc) : 120292-02

Solaris 10 (sparc) : 120292-02 (deprecated)

Solaris 10 (sparc) : 120294-01

Solaris 10 (sparc) : 120294-01

Solaris 10 (sparc) : 120329-02

Solaris 10 (sparc) : 120412-11 (deprecated)

Solaris 10 (sparc) : 120414-27 (deprecated)

Solaris 10 (sparc) : 120460-21 (deprecated)

Solaris 10 (sparc) : 120467-05

Solaris 10 (sparc) : 120469-07

Solaris 10 (sparc) : 120473-12

Solaris 10 (sparc) : 120500-28 (deprecated)

Solaris 10 (sparc) : 120543-33

Solaris 10 (sparc) : 120543-34

Solaris 10 (sparc) : 120543-35

Solaris 10 (sparc) : 120543-36 (deprecated)

Solaris 10 (sparc) : 120650-01 (deprecated)

Solaris 10 (sparc) : 120651-01 (deprecated)

Solaris 10 (sparc) : 120653-01 (deprecated)

Solaris 10 (sparc) : 120661-04

Solaris 10 (sparc) : 120664-01

Solaris 10 (sparc) : 120664-01

Solaris 10 (sparc) : 120719-07

Solaris 10 (sparc) : 120719-07 (deprecated)

Solaris 10 (sparc) : 120739-08

Solaris 10 (sparc) : 120739-08 (deprecated)

Solaris 10 (sparc) : 120830-06 (deprecated)

Solaris 10 (sparc) : 120879-08 (deprecated)

Solaris 10 (sparc) : 120954-12

Solaris 10 (sparc) : 120954-12 (deprecated)

Solaris 10 (sparc) : 120981-25

Solaris 10 (sparc) : 121004-04

Solaris 10 (sparc) : 121012-03

Solaris 10 (sparc) : 121045-04

Solaris 10 (sparc) : 121095-04

Solaris 10 (sparc) : 121095-05

Solaris 10 (sparc) : 121095-05 (deprecated)

Solaris 10 (sparc) : 121104-11

Solaris 10 (sparc) : 121104-11 (deprecated)

Solaris 10 (sparc) : 121118-21 (deprecated)

Solaris 10 (sparc) : 121132-03

Solaris 10 (sparc) : 121136-02 (deprecated)

Solaris 10 (sparc) : 121161-01

Solaris 10 (sparc) : 121161-01 (deprecated)

Solaris 10 (sparc) : 121211-02

Solaris 10 (sparc) : 121211-02 (deprecated)

Solaris 10 (sparc) : 121229-02

Solaris 10 (sparc) : 121229-02

Solaris 10 (sparc) : 121236-02

Solaris 10 (sparc) : 121239-02

Solaris 10 (sparc) : 121288-03

Solaris 10 (sparc) : 121308-20 (deprecated)

Solaris 10 (sparc) : 121394-03

Solaris 10 (sparc) : 121428-15

Solaris 10 (sparc) : 121428-15 (deprecated)

Solaris 10 (sparc) : 121453-02 (deprecated)

Solaris 10 (sparc) : 121581-20 (deprecated)

Solaris 10 (sparc) : 121657-54 (deprecated)

Solaris 10 (sparc) : 121913-20 (deprecated)

Solaris 10 (sparc) : 121956-01 (deprecated)

Solaris 10 (sparc) : 121957-01 (deprecated)

Solaris 10 (sparc) : 122073-04 (deprecated)

Solaris 10 (sparc) : 122212-46

Solaris 10 (sparc) : 122212-46 (deprecated)

Solaris 10 (sparc) : 122239-03

Solaris 10 (sparc) : 122259-06

Solaris 10 (sparc) : 122259-09

Solaris 10 (sparc) : 122259-09 (deprecated)

Solaris 10 (sparc) : 122261-03

Solaris 10 (sparc) : 122470-05 (deprecated)

Solaris 10 (sparc) : 122476-01

Solaris 10 (sparc) : 122608-07

Solaris 10 (sparc) : 122675-05

Solaris 10 (sparc) : 122793-36 (deprecated)

Solaris 10 (sparc) : 122856-03

Solaris 10 (sparc) : 122911-32

Solaris 10 (sparc) : 122911-33

Solaris 10 (sparc) : 122911-34

Solaris 10 (sparc) : 122911-35

Solaris 10 (sparc) : 122911-36

Solaris 10 (sparc) : 122911-37

Solaris 10 (sparc) : 122911-37 (deprecated)

Solaris 10 (sparc) : 122958-06

Solaris 10 (sparc) : 123005-07 (deprecated)

Solaris 10 (sparc) : 123037-01 (deprecated)

Solaris 10 (sparc) : 123038-01 (deprecated)

Solaris 10 (sparc) : 123175-01

Solaris 10 (sparc) : 123175-01 (deprecated)

Solaris 10 (sparc) : 123186-03

Solaris 10 (sparc) : 123246-11

Solaris 10 (sparc) : 123256-02

Solaris 10 (sparc) : 123304-02

Solaris 10 (sparc) : 123324-03

Solaris 10 (sparc) : 123324-03

Solaris 10 (sparc) : 123402-01

Solaris 10 (sparc) : 123402-01

Solaris 10 (sparc) : 123590-12

Solaris 10 (sparc) : 123590-12 (deprecated)

Solaris 10 (sparc) : 123611-05 (deprecated)

Solaris 10 (sparc) : 123809-02

Solaris 10 (sparc) : 123809-02

Solaris 10 (sparc) : 123870-05 (deprecated)

Solaris 10 (sparc) : 123893-77

Solaris 10 (sparc) : 123893-79

Solaris 10 (sparc) : 123893-81 (deprecated)

Solaris 10 (sparc) : 123923-12

Solaris 10 (sparc) : 123923-12 (deprecated)

Solaris 10 (sparc) : 123938-02

Solaris 10 (sparc) : 123938-03

Solaris 10 (sparc) : 123938-04

Solaris 10 (sparc) : 123938-05

Solaris 10 (sparc) : 123938-05 (deprecated)

Solaris 10 (sparc) : 124206-02

Solaris 10 (sparc) : 124208-01

Solaris 10 (sparc) : 124208-01

Solaris 10 (sparc) : 124244-02

Solaris 10 (sparc) : 124256-06

Solaris 10 (sparc) : 124258-07

Solaris 10 (sparc) : 124301-16

Solaris 10 (sparc) : 124393-12

Solaris 10 (sparc) : 124393-12 (deprecated)

Solaris 10 (sparc) : 124393-13

Solaris 10 (sparc) : 124444-01

Solaris 10 (sparc) : 124444-01

Solaris 10 (sparc) : 124457-03 (deprecated)

Solaris 10 (sparc) : 124519-05 (deprecated)

Solaris 10 (sparc) : 124520-05 (deprecated)

Solaris 10 (sparc) : 124581-08

Solaris 10 (sparc) : 124581-09

Solaris 10 (sparc) : 124581-10

Solaris 10 (sparc) : 124581-11

Solaris 10 (sparc) : 124581-11 (deprecated)

Solaris 10 (sparc) : 124614-01

Solaris 10 (sparc) : 124622-02

Solaris 10 (sparc) : 124628-10

Solaris 10 (sparc) : 124628-10 (deprecated)

Solaris 10 (sparc) : 124630-42

Solaris 10 (sparc) : 124630-42 (deprecated)

Solaris 10 (sparc) : 124672-20

Solaris 10 (sparc) : 124672-20 (deprecated)

Solaris 10 (sparc) : 124847-04 (deprecated)

Solaris 10 (sparc) : 124922-03

Solaris 10 (sparc) : 124939-05 (deprecated)

Solaris 10 (sparc) : 124943-01

Solaris 10 (sparc) : 124943-01

Solaris 10 (sparc) : 124997-01

Solaris 10 (sparc) : 124997-01 (deprecated)

Solaris 10 (sparc) : 125011-01

Solaris 10 (sparc) : 125011-01

Solaris 10 (sparc) : 125100-10

Solaris 10 (sparc) : 125123-01

Solaris 10 (sparc) : 125123-01

Solaris 10 (sparc) : 125136-71

Solaris 10 (sparc) : 125136-75

Solaris 10 (sparc) : 125136-97 (deprecated)

Solaris 10 (sparc) : 125137-71

Solaris 10 (sparc) : 125137-75

Solaris 10 (sparc) : 125137-97 (deprecated)

Solaris 10 (sparc) : 125194-04

Solaris 10 (sparc) : 125194-04 (deprecated)

Solaris 10 (sparc) : 125196-05

Solaris 10 (sparc) : 125215-04

Solaris 10 (sparc) : 125215-05

Solaris 10 (sparc) : 125215-07

Solaris 10 (sparc) : 125215-07 (deprecated)

Solaris 10 (sparc) : 125215-08

Solaris 10 (sparc) : 125251-02

Solaris 10 (sparc) : 125276-10 (deprecated)

Solaris 10 (sparc) : 125279-05 (deprecated)

Solaris 10 (sparc) : 125279-07

Solaris 10 (sparc) : 125279-09

Solaris 10 (sparc) : 125332-24

Solaris 10 (sparc) : 125332-24 (deprecated)

Solaris 10 (sparc) : 125358-15 (BEAST)

Solaris 10 (sparc) : 125358-19

Solaris 10 (sparc) : 125358-20

Solaris 10 (sparc) : 125358-21

Solaris 10 (sparc) : 125358-22

Solaris 10 (sparc) : 125358-25

Solaris 10 (sparc) : 125358-25 (deprecated)

Solaris 10 (sparc) : 125358-27

Solaris 10 (sparc) : 125388-03

Solaris 10 (sparc) : 125418-01

Solaris 10 (sparc) : 125418-01

Solaris 10 (sparc) : 125437-22

Solaris 10 (sparc) : 125437-22 (deprecated)

Solaris 10 (sparc) : 125482-03

Solaris 10 (sparc) : 125533-17

Solaris 10 (sparc) : 125533-19 (deprecated)

Solaris 10 (sparc) : 125539-06

Solaris 10 (sparc) : 125539-06

Solaris 10 (sparc) : 125541-04

Solaris 10 (sparc) : 125672-01

Solaris 10 (sparc) : 125713-02

Solaris 10 (sparc) : 125713-02 (deprecated)

Solaris 10 (sparc) : 125719-42

Solaris 10 (sparc) : 125719-54

Solaris 10 (sparc) : 125719-55

Solaris 10 (sparc) : 125719-56

Solaris 10 (sparc) : 125719-57

Solaris 10 (sparc) : 125719-58 (deprecated)

Solaris 10 (sparc) : 125719-60

Solaris 10 (sparc) : 125725-03

Solaris 10 (sparc) : 125725-03 (deprecated)

Solaris 10 (sparc) : 125731-11

Solaris 10 (sparc) : 125731-12

Solaris 10 (sparc) : 125731-13

Solaris 10 (sparc) : 125731-13 (deprecated)

Solaris 10 (sparc) : 125731-15

Solaris 10 (sparc) : 125833-05

Solaris 10 (sparc) : 125833-05 (deprecated)

Solaris 10 (sparc) : 125952-20

Solaris 10 (sparc) : 125952-20 (deprecated)

Solaris 10 (sparc) : 126050-07 (deprecated)

Solaris 10 (sparc) : 126106-42 (deprecated)

Solaris 10 (sparc) : 126119-02

Solaris 10 (sparc) : 126119-02 (deprecated)

Solaris 10 (sparc) : 126133-04

Solaris 10 (sparc) : 126206-10

Solaris 10 (sparc) : 126206-11

Solaris 10 (sparc) : 126206-12

Solaris 10 (sparc) : 126206-12 (deprecated)

Solaris 10 (sparc) : 126206-13

Solaris 10 (sparc) : 126258-03

Solaris 10 (sparc) : 126356-06

Solaris 10 (sparc) : 126363-08

Solaris 10 (sparc) : 126363-10 (deprecated)

Solaris 10 (sparc) : 126365-16 (deprecated)

Solaris 10 (sparc) : 126440-01 (deprecated)

Solaris 10 (sparc) : 126448-05

Solaris 10 (sparc) : 126479-26 (deprecated)

Solaris 10 (sparc) : 126546-04

Solaris 10 (sparc) : 126546-06

Solaris 10 (sparc) : 126546-07

Solaris 10 (sparc) : 126546-08

Solaris 10 (sparc) : 126546-10

Solaris 10 (sparc) : 126546-10 (deprecated)

Solaris 10 (sparc) : 126630-06

Solaris 10 (sparc) : 126630-06 (deprecated)

Solaris 10 (sparc) : 126661-02

Solaris 10 (sparc) : 126672-02

Solaris 10 (sparc) : 126868-04

Solaris 10 (sparc) : 126868-05

Solaris 10 (sparc) : 126868-05 (deprecated)

Solaris 10 (sparc) : 127111-11

Solaris 10 (sparc) : 127127-11 (deprecated)

Solaris 10 (sparc) : 127383-01

Solaris 10 (sparc) : 127383-01 (deprecated)

Solaris 10 (sparc) : 127411-16

Solaris 10 (sparc) : 127411-16 (deprecated)

Solaris 10 (sparc) : 127429-07 (deprecated)

Solaris 10 (sparc) : 127553-08 (deprecated)

Solaris 10 (sparc) : 127556-05 (deprecated)

Solaris 10 (sparc) : 127655-07 (deprecated)

Solaris 10 (sparc) : 127683-07

Solaris 10 (sparc) : 127683-07 (deprecated)

Solaris 10 (sparc) : 127716-01

Solaris 10 (sparc) : 127716-01

Solaris 10 (sparc) : 127718-05

Solaris 10 (sparc) : 127724-02

Solaris 10 (sparc) : 127724-02 (deprecated)

Solaris 10 (sparc) : 127737-01

Solaris 10 (sparc) : 127737-01

Solaris 10 (sparc) : 127739-03

Solaris 10 (sparc) : 127743-02

Solaris 10 (sparc) : 127753-02

Solaris 10 (sparc) : 127784-01

Solaris 10 (sparc) : 127784-01

Solaris 10 (sparc) : 127853-02

Solaris 10 (sparc) : 127872-02

Solaris 10 (sparc) : 127872-02 (deprecated)

Solaris 10 (sparc) : 127888-11

Solaris 10 (sparc) : 127959-02

Solaris 10 (sparc) : 128000-01

Solaris 10 (sparc) : 128165-02 (deprecated)

Solaris 10 (sparc) : 128294-02

Solaris 10 (sparc) : 128306-05

Solaris 10 (sparc) : 128328-01

Solaris 10 (sparc) : 128415-01

Solaris 10 (sparc) : 128415-01

Solaris 10 (sparc) : 128491-01

Solaris 10 (sparc) : 128491-01

Solaris 10 (sparc) : 128640-30

Solaris 10 (sparc) : 128640-30 (deprecated)

Solaris 10 (sparc) : 136716-01

Solaris 10 (sparc) : 136716-01

Solaris 10 (sparc) : 136839-01

Solaris 10 (sparc) : 136839-01 (deprecated)

Solaris 10 (sparc) : 136859-02 (deprecated)

Solaris 10 (sparc) : 136860-02 (deprecated)

Solaris 10 (sparc) : 136863-01 (deprecated)

Solaris 10 (sparc) : 136882-03

Solaris 10 (sparc) : 136882-04

Solaris 10 (sparc) : 136882-05

Solaris 10 (sparc) : 136882-06

Solaris 10 (sparc) : 136882-07

Solaris 10 (sparc) : 136882-08

Solaris 10 (sparc) : 136882-08 (deprecated)

Solaris 10 (sparc) : 136882-09

Solaris 10 (sparc) : 136882-10

Solaris 10 (sparc) : 136892-01

Solaris 10 (sparc) : 136892-01

Solaris 10 (sparc) : 136893-02

Solaris 10 (sparc) : 136893-02 (deprecated)

Solaris 10 (sparc) : 136998-10

Solaris 10 (sparc) : 136998-10 (deprecated)

Solaris 10 (sparc) : 137000-08

Solaris 10 (sparc) : 137000-08 (deprecated)

Solaris 10 (sparc) : 137004-09

Solaris 10 (sparc) : 137004-09 (deprecated)

Solaris 10 (sparc) : 137017-03

Solaris 10 (sparc) : 137019-02

Solaris 10 (sparc) : 137032-01 (deprecated)

Solaris 10 (sparc) : 137080-07

Solaris 10 (sparc) : 137080-09

Solaris 10 (sparc) : 137080-10

Solaris 10 (sparc) : 137080-11 (deprecated)

Solaris 10 (sparc) : 137093-01

Solaris 10 (sparc) : 137093-01 (deprecated)

Solaris 10 (sparc) : 137097-02

Solaris 10 (sparc) : 137097-02 (deprecated)

Solaris 10 (sparc) : 137111-08

Solaris 10 (sparc) : 137121-06

Solaris 10 (sparc) : 137137-09 (deprecated)

Solaris 10 (sparc) : 137147-07

Solaris 10 (sparc) : 137147-08

Solaris 10 (sparc) : 137147-08 (deprecated)

Solaris 10 (sparc) : 137204-31

Solaris 10 (sparc) : 137204-33

Solaris 10 (sparc) : 137204-34

Solaris 10 (sparc) : 137204-35

Solaris 10 (sparc) : 137204-36

Solaris 10 (sparc) : 137204-37

Solaris 10 (sparc) : 137204-38

Solaris 10 (sparc) : 137204-38 (deprecated)

Solaris 10 (sparc) : 137289-02

Solaris 10 (sparc) : 137321-02

Solaris 10 (sparc) : 137321-03

Solaris 10 (sparc) : 137321-04

Solaris 10 (sparc) : 137321-04 (deprecated)

Solaris 10 (sparc) : 137631-17

Solaris 10 (sparc) : 137871-02 (deprecated)

Solaris 10 (sparc) : 138060-04

Solaris 10 (sparc) : 138068-01

Solaris 10 (sparc) : 138068-01

Solaris 10 (sparc) : 138070-03

Solaris 10 (sparc) : 138083-01

Solaris 10 (sparc) : 138083-01

Solaris 10 (sparc) : 138104-01

Solaris 10 (sparc) : 138195-04

Solaris 10 (sparc) : 138223-03

Solaris 10 (sparc) : 138253-02

Solaris 10 (sparc) : 138263-03

Solaris 10 (sparc) : 138269-02

Solaris 10 (sparc) : 138322-03

Solaris 10 (sparc) : 138352-06 (deprecated)

Solaris 10 (sparc) : 138361-01 (deprecated)

Solaris 10 (sparc) : 138371-06

Solaris 10 (sparc) : 138373-02

Solaris 10 (sparc) : 138387-01

Solaris 10 (sparc) : 138536-01

Solaris 10 (sparc) : 138536-01 (deprecated)

Solaris 10 (sparc) : 138553-12 (deprecated)

Solaris 10 (sparc) : 138623-04

Solaris 10 (sparc) : 138627-07

Solaris 10 (sparc) : 138632-03

Solaris 10 (sparc) : 138647-01 (deprecated)

Solaris 10 (sparc) : 138686-07

Solaris 10 (sparc) : 138822-12

Solaris 10 (sparc) : 138822-12 (deprecated)

Solaris 10 (sparc) : 138824-12

Solaris 10 (sparc) : 138824-12 (deprecated)

Solaris 10 (sparc) : 138826-12

Solaris 10 (sparc) : 138826-12 (deprecated)

Solaris 10 (sparc) : 138874-05

Solaris 10 (sparc) : 138876-01

Solaris 10 (sparc) : 138876-01

Solaris 10 (sparc) : 138880-02

Solaris 10 (sparc) : 138888-08

Solaris 10 (sparc) : 139099-04

Solaris 10 (sparc) : 139099-04 (deprecated)

Solaris 10 (sparc) : 139099-07

Solaris 10 (sparc) : 139289-02

Solaris 10 (sparc) : 139289-02 (deprecated)

Solaris 10 (sparc) : 139291-02

Solaris 10 (sparc) : 139291-02 (deprecated)

Solaris 10 (sparc) : 139390-01

Solaris 10 (sparc) : 139390-01

Solaris 10 (sparc) : 139395-02 (deprecated)

Solaris 10 (sparc) : 139396-02 (deprecated)

Solaris 10 (sparc) : 139397-02 (deprecated)

Solaris 10 (sparc) : 139398-02 (deprecated)

Solaris 10 (sparc) : 139459-01

Solaris 10 (sparc) : 139459-01

Solaris 10 (sparc) : 139462-02

Solaris 10 (sparc) : 139462-02

Solaris 10 (sparc) : 139466-04

Solaris 10 (sparc) : 139478-01

Solaris 10 (sparc) : 139478-01

Solaris 10 (sparc) : 139481-01

Solaris 10 (sparc) : 139481-01

Solaris 10 (sparc) : 139483-05

Solaris 10 (sparc) : 139498-04

Solaris 10 (sparc) : 139500-04

Solaris 10 (sparc) : 139548-07 (deprecated)

Solaris 10 (sparc) : 139555-08

Solaris 10 (sparc) : 139555-08 (deprecated)

Solaris 10 (sparc) : 139560-02

Solaris 10 (sparc) : 139613-04 (deprecated)

Solaris 10 (sparc) : 139620-01

Solaris 10 (sparc) : 139620-01 (deprecated)

Solaris 10 (sparc) : 139832-12 (deprecated)

Solaris 10 (sparc) : 139967-02

Solaris 10 (sparc) : 139969-02

Solaris 10 (sparc) : 139982-04

Solaris 10 (sparc) : 139986-01 (deprecated)

Solaris 10 (sparc) : 139991-03

Solaris 10 (sparc) : 140074-09

Solaris 10 (sparc) : 140159-03

Solaris 10 (sparc) : 140196-01

Solaris 10 (sparc) : 140196-01

Solaris 10 (sparc) : 140383-01

Solaris 10 (sparc) : 140383-01

Solaris 10 (sparc) : 140386-04

Solaris 10 (sparc) : 140387-02

Solaris 10 (sparc) : 140387-02

Solaris 10 (sparc) : 140391-03

Solaris 10 (sparc) : 140397-11

Solaris 10 (sparc) : 140399-03

Solaris 10 (sparc) : 140399-03

Solaris 10 (sparc) : 140455-01

Solaris 10 (sparc) : 140455-03 (deprecated)

Solaris 10 (sparc) : 140559-01

Solaris 10 (sparc) : 140562-02

Solaris 10 (sparc) : 140563-01

Solaris 10 (sparc) : 140774-03

Solaris 10 (sparc) : 140860-02 (deprecated)

Solaris 10 (sparc) : 140917-02

Solaris 10 (sparc) : 140921-02

Solaris 10 (sparc) : 140993-05 (deprecated)

Solaris 10 (sparc) : 141008-01

Solaris 10 (sparc) : 141008-01

Solaris 10 (sparc) : 141014-01

Solaris 10 (sparc) : 141014-01

Solaris 10 (sparc) : 141020-03

Solaris 10 (sparc) : 141022-02

Solaris 10 (sparc) : 141026-14

Solaris 10 (sparc) : 141030-10

Solaris 10 (sparc) : 141104-04

Solaris 10 (sparc) : 141104-04 (deprecated)

Solaris 10 (sparc) : 141414-10

Solaris 10 (sparc) : 141444-09 (deprecated)

Solaris 10 (sparc) : 141481-03 (deprecated)

Solaris 10 (sparc) : 141500-08

Solaris 10 (sparc) : 141502-02

Solaris 10 (sparc) : 141506-09

Solaris 10 (sparc) : 141514-04

Solaris 10 (sparc) : 141552-04

Solaris 10 (sparc) : 141552-04

Solaris 10 (sparc) : 141586-01 (deprecated)

Solaris 10 (sparc) : 141590-02

Solaris 10 (sparc) : 141596-10

Solaris 10 (sparc) : 141690-02

Solaris 10 (sparc) : 141709-03

Solaris 10 (sparc) : 141709-03 (deprecated)

Solaris 10 (sparc) : 141719-01

Solaris 10 (sparc) : 141719-01

Solaris 10 (sparc) : 141733-04

Solaris 10 (sparc) : 141742-04

Solaris 10 (sparc) : 141765-01

Solaris 10 (sparc) : 141765-01

Solaris 10 (sparc) : 141778-02

Solaris 10 (sparc) : 141878-12

Solaris 10 (sparc) : 141899-03

Solaris 10 (sparc) : 141910-01

Solaris 10 (sparc) : 141930-01

Solaris 10 (sparc) : 141930-01

Solaris 10 (sparc) : 142188-01

Solaris 10 (sparc) : 142188-01 (deprecated)

Solaris 10 (sparc) : 142189-01

Solaris 10 (sparc) : 142189-01 (deprecated)

Solaris 10 (sparc) : 142240-01

Solaris 10 (sparc) : 142242-05

Solaris 10 (sparc) : 142251-02 (deprecated)

Solaris 10 (sparc) : 142259-07

Solaris 10 (sparc) : 142286-01

Solaris 10 (sparc) : 142286-01

Solaris 10 (sparc) : 142397-01 (deprecated)

Solaris 10 (sparc) : 142436-08

Solaris 10 (sparc) : 142529-01 (deprecated)

Solaris 10 (sparc) : 142529-02

Solaris 10 (sparc) : 142785-17

Solaris 10 (sparc) : 142785-17 (deprecated)

Solaris 10 (sparc) : 142824-19

Solaris 10 (sparc) : 142824-24 (POODLE)

Solaris 10 (sparc) : 142824-29

Solaris 10 (sparc) : 142824-29 (deprecated)

Solaris 10 (sparc) : 142846-04 (deprecated)

Solaris 10 (sparc) : 142900-15

Solaris 10 (sparc) : 142909-17 (deprecated)

Solaris 10 (sparc) : 143049-02 (deprecated)

Solaris 10 (sparc) : 143140-04

Solaris 10 (sparc) : 143140-04

Solaris 10 (sparc) : 143308-03 (deprecated)

Solaris 10 (sparc) : 143317-03

Solaris 10 (sparc) : 143317-03 (deprecated)

Solaris 10 (sparc) : 143390-01

Solaris 10 (sparc) : 143390-01 (deprecated)

Solaris 10 (sparc) : 143502-01

Solaris 10 (sparc) : 143502-01 (deprecated)

Solaris 10 (sparc) : 143506-06

Solaris 10 (sparc) : 143506-07

Solaris 10 (sparc) : 143506-11

Solaris 10 (sparc) : 143506-12 (deprecated)

Solaris 10 (sparc) : 143506-13

Solaris 10 (sparc) : 143506-14

Solaris 10 (sparc) : 143510-01

Solaris 10 (sparc) : 143525-01

Solaris 10 (sparc) : 143525-01

Solaris 10 (sparc) : 143559-10

Solaris 10 (sparc) : 143559-10

Solaris 10 (sparc) : 143561-09

Solaris 10 (sparc) : 143592-09

Solaris 10 (sparc) : 143615-02

Solaris 10 (sparc) : 143645-16

Solaris 10 (sparc) : 143725-01

Solaris 10 (sparc) : 143725-02

Solaris 10 (sparc) : 143725-04

Solaris 10 (sparc) : 143725-06

Solaris 10 (sparc) : 143725-09

Solaris 10 (sparc) : 143725-10

Solaris 10 (sparc) : 143725-11

Solaris 10 (sparc) : 143725-11 (deprecated)

Solaris 10 (sparc) : 143725-12

Solaris 10 (sparc) : 143725-13

Solaris 10 (sparc) : 143727-01

Solaris 10 (sparc) : 143727-02

Solaris 10 (sparc) : 143727-03

Solaris 10 (sparc) : 143727-04

Solaris 10 (sparc) : 143727-06 (deprecated)

Solaris 10 (sparc) : 143731-01

Solaris 10 (sparc) : 143731-01 (deprecated)

Solaris 10 (sparc) : 143733-01

Solaris 10 (sparc) : 143733-01 (deprecated)

Solaris 10 (sparc) : 143739-01

Solaris 10 (sparc) : 143739-01 (deprecated)

Solaris 10 (sparc) : 143749-02 (deprecated)

Solaris 10 (sparc) : 143937-03

Solaris 10 (sparc) : 143941-02

Solaris 10 (sparc) : 144047-01 (deprecated)

Solaris 10 (sparc) : 144053-04

Solaris 10 (sparc) : 144106-01

Solaris 10 (sparc) : 144106-01 (deprecated)

Solaris 10 (sparc) : 144221-12

Solaris 10 (sparc) : 144221-17 (deprecated)

Solaris 10 (sparc) : 144229-02

Solaris 10 (sparc) : 144229-02 (deprecated)

Solaris 10 (sparc) : 144254-01

Solaris 10 (sparc) : 144254-01

Solaris 10 (sparc) : 144325-01

Solaris 10 (sparc) : 144325-01 (deprecated)

Solaris 10 (sparc) : 144327-02

Solaris 10 (sparc) : 144327-02 (deprecated)

Solaris 10 (sparc) : 144488-17

Solaris 10 (sparc) : 144500-19 (deprecated)

Solaris 10 (sparc) : 144536-02

Solaris 10 (sparc) : 144674-02

Solaris 10 (sparc) : 144891-02

Solaris 10 (sparc) : 144891-02

Solaris 10 (sparc) : 144994-02

Solaris 10 (sparc) : 144994-02 (deprecated)

Solaris 10 (sparc) : 144994-03

Solaris 10 (sparc) : 144994-04

Solaris 10 (sparc) : 144996-02

Solaris 10 (sparc) : 144996-02 (deprecated)

Solaris 10 (sparc) : 145006-04

Solaris 10 (sparc) : 145006-07

Solaris 10 (sparc) : 145006-09 (deprecated)

Solaris 10 (sparc) : 145044-03

Solaris 10 (sparc) : 145069-02

Solaris 10 (sparc) : 145080-13

Solaris 10 (sparc) : 145080-15

Solaris 10 (sparc) : 145080-15 (deprecated)

Solaris 10 (sparc) : 145102-01

Solaris 10 (sparc) : 145102-01

Solaris 10 (sparc) : 145124-02

Solaris 10 (sparc) : 145124-02

Solaris 10 (sparc) : 145198-01

Solaris 10 (sparc) : 145198-01

Solaris 10 (sparc) : 145200-13

Solaris 10 (sparc) : 145200-13 (deprecated)

Solaris 10 (sparc) : 145333-33

Solaris 10 (sparc) : 145333-34

Solaris 10 (sparc) : 145333-39 (deprecated)

Solaris 10 (sparc) : 145335-22 (deprecated)

Solaris 10 (sparc) : 145337-05 (deprecated)

Solaris 10 (sparc) : 145341-06 (deprecated)

Solaris 10 (sparc) : 145343-07 (deprecated)

Solaris 10 (sparc) : 145345-04 (deprecated)

Solaris 10 (sparc) : 145638-10

Solaris 10 (sparc) : 145638-11 (deprecated)

Solaris 10 (sparc) : 145640-04

Solaris 10 (sparc) : 145644-06

Solaris 10 (sparc) : 145644-07 (deprecated)

Solaris 10 (sparc) : 145646-08

Solaris 10 (sparc) : 145646-11 (deprecated)

Solaris 10 (sparc) : 145711-07

Solaris 10 (sparc) : 145711-07 (deprecated)

Solaris 10 (sparc) : 145796-02

Solaris 10 (sparc) : 145899-08

Solaris 10 (sparc) : 145961-02

Solaris 10 (sparc) : 146018-03

Solaris 10 (sparc) : 146032-05

Solaris 10 (sparc) : 146032-05

Solaris 10 (sparc) : 146054-07 (deprecated)

Solaris 10 (sparc) : 146085-08

Solaris 10 (sparc) : 146232-21

Solaris 10 (sparc) : 146241-05 (deprecated)

Solaris 10 (sparc) : 146279-01

Solaris 10 (sparc) : 146279-01

Solaris 10 (sparc) : 146288-03 (deprecated)

Solaris 10 (sparc) : 146363-01

Solaris 10 (sparc) : 146363-01

Solaris 10 (sparc) : 146486-04

Solaris 10 (sparc) : 146486-04

Solaris 10 (sparc) : 146566-01

Solaris 10 (sparc) : 146576-01

Solaris 10 (sparc) : 146576-01

Solaris 10 (sparc) : 146666-04

Solaris 10 (sparc) : 146673-01

Solaris 10 (sparc) : 146673-01 (deprecated)

Solaris 10 (sparc) : 146694-02 (deprecated)

Solaris 10 (sparc) : 146694-03

Solaris 10 (sparc) : 146760-07 (deprecated)

Solaris 10 (sparc) : 146762-10

Solaris 10 (sparc) : 146762-14 (deprecated)

Solaris 10 (sparc) : 146769-01

Solaris 10 (sparc) : 146769-01

Solaris 10 (sparc) : 146802-03

Solaris 10 (sparc) : 146834-02

Solaris 10 (sparc) : 146834-02 (deprecated)

Solaris 10 (sparc) : 146857-01

Solaris 10 (sparc) : 146857-01

Solaris 10 (sparc) : 146861-01

Solaris 10 (sparc) : 147082-02 (deprecated)

Solaris 10 (sparc) : 147084-02 (deprecated)

Solaris 10 (sparc) : 147086-05 (deprecated)

Solaris 10 (sparc) : 147087-03 (deprecated)

Solaris 10 (sparc) : 147089-03 (deprecated)

Solaris 10 (sparc) : 147091-05 (deprecated)

Solaris 10 (sparc) : 147095-03 (deprecated)

Solaris 10 (sparc) : 147143-17 (deprecated)

Solaris 10 (sparc) : 147147-26 (deprecated)

Solaris 10 (sparc) : 147155-02 (deprecated)

Solaris 10 (sparc) : 147159-05

Solaris 10 (sparc) : 147182-01

Solaris 10 (sparc) : 147182-01

Solaris 10 (sparc) : 147217-02

Solaris 10 (sparc) : 147217-05

Solaris 10 (sparc) : 147217-05 (deprecated)

Solaris 10 (sparc) : 147219-01

Solaris 10 (sparc) : 147219-01 (deprecated)

Solaris 10 (sparc) : 147227-01

Solaris 10 (sparc) : 147266-01

Solaris 10 (sparc) : 147378-01

Solaris 10 (sparc) : 147378-01 (deprecated)

Solaris 10 (sparc) : 147416-02 (deprecated)

Solaris 10 (sparc) : 147434-01

Solaris 10 (sparc) : 147440-15

Solaris 10 (sparc) : 147446-01 (deprecated)

Solaris 10 (sparc) : 147497-02 (deprecated)

Solaris 10 (sparc) : 147673-08

Solaris 10 (sparc) : 147673-10

Solaris 10 (sparc) : 147673-11

Solaris 10 (sparc) : 147673-11 (deprecated)

Solaris 10 (sparc) : 147692-52

Solaris 10 (sparc) : 147692-65

Solaris 10 (sparc) : 147692-76

Solaris 10 (sparc) : 147692-81

Solaris 10 (sparc) : 147692-82

Solaris 10 (sparc) : 147692-91

Solaris 10 (sparc) : 147692-99 (deprecated)

Solaris 10 (sparc) : 147693-52

Solaris 10 (sparc) : 147693-65

Solaris 10 (sparc) : 147693-76

Solaris 10 (sparc) : 147693-81

Solaris 10 (sparc) : 147693-82

Solaris 10 (sparc) : 147693-91

Solaris 10 (sparc) : 147693-99 (deprecated)

Solaris 10 (sparc) : 147707-09

Solaris 10 (sparc) : 147713-01

Solaris 10 (sparc) : 147713-01

Solaris 10 (sparc) : 147715-04

Solaris 10 (sparc) : 147715-04

Solaris 10 (sparc) : 147793-09

Solaris 10 (sparc) : 147793-12

Solaris 10 (sparc) : 147793-14

Solaris 10 (sparc) : 147793-15

Solaris 10 (sparc) : 147793-16

Solaris 10 (sparc) : 147793-17

Solaris 10 (sparc) : 147793-20

Solaris 10 (sparc) : 147793-22

Solaris 10 (sparc) : 147793-22 (deprecated)

Solaris 10 (sparc) : 147793-23

Solaris 10 (sparc) : 147935-01 (deprecated)

Solaris 10 (sparc) : 147988-01

Solaris 10 (sparc) : 147988-01

Solaris 10 (sparc) : 147992-06

Solaris 10 (sparc) : 147992-10

Solaris 10 (sparc) : 147992-10 (deprecated)

Solaris 10 (sparc) : 148002-01

Solaris 10 (sparc) : 148002-01 (deprecated)

Solaris 10 (sparc) : 148004-01

Solaris 10 (sparc) : 148004-01 (deprecated)

Solaris 10 (sparc) : 148006-01

Solaris 10 (sparc) : 148006-01 (deprecated)

Solaris 10 (sparc) : 148027-03 (deprecated)

Solaris 10 (sparc) : 148071-12

Solaris 10 (sparc) : 148071-13

Solaris 10 (sparc) : 148071-14

Solaris 10 (sparc) : 148071-15

Solaris 10 (sparc) : 148071-16

Solaris 10 (sparc) : 148071-17

Solaris 10 (sparc) : 148071-18

Solaris 10 (sparc) : 148071-19 (deprecated)

Solaris 10 (sparc) : 148104-11

Solaris 10 (sparc) : 148104-21

Solaris 10 (sparc) : 148104-23

Solaris 10 (sparc) : 148104-23 (deprecated)

Solaris 10 (sparc) : 148104-26

Solaris 10 (sparc) : 148104-29

Solaris 10 (sparc) : 148112-02 (deprecated)

Solaris 10 (sparc) : 148135-01

Solaris 10 (sparc) : 148135-01 (deprecated)

Solaris 10 (sparc) : 148165-02

Solaris 10 (sparc) : 148165-02 (deprecated)

Solaris 10 (sparc) : 148241-02

Solaris 10 (sparc) : 148241-05 (deprecated)

Solaris 10 (sparc) : 148309-06

Solaris 10 (sparc) : 148309-08 (deprecated)

Solaris 10 (sparc) : 148309-10

Solaris 10 (sparc) : 148379-15

Solaris 10 (sparc) : 148383-01

Solaris 10 (sparc) : 148383-01 (deprecated)

Solaris 10 (sparc) : 148403-01

Solaris 10 (sparc) : 148403-01 (deprecated)

Solaris 10 (sparc) : 148407-01

Solaris 10 (sparc) : 148407-01 (deprecated)

Solaris 10 (sparc) : 148423-01

Solaris 10 (sparc) : 148423-01 (deprecated)

Solaris 10 (sparc) : 148561-06

Solaris 10 (sparc) : 148561-08

Solaris 10 (sparc) : 148561-11

Solaris 10 (sparc) : 148561-12

Solaris 10 (sparc) : 148561-12 (deprecated)

Solaris 10 (sparc) : 148565-01

Solaris 10 (sparc) : 148565-01 (deprecated)

Solaris 10 (sparc) : 148579-08 (deprecated)

Solaris 10 (sparc) : 148582-08 (deprecated)

Solaris 10 (sparc) : 148601-01

Solaris 10 (sparc) : 148625-01

Solaris 10 (sparc) : 148625-01 (deprecated)

Solaris 10 (sparc) : 148627-02

Solaris 10 (sparc) : 148627-02 (deprecated)

Solaris 10 (sparc) : 148657-01

Solaris 10 (sparc) : 148657-01 (deprecated)

Solaris 10 (sparc) : 148693-01

Solaris 10 (sparc) : 148693-01 (deprecated)

Solaris 10 (sparc) : 148768-01

Solaris 10 (sparc) : 148768-02

Solaris 10 (sparc) : 148768-02 (deprecated)

Solaris 10 (sparc) : 148870-01

Solaris 10 (sparc) : 148870-01 (deprecated)

Solaris 10 (sparc) : 148881-02

Solaris 10 (sparc) : 148881-03 (deprecated)

Solaris 10 (sparc) : 148888-05 (deprecated)

Solaris 10 (sparc) : 148948-01

Solaris 10 (sparc) : 148948-01 (deprecated)

Solaris 10 (sparc) : 148975-01

Solaris 10 (sparc) : 148975-01 (deprecated)

Solaris 10 (sparc) : 149067-01

Solaris 10 (sparc) : 149067-01 (deprecated)

Solaris 10 (sparc) : 149071-01

Solaris 10 (sparc) : 149071-01 (deprecated)

Solaris 10 (sparc) : 149075-01

Solaris 10 (sparc) : 149075-01 (deprecated)

Solaris 10 (sparc) : 149106-01

Solaris 10 (sparc) : 149106-01 (deprecated)

Solaris 10 (sparc) : 149108-01

Solaris 10 (sparc) : 149108-01 (deprecated)

Solaris 10 (sparc) : 149112-01

Solaris 10 (sparc) : 149112-01 (deprecated)

Solaris 10 (sparc) : 149149-01

Solaris 10 (sparc) : 149149-01 (deprecated)

Solaris 10 (sparc) : 149163-01

Solaris 10 (sparc) : 149163-01 (deprecated)

Solaris 10 (sparc) : 149165-01

Solaris 10 (sparc) : 149165-01 (deprecated)

Solaris 10 (sparc) : 149175-13

Solaris 10 (sparc) : 149175-13 (deprecated)

Solaris 10 (sparc) : 149191-01

Solaris 10 (sparc) : 149191-01 (deprecated)

Solaris 10 (sparc) : 149395-02 (deprecated)

Solaris 10 (sparc) : 149432-02 (deprecated)

Solaris 10 (sparc) : 149453-02

Solaris 10 (sparc) : 149453-02 (deprecated)

Solaris 10 (sparc) : 149483-01

Solaris 10 (sparc) : 149483-01 (deprecated)

Solaris 10 (sparc) : 149496-02

Solaris 10 (sparc) : 149496-02 (deprecated)

Solaris 10 (sparc) : 149638-02

Solaris 10 (sparc) : 149638-05 (deprecated)

Solaris 10 (sparc) : 149646-02

Solaris 10 (sparc) : 149646-02 (deprecated)

Solaris 10 (sparc) : 149895-01 (deprecated)

Solaris 10 (sparc) : 150051-01 (deprecated)

Solaris 10 (sparc) : 150100-01

Solaris 10 (sparc) : 150100-01 (deprecated)

Solaris 10 (sparc) : 150113-02

Solaris 10 (sparc) : 150113-02 (deprecated)

Solaris 10 (sparc) : 150117-01

Solaris 10 (sparc) : 150117-01

Solaris 10 (sparc) : 150119-03

Solaris 10 (sparc) : 150119-04 (deprecated)

Solaris 10 (sparc) : 150119-06

Solaris 10 (sparc) : 150123-01

Solaris 10 (sparc) : 150123-01 (deprecated)

Solaris 10 (sparc) : 150157-01

Solaris 10 (sparc) : 150157-01 (deprecated)

Solaris 10 (sparc) : 150312-06

Solaris 10 (sparc) : 150312-06 (deprecated)

Solaris 10 (sparc) : 150377-07

Solaris 10 (sparc) : 150379-02

Solaris 10 (sparc) : 150383-02

Solaris 10 (sparc) : 150383-03

Solaris 10 (sparc) : 150383-05

Solaris 10 (sparc) : 150383-06

Solaris 10 (sparc) : 150383-08

Solaris 10 (sparc) : 150383-09

Solaris 10 (sparc) : 150383-10

Solaris 10 (sparc) : 150383-12

Solaris 10 (sparc) : 150383-13

Solaris 10 (sparc) : 150383-14

Solaris 10 (sparc) : 150383-16

Solaris 10 (sparc) : 150383-17

Solaris 10 (sparc) : 150383-18

Solaris 10 (sparc) : 150383-19 (deprecated)

Solaris 10 (sparc) : 150400-06

Solaris 10 (sparc) : 150400-10

Solaris 10 (sparc) : 150400-11

Solaris 10 (sparc) : 150400-16

Solaris 10 (sparc) : 150400-23

Solaris 10 (sparc) : 150400-24

Solaris 10 (sparc) : 150400-26

Solaris 10 (sparc) : 150400-27

Solaris 10 (sparc) : 150400-35

Solaris 10 (sparc) : 150400-38

Solaris 10 (sparc) : 150400-40

Solaris 10 (sparc) : 150400-50

Solaris 10 (sparc) : 150400-51

Solaris 10 (sparc) : 150400-52

Solaris 10 (sparc) : 150400-53

Solaris 10 (sparc) : 150400-59

Solaris 10 (sparc) : 150400-59 (deprecated)

Solaris 10 (sparc) : 150400-62

Solaris 10 (sparc) : 150400-63

Solaris 10 (sparc) : 150400-64

Solaris 10 (sparc) : 150400-67

Solaris 10 (sparc) : 150400-68

Solaris 10 (sparc) : 150545-02

Solaris 10 (sparc) : 150545-02 (deprecated)

Solaris 10 (sparc) : 150584-02 (deprecated)

Solaris 10 (sparc) : 150616-01

Solaris 10 (sparc) : 150616-02

Solaris 10 (sparc) : 150616-02 (deprecated)

Solaris 10 (sparc) : 150618-02 (deprecated)

Solaris 10 (sparc) : 150817-03

Solaris 10 (sparc) : 150817-04

Solaris 10 (sparc) : 150817-04 (deprecated)

Solaris 10 (sparc) : 150832-08

Solaris 10 (sparc) : 150832-12 (deprecated)

Solaris 10 (sparc) : 150836-01

Solaris 10 (sparc) : 150836-01 (deprecated)

Solaris 10 (sparc) : 151009-11

Solaris 10 (sparc) : 151009-20

Solaris 10 (sparc) : 151009-40

Solaris 10 (sparc) : 151009-51

Solaris 10 (sparc) : 151009-60

Solaris 10 (sparc) : 151009-92

Solaris 10 (sparc) : 151009-92 (deprecated)

Solaris 10 (sparc) : 151074-02

Solaris 10 (sparc) : 151074-03

Solaris 10 (sparc) : 151074-06 (deprecated)

Solaris 10 (sparc) : 151145-01

Solaris 10 (sparc) : 151145-02 (deprecated)

Solaris 10 (sparc) : 151265-03 (deprecated)

Solaris 10 (sparc) : 151355-01

Solaris 10 (sparc) : 151355-01 (deprecated)

Solaris 10 (sparc) : 151561-01

Solaris 10 (sparc) : 151561-01 (deprecated)

Solaris 10 (sparc) : 151597-05

Solaris 10 (sparc) : 151597-05 (deprecated)

Solaris 10 (sparc) : 151672-03 (deprecated)

Solaris 10 (sparc) : 151717-01

Solaris 10 (sparc) : 151717-01 (deprecated)

Solaris 10 (sparc) : 151719-01

Solaris 10 (sparc) : 151719-01 (deprecated)

Solaris 10 (sparc) : 151721-01

Solaris 10 (sparc) : 151721-01 (deprecated)

Solaris 10 (sparc) : 151723-01

Solaris 10 (sparc) : 151723-01 (deprecated)

Solaris 10 (sparc) : 151755-01

Solaris 10 (sparc) : 151755-02 (deprecated)

Solaris 10 (sparc) : 151912-04

Solaris 10 (sparc) : 151912-05

Solaris 10 (sparc) : 151912-07

Solaris 10 (sparc) : 151912-08

Solaris 10 (sparc) : 151912-09

Solaris 10 (sparc) : 151912-10

Solaris 10 (sparc) : 151912-11

Solaris 10 (sparc) : 151912-11 (deprecated)

Solaris 10 (sparc) : 151912-12

Solaris 10 (sparc) : 151912-13

Solaris 10 (sparc) : 151912-14

Solaris 10 (sparc) : 151912-15

Solaris 10 (sparc) : 151914-04

Solaris 10 (sparc) : 151914-05

Solaris 10 (sparc) : 151914-07 (deprecated)

Solaris 10 (sparc) : 151934-01

Solaris 10 (sparc) : 151934-03

Solaris 10 (sparc) : 151934-04 (deprecated)

Solaris 10 (sparc) : 152076-41

Solaris 10 (sparc) : 152076-51

Solaris 10 (sparc) : 152076-81 (deprecated)

Solaris 10 (sparc) : 152076-91

Solaris 10 (sparc) : 152077-41

Solaris 10 (sparc) : 152077-51

Solaris 10 (sparc) : 152077-81 (deprecated)

Solaris 10 (sparc) : 152077-91

Solaris 10 (sparc) : 152096-21

Solaris 10 (sparc) : 152096-31

Solaris 10 (sparc) : 152096-61

Solaris 10 (sparc) : 152096-71

Solaris 10 (sparc) : 152096-71 (deprecated)

Solaris 10 (sparc) : 152096-91

Solaris 10 (sparc) : 152097-21

Solaris 10 (sparc) : 152097-31

Solaris 10 (sparc) : 152097-61

Solaris 10 (sparc) : 152097-71

Solaris 10 (sparc) : 152097-71 (deprecated)

Solaris 10 (sparc) : 152097-91

Solaris 10 (sparc) : 152100-12

Solaris 10 (sparc) : 152100-21

Solaris 10 (sparc) : 152100-31

Solaris 10 (sparc) : 152100-52

Solaris 10 (sparc) : 152100-62 (deprecated)

Solaris 10 (sparc) : 152100-81

Solaris 10 (sparc) : 152100-91

Solaris 10 (sparc) : 152100-92

Solaris 10 (sparc) : 152248-01

Solaris 10 (sparc) : 152248-01 (deprecated)

Solaris 10 (sparc) : 152248-02

Solaris 10 (sparc) : 152250-01

Solaris 10 (sparc) : 152250-01 (deprecated)

Solaris 10 (sparc) : 152252-01

Solaris 10 (sparc) : 152252-02

Solaris 10 (sparc) : 152252-02 (deprecated)

Solaris 10 (sparc) : 152252-03

Solaris 10 (sparc) : 152254-01

Solaris 10 (sparc) : 152254-01 (deprecated)

Solaris 10 (sparc) : 152260-01

Solaris 10 (sparc) : 152260-02

Solaris 10 (sparc) : 152260-03

Solaris 10 (sparc) : 152260-03 (deprecated)

Solaris 10 (sparc) : 152260-04

Solaris 10 (sparc) : 152264-01

Solaris 10 (sparc) : 152264-01 (deprecated)

Solaris 10 (sparc) : 152264-02

Solaris 10 (sparc) : 152363-01

Solaris 10 (sparc) : 152363-01 (deprecated)

Solaris 10 (sparc) : 152506-01

Solaris 10 (sparc) : 152506-01 (deprecated)

Solaris 10 (sparc) : 152510-03

Solaris 10 (sparc) : 152510-04

Solaris 10 (sparc) : 152510-06

Solaris 10 (sparc) : 152510-06 (deprecated)

Solaris 10 (sparc) : 152510-07

Solaris 10 (sparc) : 152510-08

Solaris 10 (sparc) : 152510-09

Solaris 10 (sparc) : 152514-01

Solaris 10 (sparc) : 152514-02

Solaris 10 (sparc) : 152514-02 (deprecated)

Solaris 10 (sparc) : 152643-03

Solaris 10 (sparc) : 152643-05

Solaris 10 (sparc) : 152643-05 (deprecated)

Solaris 10 (sparc) : 152643-06

Solaris 10 (sparc) : 152643-07

Solaris 10 (sparc) : 152643-08

Solaris 10 (sparc) : 152649-02 : dtappgather Arbitrary Directory Creation Local Privilege Escalation (EXTREMEPARR)

Solaris 10 (sparc) : 152651-01

Solaris 10 (sparc) : 152651-01 (deprecated)

Solaris 10 (sparc) : 152724-01

Solaris 10 (sparc) : 152724-02

Solaris 10 (sparc) : 152724-02 (deprecated)

Solaris 10 (sparc) : 152919-01

Solaris 10 (sparc) : 152919-11

Solaris 10 (sparc) : 152920-01

Solaris 10 (sparc) : 152920-11

Solaris 10 (sparc) : 152923-01

Solaris 10 (sparc) : 152924-01

Solaris 10 (sparc) : 152927-02

Solaris 10 (sparc) : 153056-01

Solaris 10 (sparc) : 153060-01

Solaris 10 (x86) : 108670-21 (deprecated)

Solaris 10 (x86) : 112761-13 (deprecated)

Solaris 10 (x86) : 114273-04

Solaris 10 (x86) : 114273-04 (deprecated)

Solaris 10 (x86) : 115611-25 (deprecated)

Solaris 10 (x86) : 115615-28 (deprecated)

Solaris 10 (x86) : 116649-25

Solaris 10 (x86) : 116833-04 (deprecated)

Solaris 10 (x86) : 118208-63 (deprecated)

Solaris 10 (x86) : 118345-13

Solaris 10 (x86) : 118372-10

Solaris 10 (x86) : 118541-42 (deprecated)

Solaris 10 (x86) : 118561-02

Solaris 10 (x86) : 118563-14

Solaris 10 (x86) : 118565-03

Solaris 10 (x86) : 118668-19

Solaris 10 (x86) : 118668-61

Solaris 10 (x86) : 118668-86 (deprecated)

Solaris 10 (x86) : 118669-19

Solaris 10 (x86) : 118669-61

Solaris 10 (x86) : 118669-86 (deprecated)

Solaris 10 (x86) : 118778-14 (deprecated)

Solaris 10 (x86) : 118813-03

Solaris 10 (x86) : 118844-20 (deprecated)

Solaris 10 (x86) : 118855-36 (deprecated)

Solaris 10 (x86) : 118919-21 (deprecated)

Solaris 10 (x86) : 118966-25

Solaris 10 (x86) : 118997-10

Solaris 10 (x86) : 119060-45

Solaris 10 (x86) : 119060-64

Solaris 10 (x86) : 119060-65

Solaris 10 (x86) : 119060-68

Solaris 10 (x86) : 119060-69

Solaris 10 (x86) : 119060-70

Solaris 10 (x86) : 119060-71

Solaris 10 (x86) : 119060-72 (deprecated)

Solaris 10 (x86) : 119060-73

Solaris 10 (x86) : 119062-03

Solaris 10 (x86) : 119064-01

Solaris 10 (x86) : 119064-02

Solaris 10 (x86) : 119064-02 (deprecated)

Solaris 10 (x86) : 119076-12

Solaris 10 (x86) : 119091-35

Solaris 10 (x86) : 119108-06

Solaris 10 (x86) : 119116-35 (deprecated)

Solaris 10 (x86) : 119118-52

Solaris 10 (x86) : 119118-54 (deprecated)

Solaris 10 (x86) : 119167-43

Solaris 10 (x86) : 119167-43 (deprecated)

Solaris 10 (x86) : 119214-27 (BEAST)

Solaris 10 (x86) : 119214-30

Solaris 10 (x86) : 119214-31

Solaris 10 (x86) : 119214-32

Solaris 10 (x86) : 119214-33

Solaris 10 (x86) : 119214-36

Solaris 10 (x86) : 119214-36 (deprecated)

Solaris 10 (x86) : 119214-37

Solaris 10 (x86) : 119214-38

Solaris 10 (x86) : 119253-32

Solaris 10 (x86) : 119253-32 (deprecated)

Solaris 10 (x86) : 119255-91

Solaris 10 (x86) : 119255-92

Solaris 10 (x86) : 119255-93 (deprecated)

Solaris 10 (x86) : 119281-25 (deprecated)

Solaris 10 (x86) : 119314-43 (deprecated)

Solaris 10 (x86) : 119316-19 (deprecated)

Solaris 10 (x86) : 119411-10

Solaris 10 (x86) : 119411-10 (deprecated)

Solaris 10 (x86) : 119465-17

Solaris 10 (x86) : 119465-17 (deprecated)

Solaris 10 (x86) : 119467-17 (deprecated)

Solaris 10 (x86) : 119535-29 (deprecated)

Solaris 10 (x86) : 119549-14

Solaris 10 (x86) : 119549-14 (deprecated)

Solaris 10 (x86) : 119594-01

Solaris 10 (x86) : 119594-01

Solaris 10 (x86) : 119720-01

Solaris 10 (x86) : 119720-01

Solaris 10 (x86) : 119725-06 (deprecated)

Solaris 10 (x86) : 119758-30

Solaris 10 (x86) : 119758-31

Solaris 10 (x86) : 119758-32

Solaris 10 (x86) : 119758-33

Solaris 10 (x86) : 119758-34

Solaris 10 (x86) : 119758-36

Solaris 10 (x86) : 119758-37

Solaris 10 (x86) : 119758-38

Solaris 10 (x86) : 119758-43

Solaris 10 (x86) : 119758-43 (deprecated)

Solaris 10 (x86) : 119758-44

Solaris 10 (x86) : 119765-07

Solaris 10 (x86) : 119765-07 (deprecated)

Solaris 10 (x86) : 119778-19 (deprecated)

Solaris 10 (x86) : 119784-25

Solaris 10 (x86) : 119784-29

Solaris 10 (x86) : 119784-30

Solaris 10 (x86) : 119784-31

Solaris 10 (x86) : 119784-32

Solaris 10 (x86) : 119784-33

Solaris 10 (x86) : 119784-36

Solaris 10 (x86) : 119784-37

Solaris 10 (x86) : 119784-38

Solaris 10 (x86) : 119784-39

Solaris 10 (x86) : 119784-40

Solaris 10 (x86) : 119784-40 (deprecated)

Solaris 10 (x86) : 119784-41

Solaris 10 (x86) : 119784-42

Solaris 10 (x86) : 119784-43

Solaris 10 (x86) : 119784-44

Solaris 10 (x86) : 119811-07

Solaris 10 (x86) : 119811-08

Solaris 10 (x86) : 119811-08 (deprecated)

Solaris 10 (x86) : 119813-18

Solaris 10 (x86) : 119813-20

Solaris 10 (x86) : 119813-22

Solaris 10 (x86) : 119813-24 (deprecated)

Solaris 10 (x86) : 119901-15

Solaris 10 (x86) : 119901-16

Solaris 10 (x86) : 119901-17

Solaris 10 (x86) : 119901-17 (deprecated)

Solaris 10 (x86) : 119904-02 (deprecated)

Solaris 10 (x86) : 119907-18

Solaris 10 (x86) : 119907-22 (deprecated)

Solaris 10 (x86) : 119999-03

Solaris 10 (x86) : 120012-14 (deprecated)

Solaris 10 (x86) : 120037-22

Solaris 10 (x86) : 120051-06

Solaris 10 (x86) : 120069-03

Solaris 10 (x86) : 120086-02

Solaris 10 (x86) : 120095-35

Solaris 10 (x86) : 120095-36

Solaris 10 (x86) : 120095-36 (deprecated)

Solaris 10 (x86) : 120186-23

Solaris 10 (x86) : 120190-23

Solaris 10 (x86) : 120202-07

Solaris 10 (x86) : 120202-08

Solaris 10 (x86) : 120202-08 (deprecated)

Solaris 10 (x86) : 120202-09

Solaris 10 (x86) : 120229-45 (deprecated)

Solaris 10 (x86) : 120273-33

Solaris 10 (x86) : 120273-42 (deprecated)

Solaris 10 (x86) : 120287-03

Solaris 10 (x86) : 120287-04 (deprecated)

Solaris 10 (x86) : 120293-02

Solaris 10 (x86) : 120293-02 (deprecated)

Solaris 10 (x86) : 120295-01

Solaris 10 (x86) : 120295-01

Solaris 10 (x86) : 120330-02

Solaris 10 (x86) : 120413-11 (deprecated)

Solaris 10 (x86) : 120415-27 (deprecated)

Solaris 10 (x86) : 120461-21 (deprecated)

Solaris 10 (x86) : 120468-05

Solaris 10 (x86) : 120470-02

Solaris 10 (x86) : 120501-28 (deprecated)

Solaris 10 (x86) : 120544-33

Solaris 10 (x86) : 120544-34

Solaris 10 (x86) : 120544-35

Solaris 10 (x86) : 120544-36 (deprecated)

Solaris 10 (x86) : 120652-01 (deprecated)

Solaris 10 (x86) : 120662-05

Solaris 10 (x86) : 120665-01

Solaris 10 (x86) : 120665-01

Solaris 10 (x86) : 120720-07

Solaris 10 (x86) : 120720-07 (deprecated)

Solaris 10 (x86) : 120740-08

Solaris 10 (x86) : 120740-08 (deprecated)

Solaris 10 (x86) : 120831-06 (deprecated)

Solaris 10 (x86) : 120955-12

Solaris 10 (x86) : 120955-12 (deprecated)

Solaris 10 (x86) : 120982-25

Solaris 10 (x86) : 121005-04

Solaris 10 (x86) : 121013-03

Solaris 10 (x86) : 121096-04

Solaris 10 (x86) : 121096-05

Solaris 10 (x86) : 121096-05 (deprecated)

Solaris 10 (x86) : 121119-21 (deprecated)

Solaris 10 (x86) : 121161-01

Solaris 10 (x86) : 121161-01 (deprecated)

Solaris 10 (x86) : 121208-03

Solaris 10 (x86) : 121212-02

Solaris 10 (x86) : 121212-02 (deprecated)

Solaris 10 (x86) : 121230-02

Solaris 10 (x86) : 121230-02

Solaris 10 (x86) : 121240-02

Solaris 10 (x86) : 121289-04

Solaris 10 (x86) : 121309-20 (deprecated)

Solaris 10 (x86) : 121395-03

Solaris 10 (x86) : 121429-15

Solaris 10 (x86) : 121429-15 (deprecated)

Solaris 10 (x86) : 121454-02 (deprecated)

Solaris 10 (x86) : 121582-20 (deprecated)

Solaris 10 (x86) : 121658-54 (deprecated)

Solaris 10 (x86) : 121914-20 (deprecated)

Solaris 10 (x86) : 121958-01 (deprecated)

Solaris 10 (x86) : 121959-01 (deprecated)

Solaris 10 (x86) : 122078-04

Solaris 10 (x86) : 122082-01

Solaris 10 (x86) : 122082-01

Solaris 10 (x86) : 122213-46

Solaris 10 (x86) : 122213-46 (deprecated)

Solaris 10 (x86) : 122240-03

Solaris 10 (x86) : 122260-06

Solaris 10 (x86) : 122260-09

Solaris 10 (x86) : 122260-09 (deprecated)

Solaris 10 (x86) : 122262-03

Solaris 10 (x86) : 122471-05 (deprecated)

Solaris 10 (x86) : 122676-05

Solaris 10 (x86) : 122794-36 (deprecated)

Solaris 10 (x86) : 122857-04

Solaris 10 (x86) : 122912-32

Solaris 10 (x86) : 122912-33

Solaris 10 (x86) : 122912-34

Solaris 10 (x86) : 122912-35

Solaris 10 (x86) : 122912-36

Solaris 10 (x86) : 122912-37

Solaris 10 (x86) : 122912-37 (deprecated)

Solaris 10 (x86) : 122959-06

Solaris 10 (x86) : 123006-07 (deprecated)

Solaris 10 (x86) : 123039-01 (deprecated)

Solaris 10 (x86) : 123040-01 (deprecated)

Solaris 10 (x86) : 123175-01

Solaris 10 (x86) : 123175-01 (deprecated)

Solaris 10 (x86) : 123247-11

Solaris 10 (x86) : 123325-03

Solaris 10 (x86) : 123325-03

Solaris 10 (x86) : 123403-01

Solaris 10 (x86) : 123403-01

Solaris 10 (x86) : 123591-12

Solaris 10 (x86) : 123591-12 (deprecated)

Solaris 10 (x86) : 123612-06 (deprecated)

Solaris 10 (x86) : 123614-02

Solaris 10 (x86) : 123614-02 (deprecated)

Solaris 10 (x86) : 123779-02

Solaris 10 (x86) : 123779-02

Solaris 10 (x86) : 123896-77

Solaris 10 (x86) : 123896-79

Solaris 10 (x86) : 123896-81 (deprecated)

Solaris 10 (x86) : 123924-11

Solaris 10 (x86) : 123924-11 (deprecated)

Solaris 10 (x86) : 123939-02

Solaris 10 (x86) : 123939-03

Solaris 10 (x86) : 123939-04

Solaris 10 (x86) : 123939-05

Solaris 10 (x86) : 123939-05 (deprecated)

Solaris 10 (x86) : 124207-02

Solaris 10 (x86) : 124209-01

Solaris 10 (x86) : 124209-01

Solaris 10 (x86) : 124245-02

Solaris 10 (x86) : 124259-06

Solaris 10 (x86) : 124302-16

Solaris 10 (x86) : 124394-12

Solaris 10 (x86) : 124394-12 (deprecated)

Solaris 10 (x86) : 124394-13

Solaris 10 (x86) : 124445-01

Solaris 10 (x86) : 124445-01

Solaris 10 (x86) : 124458-03 (deprecated)

Solaris 10 (x86) : 124521-05 (deprecated)

Solaris 10 (x86) : 124522-05 (deprecated)

Solaris 10 (x86) : 124582-08

Solaris 10 (x86) : 124582-09

Solaris 10 (x86) : 124582-10

Solaris 10 (x86) : 124582-11

Solaris 10 (x86) : 124582-11 (deprecated)

Solaris 10 (x86) : 124629-12

Solaris 10 (x86) : 124629-12 (deprecated)

Solaris 10 (x86) : 124631-42

Solaris 10 (x86) : 124631-42 (deprecated)

Solaris 10 (x86) : 124673-20

Solaris 10 (x86) : 124673-20 (deprecated)

Solaris 10 (x86) : 124848-04 (deprecated)

Solaris 10 (x86) : 124923-03

Solaris 10 (x86) : 124939-05 (deprecated)

Solaris 10 (x86) : 124944-01

Solaris 10 (x86) : 124944-01

Solaris 10 (x86) : 124998-01

Solaris 10 (x86) : 124998-01 (deprecated)

Solaris 10 (x86) : 125012-01

Solaris 10 (x86) : 125012-01

Solaris 10 (x86) : 125101-10

Solaris 10 (x86) : 125124-01

Solaris 10 (x86) : 125124-01

Solaris 10 (x86) : 125138-71

Solaris 10 (x86) : 125138-75

Solaris 10 (x86) : 125138-97 (deprecated)

Solaris 10 (x86) : 125139-71

Solaris 10 (x86) : 125139-75

Solaris 10 (x86) : 125139-97 (deprecated)

Solaris 10 (x86) : 125197-06

Solaris 10 (x86) : 125216-04

Solaris 10 (x86) : 125216-05

Solaris 10 (x86) : 125216-07

Solaris 10 (x86) : 125216-07 (deprecated)

Solaris 10 (x86) : 125216-08

Solaris 10 (x86) : 125252-02

Solaris 10 (x86) : 125280-05 (deprecated)

Solaris 10 (x86) : 125280-07

Solaris 10 (x86) : 125280-09

Solaris 10 (x86) : 125333-23

Solaris 10 (x86) : 125333-23 (deprecated)

Solaris 10 (x86) : 125359-15 (BEAST)

Solaris 10 (x86) : 125359-19

Solaris 10 (x86) : 125359-20

Solaris 10 (x86) : 125359-21

Solaris 10 (x86) : 125359-22

Solaris 10 (x86) : 125359-25

Solaris 10 (x86) : 125359-25 (deprecated)

Solaris 10 (x86) : 125359-27

Solaris 10 (x86) : 125389-03

Solaris 10 (x86) : 125419-01

Solaris 10 (x86) : 125423-02

Solaris 10 (x86) : 125438-22

Solaris 10 (x86) : 125438-22 (deprecated)

Solaris 10 (x86) : 125483-03

Solaris 10 (x86) : 125534-17

Solaris 10 (x86) : 125534-19 (deprecated)

Solaris 10 (x86) : 125540-06

Solaris 10 (x86) : 125540-06

Solaris 10 (x86) : 125542-04

Solaris 10 (x86) : 125720-59

Solaris 10 (x86) : 125720-65

Solaris 10 (x86) : 125720-66

Solaris 10 (x86) : 125720-67

Solaris 10 (x86) : 125720-68

Solaris 10 (x86) : 125720-70 (deprecated)

Solaris 10 (x86) : 125720-71

Solaris 10 (x86) : 125726-03

Solaris 10 (x86) : 125726-03 (deprecated)

Solaris 10 (x86) : 125732-11

Solaris 10 (x86) : 125732-12

Solaris 10 (x86) : 125732-13

Solaris 10 (x86) : 125732-13 (deprecated)

Solaris 10 (x86) : 125732-15

Solaris 10 (x86) : 125794-02

Solaris 10 (x86) : 125907-02

Solaris 10 (x86) : 125907-02 (deprecated)

Solaris 10 (x86) : 125953-20

Solaris 10 (x86) : 125953-20 (deprecated)

Solaris 10 (x86) : 126107-42 (deprecated)

Solaris 10 (x86) : 126120-02

Solaris 10 (x86) : 126120-02 (deprecated)

Solaris 10 (x86) : 126134-04

Solaris 10 (x86) : 126207-10

Solaris 10 (x86) : 126207-11

Solaris 10 (x86) : 126207-12

Solaris 10 (x86) : 126207-12 (deprecated)

Solaris 10 (x86) : 126207-13

Solaris 10 (x86) : 126254-02

Solaris 10 (x86) : 126257-07

Solaris 10 (x86) : 126259-03

Solaris 10 (x86) : 126357-06

Solaris 10 (x86) : 126364-08

Solaris 10 (x86) : 126364-10 (deprecated)

Solaris 10 (x86) : 126366-16 (deprecated)

Solaris 10 (x86) : 126422-02

Solaris 10 (x86) : 126441-01 (deprecated)

Solaris 10 (x86) : 126449-05

Solaris 10 (x86) : 126480-26 (deprecated)

Solaris 10 (x86) : 126547-04

Solaris 10 (x86) : 126547-06

Solaris 10 (x86) : 126547-07

Solaris 10 (x86) : 126547-08

Solaris 10 (x86) : 126547-10

Solaris 10 (x86) : 126547-10 (deprecated)

Solaris 10 (x86) : 126631-06

Solaris 10 (x86) : 126631-06 (deprecated)

Solaris 10 (x86) : 126662-02

Solaris 10 (x86) : 126837-01

Solaris 10 (x86) : 126837-01

Solaris 10 (x86) : 126869-05

Solaris 10 (x86) : 126869-06

Solaris 10 (x86) : 126869-06 (deprecated)

Solaris 10 (x86) : 127112-11

Solaris 10 (x86) : 127128-11 (deprecated)

Solaris 10 (x86) : 127413-16

Solaris 10 (x86) : 127413-16 (deprecated)

Solaris 10 (x86) : 127430-07 (deprecated)

Solaris 10 (x86) : 127431-07 (deprecated)

Solaris 10 (x86) : 127557-05 (deprecated)

Solaris 10 (x86) : 127656-07 (deprecated)

Solaris 10 (x86) : 127717-01

Solaris 10 (x86) : 127717-01

Solaris 10 (x86) : 127719-05

Solaris 10 (x86) : 127725-02

Solaris 10 (x86) : 127725-02 (deprecated)

Solaris 10 (x86) : 127738-01

Solaris 10 (x86) : 127738-01

Solaris 10 (x86) : 127740-03

Solaris 10 (x86) : 127744-02

Solaris 10 (x86) : 127751-02

Solaris 10 (x86) : 127785-01

Solaris 10 (x86) : 127785-01

Solaris 10 (x86) : 127854-02

Solaris 10 (x86) : 127873-02

Solaris 10 (x86) : 127873-02 (deprecated)

Solaris 10 (x86) : 127889-11

Solaris 10 (x86) : 127954-06

Solaris 10 (x86) : 127960-02

Solaris 10 (x86) : 128001-01

Solaris 10 (x86) : 128166-02 (deprecated)

Solaris 10 (x86) : 128295-02

Solaris 10 (x86) : 128307-05

Solaris 10 (x86) : 128329-01

Solaris 10 (x86) : 128338-02

Solaris 10 (x86) : 128412-01 (deprecated)

Solaris 10 (x86) : 128416-01

Solaris 10 (x86) : 128416-01

Solaris 10 (x86) : 128492-01

Solaris 10 (x86) : 128492-01

Solaris 10 (x86) : 128641-30

Solaris 10 (x86) : 128641-30 (deprecated)

Solaris 10 (x86) : 136717-01

Solaris 10 (x86) : 136717-01

Solaris 10 (x86) : 136840-01

Solaris 10 (x86) : 136840-01 (deprecated)

Solaris 10 (x86) : 136864-01 (deprecated)

Solaris 10 (x86) : 136883-03

Solaris 10 (x86) : 136883-04

Solaris 10 (x86) : 136883-05

Solaris 10 (x86) : 136883-06

Solaris 10 (x86) : 136883-07

Solaris 10 (x86) : 136883-08

Solaris 10 (x86) : 136883-08 (deprecated)

Solaris 10 (x86) : 136883-09

Solaris 10 (x86) : 136883-10

Solaris 10 (x86) : 136894-02

Solaris 10 (x86) : 136894-02 (deprecated)

Solaris 10 (x86) : 136999-10

Solaris 10 (x86) : 136999-10 (deprecated)

Solaris 10 (x86) : 137001-08

Solaris 10 (x86) : 137001-08 (deprecated)

Solaris 10 (x86) : 137005-09

Solaris 10 (x86) : 137005-09 (deprecated)

Solaris 10 (x86) : 137018-03

Solaris 10 (x86) : 137020-02

Solaris 10 (x86) : 137022-03

Solaris 10 (x86) : 137033-01 (deprecated)

Solaris 10 (x86) : 137081-07

Solaris 10 (x86) : 137081-09

Solaris 10 (x86) : 137081-10

Solaris 10 (x86) : 137081-11 (deprecated)

Solaris 10 (x86) : 137094-01

Solaris 10 (x86) : 137094-01 (deprecated)

Solaris 10 (x86) : 137098-02

Solaris 10 (x86) : 137098-02 (deprecated)

Solaris 10 (x86) : 137112-08

Solaris 10 (x86) : 137122-06

Solaris 10 (x86) : 137138-09 (deprecated)

Solaris 10 (x86) : 137148-07

Solaris 10 (x86) : 137148-08

Solaris 10 (x86) : 137148-08 (deprecated)

Solaris 10 (x86) : 137205-31

Solaris 10 (x86) : 137205-33

Solaris 10 (x86) : 137205-34

Solaris 10 (x86) : 137205-35

Solaris 10 (x86) : 137205-36

Solaris 10 (x86) : 137205-37

Solaris 10 (x86) : 137205-38

Solaris 10 (x86) : 137205-38 (deprecated)

Solaris 10 (x86) : 137293-02

Solaris 10 (x86) : 137322-02

Solaris 10 (x86) : 137322-03

Solaris 10 (x86) : 137322-04

Solaris 10 (x86) : 137322-04 (deprecated)

Solaris 10 (x86) : 137632-17

Solaris 10 (x86) : 137872-02 (deprecated)

Solaris 10 (x86) : 138061-04

Solaris 10 (x86) : 138069-01

Solaris 10 (x86) : 138069-01

Solaris 10 (x86) : 138071-03

Solaris 10 (x86) : 138084-01

Solaris 10 (x86) : 138084-01

Solaris 10 (x86) : 138105-01

Solaris 10 (x86) : 138224-03

Solaris 10 (x86) : 138254-02

Solaris 10 (x86) : 138264-03

Solaris 10 (x86) : 138266-01 (deprecated)

Solaris 10 (x86) : 138270-02

Solaris 10 (x86) : 138323-03

Solaris 10 (x86) : 138353-06 (deprecated)

Solaris 10 (x86) : 138362-01 (deprecated)

Solaris 10 (x86) : 138372-06

Solaris 10 (x86) : 138374-02

Solaris 10 (x86) : 138536-01

Solaris 10 (x86) : 138536-01 (deprecated)

Solaris 10 (x86) : 138554-12 (deprecated)

Solaris 10 (x86) : 138624-04

Solaris 10 (x86) : 138628-07

Solaris 10 (x86) : 138648-01 (deprecated)

Solaris 10 (x86) : 138687-07

Solaris 10 (x86) : 138823-12

Solaris 10 (x86) : 138823-12 (deprecated)

Solaris 10 (x86) : 138825-12

Solaris 10 (x86) : 138825-12 (deprecated)

Solaris 10 (x86) : 138827-12

Solaris 10 (x86) : 138827-12 (deprecated)

Solaris 10 (x86) : 138863-02

Solaris 10 (x86) : 138875-05

Solaris 10 (x86) : 138877-01

Solaris 10 (x86) : 138877-01

Solaris 10 (x86) : 138881-02

Solaris 10 (x86) : 138882-02

Solaris 10 (x86) : 138889-08

Solaris 10 (x86) : 139100-04

Solaris 10 (x86) : 139100-04 (deprecated)

Solaris 10 (x86) : 139100-07

Solaris 10 (x86) : 139290-02

Solaris 10 (x86) : 139290-02 (deprecated)

Solaris 10 (x86) : 139292-02

Solaris 10 (x86) : 139292-02 (deprecated)

Solaris 10 (x86) : 139391-01

Solaris 10 (x86) : 139391-01

Solaris 10 (x86) : 139463-02

Solaris 10 (x86) : 139463-02

Solaris 10 (x86) : 139467-04

Solaris 10 (x86) : 139479-01

Solaris 10 (x86) : 139479-01

Solaris 10 (x86) : 139482-01

Solaris 10 (x86) : 139482-01

Solaris 10 (x86) : 139484-05

Solaris 10 (x86) : 139499-04

Solaris 10 (x86) : 139501-02

Solaris 10 (x86) : 139501-02

Solaris 10 (x86) : 139556-08

Solaris 10 (x86) : 139556-08 (deprecated)

Solaris 10 (x86) : 139561-02

Solaris 10 (x86) : 139621-01

Solaris 10 (x86) : 139621-01 (deprecated)

Solaris 10 (x86) : 139833-12 (deprecated)

Solaris 10 (x86) : 139834-12 (deprecated)

Solaris 10 (x86) : 140084-02

Solaris 10 (x86) : 140102-01 (deprecated)

Solaris 10 (x86) : 140106-02

Solaris 10 (x86) : 140109-03

Solaris 10 (x86) : 140119-11

Solaris 10 (x86) : 140130-10

Solaris 10 (x86) : 140160-03

Solaris 10 (x86) : 140384-01

Solaris 10 (x86) : 140384-01

Solaris 10 (x86) : 140388-02

Solaris 10 (x86) : 140388-02

Solaris 10 (x86) : 140392-03

Solaris 10 (x86) : 140400-03

Solaris 10 (x86) : 140400-03

Solaris 10 (x86) : 140414-01

Solaris 10 (x86) : 140414-01

Solaris 10 (x86) : 140456-01

Solaris 10 (x86) : 140456-03 (deprecated)

Solaris 10 (x86) : 140560-01

Solaris 10 (x86) : 140564-01

Solaris 10 (x86) : 140566-02

Solaris 10 (x86) : 140775-03

Solaris 10 (x86) : 140861-02 (deprecated)

Solaris 10 (x86) : 140918-02

Solaris 10 (x86) : 140922-02

Solaris 10 (x86) : 141009-01

Solaris 10 (x86) : 141009-01

Solaris 10 (x86) : 141015-01

Solaris 10 (x86) : 141015-01

Solaris 10 (x86) : 141021-03

Solaris 10 (x86) : 141023-02

Solaris 10 (x86) : 141031-11

Solaris 10 (x86) : 141105-04

Solaris 10 (x86) : 141105-04 (deprecated)

Solaris 10 (x86) : 141415-10

Solaris 10 (x86) : 141445-09 (deprecated)

Solaris 10 (x86) : 141482-03 (deprecated)

Solaris 10 (x86) : 141501-09

Solaris 10 (x86) : 141503-02

Solaris 10 (x86) : 141505-09

Solaris 10 (x86) : 141511-07

Solaris 10 (x86) : 141525-10

Solaris 10 (x86) : 141525-10

Solaris 10 (x86) : 141553-04

Solaris 10 (x86) : 141553-04

Solaris 10 (x86) : 141587-01 (deprecated)

Solaris 10 (x86) : 141591-02

Solaris 10 (x86) : 141691-02

Solaris 10 (x86) : 141710-03

Solaris 10 (x86) : 141710-03 (deprecated)

Solaris 10 (x86) : 141720-01

Solaris 10 (x86) : 141720-01

Solaris 10 (x86) : 141732-02

Solaris 10 (x86) : 141734-04

Solaris 10 (x86) : 141766-01

Solaris 10 (x86) : 141766-01

Solaris 10 (x86) : 141779-05

Solaris 10 (x86) : 141879-11

Solaris 10 (x86) : 141897-10

Solaris 10 (x86) : 141911-01

Solaris 10 (x86) : 141931-01

Solaris 10 (x86) : 141931-01

Solaris 10 (x86) : 142048-06

Solaris 10 (x86) : 142190-01

Solaris 10 (x86) : 142190-01 (deprecated)

Solaris 10 (x86) : 142191-01

Solaris 10 (x86) : 142191-01 (deprecated)

Solaris 10 (x86) : 142241-01 (deprecated)

Solaris 10 (x86) : 142252-02 (deprecated)

Solaris 10 (x86) : 142260-06

Solaris 10 (x86) : 142285-01

Solaris 10 (x86) : 142285-01

Solaris 10 (x86) : 142398-01 (deprecated)

Solaris 10 (x86) : 142437-08

Solaris 10 (x86) : 142530-01 (deprecated)

Solaris 10 (x86) : 142530-02

Solaris 10 (x86) : 142786-17

Solaris 10 (x86) : 142786-17 (deprecated)

Solaris 10 (x86) : 142848-04 (deprecated)

Solaris 10 (x86) : 142901-15

Solaris 10 (x86) : 142910-17 (deprecated)

Solaris 10 (x86) : 143309-03 (deprecated)

Solaris 10 (x86) : 143318-03

Solaris 10 (x86) : 143318-03 (deprecated)

Solaris 10 (x86) : 143391-01

Solaris 10 (x86) : 143391-01 (deprecated)

Solaris 10 (x86) : 143503-01

Solaris 10 (x86) : 143503-01 (deprecated)

Solaris 10 (x86) : 143507-06

Solaris 10 (x86) : 143507-07

Solaris 10 (x86) : 143507-11

Solaris 10 (x86) : 143507-12 (deprecated)

Solaris 10 (x86) : 143507-13

Solaris 10 (x86) : 143507-14

Solaris 10 (x86) : 143511-01

Solaris 10 (x86) : 143526-01

Solaris 10 (x86) : 143526-01

Solaris 10 (x86) : 143562-09

Solaris 10 (x86) : 143593-08

Solaris 10 (x86) : 143616-02

Solaris 10 (x86) : 143646-16

Solaris 10 (x86) : 143726-01

Solaris 10 (x86) : 143726-02

Solaris 10 (x86) : 143726-04

Solaris 10 (x86) : 143726-06

Solaris 10 (x86) : 143726-09

Solaris 10 (x86) : 143726-10

Solaris 10 (x86) : 143726-11

Solaris 10 (x86) : 143726-11 (deprecated)

Solaris 10 (x86) : 143726-12

Solaris 10 (x86) : 143726-13

Solaris 10 (x86) : 143728-01

Solaris 10 (x86) : 143728-02

Solaris 10 (x86) : 143728-03

Solaris 10 (x86) : 143728-04

Solaris 10 (x86) : 143728-06 (deprecated)

Solaris 10 (x86) : 143732-01

Solaris 10 (x86) : 143732-01 (deprecated)

Solaris 10 (x86) : 143734-01

Solaris 10 (x86) : 143734-01 (deprecated)

Solaris 10 (x86) : 143740-01

Solaris 10 (x86) : 143740-01 (deprecated)

Solaris 10 (x86) : 143750-02 (deprecated)

Solaris 10 (x86) : 143913-01

Solaris 10 (x86) : 143913-01 (deprecated)

Solaris 10 (x86) : 143938-03

Solaris 10 (x86) : 144048-01 (deprecated)

Solaris 10 (x86) : 144054-04

Solaris 10 (x86) : 144107-01

Solaris 10 (x86) : 144107-01 (deprecated)

Solaris 10 (x86) : 144222-11

Solaris 10 (x86) : 144222-16 (deprecated)

Solaris 10 (x86) : 144230-02

Solaris 10 (x86) : 144230-02 (deprecated)

Solaris 10 (x86) : 144255-01

Solaris 10 (x86) : 144255-01

Solaris 10 (x86) : 144326-01

Solaris 10 (x86) : 144326-01 (deprecated)

Solaris 10 (x86) : 144328-02

Solaris 10 (x86) : 144328-02 (deprecated)

Solaris 10 (x86) : 144489-17

Solaris 10 (x86) : 144501-19 (deprecated)

Solaris 10 (x86) : 144537-02

Solaris 10 (x86) : 144675-02

Solaris 10 (x86) : 144892-02

Solaris 10 (x86) : 144892-02

Solaris 10 (x86) : 144995-02

Solaris 10 (x86) : 144995-02 (deprecated)

Solaris 10 (x86) : 144995-03

Solaris 10 (x86) : 144995-04

Solaris 10 (x86) : 144997-02

Solaris 10 (x86) : 144997-02 (deprecated)

Solaris 10 (x86) : 145007-04

Solaris 10 (x86) : 145007-07

Solaris 10 (x86) : 145007-09 (deprecated)

Solaris 10 (x86) : 145045-03

Solaris 10 (x86) : 145070-02

Solaris 10 (x86) : 145081-12

Solaris 10 (x86) : 145081-14

Solaris 10 (x86) : 145081-14 (deprecated)

Solaris 10 (x86) : 145125-02

Solaris 10 (x86) : 145125-02

Solaris 10 (x86) : 145199-01

Solaris 10 (x86) : 145199-01

Solaris 10 (x86) : 145201-13

Solaris 10 (x86) : 145201-13 (deprecated)

Solaris 10 (x86) : 145334-33

Solaris 10 (x86) : 145334-34

Solaris 10 (x86) : 145334-39 (deprecated)

Solaris 10 (x86) : 145336-22 (deprecated)

Solaris 10 (x86) : 145338-04 (deprecated)

Solaris 10 (x86) : 145342-06 (deprecated)

Solaris 10 (x86) : 145344-07 (deprecated)

Solaris 10 (x86) : 145346-04 (deprecated)

Solaris 10 (x86) : 145639-10

Solaris 10 (x86) : 145639-11 (deprecated)

Solaris 10 (x86) : 145641-04

Solaris 10 (x86) : 145645-06

Solaris 10 (x86) : 145645-07 (deprecated)

Solaris 10 (x86) : 145647-08

Solaris 10 (x86) : 145647-11 (deprecated)

Solaris 10 (x86) : 145712-07

Solaris 10 (x86) : 145712-07 (deprecated)

Solaris 10 (x86) : 145797-02

Solaris 10 (x86) : 145802-06

Solaris 10 (x86) : 145802-06

Solaris 10 (x86) : 145900-08 (deprecated)

Solaris 10 (x86) : 145962-02

Solaris 10 (x86) : 146033-05

Solaris 10 (x86) : 146033-05

Solaris 10 (x86) : 146055-07 (deprecated)

Solaris 10 (x86) : 146086-08

Solaris 10 (x86) : 146233-20

Solaris 10 (x86) : 146280-01

Solaris 10 (x86) : 146280-01

Solaris 10 (x86) : 146289-03 (deprecated)

Solaris 10 (x86) : 146364-01

Solaris 10 (x86) : 146364-01

Solaris 10 (x86) : 146567-01

Solaris 10 (x86) : 146577-01

Solaris 10 (x86) : 146577-01 (deprecated)

Solaris 10 (x86) : 146667-04

Solaris 10 (x86) : 146672-10

Solaris 10 (x86) : 146674-01

Solaris 10 (x86) : 146674-01 (deprecated)

Solaris 10 (x86) : 146695-02 (deprecated)

Solaris 10 (x86) : 146695-03

Solaris 10 (x86) : 146773-01

Solaris 10 (x86) : 146773-01

Solaris 10 (x86) : 146803-03

Solaris 10 (x86) : 146835-02

Solaris 10 (x86) : 146835-02 (deprecated)

Solaris 10 (x86) : 146859-01

Solaris 10 (x86) : 146859-01

Solaris 10 (x86) : 146862-02 (deprecated)

Solaris 10 (x86) : 147083-02 (deprecated)

Solaris 10 (x86) : 147085-02 (deprecated)

Solaris 10 (x86) : 147088-03 (deprecated)

Solaris 10 (x86) : 147090-03 (deprecated)

Solaris 10 (x86) : 147092-05 (deprecated)

Solaris 10 (x86) : 147096-03 (deprecated)

Solaris 10 (x86) : 147144-17 (deprecated)

Solaris 10 (x86) : 147148-26 (deprecated)

Solaris 10 (x86) : 147183-01

Solaris 10 (x86) : 147183-01

Solaris 10 (x86) : 147218-02

Solaris 10 (x86) : 147218-04

Solaris 10 (x86) : 147218-04 (deprecated)

Solaris 10 (x86) : 147220-01

Solaris 10 (x86) : 147220-01 (deprecated)

Solaris 10 (x86) : 147228-01

Solaris 10 (x86) : 147267-05

Solaris 10 (x86) : 147379-01

Solaris 10 (x86) : 147379-01 (deprecated)

Solaris 10 (x86) : 147435-01

Solaris 10 (x86) : 147441-27

Solaris 10 (x86) : 147447-01 (deprecated)

Solaris 10 (x86) : 147498-02 (deprecated)

Solaris 10 (x86) : 147674-08

Solaris 10 (x86) : 147674-10

Solaris 10 (x86) : 147674-11

Solaris 10 (x86) : 147674-11 (deprecated)

Solaris 10 (x86) : 147694-52

Solaris 10 (x86) : 147694-65

Solaris 10 (x86) : 147694-76

Solaris 10 (x86) : 147694-81

Solaris 10 (x86) : 147694-82

Solaris 10 (x86) : 147694-91

Solaris 10 (x86) : 147694-99 (deprecated)

Solaris 10 (x86) : 147695-52

Solaris 10 (x86) : 147695-65

Solaris 10 (x86) : 147695-76

Solaris 10 (x86) : 147695-81

Solaris 10 (x86) : 147695-82

Solaris 10 (x86) : 147695-91

Solaris 10 (x86) : 147695-99 (deprecated)

Solaris 10 (x86) : 147714-01

Solaris 10 (x86) : 147714-01

Solaris 10 (x86) : 147716-04

Solaris 10 (x86) : 147716-04

Solaris 10 (x86) : 147794-09

Solaris 10 (x86) : 147794-12

Solaris 10 (x86) : 147794-14

Solaris 10 (x86) : 147794-15

Solaris 10 (x86) : 147794-16

Solaris 10 (x86) : 147794-17

Solaris 10 (x86) : 147794-20

Solaris 10 (x86) : 147794-22

Solaris 10 (x86) : 147794-22 (deprecated)

Solaris 10 (x86) : 147794-23

Solaris 10 (x86) : 147936-01 (deprecated)

Solaris 10 (x86) : 147989-01

Solaris 10 (x86) : 147989-01 (deprecated)

Solaris 10 (x86) : 147993-06

Solaris 10 (x86) : 147993-10

Solaris 10 (x86) : 147993-10 (deprecated)

Solaris 10 (x86) : 148003-01

Solaris 10 (x86) : 148003-01 (deprecated)

Solaris 10 (x86) : 148005-01

Solaris 10 (x86) : 148005-01 (deprecated)

Solaris 10 (x86) : 148007-01

Solaris 10 (x86) : 148007-01 (deprecated)

Solaris 10 (x86) : 148028-03 (deprecated)

Solaris 10 (x86) : 148072-12

Solaris 10 (x86) : 148072-13

Solaris 10 (x86) : 148072-14

Solaris 10 (x86) : 148072-15

Solaris 10 (x86) : 148072-16

Solaris 10 (x86) : 148072-17

Solaris 10 (x86) : 148072-18

Solaris 10 (x86) : 148072-19 (deprecated)

Solaris 10 (x86) : 148076-18 (deprecated)

Solaris 10 (x86) : 148082-02

Solaris 10 (x86) : 148082-02

Solaris 10 (x86) : 148105-11

Solaris 10 (x86) : 148105-21

Solaris 10 (x86) : 148105-23

Solaris 10 (x86) : 148105-23 (deprecated)

Solaris 10 (x86) : 148105-26

Solaris 10 (x86) : 148105-29

Solaris 10 (x86) : 148113-02 (deprecated)

Solaris 10 (x86) : 148136-01

Solaris 10 (x86) : 148136-01 (deprecated)

Solaris 10 (x86) : 148166-02

Solaris 10 (x86) : 148166-02 (deprecated)

Solaris 10 (x86) : 148242-02

Solaris 10 (x86) : 148242-05 (deprecated)

Solaris 10 (x86) : 148310-06

Solaris 10 (x86) : 148310-08 (deprecated)

Solaris 10 (x86) : 148310-10

Solaris 10 (x86) : 148380-15

Solaris 10 (x86) : 148384-01

Solaris 10 (x86) : 148384-01 (deprecated)

Solaris 10 (x86) : 148404-01

Solaris 10 (x86) : 148404-01 (deprecated)

Solaris 10 (x86) : 148408-01

Solaris 10 (x86) : 148408-01 (deprecated)

Solaris 10 (x86) : 148424-01

Solaris 10 (x86) : 148424-01 (deprecated)

Solaris 10 (x86) : 148562-06

Solaris 10 (x86) : 148562-08

Solaris 10 (x86) : 148562-11

Solaris 10 (x86) : 148562-12

Solaris 10 (x86) : 148562-12 (deprecated)

Solaris 10 (x86) : 148566-01

Solaris 10 (x86) : 148566-01 (deprecated)

Solaris 10 (x86) : 148580-08 (deprecated)

Solaris 10 (x86) : 148583-08 (deprecated)

Solaris 10 (x86) : 148602-01

Solaris 10 (x86) : 148626-01

Solaris 10 (x86) : 148626-01 (deprecated)

Solaris 10 (x86) : 148628-02

Solaris 10 (x86) : 148628-02 (deprecated)

Solaris 10 (x86) : 148658-01

Solaris 10 (x86) : 148658-01 (deprecated)

Solaris 10 (x86) : 148694-01

Solaris 10 (x86) : 148694-01 (deprecated)

Solaris 10 (x86) : 148769-01

Solaris 10 (x86) : 148769-02

Solaris 10 (x86) : 148769-02 (deprecated)

Solaris 10 (x86) : 148871-01

Solaris 10 (x86) : 148871-01 (deprecated)

Solaris 10 (x86) : 148882-02

Solaris 10 (x86) : 148882-03 (deprecated)

Solaris 10 (x86) : 148889-05 (deprecated)

Solaris 10 (x86) : 148949-01

Solaris 10 (x86) : 148949-01 (deprecated)

Solaris 10 (x86) : 148955-01

Solaris 10 (x86) : 148955-01 (deprecated)

Solaris 10 (x86) : 148976-01

Solaris 10 (x86) : 148976-01 (deprecated)

Solaris 10 (x86) : 149068-01

Solaris 10 (x86) : 149068-01 (deprecated)

Solaris 10 (x86) : 149072-01

Solaris 10 (x86) : 149072-01 (deprecated)

Solaris 10 (x86) : 149076-01

Solaris 10 (x86) : 149076-01 (deprecated)

Solaris 10 (x86) : 149107-01

Solaris 10 (x86) : 149107-01 (deprecated)

Solaris 10 (x86) : 149109-01

Solaris 10 (x86) : 149109-01 (deprecated)

Solaris 10 (x86) : 149113-01

Solaris 10 (x86) : 149113-01 (deprecated)

Solaris 10 (x86) : 149150-01

Solaris 10 (x86) : 149150-01 (deprecated)

Solaris 10 (x86) : 149164-01

Solaris 10 (x86) : 149164-01 (deprecated)

Solaris 10 (x86) : 149166-01

Solaris 10 (x86) : 149166-01 (deprecated)

Solaris 10 (x86) : 149176-13

Solaris 10 (x86) : 149176-13 (deprecated)

Solaris 10 (x86) : 149192-01

Solaris 10 (x86) : 149192-01 (deprecated)

Solaris 10 (x86) : 149396-01 (deprecated)

Solaris 10 (x86) : 149433-02 (deprecated)

Solaris 10 (x86) : 149454-02

Solaris 10 (x86) : 149454-02 (deprecated)

Solaris 10 (x86) : 149484-01

Solaris 10 (x86) : 149484-01 (deprecated)

Solaris 10 (x86) : 149497-02

Solaris 10 (x86) : 149497-02 (deprecated)

Solaris 10 (x86) : 149639-02

Solaris 10 (x86) : 149639-02 (deprecated)

Solaris 10 (x86) : 149647-02

Solaris 10 (x86) : 149647-02 (deprecated)

Solaris 10 (x86) : 149896-01 (deprecated)

Solaris 10 (x86) : 150052-01 (deprecated)

Solaris 10 (x86) : 150101-01

Solaris 10 (x86) : 150101-01 (deprecated)

Solaris 10 (x86) : 150114-02

Solaris 10 (x86) : 150114-02 (deprecated)

Solaris 10 (x86) : 150118-01

Solaris 10 (x86) : 150118-01

Solaris 10 (x86) : 150120-03

Solaris 10 (x86) : 150120-04 (deprecated)

Solaris 10 (x86) : 150120-06

Solaris 10 (x86) : 150124-01

Solaris 10 (x86) : 150124-01 (deprecated)

Solaris 10 (x86) : 150158-01

Solaris 10 (x86) : 150158-01 (deprecated)

Solaris 10 (x86) : 150313-06

Solaris 10 (x86) : 150313-06 (deprecated)

Solaris 10 (x86) : 150378-07

Solaris 10 (x86) : 150380-02

Solaris 10 (x86) : 150401-06

Solaris 10 (x86) : 150401-10

Solaris 10 (x86) : 150401-11

Solaris 10 (x86) : 150401-13

Solaris 10 (x86) : 150401-20

Solaris 10 (x86) : 150401-23

Solaris 10 (x86) : 150401-24

Solaris 10 (x86) : 150401-27

Solaris 10 (x86) : 150401-35

Solaris 10 (x86) : 150401-38

Solaris 10 (x86) : 150401-41

Solaris 10 (x86) : 150401-50

Solaris 10 (x86) : 150401-51

Solaris 10 (x86) : 150401-52

Solaris 10 (x86) : 150401-53

Solaris 10 (x86) : 150401-59

Solaris 10 (x86) : 150401-59 (deprecated)

Solaris 10 (x86) : 150401-62

Solaris 10 (x86) : 150401-63

Solaris 10 (x86) : 150401-64

Solaris 10 (x86) : 150401-67

Solaris 10 (x86) : 150401-68

Solaris 10 (x86) : 150437-03 (deprecated)

Solaris 10 (x86) : 150546-02

Solaris 10 (x86) : 150546-02 (deprecated)

Solaris 10 (x86) : 150585-02 (deprecated)

Solaris 10 (x86) : 150617-01

Solaris 10 (x86) : 150617-03

Solaris 10 (x86) : 150617-03 (deprecated)

Solaris 10 (x86) : 150619-02 (deprecated)

Solaris 10 (x86) : 150833-08

Solaris 10 (x86) : 150833-12 (deprecated)

Solaris 10 (x86) : 150837-01

Solaris 10 (x86) : 150837-01 (deprecated)

Solaris 10 (x86) : 151010-11

Solaris 10 (x86) : 151010-20

Solaris 10 (x86) : 151010-40

Solaris 10 (x86) : 151010-51

Solaris 10 (x86) : 151010-60

Solaris 10 (x86) : 151010-92

Solaris 10 (x86) : 151010-92 (deprecated)

Solaris 10 (x86) : 151075-02

Solaris 10 (x86) : 151075-03

Solaris 10 (x86) : 151075-06 (deprecated)

Solaris 10 (x86) : 151266-03 (deprecated)

Solaris 10 (x86) : 151562-01

Solaris 10 (x86) : 151562-01 (deprecated)

Solaris 10 (x86) : 151673-03 (deprecated)

Solaris 10 (x86) : 151718-01

Solaris 10 (x86) : 151718-01 (deprecated)

Solaris 10 (x86) : 151720-01

Solaris 10 (x86) : 151720-01 (deprecated)

Solaris 10 (x86) : 151722-01

Solaris 10 (x86) : 151722-01 (deprecated)

Solaris 10 (x86) : 151724-01

Solaris 10 (x86) : 151724-01 (deprecated)

Solaris 10 (x86) : 151913-04

Solaris 10 (x86) : 151913-05

Solaris 10 (x86) : 151913-07

Solaris 10 (x86) : 151913-08

Solaris 10 (x86) : 151913-09

Solaris 10 (x86) : 151913-10

Solaris 10 (x86) : 151913-11

Solaris 10 (x86) : 151913-11 (deprecated)

Solaris 10 (x86) : 151913-12

Solaris 10 (x86) : 151913-13

Solaris 10 (x86) : 151913-14

Solaris 10 (x86) : 151913-15

Solaris 10 (x86) : 151915-04

Solaris 10 (x86) : 151915-05

Solaris 10 (x86) : 151915-07 (deprecated)

Solaris 10 (x86) : 152078-41

Solaris 10 (x86) : 152078-51

Solaris 10 (x86) : 152078-81 (deprecated)

Solaris 10 (x86) : 152078-91

Solaris 10 (x86) : 152079-41

Solaris 10 (x86) : 152079-51

Solaris 10 (x86) : 152079-81 (deprecated)

Solaris 10 (x86) : 152079-91

Solaris 10 (x86) : 152098-21

Solaris 10 (x86) : 152098-31

Solaris 10 (x86) : 152098-61

Solaris 10 (x86) : 152098-71

Solaris 10 (x86) : 152098-71 (deprecated)

Solaris 10 (x86) : 152098-91

Solaris 10 (x86) : 152099-21

Solaris 10 (x86) : 152099-31

Solaris 10 (x86) : 152099-61

Solaris 10 (x86) : 152099-71

Solaris 10 (x86) : 152099-71 (deprecated)

Solaris 10 (x86) : 152099-91

Solaris 10 (x86) : 152101-12

Solaris 10 (x86) : 152101-21

Solaris 10 (x86) : 152101-31

Solaris 10 (x86) : 152101-52

Solaris 10 (x86) : 152101-62 (deprecated)

Solaris 10 (x86) : 152101-81

Solaris 10 (x86) : 152101-91

Solaris 10 (x86) : 152101-92

Solaris 10 (x86) : 152249-01

Solaris 10 (x86) : 152249-01 (deprecated)

Solaris 10 (x86) : 152249-02

Solaris 10 (x86) : 152251-01

Solaris 10 (x86) : 152251-01 (deprecated)

Solaris 10 (x86) : 152253-01

Solaris 10 (x86) : 152253-02

Solaris 10 (x86) : 152253-02 (deprecated)

Solaris 10 (x86) : 152253-03

Solaris 10 (x86) : 152255-01

Solaris 10 (x86) : 152255-01 (deprecated)

Solaris 10 (x86) : 152261-01

Solaris 10 (x86) : 152261-02

Solaris 10 (x86) : 152261-03

Solaris 10 (x86) : 152261-03 (deprecated)

Solaris 10 (x86) : 152261-04

Solaris 10 (x86) : 152265-01

Solaris 10 (x86) : 152265-01 (deprecated)

Solaris 10 (x86) : 152265-02

Solaris 10 (x86) : 152364-01

Solaris 10 (x86) : 152364-01 (deprecated)

Solaris 10 (x86) : 152507-01

Solaris 10 (x86) : 152507-01 (deprecated)

Solaris 10 (x86) : 152511-03

Solaris 10 (x86) : 152511-04

Solaris 10 (x86) : 152511-06

Solaris 10 (x86) : 152511-06 (deprecated)

Solaris 10 (x86) : 152511-07

Solaris 10 (x86) : 152511-08

Solaris 10 (x86) : 152511-09

Solaris 10 (x86) : 152515-01

Solaris 10 (x86) : 152515-02

Solaris 10 (x86) : 152515-02 (deprecated)

Solaris 10 (x86) : 152644-03

Solaris 10 (x86) : 152644-05

Solaris 10 (x86) : 152644-05 (deprecated)

Solaris 10 (x86) : 152644-06

Solaris 10 (x86) : 152644-07

Solaris 10 (x86) : 152644-08

Solaris 10 (x86) : 152650-02 : dtappgather Arbitrary Directory Creation Local Privilege Escalation (EXTREMEPARR)

Solaris 10 (x86) : 152652-01

Solaris 10 (x86) : 152652-01 (deprecated)

Solaris 10 (x86) : 152725-01

Solaris 10 (x86) : 152725-02

Solaris 10 (x86) : 152725-02 (deprecated)

Solaris 10 (x86) : 152921-01

Solaris 10 (x86) : 152921-11

Solaris 10 (x86) : 152922-01

Solaris 10 (x86) : 152922-11

Solaris 10 (x86) : 152925-01

Solaris 10 (x86) : 152926-01

Solaris 10 (x86) : 152928-02

Solaris 10 (x86) : 153057-01

Solaris 10 (x86) : 153061-01

Solaris 11 : Multiple Kernel Vulnerabilities

Solaris 2.4 (sparc) : 104178-04

Solaris 4 (sparc) : 103670-10

Solaris 4 (sparc) : 103882-16

Solaris 4 (sparc) : 104471-05

Solaris 4 (sparc) : 104498-05

Solaris 4 (sparc) : 104552-05

Solaris 4 (sparc) : 104661-09

Solaris 4 (sparc) : 105076-04

Solaris 4 (sparc) : 105716-07

Solaris 4 (sparc) : 108194-03

Solaris 4 (sparc) : 108205-01

Solaris 4 (sparc) : 108289-02

Solaris 4 (sparc) : 108363-02

Solaris 4 (x86) : 103717-11

Solaris 4 (x86) : 103886-15

Solaris 4 (x86) : 104185-04

Solaris 4 (x86) : 104472-05

Solaris 4 (x86) : 104500-05

Solaris 4 (x86) : 104554-04

Solaris 4 (x86) : 104663-10

Solaris 4 (x86) : 105354-04

Solaris 4 (x86) : 105717-06

Solaris 4 (x86) : 108196-03

Solaris 4 (x86) : 108206-01

Solaris 4 (x86) : 108290-03

Solaris 4 (x86) : 108364-02

Solaris 5.10 (sparc) : 118950-38

Solaris 5.10 (sparc) : 119044-04

Solaris 5.10 (sparc) : 119345-07

Solaris 5.10 (sparc) : 120185-19

Solaris 5.10 (sparc) : 120189-19

Solaris 5.10 (sparc) : 120981-18

Solaris 5.10 (sparc) : 124301-13

Solaris 5.10 (sparc) : 125407-01

Solaris 5.10 (sparc) : 126356-03

Solaris 5.10 (sparc) : 137179-12

Solaris 5.10 (sparc) : 137182-12

Solaris 5.10 (sparc) : 137185-12

Solaris 5.10 (sparc) : 138686-03

Solaris 5.10 (sparc) : 139335-01

Solaris 5.10 (sparc) : 139336-01

Solaris 5.10 (x86) : 116649-23

Solaris 5.10 (x86) : 118951-38

Solaris 5.10 (x86) : 119044-04

Solaris 5.10 (x86) : 119346-07

Solaris 5.10 (x86) : 120186-19

Solaris 5.10 (x86) : 120190-19

Solaris 5.10 (x86) : 120880-08

Solaris 5.10 (x86) : 120982-18

Solaris 5.10 (x86) : 124302-13

Solaris 5.10 (x86) : 125278-08

Solaris 5.10 (x86) : 125407-01

Solaris 5.10 (x86) : 126357-03

Solaris 5.10 (x86) : 127554-06

Solaris 5.10 (x86) : 137180-12

Solaris 5.10 (x86) : 137183-12

Solaris 5.10 (x86) : 138687-03

Solaris 5.10 (x86) : 139337-01

Solaris 5.10 (x86) : 139338-01

Solaris 6 (sparc) : 107715-26

Solaris 6 (sparc) : 110057-08

Solaris 6 (sparc) : 110936-22

Solaris 6 (sparc) : 110948-04

Solaris 6 (sparc) : 110971-22

Solaris 6 (sparc) : 111754-01

Solaris 6 (sparc) : 112327-27

Solaris 6 (sparc) : 112534-03

Solaris 6 (sparc) : 112583-01

Solaris 6 (sparc) : 112587-01

Solaris 6 (sparc) : 113531-10

Solaris 6 (sparc) : 116505-01

Solaris 6 (sparc) : 116525-01

Solaris 6 (sparc) : 118386-09

Solaris 6 (sparc) : 119004-02

Solaris 6 (sparc) : 119005-02

Solaris 6 (sparc) : 121209-01

Solaris 6 (sparc) : 121332-01

Solaris 6 (x86) : 110058-08

Solaris 7 (sparc) : 108669-21

Solaris 7 (sparc) : 110057-08

Solaris 7 (sparc) : 110937-22

Solaris 7 (sparc) : 110948-04

Solaris 7 (sparc) : 110972-22

Solaris 7 (sparc) : 111754-01

Solaris 7 (sparc) : 112190-02

Solaris 7 (sparc) : 112327-27

Solaris 7 (sparc) : 112536-06

Solaris 7 (sparc) : 112584-01

Solaris 7 (sparc) : 112588-01

Solaris 7 (sparc) : 112760-19

Solaris 7 (sparc) : 113170-10

Solaris 7 (sparc) : 113173-10

Solaris 7 (sparc) : 113531-10

Solaris 7 (sparc) : 115217-05

Solaris 7 (sparc) : 116264-09

Solaris 7 (sparc) : 116271-10

Solaris 7 (sparc) : 116826-06

Solaris 7 (sparc) : 116828-04

Solaris 7 (sparc) : 116831-04

Solaris 7 (sparc) : 116832-04

Solaris 7 (sparc) : 116834-04

Solaris 7 (sparc) : 118387-09

Solaris 7 (sparc) : 119004-02

Solaris 7 (sparc) : 119005-02

Solaris 7 (sparc) : 119006-01

Solaris 7 (sparc) : 119007-01

Solaris 7 (sparc) : 119010-01

Solaris 7 (sparc) : 119011-01

Solaris 7 (sparc) : 119670-01

Solaris 7 (sparc) : 120649-01

Solaris 7 (sparc) : 120650-01

Solaris 7 (sparc) : 120651-01

Solaris 7 (sparc) : 120653-01

Solaris 7 (sparc) : 121209-01

Solaris 7 (sparc) : 121332-01

Solaris 7 (sparc) : 121956-01

Solaris 7 (sparc) : 121957-01

Solaris 7 (sparc) : 123037-01

Solaris 7 (sparc) : 123038-01

Solaris 7 (sparc) : 123919-12

Solaris 7 (sparc) : 124519-05

Solaris 7 (sparc) : 124520-05

Solaris 7 (x86) : 108670-21

Solaris 7 (x86) : 110058-08

Solaris 7 (x86) : 112537-06

Solaris 7 (x86) : 112761-13

Solaris 7 (x86) : 116827-07

Solaris 7 (x86) : 116833-04

Solaris 7 (x86) : 119671-01

Solaris 7 (x86) : 120652-01

Solaris 8 (sparc) : 108528-29

Solaris 8 (sparc) : 108669-21

Solaris 8 (sparc) : 108773-28

Solaris 8 (sparc) : 108835-04

Solaris 8 (sparc) : 108869-36

Solaris 8 (sparc) : 108899-04

Solaris 8 (sparc) : 108909-13

Solaris 8 (sparc) : 108919-30

Solaris 8 (sparc) : 108940-76

Solaris 8 (sparc) : 108949-09

Solaris 8 (sparc) : 108964-11

Solaris 8 (sparc) : 108968-12

Solaris 8 (sparc) : 108975-10

Solaris 8 (sparc) : 108981-15

Solaris 8 (sparc) : 108985-03

Solaris 8 (sparc) : 108987-19

Solaris 8 (sparc) : 109007-28

Solaris 8 (sparc) : 109023-08

Solaris 8 (sparc) : 109025-07

Solaris 8 (sparc) : 109039-13

Solaris 8 (sparc) : 109077-21

Solaris 8 (sparc) : 109091-10

Solaris 8 (sparc) : 109134-33

Solaris 8 (sparc) : 109147-44

Solaris 8 (sparc) : 109149-02

Solaris 8 (sparc) : 109152-03

Solaris 8 (sparc) : 109154-21

Solaris 8 (sparc) : 109202-06

Solaris 8 (sparc) : 109223-10

Solaris 8 (sparc) : 109238-02

Solaris 8 (sparc) : 109320-22

Solaris 8 (sparc) : 109324-10

Solaris 8 (sparc) : 109326-24

Solaris 8 (sparc) : 109328-07

Solaris 8 (sparc) : 109354-26

Solaris 8 (sparc) : 109454-06

Solaris 8 (sparc) : 109458-04

Solaris 8 (sparc) : 109611-01

Solaris 8 (sparc) : 109613-07

Solaris 8 (sparc) : 109667-07

Solaris 8 (sparc) : 109695-03

Solaris 8 (sparc) : 109736-13

Solaris 8 (sparc) : 109764-06

Solaris 8 (sparc) : 109783-03

Solaris 8 (sparc) : 109793-33

Solaris 8 (sparc) : 109815-23

Solaris 8 (sparc) : 109862-05

Solaris 8 (sparc) : 109887-18

Solaris 8 (sparc) : 109893-04

Solaris 8 (sparc) : 109894-01

Solaris 8 (sparc) : 109896-37

Solaris 8 (sparc) : 109922-04

Solaris 8 (sparc) : 109931-10

Solaris 8 (sparc) : 109951-01

Solaris 8 (sparc) : 110046-02

Solaris 8 (sparc) : 110068-04

Solaris 8 (sparc) : 110075-03

Solaris 8 (sparc) : 110286-16

Solaris 8 (sparc) : 110322-02

Solaris 8 (sparc) : 110335-03

Solaris 8 (sparc) : 110386-04

Solaris 8 (sparc) : 110389-05

Solaris 8 (sparc) : 110416-07

Solaris 8 (sparc) : 110453-04

Solaris 8 (sparc) : 110458-02

Solaris 8 (sparc) : 110461-03

Solaris 8 (sparc) : 110615-18

Solaris 8 (sparc) : 110648-40

Solaris 8 (sparc) : 110668-05

Solaris 8 (sparc) : 110670-04

Solaris 8 (sparc) : 110794-06

Solaris 8 (sparc) : 110820-12

Solaris 8 (sparc) : 110896-03

Solaris 8 (sparc) : 110898-15

Solaris 8 (sparc) : 110903-08

Solaris 8 (sparc) : 110910-12

Solaris 8 (sparc) : 110916-07

Solaris 8 (sparc) : 110934-28

Solaris 8 (sparc) : 110938-22

Solaris 8 (sparc) : 110943-04

Solaris 8 (sparc) : 110945-10

Solaris 8 (sparc) : 110948-04

Solaris 8 (sparc) : 110953-08

Solaris 8 (sparc) : 110955-06

Solaris 8 (sparc) : 110957-02

Solaris 8 (sparc) : 110973-22

Solaris 8 (sparc) : 111069-01

Solaris 8 (sparc) : 111071-01

Solaris 8 (sparc) : 111232-01

Solaris 8 (sparc) : 111234-01

Solaris 8 (sparc) : 111313-06

Solaris 8 (sparc) : 111321-05

Solaris 8 (sparc) : 111325-02

Solaris 8 (sparc) : 111327-06

Solaris 8 (sparc) : 111332-08

Solaris 8 (sparc) : 111400-04

Solaris 8 (sparc) : 111488-08

Solaris 8 (sparc) : 111504-02

Solaris 8 (sparc) : 111548-01

Solaris 8 (sparc) : 111555-08

Solaris 8 (sparc) : 111570-04

Solaris 8 (sparc) : 111596-03

Solaris 8 (sparc) : 111606-07

Solaris 8 (sparc) : 111626-04

Solaris 8 (sparc) : 111647-01

Solaris 8 (sparc) : 111754-01

Solaris 8 (sparc) : 111826-01

Solaris 8 (sparc) : 111844-04

Solaris 8 (sparc) : 111857-09

Solaris 8 (sparc) : 111874-09

Solaris 8 (sparc) : 111881-03

Solaris 8 (sparc) : 111883-36

Solaris 8 (sparc) : 112039-01

Solaris 8 (sparc) : 112045-08

Solaris 8 (sparc) : 112169-07

Solaris 8 (sparc) : 112190-02

Solaris 8 (sparc) : 112237-16

Solaris 8 (sparc) : 112390-14

Solaris 8 (sparc) : 112459-01

Solaris 8 (sparc) : 112585-01

Solaris 8 (sparc) : 112589-01

Solaris 8 (sparc) : 112609-02

Solaris 8 (sparc) : 112611-02

Solaris 8 (sparc) : 112647-02

Solaris 8 (sparc) : 112668-04

Solaris 8 (sparc) : 112760-19

Solaris 8 (sparc) : 112792-01

Solaris 8 (sparc) : 112796-01

Solaris 8 (sparc) : 112846-01

Solaris 8 (sparc) : 112869-02

Solaris 8 (sparc) : 113105-01

Solaris 8 (sparc) : 113171-10

Solaris 8 (sparc) : 113174-10

Solaris 8 (sparc) : 113355-11

Solaris 8 (sparc) : 113505-02

Solaris 8 (sparc) : 113531-10

Solaris 8 (sparc) : 113650-02

Solaris 8 (sparc) : 113685-07

Solaris 8 (sparc) : 113687-02

Solaris 8 (sparc) : 113749-02

Solaris 8 (sparc) : 113792-01

Solaris 8 (sparc) : 113800-12

Solaris 8 (sparc) : 114045-14

Solaris 8 (sparc) : 114162-01

Solaris 8 (sparc) : 114644-04

Solaris 8 (sparc) : 114648-01

Solaris 8 (sparc) : 114669-04

Solaris 8 (sparc) : 114673-01

Solaris 8 (sparc) : 114795-05

Solaris 8 (sparc) : 114796-04

Solaris 8 (sparc) : 114802-02

Solaris 8 (sparc) : 114814-01

Solaris 8 (sparc) : 114816-04

Solaris 8 (sparc) : 114880-12

Solaris 8 (sparc) : 114984-02

Solaris 8 (sparc) : 115054-01

Solaris 8 (sparc) : 115217-05

Solaris 8 (sparc) : 115298-01

Solaris 8 (sparc) : 115610-25

Solaris 8 (sparc) : 115614-28

Solaris 8 (sparc) : 115732-10

Solaris 8 (sparc) : 115766-15

Solaris 8 (sparc) : 115797-01

Solaris 8 (sparc) : 115924-10

Solaris 8 (sparc) : 116264-09

Solaris 8 (sparc) : 116271-10

Solaris 8 (sparc) : 116286-20

Solaris 8 (sparc) : 116292-14

Solaris 8 (sparc) : 116296-21

Solaris 8 (sparc) : 116298-21

Solaris 8 (sparc) : 116300-21

Solaris 8 (sparc) : 116455-01

Solaris 8 (sparc) : 116568-99

Solaris 8 (sparc) : 116610-01

Solaris 8 (sparc) : 116648-25

Solaris 8 (sparc) : 116736-25

Solaris 8 (sparc) : 116738-23

Solaris 8 (sparc) : 116740-23

Solaris 8 (sparc) : 116742-23

Solaris 8 (sparc) : 116826-06

Solaris 8 (sparc) : 116828-04

Solaris 8 (sparc) : 116831-04

Solaris 8 (sparc) : 116832-04

Solaris 8 (sparc) : 116834-04

Solaris 8 (sparc) : 116856-35

Solaris 8 (sparc) : 116959-21

Solaris 8 (sparc) : 116965-34

Solaris 8 (sparc) : 116973-07

Solaris 8 (sparc) : 116984-01

Solaris 8 (sparc) : 116986-02

Solaris 8 (sparc) : 116993-01

Solaris 8 (sparc) : 116997-01

Solaris 8 (sparc) : 117000-05

Solaris 8 (sparc) : 117350-62

Solaris 8 (sparc) : 117586-22

Solaris 8 (sparc) : 117654-67

Solaris 8 (sparc) : 117722-10

Solaris 8 (sparc) : 117765-05

Solaris 8 (sparc) : 117950-43

Solaris 8 (sparc) : 118128-13

Solaris 8 (sparc) : 118207-63

Solaris 8 (sparc) : 118263-25

Solaris 8 (sparc) : 118388-11

Solaris 8 (sparc) : 118540-42

Solaris 8 (sparc) : 118666-86

Solaris 8 (sparc) : 118667-86

Solaris 8 (sparc) : 118828-04

Solaris 8 (sparc) : 118979-04

Solaris 8 (sparc) : 119004-02

Solaris 8 (sparc) : 119005-02

Solaris 8 (sparc) : 119006-01

Solaris 8 (sparc) : 119007-01

Solaris 8 (sparc) : 119008-01

Solaris 8 (sparc) : 119009-11

Solaris 8 (sparc) : 119010-01

Solaris 8 (sparc) : 119011-01

Solaris 8 (sparc) : 119044-04

Solaris 8 (sparc) : 119067-11

Solaris 8 (sparc) : 119166-43

Solaris 8 (sparc) : 119209-36

Solaris 8 (sparc) : 119465-17

Solaris 8 (sparc) : 119466-17

Solaris 8 (sparc) : 119670-01

Solaris 8 (sparc) : 119725-06

Solaris 8 (sparc) : 119777-19

Solaris 8 (sparc) : 120649-01

Solaris 8 (sparc) : 120650-01

Solaris 8 (sparc) : 120651-01

Solaris 8 (sparc) : 120653-01

Solaris 8 (sparc) : 120671-08

Solaris 8 (sparc) : 120879-08

Solaris 8 (sparc) : 120954-12

Solaris 8 (sparc) : 121209-01

Solaris 8 (sparc) : 121332-01

Solaris 8 (sparc) : 121913-20

Solaris 8 (sparc) : 121956-01

Solaris 8 (sparc) : 121957-01

Solaris 8 (sparc) : 121972-06

Solaris 8 (sparc) : 122073-04

Solaris 8 (sparc) : 122091-01

Solaris 8 (sparc) : 123037-01

Solaris 8 (sparc) : 123038-01

Solaris 8 (sparc) : 123870-05

Solaris 8 (sparc) : 123893-81

Solaris 8 (sparc) : 123920-12

Solaris 8 (sparc) : 124420-04

Solaris 8 (sparc) : 124519-05

Solaris 8 (sparc) : 124520-05

Solaris 8 (sparc) : 124672-20

Solaris 8 (sparc) : 124847-04

Solaris 8 (sparc) : 124969-01

Solaris 8 (sparc) : 125136-97

Solaris 8 (sparc) : 125137-97

Solaris 8 (sparc) : 125191-04

Solaris 8 (sparc) : 125358-25

Solaris 8 (sparc) : 125437-22

Solaris 8 (sparc) : 125713-02

Solaris 8 (sparc) : 126928-02

Solaris 8 (sparc) : 127033-01

Solaris 8 (sparc) : 127380-01

Solaris 8 (sparc) : 127429-07

Solaris 8 (sparc) : 127548-01

Solaris 8 (sparc) : 127655-07

Solaris 8 (sparc) : 127680-07

Solaris 8 (sparc) : 128624-11

Solaris 8 (sparc) : 136859-02

Solaris 8 (sparc) : 136860-02

Solaris 8 (sparc) : 136863-01

Solaris 8 (sparc) : 136987-03

Solaris 8 (sparc) : 138441-01

Solaris 8 (sparc) : 138536-01

Solaris 8 (sparc) : 138885-01

Solaris 8 (sparc) : 139093-03

Solaris 8 (sparc) : 139832-12

Solaris 8 (sparc) : 140837-01

Solaris 8 (sparc) : 142188-01

Solaris 8 (sparc) : 142189-01

Solaris 8 (sparc) : 143047-02

Solaris 8 (sparc) : 143320-05

Solaris 8 (sparc) : 147692-99

Solaris 8 (sparc) : 147693-99

Solaris 8 (sparc) : 150508-01

Solaris 8 (sparc) : 150863-01

Solaris 8 (sparc) : 151009-31

Solaris 8 (sparc) : 152076-51

Solaris 8 (sparc) : 152077-51

Solaris 8 (sparc) : 152096-53

Solaris 8 (sparc) : 152097-53

Solaris 8 (x86) : 108529-29

Solaris 8 (x86) : 108670-21

Solaris 8 (x86) : 108774-28

Solaris 8 (x86) : 108836-04

Solaris 8 (x86) : 108870-36

Solaris 8 (x86) : 108900-04

Solaris 8 (x86) : 108920-30

Solaris 8 (x86) : 108941-76

Solaris 8 (x86) : 108950-09

Solaris 8 (x86) : 108965-11

Solaris 8 (x86) : 108969-12

Solaris 8 (x86) : 108976-10

Solaris 8 (x86) : 108986-03

Solaris 8 (x86) : 108988-19

Solaris 8 (x86) : 109008-28

Solaris 8 (x86) : 109024-08

Solaris 8 (x86) : 109026-08

Solaris 8 (x86) : 109078-21

Solaris 8 (x86) : 109092-10

Solaris 8 (x86) : 109135-33

Solaris 8 (x86) : 109148-42

Solaris 8 (x86) : 109150-02

Solaris 8 (x86) : 109155-01

Solaris 8 (x86) : 109224-10

Solaris 8 (x86) : 109239-02

Solaris 8 (x86) : 109321-22

Solaris 8 (x86) : 109325-10

Solaris 8 (x86) : 109327-24

Solaris 8 (x86) : 109329-07

Solaris 8 (x86) : 109355-25

Solaris 8 (x86) : 109401-14

Solaris 8 (x86) : 109455-06

Solaris 8 (x86) : 109459-04

Solaris 8 (x86) : 109612-01

Solaris 8 (x86) : 109614-07

Solaris 8 (x86) : 109668-07

Solaris 8 (x86) : 109737-13

Solaris 8 (x86) : 109765-06

Solaris 8 (x86) : 109784-03

Solaris 8 (x86) : 109798-04

Solaris 8 (x86) : 109863-05

Solaris 8 (x86) : 109895-02

Solaris 8 (x86) : 109897-20

Solaris 8 (x86) : 109923-05

Solaris 8 (x86) : 109932-10

Solaris 8 (x86) : 109952-01

Solaris 8 (x86) : 110069-04

Solaris 8 (x86) : 110076-03

Solaris 8 (x86) : 110287-16

Solaris 8 (x86) : 110323-02

Solaris 8 (x86) : 110325-04

Solaris 8 (x86) : 110336-03

Solaris 8 (x86) : 110400-04

Solaris 8 (x86) : 110417-07

Solaris 8 (x86) : 110454-04

Solaris 8 (x86) : 110459-02

Solaris 8 (x86) : 110462-03

Solaris 8 (x86) : 110616-18

Solaris 8 (x86) : 110669-05

Solaris 8 (x86) : 110671-04

Solaris 8 (x86) : 110672-05

Solaris 8 (x86) : 110897-03

Solaris 8 (x86) : 110899-15

Solaris 8 (x86) : 110904-08

Solaris 8 (x86) : 110911-12

Solaris 8 (x86) : 110917-07

Solaris 8 (x86) : 110935-28

Solaris 8 (x86) : 110944-04

Solaris 8 (x86) : 110946-10

Solaris 8 (x86) : 110954-08

Solaris 8 (x86) : 110956-06

Solaris 8 (x86) : 110958-02

Solaris 8 (x86) : 111070-01

Solaris 8 (x86) : 111072-01

Solaris 8 (x86) : 111233-01

Solaris 8 (x86) : 111235-01

Solaris 8 (x86) : 111314-06

Solaris 8 (x86) : 111322-05

Solaris 8 (x86) : 111326-02

Solaris 8 (x86) : 111328-05

Solaris 8 (x86) : 111401-04

Solaris 8 (x86) : 111505-02

Solaris 8 (x86) : 111549-01

Solaris 8 (x86) : 111571-04

Solaris 8 (x86) : 111597-03

Solaris 8 (x86) : 111607-07

Solaris 8 (x86) : 111627-03

Solaris 8 (x86) : 111827-01

Solaris 8 (x86) : 111845-04

Solaris 8 (x86) : 111875-09

Solaris 8 (x86) : 111882-03

Solaris 8 (x86) : 112040-01

Solaris 8 (x86) : 112238-15

Solaris 8 (x86) : 112240-13

Solaris 8 (x86) : 112352-02

Solaris 8 (x86) : 112460-01

Solaris 8 (x86) : 112612-02

Solaris 8 (x86) : 112669-04

Solaris 8 (x86) : 112761-13

Solaris 8 (x86) : 112793-01

Solaris 8 (x86) : 112797-01

Solaris 8 (x86) : 112847-01

Solaris 8 (x86) : 113651-02

Solaris 8 (x86) : 113686-06

Solaris 8 (x86) : 113688-02

Solaris 8 (x86) : 113750-02

Solaris 8 (x86) : 113793-01

Solaris 8 (x86) : 114046-03

Solaris 8 (x86) : 114154-02

Solaris 8 (x86) : 114163-01

Solaris 8 (x86) : 114617-01

Solaris 8 (x86) : 114645-04

Solaris 8 (x86) : 114649-01

Solaris 8 (x86) : 114670-04

Solaris 8 (x86) : 114674-01

Solaris 8 (x86) : 114815-01

Solaris 8 (x86) : 114817-04

Solaris 8 (x86) : 114985-02

Solaris 8 (x86) : 115299-01

Solaris 8 (x86) : 115798-01

Solaris 8 (x86) : 116442-01

Solaris 8 (x86) : 116611-01

Solaris 8 (x86) : 116645-10

Solaris 8 (x86) : 116827-07

Solaris 8 (x86) : 116833-04

Solaris 8 (x86) : 116960-21

Solaris 8 (x86) : 116966-33

Solaris 8 (x86) : 116974-07

Solaris 8 (x86) : 116985-01

Solaris 8 (x86) : 116987-02

Solaris 8 (x86) : 116994-01

Solaris 8 (x86) : 116998-01

Solaris 8 (x86) : 117001-05

Solaris 8 (x86) : 117351-61

Solaris 8 (x86) : 117757-34

Solaris 8 (x86) : 117766-05

Solaris 8 (x86) : 118264-25

Solaris 8 (x86) : 118668-86

Solaris 8 (x86) : 118669-86

Solaris 8 (x86) : 119068-11

Solaris 8 (x86) : 119465-17

Solaris 8 (x86) : 119671-01

Solaris 8 (x86) : 120652-01

Solaris 8 (x86) : 120672-08

Solaris 8 (x86) : 121914-20

Solaris 8 (x86) : 121958-01

Solaris 8 (x86) : 121973-06

Solaris 8 (x86) : 122092-01

Solaris 8 (x86) : 123039-01

Solaris 8 (x86) : 124421-04

Solaris 8 (x86) : 124521-05

Solaris 8 (x86) : 124970-01

Solaris 8 (x86) : 125138-97

Solaris 8 (x86) : 125139-97

Solaris 8 (x86) : 125359-25

Solaris 8 (x86) : 126929-02

Solaris 8 (x86) : 127034-01

Solaris 8 (x86) : 127549-01

Solaris 8 (x86) : 128625-11

Solaris 8 (x86) : 136986-03

Solaris 8 (x86) : 138442-01

Solaris 8 (x86) : 138886-01

Solaris 8 (x86) : 139094-03

Solaris 8 (x86) : 140838-01

Solaris 8 (x86) : 142190-01

Solaris 8 (x86) : 142191-01

Solaris 8 (x86) : 147694-99

Solaris 8 (x86) : 147695-99

Solaris 8 (x86) : 150509-01

Solaris 8 (x86) : 151010-31

Solaris 8 (x86) : 152078-51

Solaris 8 (x86) : 152079-51

Solaris 8 (x86) : 152098-53

Solaris 8 (x86) : 152099-53

Solaris 9 (sparc) : 108669-21

Solaris 9 (sparc) : 110938-22

Solaris 9 (sparc) : 110973-22

Solaris 9 (sparc) : 111555-08

Solaris 9 (sparc) : 112233-12

Solaris 9 (sparc) : 112601-10

Solaris 9 (sparc) : 112661-13

Solaris 9 (sparc) : 112760-19

Solaris 9 (sparc) : 112771-34

Solaris 9 (sparc) : 112785-65

Solaris 9 (sparc) : 112807-22

Solaris 9 (sparc) : 112808-11

Solaris 9 (sparc) : 112810-06

Solaris 9 (sparc) : 112811-02

Solaris 9 (sparc) : 112817-33

Solaris 9 (sparc) : 112837-24

Solaris 9 (sparc) : 112874-47

Solaris 9 (sparc) : 112875-01

Solaris 9 (sparc) : 112908-38

Solaris 9 (sparc) : 112915-06

Solaris 9 (sparc) : 112920-03

Solaris 9 (sparc) : 112921-10

Solaris 9 (sparc) : 112923-04

Solaris 9 (sparc) : 112925-08

Solaris 9 (sparc) : 112926-06

Solaris 9 (sparc) : 112945-46

Solaris 9 (sparc) : 112951-15

Solaris 9 (sparc) : 112963-35

Solaris 9 (sparc) : 112964-18

Solaris 9 (sparc) : 112998-05

Solaris 9 (sparc) : 113031-04

Solaris 9 (sparc) : 113072-08

Solaris 9 (sparc) : 113073-14

Solaris 9 (sparc) : 113106-01

Solaris 9 (sparc) : 113146-13

Solaris 9 (sparc) : 113172-10

Solaris 9 (sparc) : 113175-10

Solaris 9 (sparc) : 113240-13

Solaris 9 (sparc) : 113279-01

Solaris 9 (sparc) : 113280-10

Solaris 9 (sparc) : 113322-04

Solaris 9 (sparc) : 113335-05

Solaris 9 (sparc) : 113355-11

Solaris 9 (sparc) : 113434-38

Solaris 9 (sparc) : 113508-02

Solaris 9 (sparc) : 113531-10

Solaris 9 (sparc) : 113575-11

Solaris 9 (sparc) : 113713-30

Solaris 9 (sparc) : 113718-05

Solaris 9 (sparc) : 113798-02

Solaris 9 (sparc) : 113801-12

Solaris 9 (sparc) : 113859-04

Solaris 9 (sparc) : 113911-02

Solaris 9 (sparc) : 113923-05

Solaris 9 (sparc) : 113981-06

Solaris 9 (sparc) : 114008-01

Solaris 9 (sparc) : 114014-28

Solaris 9 (sparc) : 114016-08

Solaris 9 (sparc) : 114049-14

Solaris 9 (sparc) : 114125-01

Solaris 9 (sparc) : 114133-04

Solaris 9 (sparc) : 114135-03

Solaris 9 (sparc) : 114219-11

Solaris 9 (sparc) : 114344-43

Solaris 9 (sparc) : 114361-01

Solaris 9 (sparc) : 114495-01

Solaris 9 (sparc) : 114503-17

Solaris 9 (sparc) : 114564-16

Solaris 9 (sparc) : 114569-02

Solaris 9 (sparc) : 114586-05

Solaris 9 (sparc) : 114636-05

Solaris 9 (sparc) : 114677-15

Solaris 9 (sparc) : 114684-17

Solaris 9 (sparc) : 114686-03

Solaris 9 (sparc) : 114690-01

Solaris 9 (sparc) : 114713-03

Solaris 9 (sparc) : 114716-05

Solaris 9 (sparc) : 114729-01

Solaris 9 (sparc) : 114795-05

Solaris 9 (sparc) : 114796-04

Solaris 9 (sparc) : 114818-07

Solaris 9 (sparc) : 114820-05

Solaris 9 (sparc) : 114861-01

Solaris 9 (sparc) : 114875-01

Solaris 9 (sparc) : 114880-12

Solaris 9 (sparc) : 114971-03

Solaris 9 (sparc) : 115055-01

Solaris 9 (sparc) : 115158-14

Solaris 9 (sparc) : 115172-01

Solaris 9 (sparc) : 115217-05

Solaris 9 (sparc) : 115336-06

Solaris 9 (sparc) : 115553-31

Solaris 9 (sparc) : 115610-25

Solaris 9 (sparc) : 115614-28

Solaris 9 (sparc) : 115677-02

Solaris 9 (sparc) : 115695-06

Solaris 9 (sparc) : 115732-10

Solaris 9 (sparc) : 115738-06

Solaris 9 (sparc) : 115754-02

Solaris 9 (sparc) : 115766-15

Solaris 9 (sparc) : 115835-05

Solaris 9 (sparc) : 115926-10

Solaris 9 (sparc) : 116014-07

Solaris 9 (sparc) : 116047-03

Solaris 9 (sparc) : 116237-01

Solaris 9 (sparc) : 116247-01

Solaris 9 (sparc) : 116264-09

Solaris 9 (sparc) : 116271-10

Solaris 9 (sparc) : 116286-20

Solaris 9 (sparc) : 116292-14

Solaris 9 (sparc) : 116296-21

Solaris 9 (sparc) : 116298-21

Solaris 9 (sparc) : 116300-21

Solaris 9 (sparc) : 116308-01

Solaris 9 (sparc) : 116340-09

Solaris 9 (sparc) : 116453-03

Solaris 9 (sparc) : 116462-06

Solaris 9 (sparc) : 116482-04

Solaris 9 (sparc) : 116489-01

Solaris 9 (sparc) : 116494-01

Solaris 9 (sparc) : 116552-04

Solaris 9 (sparc) : 116559-01

Solaris 9 (sparc) : 116568-99

Solaris 9 (sparc) : 116648-25

Solaris 9 (sparc) : 116669-40

Solaris 9 (sparc) : 116670-06

Solaris 9 (sparc) : 116736-25

Solaris 9 (sparc) : 116738-23

Solaris 9 (sparc) : 116740-23

Solaris 9 (sparc) : 116742-23

Solaris 9 (sparc) : 116774-04

Solaris 9 (sparc) : 116807-02

Solaris 9 (sparc) : 116826-06

Solaris 9 (sparc) : 116828-04

Solaris 9 (sparc) : 116831-04

Solaris 9 (sparc) : 116832-04

Solaris 9 (sparc) : 116834-04

Solaris 9 (sparc) : 116856-35

Solaris 9 (sparc) : 117071-01

Solaris 9 (sparc) : 117123-10

Solaris 9 (sparc) : 117127-03

Solaris 9 (sparc) : 117143-02

Solaris 9 (sparc) : 117201-09

Solaris 9 (sparc) : 117445-01

Solaris 9 (sparc) : 117455-01

Solaris 9 (sparc) : 117471-04

Solaris 9 (sparc) : 117477-01

Solaris 9 (sparc) : 117485-01

Solaris 9 (sparc) : 117586-22

Solaris 9 (sparc) : 117654-67

Solaris 9 (sparc) : 117724-10

Solaris 9 (sparc) : 117767-05

Solaris 9 (sparc) : 117949-43

Solaris 9 (sparc) : 118128-13

Solaris 9 (sparc) : 118191-05

Solaris 9 (sparc) : 118193-04

Solaris 9 (sparc) : 118207-63

Solaris 9 (sparc) : 118263-25

Solaris 9 (sparc) : 118300-02

Solaris 9 (sparc) : 118335-10

Solaris 9 (sparc) : 118389-12

Solaris 9 (sparc) : 118535-06

Solaris 9 (sparc) : 118540-42

Solaris 9 (sparc) : 118558-39

Solaris 9 (sparc) : 118666-86

Solaris 9 (sparc) : 118667-86

Solaris 9 (sparc) : 118829-04

Solaris 9 (sparc) : 118979-04

Solaris 9 (sparc) : 119004-02

Solaris 9 (sparc) : 119005-02

Solaris 9 (sparc) : 119006-01

Solaris 9 (sparc) : 119007-01

Solaris 9 (sparc) : 119008-01

Solaris 9 (sparc) : 119009-11

Solaris 9 (sparc) : 119010-01

Solaris 9 (sparc) : 119011-01

Solaris 9 (sparc) : 119166-43

Solaris 9 (sparc) : 119211-36

Solaris 9 (sparc) : 119433-01

Solaris 9 (sparc) : 119447-02

Solaris 9 (sparc) : 119449-02

Solaris 9 (sparc) : 119465-17

Solaris 9 (sparc) : 119466-17

Solaris 9 (sparc) : 119670-01

Solaris 9 (sparc) : 119725-06

Solaris 9 (sparc) : 119777-19

Solaris 9 (sparc) : 120228-45

Solaris 9 (sparc) : 120240-01

Solaris 9 (sparc) : 120649-01

Solaris 9 (sparc) : 120650-01

Solaris 9 (sparc) : 120651-01

Solaris 9 (sparc) : 120653-01

Solaris 9 (sparc) : 120671-08

Solaris 9 (sparc) : 120879-08

Solaris 9 (sparc) : 120954-12

Solaris 9 (sparc) : 121194-02

Solaris 9 (sparc) : 121209-01

Solaris 9 (sparc) : 121332-01

Solaris 9 (sparc) : 121430-89

Solaris 9 (sparc) : 121581-20

Solaris 9 (sparc) : 121657-54

Solaris 9 (sparc) : 121913-20

Solaris 9 (sparc) : 121956-01

Solaris 9 (sparc) : 121957-01

Solaris 9 (sparc) : 121996-01

Solaris 9 (sparc) : 122073-04

Solaris 9 (sparc) : 122300-61

Solaris 9 (sparc) : 122716-02

Solaris 9 (sparc) : 122793-36

Solaris 9 (sparc) : 123037-01

Solaris 9 (sparc) : 123038-01

Solaris 9 (sparc) : 123368-01

Solaris 9 (sparc) : 123372-02

Solaris 9 (sparc) : 123376-01

Solaris 9 (sparc) : 123396-01

Solaris 9 (sparc) : 123870-05

Solaris 9 (sparc) : 123893-81

Solaris 9 (sparc) : 123921-12

Solaris 9 (sparc) : 124519-05

Solaris 9 (sparc) : 124520-05

Solaris 9 (sparc) : 124672-20

Solaris 9 (sparc) : 124830-01

Solaris 9 (sparc) : 124847-04

Solaris 9 (sparc) : 125136-97

Solaris 9 (sparc) : 125137-97

Solaris 9 (sparc) : 125192-04

Solaris 9 (sparc) : 125326-03

Solaris 9 (sparc) : 125358-25

Solaris 9 (sparc) : 125407-01

Solaris 9 (sparc) : 125437-22

Solaris 9 (sparc) : 125713-02

Solaris 9 (sparc) : 125950-20

Solaris 9 (sparc) : 126049-07

Solaris 9 (sparc) : 126105-42

Solaris 9 (sparc) : 126479-26

Solaris 9 (sparc) : 127381-01

Solaris 9 (sparc) : 127411-16

Solaris 9 (sparc) : 127429-07

Solaris 9 (sparc) : 127655-07

Solaris 9 (sparc) : 127681-07

Solaris 9 (sparc) : 128640-30

Solaris 9 (sparc) : 136859-02

Solaris 9 (sparc) : 136860-02

Solaris 9 (sparc) : 136863-01

Solaris 9 (sparc) : 137038-01

Solaris 9 (sparc) : 137400-01

Solaris 9 (sparc) : 137402-02

Solaris 9 (sparc) : 137910-02

Solaris 9 (sparc) : 138536-01

Solaris 9 (sparc) : 138575-01

Solaris 9 (sparc) : 138577-01

Solaris 9 (sparc) : 138896-01

Solaris 9 (sparc) : 139832-12

Solaris 9 (sparc) : 140426-01

Solaris 9 (sparc) : 141709-03

Solaris 9 (sparc) : 142188-01

Solaris 9 (sparc) : 142189-01

Solaris 9 (sparc) : 142785-17

Solaris 9 (sparc) : 142846-04

Solaris 9 (sparc) : 143048-02

Solaris 9 (sparc) : 143308-03

Solaris 9 (sparc) : 143321-05

Solaris 9 (sparc) : 143749-02

Solaris 9 (sparc) : 144220-15

Solaris 9 (sparc) : 144323-01

Solaris 9 (sparc) : 147264-01

Solaris 9 (sparc) : 147416-02

Solaris 9 (sparc) : 147692-99

Solaris 9 (sparc) : 147693-99

Solaris 9 (sparc) : 149073-01

Solaris 9 (sparc) : 149079-01

Solaris 9 (sparc) : 149079-03

Solaris 9 (sparc) : 150506-01

Solaris 9 (sparc) : 151009-31

Solaris 9 (sparc) : 152076-51

Solaris 9 (sparc) : 152077-51

Solaris 9 (sparc) : 152096-53

Solaris 9 (sparc) : 152097-53

Solaris 9 (x86) : 108670-21

Solaris 9 (x86) : 112662-09

Solaris 9 (x86) : 112761-13

Solaris 9 (x86) : 112786-54

Solaris 9 (x86) : 113124-04

Solaris 9 (x86) : 113241-13

Solaris 9 (x86) : 113797-09

Solaris 9 (x86) : 113838-02

Solaris 9 (x86) : 113867-29

Solaris 9 (x86) : 113870-05

Solaris 9 (x86) : 113924-05

Solaris 9 (x86) : 113986-29

Solaris 9 (x86) : 113996-06

Solaris 9 (x86) : 113999-06

Solaris 9 (x86) : 114009-01

Solaris 9 (x86) : 114015-28

Solaris 9 (x86) : 114017-07

Solaris 9 (x86) : 114050-14

Solaris 9 (x86) : 114134-04

Solaris 9 (x86) : 114136-02

Solaris 9 (x86) : 114137-10

Solaris 9 (x86) : 114145-12

Solaris 9 (x86) : 114193-36

Solaris 9 (x86) : 114194-12

Solaris 9 (x86) : 114196-36

Solaris 9 (x86) : 114210-21

Solaris 9 (x86) : 114220-11

Solaris 9 (x86) : 114262-05

Solaris 9 (x86) : 114265-23

Solaris 9 (x86) : 114273-04

Solaris 9 (x86) : 114343-16

Solaris 9 (x86) : 114348-16

Solaris 9 (x86) : 114362-01

Solaris 9 (x86) : 114423-09

Solaris 9 (x86) : 114432-36

Solaris 9 (x86) : 114436-01

Solaris 9 (x86) : 114496-01

Solaris 9 (x86) : 114504-17

Solaris 9 (x86) : 114565-16

Solaris 9 (x86) : 114568-29

Solaris 9 (x86) : 114570-01

Solaris 9 (x86) : 114587-05

Solaris 9 (x86) : 114637-05

Solaris 9 (x86) : 114678-15

Solaris 9 (x86) : 114685-17

Solaris 9 (x86) : 114687-03

Solaris 9 (x86) : 114691-01

Solaris 9 (x86) : 114714-02

Solaris 9 (x86) : 114715-01

Solaris 9 (x86) : 114717-05

Solaris 9 (x86) : 114730-01

Solaris 9 (x86) : 114819-07

Solaris 9 (x86) : 114862-01

Solaris 9 (x86) : 114876-01

Solaris 9 (x86) : 114932-03

Solaris 9 (x86) : 115159-14

Solaris 9 (x86) : 115167-09

Solaris 9 (x86) : 115168-24

Solaris 9 (x86) : 115337-05

Solaris 9 (x86) : 115554-26

Solaris 9 (x86) : 115611-25

Solaris 9 (x86) : 115615-28

Solaris 9 (x86) : 115678-02

Solaris 9 (x86) : 115696-06

Solaris 9 (x86) : 115739-06

Solaris 9 (x86) : 115755-02

Solaris 9 (x86) : 115836-05

Solaris 9 (x86) : 115880-03

Solaris 9 (x86) : 115927-10

Solaris 9 (x86) : 116015-06

Solaris 9 (x86) : 116044-04

Solaris 9 (x86) : 116045-02

Solaris 9 (x86) : 116046-10

Solaris 9 (x86) : 116175-05

Solaris 9 (x86) : 116238-01

Solaris 9 (x86) : 116248-01

Solaris 9 (x86) : 116287-20

Solaris 9 (x86) : 116293-14

Solaris 9 (x86) : 116297-20

Solaris 9 (x86) : 116299-20

Solaris 9 (x86) : 116301-20

Solaris 9 (x86) : 116309-01

Solaris 9 (x86) : 116341-09

Solaris 9 (x86) : 116454-03

Solaris 9 (x86) : 116479-02

Solaris 9 (x86) : 116553-04

Solaris 9 (x86) : 116569-99

Solaris 9 (x86) : 116645-10

Solaris 9 (x86) : 116737-25

Solaris 9 (x86) : 116739-23

Solaris 9 (x86) : 116741-23

Solaris 9 (x86) : 116743-23

Solaris 9 (x86) : 116775-04

Solaris 9 (x86) : 116808-02

Solaris 9 (x86) : 116827-07

Solaris 9 (x86) : 116833-04

Solaris 9 (x86) : 116838-04

Solaris 9 (x86) : 117072-01

Solaris 9 (x86) : 117122-03

Solaris 9 (x86) : 117144-02

Solaris 9 (x86) : 117172-17

Solaris 9 (x86) : 117202-09

Solaris 9 (x86) : 117419-04

Solaris 9 (x86) : 117446-01

Solaris 9 (x86) : 117456-02

Solaris 9 (x86) : 117472-04

Solaris 9 (x86) : 117475-05

Solaris 9 (x86) : 117478-01

Solaris 9 (x86) : 117486-01

Solaris 9 (x86) : 117714-17

Solaris 9 (x86) : 117757-34

Solaris 9 (x86) : 117768-05

Solaris 9 (x86) : 117909-43

Solaris 9 (x86) : 118192-05

Solaris 9 (x86) : 118194-04

Solaris 9 (x86) : 118208-63

Solaris 9 (x86) : 118264-25

Solaris 9 (x86) : 118301-02

Solaris 9 (x86) : 118462-03

Solaris 9 (x86) : 118536-06

Solaris 9 (x86) : 118541-42

Solaris 9 (x86) : 118559-39

Solaris 9 (x86) : 118668-86

Solaris 9 (x86) : 118669-86

Solaris 9 (x86) : 118908-06

Solaris 9 (x86) : 119167-43

Solaris 9 (x86) : 119212-36

Solaris 9 (x86) : 119434-01

Solaris 9 (x86) : 119435-29

Solaris 9 (x86) : 119450-02

Solaris 9 (x86) : 119465-17

Solaris 9 (x86) : 119467-17

Solaris 9 (x86) : 119671-01

Solaris 9 (x86) : 119725-06

Solaris 9 (x86) : 119778-19

Solaris 9 (x86) : 119902-01

Solaris 9 (x86) : 120229-45

Solaris 9 (x86) : 120239-01

Solaris 9 (x86) : 120463-07

Solaris 9 (x86) : 120652-01

Solaris 9 (x86) : 120672-08

Solaris 9 (x86) : 120955-12

Solaris 9 (x86) : 121092-01

Solaris 9 (x86) : 121093-01

Solaris 9 (x86) : 121195-02

Solaris 9 (x86) : 121431-90

Solaris 9 (x86) : 121582-20

Solaris 9 (x86) : 121658-54

Solaris 9 (x86) : 121775-01

Solaris 9 (x86) : 121914-20

Solaris 9 (x86) : 121958-01

Solaris 9 (x86) : 121995-01

Solaris 9 (x86) : 121997-02

Solaris 9 (x86) : 122301-61

Solaris 9 (x86) : 122371-15

Solaris 9 (x86) : 122715-03

Solaris 9 (x86) : 122717-02

Solaris 9 (x86) : 122794-36

Solaris 9 (x86) : 123039-01

Solaris 9 (x86) : 123369-01

Solaris 9 (x86) : 123373-02

Solaris 9 (x86) : 123377-01

Solaris 9 (x86) : 123397-01

Solaris 9 (x86) : 123896-81

Solaris 9 (x86) : 123922-11

Solaris 9 (x86) : 124521-05

Solaris 9 (x86) : 124673-20

Solaris 9 (x86) : 124831-01

Solaris 9 (x86) : 124833-02

Solaris 9 (x86) : 125138-97

Solaris 9 (x86) : 125139-97

Solaris 9 (x86) : 125327-03

Solaris 9 (x86) : 125359-25

Solaris 9 (x86) : 125438-22

Solaris 9 (x86) : 125951-20

Solaris 9 (x86) : 126480-26

Solaris 9 (x86) : 127413-16

Solaris 9 (x86) : 127430-07

Solaris 9 (x86) : 127682-07

Solaris 9 (x86) : 128641-30

Solaris 9 (x86) : 137039-01

Solaris 9 (x86) : 137401-01

Solaris 9 (x86) : 137403-02

Solaris 9 (x86) : 137911-02

Solaris 9 (x86) : 138536-01

Solaris 9 (x86) : 138570-01

Solaris 9 (x86) : 138574-01

Solaris 9 (x86) : 138576-01

Solaris 9 (x86) : 138578-01

Solaris 9 (x86) : 138897-01

Solaris 9 (x86) : 139833-12

Solaris 9 (x86) : 140427-01

Solaris 9 (x86) : 141710-03

Solaris 9 (x86) : 142190-01

Solaris 9 (x86) : 142191-01

Solaris 9 (x86) : 142786-17

Solaris 9 (x86) : 142848-04

Solaris 9 (x86) : 143322-06

Solaris 9 (x86) : 143750-02

Solaris 9 (x86) : 144324-01

Solaris 9 (x86) : 147265-01

Solaris 9 (x86) : 147694-99

Solaris 9 (x86) : 147695-99

Solaris 9 (x86) : 149074-01

Solaris 9 (x86) : 149080-01

Solaris 9 (x86) : 149080-02

Solaris 9 (x86) : 150507-01

Solaris 9 (x86) : 151010-31

Solaris 9 (x86) : 152078-51

Solaris 9 (x86) : 152079-51

Solaris 9 (x86) : 152098-53

Solaris 9 (x86) : 152099-53

Solaris Unbundled (sparc) : 138195-04

# SNMP

Sitemaps

Sitemap test

Create new sitemap

\_root

ID Selector type Multiple Parent selectors Actions

111 td.plugin-family-plugin-name SelectorText yes \_root

×

Data Preview

111

ARRIS Touchstone DG950A SNMP Information Disclosure (CVE-2014-4863)

ASG-Sentry SNMP Agent Detection

BMC SNMP Agent Default Community Name (public)

Cisco CatOS VACM read-write Community String Device Configuration Manipulation

Cisco Digital Media Manager < 5.3 Privilege Escalation

D-Link DSL Broadband Modem SNMP Cleartext ISP Credential Disclosure

HP JetDirect Device SNMP Request Cleartext Admin Credential Disclosure

HP/H3C and Huawei SNMP User Data Information Disclosure

Microsoft Windows LAN Manager SNMP LanMan Services Disclosure

Microsoft Windows LAN Manager SNMP LanMan Shares Disclosure

Microsoft Windows LAN Manager SNMP LanMan Users Disclosure

Multiple Vendor HMAC Authentication SNMPv3 Authentication Bypass

Multiple Vendor Malformed SNMP Message-Handling DoS

Multiple Vendor Malformed SNMP Trap Handling DoS

Multiple Vendor SNMP public Community String Information Disclosure

Samsung / Dell Printer SNMP Backdoor

SNMP 'GETBULK' Reflection DDoS

SNMP Agent Default Community Name (public)

SNMP Agent Default Community Names

SNMP GETBULK Large max-repetitions Remote DoS

SNMP Protocol Version Detection

SNMP Query Airport Version

SNMP Query Installed Software Disclosure

SNMP Query Routing Information Disclosure

SNMP Query Running Process List Disclosure

SNMP Query System Information Disclosure

SNMP Query WLAN SSID (Cisco)

SNMP Request Cisco Router Information Disclosure

SNMP Request Network Interfaces Enumeration

SNMP Supported Protocols Detection

SNMP Zero Length UDP Packet Remote DoS

SNMPc Management Server Detection

Solaris mibiisa MIB Parsing Remote Overflow

# SMTP problems

Ability Mail Server < 2.61 Multiple Remote DoS

Anonymous SMTP Authentication Enabled

ASN.1 Multiple Integer Overflows (SMTP check)

BaSoMail SMTP Multiple Command Remote Overflow DoS

BusinessMail Multiple SMTP Command Remote Buffer Overflows

Canon ImageRUNNER SMTP Arbitrary Content Printing

Citadel SMTP makeuserkey Function RCPT TO Command Remote Overflow

ClamAV clamav-milter black-hole-mode Sendmail Recipient Field Arbitrary Command Execution

CMail MAIL FROM Command Remote Overflow

CommuniGate Pro LISTS Module Malformed Multipart Message DoS

Courier < 0.45 Multiple Remote Overflows

Courier Mail Server < 0.50.1 DNS SPF Record Lookup Failure Memory Corruption DoS

CSM Mail Server MTA 'HELO' DoS

Debian GNU/Linux Sendmail Default SASL Password

Eudora Internet Mail Server (EIMS) < 3.2.8 Multiple DoS

Exchange Malformed MIME Header Handling DoS

Exchange XEXCH50 Remote Buffer Overflow

Exim 4.70 - 4.80 DKIM DNS Record Parsing Remote Buffer Overflow

Exim 4.87 < 4.92 Remote Command Execution

Exim 4.92.x < 4.92.3 Heap Buffer Overflow

Exim < 3.36 / 4.33 Multiple Remote Overflows

Exim < 4.22 smtp\_in.c HELO/EHLO Remote Overflow

Exim < 4.44 Multiple Overflows

Exim < 4.72 Multiple Vulnerabilities

Exim < 4.74 Local Privilege Escalation

Exim < 4.76 dkim\_exim\_verify\_finish() DKIM-Signature Header Format String

Exim < 4.83 Math Comparison Functions Data Insertion

Exim < 4.89.1 Use-After-Free BDAT Remote Code Execution

Exim < 4.90.1 Buffer Overflow RCE Vulnerability

Exim < 4.92.1 Input-Validation RCE

Exim < 4.92.2

Exim < 4.93 Privilege Escalation vulnerability

Exim deliver\_message() Function Remote Command Execution Vulnerability (Remote)

Exim string\_format Function Remote Overflow

Exim with Dovecot use\_shell Command Injection

eXtremail Multiple SMTP Command flog Function Format String

FTGatePro Mail Server Multiple Command Remote Overflow

GoodTech SMTP Server < 5.17 Multiple Buffer Overflows

GoodTech SMTP Server Malformed RCPT TO Command DoS

GroupWise Internet Agent < 8.0.2 HP3 iCalendar TZNAME Property Heap Overflow

IBM Lotus Domino iCalendar Email Address ORGANIZER:mailto Header Remote Overflow

IBM Lotus Domino SMTP Server Malformed Meeting Request (vCal) DoS

Imate SMTP Server HELO Command Remote Overflow DoS

Inframail SMTP MAIL FROM Command Remote Overflow DoS

Ipswitch Collaboration Suite / IMail SMTPD Multiple Commands Format String

Ipswitch IMail / SLMail VRFY Command Remote Overflow

Ipswitch IMail Server SMTP Service Crafted RCPT String Remote Overflow

IPSwitch IMail SMTP Multiple Vulnerabilities (OF, DoS)

ISMail Multiple Command Domain Name Handling Remote Overflow

ITHouse Mail Server v1.04 To: Field Handling Overflow

Kerio MailServer < 6.0.3 Unspecified Vulnerability

Kerio MailServer < 6.4.1 Attachment Filter Unspecified Vulnerability

Lotus Domino SMTP ENVID Variable Handling RCE

Lotus Domino SMTP MAIL FROM Command Remote Overflow

Lotus Domino SMTP Server Forged Localhost Mail Header DoS

Lotus Notes SMTP Server HELO Command Overflow DoS

Mail Transfer Agent and Mail Delivery Agent Remote Command Execution via Shellshock

MailCarrier < 3.0.1 SMTP EHLO Command Remote Overflow

MailEnable Professional Webmail < 1.5.1 Unspecified Vulnerability

MailEnable SMTP Connector Multiple NTLM Authentication Vulnerabilities

MailEnable SMTP Connector Service DNS MX Response DoS

MailEnable SMTP Connector Service SPF Record Crafted Lookup DoS

MailEnable SMTP Server HELO Command Remote DoS

MailEnable SMTP Service Denial of Service Vulnerabilities (ME-10044)

MailEnable Standard SMTP mailto: Request Format String

MAILsweeper for SMTP PowerPoint Document Processing DoS

McAfee WebShield SMTP 4.5 Multiple Vulnerabilities

McAfee WebShield SMTP Unsupported

MDaemon < 6.5.2 Multiple Remote Buffer Overflows

MDaemon Connection Saturation Remote DoS

MDaemon File Creation Local Privilege Escalation

MDaemon SMTP HELO Command Remote Overflow DoS

MERCUR SMTP Server EXPN Command Remote Overflow

Mercury SMTP Server AUTH CRAM-MD5 Remote Buffer Overflow

Microsoft Windows SMTP Incorrect Credentials Authentication Bypass

Microsoft Windows SMTP Service Malformed BDAT Request Remote DoS

Microsoft Windows SMTP Service NTLM Null Session Authorization Bypass (uncredentialed check)

Microsoft Windows/Exchange SMTP DNS Lookup Overflow (885881)

MS02-037: Microsoft Exchange EHLO Long Hostname Overflow

MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)

MTA Open Mail Relaying Allowed

MTA Open Mail Relaying Allowed (internal)

MTA Open Mail Relaying Allowed (thorough test)

Multiple Anti-Virus SMTP Message Long Line Parsing DoS

Multiple Mail Server EXPN/VRFY Information Disclosure

Multiple MTA HELO Command Remote Overflow

NetManage Chameleon SMTPd Remote Overflow DoS

NetWin DSMTP (Dmail) ETRN Command Overflow

NetWin SurgeMail Multiple Remote Unspecified Vulnerabilities

NTMail3 Arbitrary Mail Relay

OpenSMTPD Critical LPE / RCE Vulnerability Remote Check

OpenSMTPD TLS Blocking Socket Remote DoS

poprelayd & sendmail Arbitrary Mail Relay

Postfix 2.x Mail Message Date Field RCE (ENTERSEED)

Postfix < 2.0 Multiple Vulnerabilities

Postfix Cyrus SASL Authentication Context Data Reuse Memory Corruption

Postfix Cyrus SASL Authentication Context Data Reuse Memory Corruption (exploit)

Postfix epoll File Descriptor Leak Local DoS

Postfix Script Remote Command Execution via Shellshock

Qmail Remote Command Execution via Shellshock

Sendmail -C Malformed Configuration Privilege Escalation

Sendmail 8.6.9 IDENT Remote Overflow

Sendmail 8.8.8 - 8.12.7 Multiple Vulnerabilities (Bypass, OF)

Sendmail < 8.10.0 mail.local Newline Handling Remote DoS

Sendmail < 8.11.2 -bt Option Local Overflow

Sendmail < 8.11.6 -d category Value Local Overflow

Sendmail < 8.12.1 RestrictQueueRun Option Multiple Argument Local DoS

Sendmail < 8.12.10 prescan() Function Remote Overflow

Sendmail < 8.12.9 NOCHAR Control Value prescan Overflow

Sendmail < 8.13.2 Mail X-Header Handling Remote Overflow

Sendmail < 8.13.8 Header Processing Overflow DoS

Sendmail < 8.14.4 SSL Certificate NULL Character Spoofing

Sendmail < 8.14.9 close-on-exec SMTP Connection Manipulation

Sendmail < 8.6.8 -debug Local Privilege Escalation

Sendmail < 8.7.6 Multiple Local Vulnerabilities

Sendmail < 8.8.3 Daemon Mode Local Privilege Escalation

Sendmail < 8.8.4 Group Write File Hardlink Privilege Escalation

Sendmail < 8.8.5 MIME Conversion Malformed Header Overflow

Sendmail < 8.9.3 Header Prescan Function Message Header DoS

Sendmail Crafted ETRN Commands Remote DoS

Sendmail Custom DNS Map TXT Query Overflow

Sendmail DEBUG/WIZ Remote Command Execution

Sendmail decode Alias Arbitrary File Overwrite

Sendmail headers.c crackaddr Function Address Field Handling Remote Overflow

Sendmail MAIL FROM Command Arbitrary Remote Command Execution

Sendmail mail from/rcpt to Pipe Arbitrary Command Execution

Sendmail mime7to8() Function Remote Overflow

Sendmail RCPT TO Command Arbitrary File Overwrite

Sendmail Redirection Relaying Allowed

Sendmail RestrictQueueRun Option Debug Mode Information Disclosure

Sendmail Service Detection

SLMail < 5.1.0.4433 Multiple Command Remote Overflows

SLMail HELO Command Remote Overflow

Smail-3 < 3.2.0.121 Multiple Vulnerabilities

SMTP Authentication Methods

SMTP Generic Overflow Detection

SMTP Host Information in NTLM SSP

SMTP Server Connection Check

SMTP Service Cleartext Login Permitted

SMTP Service STARTTLS Command Support

SMTP Service STARTTLS Plaintext Command Injection

smtpscan SMTP Fingerprinting

Solaris sendmail .forward Local Privilege Escalation

SpamAssassin Milter Plugin 'mlfi\_envrcpt()' Remote Arbitrary Command Injection

TFS SMTP 3.2 MAIL FROM overflow

Trend Micro InterScan 3.32 SMTP HELO Command Remote Overflow DoS

XtraMail SMTP HELO Command Remote Overflow

Youngzsoft CMailServer < 5.2.1 Multiple Remote Vulnerabilities

# Slackware Local Security Checks

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2011-147-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2011-224-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2012-166-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 8.1 / 9.0 / 9.1 / current : fetchmail (SSA:2011-171-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2011-210-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2012-206-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 9.0 / 9.1 / current : libtiff (SSA:2012-098-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2010-176-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2010-350-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : bzip2 (SSA:2010-263-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2010-180-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : samba (SSA:2011-059-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : sudo (SSA:2010-257-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : sudo (SSA:2011-041-05)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 8.1 / 9.0 / 9.1 / current : sudo redo (SSA:2010-258-03)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 9.0 / 9.1 / current : dhcp (SSA:2011-097-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 9.0 / 9.1 / current : libtiff (SSA:2010-180-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 9.0 / 9.1 / current : libtiff (SSA:2011-098-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 9.1 / current : xpdf (SSA:2010-324-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : samba (SSA:2010-257-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2009-336-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 8.1 / 9.0 / 9.1 / current : fetchmail (SSA:2010-136-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 8.1 / 9.0 / 9.1 / current : ntp (SSA:2009-343-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 8.1 / 9.0 / 9.1 / current : sudo (SSA:2010-110-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 9.1 / current : xpdf (SSA:2009-302-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : samba (SSA:2009-276-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 : samba (SSA:2010-169-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2009-014-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2009-210-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : dhcp (SSA:2009-195-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : fetchmail (SSA:2009-218-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2009-051-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2009-170-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : ntp (SSA:2009-014-03)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 8.1 / 9.0 / 9.1 / current : ntp (SSA:2009-154-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 9.1 / current : curl (SSA:2009-069-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 9.1 / current : curl (SSA:2009-226-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 9.1 / current : xpdf (SSA:2009-129-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : lcms (SSA:2009-083-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : samba (SSA:2009-177-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 8.1 / 9.0 / 9.1 / current : bind (SSA:2008-191-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 8.1 / 9.0 / 9.1 / current : fetchmail (SSA:2008-210-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / current : dnsmasq (SSA:2008-205-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / current : libxml2 (SSA:2008-324-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / current : samba (SSA:2008-149-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / current : samba (SSA:2008-333-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 / current : bzip2 (SSA:2008-098-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 / current : cups (SSA:2007-305-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2007-325-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2008-119-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 / current : m4 (SSA:2008-098-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 / current : openssh (SSA:2008-095-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 / current : rsync (SSA:2007-335-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 : bind (SSA:2007-207-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 : glibc-zoneinfo (SSA:2007-283-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 : java (jre, jdk) (SSA:2007-243-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 8.1 / 9.0 / 9.1 : openssh (SSA:2007-255-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 9.0 / 9.1 : tcpdump (SSA:2007-230-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 9.1 / current : xpdf/poppler/koffice/kdegraphics (SSA:2007-316-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / 9.1 : xpdf (SSA:2007-222-05)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / current : samba (SSA:2007-320-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / current : samba (SSA:2007-344-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / current : xine-lib (SSA:2008-089-03)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / current : xine-lib (SSA:2008-092-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 / current : xine-lib (SSA:2008-111-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 12.0 : samba (SSA:2007-255-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 / current : file [and bin package] (SSA:2007-093-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2007-136-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : apache (SSA:2008-045-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : bind (SSA:2006-310-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : bind (SSA:2007-026-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : fetchmail (SSA:2007-024-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : libpng (SSA:2006-335-03)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : proftpd (SSA:2006-335-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : screen (SSA:2006-307-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 8.1 / 9.0 / 9.1 : tar (SSA:2006-335-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 9.0 / 9.1 : gnupg (SSA:2006-340-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 9.0 / 9.1 : gnupg (SSA:2007-066-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / 9.1 : xine-lib (SSA:2006-357-05)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / current : samba (SSA:2007-134-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 / current : xine-lib (SSA:2007-109-02)

Slackware 10.0 / 10.1 / 10.2 / 11.0 : qt (SSA:2006-298-01)

Slackware 10.0 / 10.1 / 10.2 / 11.0 : samba (SSA:2007-038-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : apache (SSA:2005-310-04)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : Apache httpd (SSA:2006-129-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : Apache httpd (SSA:2006-209-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : Apache httpd redux (SSA:2006-130-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : curl/wget (SSA:2005-310-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : elm mailer (SSA:2005-311-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : fetchmail (SSA:2006-045-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : gzip (SSA:2006-262-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : imapd (SSA:2005-310-06)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : lynx (SSA:2005-310-03)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : mutt (SSA:2006-207-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : openssh (SSA:2006-045-06)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : openssh (SSA:2006-272-02)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : OpenSSL (SSA:2005-286-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : openssl (SSA:2006-257-02)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : sendmail (SSA:2006-081-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : sendmail (SSA:2006-166-01)

Slackware 10.0 / 10.1 / 10.2 / 8.1 / 9.0 / 9.1 / current : sudo (SSA:2006-045-08)

Slackware 10.0 / 10.1 / 10.2 / 9.0 / 9.1 / current : bind DoS (SSA:2006-257-01)

Slackware 10.0 / 10.1 / 10.2 / 9.0 / 9.1 / current : gnupg (SSA:2006-072-02)

Slackware 10.0 / 10.1 / 10.2 / 9.0 / 9.1 / current : gnupg (SSA:2006-215-01)

Slackware 10.0 / 10.1 / 10.2 / 9.0 / 9.1 / current : gnupg DoS (SSA:2006-178-02)

Slackware 10.0 / 10.1 / 10.2 / 9.0 / 9.1 / current : libtiff (SSA:2006-230-01)

Slackware 10.0 / 10.1 / 10.2 / 9.0 / 9.1 / current : openssl (SSA:2006-272-01)

Slackware 10.0 / 10.1 / 10.2 / 9.0 / 9.1 / current : xpdf (SSA:2006-045-09)

Slackware 10.0 / 10.1 / 10.2 / 9.1 / current : KOffice/KWord (SSA:2005-310-02)

Slackware 10.0 / 10.1 / 10.2 / 9.1 / current : mysql (SSA:2006-155-01)

Slackware 10.0 / 10.1 / 10.2 / 9.1 / current : xine-lib (SSA:2005-283-01)

Slackware 10.0 / 10.1 / 10.2 / current : arts (SSA:2006-178-03)

Slackware 10.0 / 10.1 / 10.2 / current : kdebase kdm local file reading vulnerability (SSA:2006-178-01)

Slackware 10.0 / 10.1 / 10.2 / current : kdegraphics (SSA:2006-045-04)

Slackware 10.0 / 10.1 / 10.2 / current : mozilla security/EOL (SSA:2006-114-01)

Slackware 10.0 / 10.1 / 10.2 / current : Mozilla/Firefox (SSA:2005-269-01)

Slackware 10.0 / 10.1 / 10.2 / current : Samba 2.0.23 repackaged (SSA:2006-200-01)

Slackware 10.0 / 10.1 / 10.2 / current : Samba DoS (SSA:2006-195-01)

Slackware 10.0 / 10.1 / 10.2 / current : X.Org pixmap overflow (SSA:2005-269-02)

Slackware 10.0 / 10.1 / 10.2 : kdelibs (SSA:2006-045-05)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : CVS (SSA:2005-111-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : dhcpcd DoS (SSA:2005-255-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : fetchmail (SSA:2005-203-05)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : infozip (SSA:2005-121-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : java (jre, j2sdk) (SSA:2005-170-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : mod\_ssl (SSA:2005-251-02)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : PCRE library (SSA:2005-242-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : PHP (SSA:2005-095-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : PHP (SSA:2005-192-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : PHP (SSA:2005-242-02)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : Python SimpleXMLRPCServer module (SSA:2005-111-02)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : sudo (SSA:2005-172-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : tcpdump DoS (SSA:2005-195-10)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : telnet client (SSA:2005-210-01)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : util-linux umount privilege escalation (SSA:2005-255-02)

Slackware 10.0 / 10.1 / 8.1 / 9.0 / 9.1 / current : XV (SSA:2005-195-02)

Slackware 10.0 / 10.1 / 9.0 / 9.1 / current : gaim (SSA:2005-111-03)

Slackware 10.0 / 10.1 / 9.0 / 9.1 / current : gaim (SSA:2005-133-01)

Slackware 10.0 / 10.1 / 9.0 / 9.1 / current : gaim (SSA:2005-162-01)

Slackware 10.0 / 10.1 / 9.0 / 9.1 / current : gaim (SSA:2005-242-03)

Slackware 10.0 / 10.1 / 9.1 / current : Mozilla/Firefox/Thunderbird (SSA:2005-085-01)

Slackware 10.0 / 10.1 / current : dnsmasq (SSA:2005-201-01)

Slackware 10.0 / 10.1 / current : gxine format string vulnerability (SSA:2005-203-04)

Slackware 10.0 / 10.1 / current : kcheckpass in kdebase (SSA:2005-251-01)

Slackware 10.0 / 10.1 / current : kdenetwork (SSA:2005-203-02)

Slackware 10.0 / 10.1 / current : Mozilla/Firefox (SSA:2005-111-04)

Slackware 10.0 / 10.1 / current : Mozilla/Firefox (SSA:2005-135-01)

Slackware 10.0 / 10.1 / current : Mozilla/Firefox (SSA:2005-203-01)

Slackware 10.0 / 10.1 / current : ncftp (SSA:2005-135-02)

Slackware 10.0 / 10.1 / current : xine-lib (SSA:2005-121-02)

Slackware 10.0 / 10.1 / current : zlib (SSA:2005-203-03)

Slackware 10.0 / 10.1 / current : zlib DoS (SSA:2005-189-01)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : apache+mod\_ssl (SSA:2004-305-01)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : apache, mod\_ssl, php (SSA:2004-299-01)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : libpng (SSA:2004-222-01)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : libtiff (SSA:2004-305-02)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : new mod\_ssl packages (SSA:2004-207-02)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : new samba packages (SSA:2004-207-01)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : PHP (SSA:2004-202-01)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : rsync (SSA:2004-285-01)

Slackware 10.0 / 8.1 / 9.0 / 9.1 / current : sox (SSA:2004-223-03)

Slackware 10.0 / 9.0 / 9.1 / current : gaim (SSA:2004-296-01)

Slackware 10.0 / 9.0 / 9.1 / current : Qt (SSA:2004-236-01)

Slackware 10.0 / 9.1 / current : CUPS DoS (SSA:2004-266-01)

Slackware 10.0 / 9.1 / current : gaim (SSA:2004-239-01)

Slackware 10.0 / 9.1 / current : gaim updated again (SSA:2004-240-01)

Slackware 10.0 / 9.1 / current : getmail (SSA:2004-278-01)

Slackware 10.0 / 9.1 / current : imagemagick (SSA:2004-223-02)

Slackware 10.0 / 9.1 / current : kde (SSA:2004-247-01)

Slackware 10.0 / 9.1 / current : Mozilla (SSA:2004-223-01)

Slackware 10.0 / current : alternate samba package for Slackware 10.0 (SSA:2004-208-01)

Slackware 10.0 / current : GTK+ image loading flaws (SSA:2004-266-02)

Slackware 10.0 / current : Mozilla (SSA:2004-266-03)

Slackware 10.0 / current : samba DoS (SSA:2004-257-01)

Slackware 10.0 / current : xine-lib (SSA:2004-266-04)

Slackware 10.0 / current : zlib DoS (SSA:2004-278-02)

Slackware 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : irssi (SSA:2010-116-01)

Slackware 10.1 / 10.2 / 11.0 / 12.0 / 12.1 / current : python (SSA:2008-217-01)

Slackware 10.1 / 10.2 / 11.0 / 12.0 / current : php (SSA:2007-314-01)

Slackware 10.1 / 10.2 / 11.0 / 12.0 : php (SSA:2007-255-03)

Slackware 10.1 / 10.2 / 11.0 / current : freetype (SSA:2007-109-01)

Slackware 10.1 / 10.2 / current : xorg server overflow (SSA:2006-123-01)

Slackware 10.1 / current : emacs movemail POP utility (SSA:2005-201-02)

Slackware 10.1 : php5 in Slackware 10.1 (SSA:2005-251-04)

Slackware 10.1 : Slackware 10.1 kdegraphics (SSA:2006-072-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : mozilla-thunderbird (SSA:2010-095-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : cyrus-sasl (SSA:2009-134-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : mozilla-firefox (SSA:2008-353-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : mozilla-thunderbird (SSA:2008-366-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : mozilla-thunderbird (SSA:2009-083-03)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : mozilla-thunderbird (SSA:2009-178-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : mozilla-thunderbird (SSA:2009-232-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / 12.2 / current : udev (SSA:2009-111-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / current : mozilla-firefox (SSA:2008-269-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / current : mozilla-firefox (SSA:2008-320-03)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / current : mozilla-thunderbird (SSA:2008-128-02)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / current : mozilla-thunderbird (SSA:2008-210-05)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / current : mozilla-thunderbird (SSA:2008-270-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / current : mozilla-thunderbird (SSA:2008-325-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 / current : php (SSA:2008-128-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 : mozilla-firefox (SSA:2008-191-01)

Slackware 10.2 / 11.0 / 12.0 / 12.1 : mozilla-firefox (SSA:2008-198-01)

Slackware 10.2 / 11.0 / 12.0 / current : firefox (SSA:2007-331-01)

Slackware 10.2 / 11.0 / 12.0 / current : firefox, seamonkey (SSA:2007-297-01)

Slackware 10.2 / 11.0 / 12.0 / current : firefox, seamonkey (SSA:2008-043-01)

Slackware 10.2 / 11.0 / 12.0 / current : mozilla-firefox (SSA:2008-089-01)

Slackware 10.2 / 11.0 / 12.0 / current : mozilla-firefox (SSA:2008-108-01)

Slackware 10.2 / 11.0 / 12.0 / current : mozilla-thunderbird (SSA:2007-324-01)

Slackware 10.2 / 11.0 / 12.0 / current : mozilla-thunderbird (SSA:2008-061-01)

Slackware 10.2 / 11.0 / 12.0 : gimp (SSA:2007-222-01)

Slackware 10.2 / 11.0 / 12.0 : qt (SSA:2007-222-03)

Slackware 10.2 / 11.0 / current : firefox-seamonkey-thunderbird (SSA:2007-152-02)

Slackware 10.2 / 11.0 / current : libexif (SSA:2007-164-01)

Slackware 10.2 / 11.0 / current : libwpd (SSA:2007-085-02)

Slackware 10.2 / 11.0 / current : mozilla-firefox (SSA:2007-085-01)

Slackware 10.2 / 11.0 / current : php (SSA:2007-127-01)

Slackware 10.2 / 11.0 / current : php5 (SSA:2007-152-01)

Slackware 10.2 / 11.0 / current : qt (SSA:2007-093-03)

Slackware 10.2 / 11.0 : [fixed URLs] firefox/thunderbird/seamonkey (SSA:2006-313-01)

Slackware 10.2 / 11.0 : bind 10.2/11.0 recompile (SSA:2009-015-01)

Slackware 10.2 / 11.0 : mozilla-firefox (SSA:2006-357-01)

Slackware 10.2 / 11.0 : mozilla-firefox (SSA:2007-066-03)

Slackware 10.2 / 11.0 : mozilla-thunderbird (SSA:2006-357-02)

Slackware 10.2 / 11.0 : mozilla-thunderbird (SSA:2007-066-04)

Slackware 10.2 / 11.0 : php (SSA:2006-307-01)

Slackware 10.2 / 11.0 : php (SSA:2007-053-01)

Slackware 10.2 / 11.0 : php (SSA:2008-045-03)

Slackware 10.2 / 11.0 : php (SSA:2008-247-01)

Slackware 10.2 / 11.0 : x11 (SSA:2007-066-02)

Slackware 10.2 / current : firefox (SSA:2006-045-02)

Slackware 10.2 / current : firefox (SSA:2006-107-01)

Slackware 10.2 / current : firefox (SSA:2006-123-02)

Slackware 10.2 / current : firefox/thunderbird/seamonkey (SSA:2006-155-02)

Slackware 10.2 / current : firefox/thunderbird/seamonkey (SSA:2006-208-01)

Slackware 10.2 / current : firefox/thunderbird/seamonkey (SSA:2006-257-03)

Slackware 10.2 / current : gimp (SSA:2006-207-03)

Slackware 10.2 / current : imagemagick (SSA:2006-045-03)

Slackware 10.2 / current : mysql (SSA:2006-129-02)

Slackware 10.2 / current : PHP (SSA:2005-310-05)

Slackware 10.2 / current : php (SSA:2006-045-07)

Slackware 10.2 / current : php (SSA:2006-217-01)

Slackware 10.2 / current : php (SSA:2006-230-02)

Slackware 10.2 / current : tetex PDF security (SSA:2006-142-01)

Slackware 10.2 / current : thunderbird (SSA:2006-120-01)

Slackware 10.2 / current : Thunderbird email client (SSA:2005-278-01)

Slackware 10.2 / current : x11 (SSA:2006-207-02)

Slackware 10.2 / current : x11 (SSA:2006-259-01)

Slackware 10.2 / current : xine-lib (SSA:2006-207-04)

Slackware 10.2 / current : zoo archiver overflow (SSA:2006-142-02)

Slackware 10.2 : koffice (SSA:2006-357-04)

Slackware 10.2 : mysql (SSA:2006-211-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : apr/apr-util (SSA:2011-133-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : apr/apr-util (SSA:2011-145-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : freetype (SSA:2012-176-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : libexif (SSA:2012-200-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : php (SSA:2011-237-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : proftpd (SSA:2012-041-04)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : vsftpd (SSA:2012-041-05)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : acl (SSA:2011-108-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : apr-util (SSA:2011-041-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : expat (SSA:2011-041-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : openssl (SSA:2010-326-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : openssl (SSA:2010-340-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : openssl (SSA:2011-041-04)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : php (SSA:2010-240-04)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : php (SSA:2010-357-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : php (SSA:2011-010-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : proftpd (SSA:2010-305-03)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : proftpd (SSA:2010-357-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : proftpd (SSA:2011-095-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : rdesktop (SSA:2011-110-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : openssl (SSA:2009-320-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : openssl (SSA:2010-060-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : openssl (SSA:2010-090-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : php (SSA:2010-024-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / 13.0 / current : seamonkey (SSA:2009-250-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : apr (SSA:2009-219-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : apr-util (SSA:2009-167-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : apr-util (SSA:2009-219-03)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : openssl (SSA:2009-014-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : openssl (SSA:2009-098-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : php (SSA:2009-098-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : ruby (SSA:2009-120-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : ruby (SSA:2009-170-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : seamonkey (SSA:2008-362-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : seamonkey (SSA:2009-083-02)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : seamonkey (SSA:2009-103-01)

Slackware 11.0 / 12.0 / 12.1 / 12.2 / current : seamonkey (SSA:2009-176-01)

Slackware 11.0 / 12.0 / 12.1 / current : amarok (SSA:2008-241-01)

Slackware 11.0 / 12.0 / 12.1 / current : links (SSA:2008-210-04)

Slackware 11.0 / 12.0 / 12.1 / current : openssl (SSA:2008-210-08)

Slackware 11.0 / 12.0 / 12.1 / current : rdesktop (SSA:2008-148-01)

Slackware 11.0 / 12.0 / 12.1 / current : ruby (SSA:2008-179-01)

Slackware 11.0 / 12.0 / 12.1 / current : seamonkey (SSA:2008-191-03)

Slackware 11.0 / 12.0 / 12.1 / current : seamonkey (SSA:2008-198-02)

Slackware 11.0 / 12.0 / 12.1 / current : seamonkey (SSA:2008-269-02)

Slackware 11.0 / 12.0 / 12.1 / current : seamonkey (SSA:2008-320-04)

Slackware 11.0 / 12.0 / 12.1 / current : vim (SSA:2008-210-10)

Slackware 11.0 / 12.0 / 12.1 : ruby (SSA:2008-334-01)

Slackware 11.0 / 12.0 / 12.1 : seamonkey (SSA:2010-090-03)

Slackware 11.0 / 12.0 / current : cairo (SSA:2007-337-01)

Slackware 11.0 / 12.0 / current : espgs/ghostscript (SSA:2008-062-01)

Slackware 11.0 / 12.0 / current : mysql (SSA:2007-348-01)

Slackware 11.0 / 12.0 / current : seamonkey (SSA:2007-333-01)

Slackware 11.0 / 12.0 / current : seamonkey (SSA:2008-089-02)

Slackware 11.0 / 12.0 : firefox (SSA:2007-200-01)

Slackware 11.0 / 12.0 : firefox (SSA:2007-213-01)

Slackware 11.0 / 12.0 : seamonkey (SSA:2007-205-02)

Slackware 11.0 / 12.0 : seamonkey (SSA:2007-222-04)

Slackware 11.0 / 12.0 : thunderbird (SSA:2007-205-01)

Slackware 11.0 / 12.0 : thunderbird (SSA:2007-215-01)

Slackware 11.0 / current : gd (SSA:2007-178-01)

Slackware 11.0 / current : ktorrent (SSA:2007-093-02)

Slackware 11.0 : imagemagick (SSA:2007-066-06)

Slackware 11.0 : php for Slackware 11.0 reissued (SSA:2007-314-02)

Slackware 11.0 : seamonkey (SSA:2006-357-03)

Slackware 11.0 : seamonkey (SSA:2007-066-05)

Slackware 11.0 : Slackware 11.0 x11-6.9.0 patch fix (SSA:2007-110-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : bind (SSA:2012-209-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : httpd (SSA:2011-133-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : httpd (SSA:2011-145-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : httpd (SSA:2011-252-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : httpd (SSA:2011-284-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : httpd (SSA:2012-041-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : php (SSA:2012-041-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : php (SSA:2012-195-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : php (SSA:2012-204-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : cups (SSA:2010-333-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : glibc (SSA:2010-295-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : glibc (SSA:2010-301-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : gnupg2 (SSA:2010-240-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : httpd (SSA:2010-240-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : httpd (SSA:2011-041-03)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : pidgin (SSA:2010-240-05)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : pidgin (SSA:2010-305-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : pidgin (SSA:2010-361-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : pidgin (SSA:2011-055-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : pidgin (SSA:2011-070-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : poppler (SSA:2010-324-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : subversion (SSA:2011-070-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : xorg-server (SSA:2010-240-06)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / 13.1 / current : xrdb (SSA:2011-096-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : httpd (SSA:2010-024-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : httpd (SSA:2010-067-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : php (SSA:2009-276-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : pidgin (SSA:2009-290-02)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : pidgin (SSA:2010-024-03)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : pidgin (SSA:2010-069-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : pidgin (SSA:2010-138-01)

Slackware 12.0 / 12.1 / 12.2 / 13.0 / current : poppler (SSA:2009-302-02)

Slackware 12.0 / 12.1 / 12.2 / current : cups (SSA:2009-116-01)

Slackware 12.0 / 12.1 / 12.2 / current : git (SSA:2009-051-02)

Slackware 12.0 / 12.1 / 12.2 / current : glib2 (SSA:2009-086-02)

Slackware 12.0 / 12.1 / 12.2 / current : gnutls (SSA:2009-128-01)

Slackware 12.0 / 12.1 / 12.2 / current : httpd (SSA:2009-214-01)

Slackware 12.0 / 12.1 / 12.2 / current : pidgin (SSA:2009-146-01)

Slackware 12.0 / 12.1 / 12.2 / current : pidgin (SSA:2009-231-02)

Slackware 12.0 / 12.1 / 12.2 / current : subversion (SSA:2009-219-01)

Slackware 12.0 / 12.1 / 12.2 / current : xine-lib (SSA:2009-098-03)

Slackware 12.0 / 12.1 / 12.2 / current : xterm (SSA:2009-069-03)

Slackware 12.0 / 12.1 / current : cups (SSA:2008-312-01)

Slackware 12.0 / 12.1 / current : gnutls (SSA:2008-180-01)

Slackware 12.0 / 12.1 / current : gnutls (SSA:2008-315-01)

Slackware 12.0 / 12.1 / current : gnutls (SSA:2008-320-01)

Slackware 12.0 / 12.1 / current : httpd (SSA:2008-210-02)

Slackware 12.0 / 12.1 / current : libxslt (SSA:2008-210-03)

Slackware 12.0 / 12.1 / current : mtr (SSA:2008-210-06)

Slackware 12.0 / 12.1 / current : net-snmp (SSA:2008-210-07)

Slackware 12.0 / 12.1 / current : net-snmp (SSA:2008-320-02)

Slackware 12.0 / 12.1 / current : pan (SSA:2008-217-02)

Slackware 12.0 / 12.1 / current : pcre (SSA:2008-210-09)

Slackware 12.0 / 12.1 / current : php (SSA:2008-339-01)

Slackware 12.0 / current : cups (SSA:2008-094-01)

Slackware 12.0 / current : httpd (SSA:2008-045-01)

Slackware 12.0 / current : kdelibs (SSA:2008-116-01)

Slackware 12.0 / current : kernel exploit fix (SSA:2008-042-01)

Slackware 12.0 : kdebase, kdelibs (SSA:2007-264-01)

Slackware 12.0 : pidgin (SSA:2007-275-01)

Slackware 12.0 : poppler (SSA:2007-222-02)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : bind (SSA:2012-284-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : bind (SSA:2012-341-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : bind (SSA:2013-086-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : bind (SSA:2013-218-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : curl (SSA:2013-174-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : dhcp (SSA:2013-086-02)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : freetype (SSA:2013-015-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : gnupg (SSA:2013-287-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : gnupg / libgcrypt (SSA:2013-215-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : hplip (SSA:2013-233-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : httpd (SSA:2013-062-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : httpd (SSA:2013-218-02)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : libtiff (SSA:2013-290-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : libxml2 (SSA:2012-341-03)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : mysql (SSA:2013-022-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : openssl (SSA:2013-040-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : php (SSA:2013-081-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : php (SSA:2013-161-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : php (SSA:2013-197-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : sudo (SSA:2013-065-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : xorg-server (SSA:2013-287-05)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : xpdf (SSA:2013-233-02)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : bind (SSA:2012-257-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : dhcp (SSA:2012-237-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : dhcp (SSA:2012-258-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : patch (SSA:2012-257-02)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : slocate (SSA:2012-244-05)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 / current : t1lib (SSA:2012-228-01)

Slackware 12.1 / 12.2 / 13.0 / 13.1 / 13.37 : gnutls (SSA:2013-287-03)

Slackware 12.1 / 12.2 / 13.0 / current : gimp (SSA:2009-345-01)

Slackware 12.1 / 12.2 / 13.0 / current : gnutls (SSA:2009-290-01)

Slackware 12.1 / 12.2 / current : ghostscript (SSA:2009-181-01)

Slackware 12.1 / current : xorg-server (SSA:2008-183-01)

Slackware 12.2 / 13.0 / 13.1 / 13.37 / 14.0 / current : pidgin (SSA:2013-044-01)

Slackware 12.2 / 13.0 / 13.1 / 13.37 / current : pidgin (SSA:2011-178-01)

Slackware 12.2 / 13.0 / 13.1 / 13.37 / current : pidgin (SSA:2012-195-02)

Slackware 12.2 / 13.0 / 13.1 / current : mozilla-firefox (SSA:2010-202-01)

Slackware 12.2 / 13.0 / 13.1 / current : mozilla-firefox (SSA:2010-253-01)

Slackware 12.2 / 13.0 / 13.1 / current : seamonkey (SSA:2010-176-03)

Slackware 12.2 / 13.0 / 13.1 / current : seamonkey (SSA:2010-202-03)

Slackware 12.2 / 13.0 / 13.1 / current : seamonkey (SSA:2010-253-03)

Slackware 12.2 / 13.0 / 13.1 / current : seamonkey (SSA:2010-300-01)

Slackware 12.2 / 13.0 / 13.1 / current : seamonkey (SSA:2010-305-01)

Slackware 12.2 / 13.0 / 13.1 / current : seamonkey (SSA:2011-068-01)

Slackware 12.2 / 13.0 / 13.1 / current : seamonkey (SSA:2011-086-01)

Slackware 12.2 / 13.0 / 13.1 : seamonkey (SSA:2010-344-01)

Slackware 12.2 / 13.0 / 13.1 : seamonkey (SSA:2011-122-03)

Slackware 12.2 / 13.0 / current : mozilla-firefox (SSA:2009-257-01)

Slackware 12.2 / 13.0 / current : mozilla-firefox (SSA:2009-306-01)

Slackware 12.2 / 13.0 / current : mozilla-firefox (SSA:2009-351-01)

Slackware 12.2 / 13.0 / current : mozilla-firefox (SSA:2010-095-02)

Slackware 12.2 / 13.0 / current : seamonkey (SSA:2009-352-01)

Slackware 12.2 / 13.0 / current : seamonkey (SSA:2010-095-03)

Slackware 12.2 / current : kernel (SSA:2009-230-01)

Slackware 12.2 / current : mozilla-firefox (SSA:2009-036-01)

Slackware 12.2 / current : mozilla-firefox (SSA:2009-069-02)

Slackware 12.2 / current : mozilla-firefox (SSA:2009-086-01)

Slackware 12.2 / current : mozilla-firefox (SSA:2009-112-01)

Slackware 12.2 / current : mozilla-firefox (SSA:2009-118-01)

Slackware 12.2 / current : mozilla-firefox (SSA:2009-167-01)

Slackware 12.2 / current : samba (SSA:2009-005-01)

Slackware 12.2 / current : udev reissued for 12.2/current (SSA:2009-111-02)

Slackware 12.2 / current : wicd (SSA:2009-040-01)

Slackware 12.2 / current : xdg-utils (SSA:2009-033-01)

Slackware 12.2 : kernel [updated] (SSA:2009-231-01)

Slackware 12.2 : mozilla-firefox (Slackware 12.2) (SSA:2010-065-01)

Slackware 12.2 : mozilla-firefox (SSA:2009-209-01)

Slackware 12.2 : mozilla-firefox (SSA:2009-215-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2016-204-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2016-271-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2016-308-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2017-011-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2017-041-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2017-103-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2017-165-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2017-180-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bind (SSA:2018-017-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : curl (SSA:2016-219-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : curl (SSA:2016-259-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : curl (SSA:2016-308-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : curl (SSA:2017-221-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : dhcp (SSA:2018-060-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : dnsmasq (SSA:2017-275-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : emacs (SSA:2017-255-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : expat (SSA:2016-359-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : expat (SSA:2017-199-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : freetype (SSA:2017-136-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : git (SSA:2017-223-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : git (SSA:2018-152-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : gnupg (SSA:2016-236-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : gnupg (SSA:2017-213-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : gnupg (SSA:2018-170-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : httpd (SSA:2017-180-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : httpd (SSA:2017-194-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : httpd (SSA:2017-261-01) (Optionsbleed)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : irssi (SSA:2016-265-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : irssi (SSA:2017-011-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : irssi (SSA:2017-158-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : libgcrypt (SSA:2016-236-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : libidn (SSA:2016-210-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : libidn (SSA:2018-091-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : libpng (SSA:2016-365-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : libwmf (SSA:2018-120-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : libXcursor (SSA:2017-333-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : minicom (SSA:2017-108-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : mozilla-firefox (SSA:2017-165-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : ntp (SSA:2016-326-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : ntp (SSA:2017-112-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : openssh (SSA:2016-219-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : openssh (SSA:2016-358-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : openssh (SSA:2018-067-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : openssl (SSA:2017-342-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : openvpn (SSA:2017-172-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : openvpn (SSA:2018-116-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : patch (SSA:2018-096-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : pidgin (SSA:2016-265-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : pidgin (SSA:2017-074-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : proftpd (SSA:2017-112-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : rsync (SSA:2018-032-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : rxvt (SSA:2017-121-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : stunnel (SSA:2016-219-04)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : sudo (SSA:2017-150-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : wget (SSA:2017-300-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : wget (SSA:2018-129-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : x11 (SSA:2016-305-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : xorg-server (SSA:2017-227-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / 14.2 : libXfont (SSA:2017-333-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bash (SSA:2014-267-01) (Shellshock)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bash (SSA:2014-268-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bash (SSA:2014-272-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2014-028-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2014-175-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2014-344-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2015-111-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2015-188-04)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2015-209-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2015-245-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2015-349-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2016-054-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : bind (SSA:2016-069-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : cups (SSA:2015-188-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : curl (SSA:2014-044-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : curl (SSA:2014-086-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : curl (SSA:2015-302-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : curl (SSA:2016-039-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : curl (SSA:2016-141-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : dhcp (SSA:2016-012-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : freetype (SSA:2015-016-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : git (SSA:2016-075-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : git (SSA:2016-078-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : glibc (SSA:2015-028-01) (GHOST)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : gnupg (SSA:2013-354-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : gnupg (SSA:2014-175-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : gnupg (SSA:2015-111-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : gnutls (SSA:2014-062-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : gnutls (SSA:2014-156-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : httpd (SSA:2014-204-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : httpd (SSA:2015-111-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : jasper (SSA:2015-302-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : libgcrypt (SSA:2016-054-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : libjpeg (SSA:2013-350-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : libpng (SSA:2015-337-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : libpng (SSA:2015-349-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : libpng (SSA:2015-351-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : libXfont (SSA:2014-013-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : mailx (SSA:2016-062-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : mariadb, mysql (SSA:2014-050-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : mercurial (SSA:2016-092-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : mercurial (SSA:2016-123-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : MPlayer (SSA:2016-034-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2014-044-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2014-356-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2015-111-08)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2015-188-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2015-302-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2016-054-04)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2016-120-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ntp (SSA:2016-155-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssh (SSA:2014-086-06)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssh (SSA:2014-293-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssh (SSA:2016-014-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssh (SSA:2016-070-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2014-156-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2014-220-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2014-288-01) (POODLE)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2015-009-01) (FREAK)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2015-111-09)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2015-162-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2015-349-04)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openssl (SSA:2016-062-02) (DROWN)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : openvpn (SSA:2014-344-04)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : patch (SSA:2015-047-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : php (SSA:2014-160-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : php (SSA:2014-247-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : pidgin (SSA:2014-034-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : pidgin (SSA:2014-296-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : pidgin (SSA:2014-344-05)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : ppp (SSA:2015-111-11)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : proftpd (SSA:2015-111-12)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : sendmail (SSA:2014-156-04)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : sudo (SSA:2015-047-03)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : wget (SSA:2014-302-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 / current : wget (SSA:2016-165-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / 14.1 : pidgin (SSA:2016-266-02)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / current : glibc (SSA:2013-260-01)

Slackware 13.0 / 13.1 / 13.37 / 14.0 / current : subversion (SSA:2013-095-01)

Slackware 13.0 / 13.1 / 13.37 / current : dhcpcd (SSA:2011-210-02)

Slackware 13.0 / 13.1 / 13.37 / current : mozilla-firefox (SSA:2011-122-01)

Slackware 13.0 / 13.1 / 13.37 / current : mozilla-firefox (SSA:2011-174-01)

Slackware 13.0 / 13.1 / 13.37 / current : mozilla-firefox (SSA:2011-249-01)

Slackware 13.0 / 13.1 / 13.37 / current : mozilla-thunderbird (SSA:2011-122-02)

Slackware 13.0 / 13.1 / 13.37 / current : mozilla-thunderbird (SSA:2011-189-02)

Slackware 13.0 / 13.1 / 13.37 / current : mozilla-thunderbird (SSA:2011-249-02)

Slackware 13.0 / 13.1 / 13.37 : sudo (SSA:2014-064-01)

Slackware 13.0 / 13.1 / current : mozilla-firefox (SSA:2010-176-02)

Slackware 13.0 / 13.1 / current : mozilla-firefox (SSA:2010-204-01)

Slackware 13.0 / 13.1 / current : mozilla-firefox (SSA:2010-295-02)

Slackware 13.0 / 13.1 / current : mozilla-firefox (SSA:2010-301-02)

Slackware 13.0 / 13.1 / current : mozilla-firefox (SSA:2010-343-01)

Slackware 13.0 / 13.1 / current : mozilla-firefox (SSA:2011-060-01)

Slackware 13.0 / 13.1 / current : mozilla-firefox (SSA:2011-068-02)

Slackware 13.0 / 13.1 / current : mozilla-thunderbird (SSA:2010-317-01)

Slackware 13.0 / 13.1 / current : mozilla-thunderbird (SSA:2010-343-02)

Slackware 13.0 / 13.1 : mozilla-firefox (SSA:2011-086-02)

Slackware 13.0 / 13.1 : mozilla-firefox (SSA:2011-195-02)

Slackware 13.0 / current : gzip (SSA:2010-060-03)

Slackware 13.0 / current : kdebase-workspace (SSA:2010-110-02)

Slackware 13.0 / current : mozilla-firefox (SSA:2010-090-02)

Slackware 13.0 : bash (rebuild for Slackware 13.0 only) (SSA:2014-268-02)

Slackware 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : bluez (SSA:2017-258-01) (BlueBorne)

Slackware 13.1 / 13.37 / 14.0 / 14.1 / 14.2 / current : samba (SSA:2017-144-01) (SambaCry)

Slackware 13.1 / 13.37 / 14.0 / 14.1 / 14.2 : bash (SSA:2017-251-01)

Slackware 13.1 / 13.37 / 14.0 / 14.1 / current : dhcpcd (SSA:2014-213-02)

Slackware 13.1 / 13.37 / 14.0 / 14.1 / current : libiodbc (SSA:2013-350-01)

Slackware 13.1 / 13.37 / 14.0 / 14.1 / current : libyaml (SSA:2014-111-01)

Slackware 13.1 / 13.37 / 14.0 / 14.1 / current : ruby (SSA:2013-350-06)

Slackware 13.1 / 13.37 / 14.0 / current : hplip (SSA:2013-291-01)

Slackware 13.1 / 13.37 / 14.0 / current : perl (SSA:2013-072-01)

Slackware 13.1 / 13.37 / 14.0 / current : ruby (SSA:2012-341-04)

Slackware 13.1 / 13.37 / 14.0 / current : ruby (SSA:2013-075-01)

Slackware 13.1 / 13.37 / 14.0 / current : ruby (SSA:2013-136-02)

Slackware 13.1 / 13.37 / 14.0 / current : ruby (SSA:2013-178-01)

Slackware 13.1 / 13.37 / 14.0 / current : samba (SSA:2013-218-03)

Slackware 13.1 / 13.37 / current : emacs (SSA:2012-228-02)

Slackware 13.1 / 13.37 / current : glibc (SSA:2012-041-03)

Slackware 13.1 / 13.37 / current : glibc (SSA:2012-244-01)

Slackware 13.1 / 13.37 / current : samba (SSA:2011-210-03)

Slackware 13.1 / current : cups (SSA:2010-176-05)

Slackware 13.1 / current : mozilla-thunderbird (SSA:2010-176-04)

Slackware 13.1 / current : mozilla-thunderbird (SSA:2010-202-02)

Slackware 13.1 / current : mozilla-thunderbird (SSA:2010-253-02)

Slackware 13.1 / current : mozilla-thunderbird (SSA:2010-295-03)

Slackware 13.1 / current : polkit (SSA:2011-109-01)

Slackware 13.1 / current : shadow (SSA:2011-086-03)

Slackware 13.1 / current : shadow (SSA:2011-101-01)

Slackware 13.1 : kdegraphics (SSA:2010-240-03)

Slackware 13.1 : kdelibs (SSA:2011-101-02)

Slackware 13.37 / 14.0 / 14.1 / 14.2 / current : gnupg2 (SSA:2018-159-01)

Slackware 13.37 / 14.0 / 14.1 / 14.2 / current : kdelibs (SSA:2017-136-02)

Slackware 13.37 / 14.0 / 14.1 / 14.2 / current : libvorbis (SSA:2018-076-01)

Slackware 13.37 / 14.0 / 14.1 / 14.2 / current : tcpdump (SSA:2017-041-04)

Slackware 13.37 / 14.0 / 14.1 / 14.2 / current : tcpdump (SSA:2017-205-01)

Slackware 13.37 / 14.0 / 14.1 / 14.2 / current : tcpdump (SSA:2017-251-03)

Slackware 13.37 / 14.0 / 14.1 / current : blueman (SSA:2015-356-01)

Slackware 13.37 / 14.0 / 14.1 / current : gdk-pixbuf2 (SSA:2015-244-01)

Slackware 13.37 / 14.0 / 14.1 / current : gnupg2 (SSA:2014-175-03)

Slackware 13.37 / 14.0 / 14.1 / current : libsndfile (SSA:2016-039-02)

Slackware 13.37 / 14.0 / 14.1 / current : mozilla-firefox (SSA:2013-322-01)

Slackware 13.37 / 14.0 / 14.1 / current : mozilla-thunderbird (SSA:2013-339-02)

Slackware 13.37 / 14.0 / 14.1 / current : mutt (SSA:2014-071-01)

Slackware 13.37 / 14.0 / 14.1 / current : mutt (SSA:2015-111-07)

Slackware 13.37 / 14.0 / 14.1 / current : wpa\_supplicant (SSA:2014-344-07)

Slackware 13.37 / 14.0 / current : gnupg2 (SSA:2013-287-02)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2012-283-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2012-285-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2012-300-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2012-326-02)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-009-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-050-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-068-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-093-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-135-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-180-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-219-01)

Slackware 13.37 / 14.0 / current : mozilla-firefox (SSA:2013-260-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2012-285-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2012-304-01)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2012-326-03)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-009-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-050-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-068-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-093-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-135-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-180-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-219-02)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-260-03)

Slackware 13.37 / 14.0 / current : mozilla-thunderbird (SSA:2013-307-01)

Slackware 13.37 / 14.0 / current : seamonkey (SSA:2012-288-01)

Slackware 13.37 / 14.0 / current : seamonkey (SSA:2012-304-02)

Slackware 13.37 / 14.0 / current : seamonkey (SSA:2012-326-01)

Slackware 13.37 / 14.0 / current : seamonkey (SSA:2013-009-03)

Slackware 13.37 / 14.0 / current : seamonkey (SSA:2013-056-01)

Slackware 13.37 / 14.0 / current : seamonkey (SSA:2013-072-02)

Slackware 13.37 / 14.0 / current : seamonkey (SSA:2013-097-01)

Slackware 13.37 / 14.0 / current : xorg-server (SSA:2013-109-01)

Slackware 13.37 / 14.0 : kernel (SSA:2013-140-01)

Slackware 13.37 / 14.0 : libgpg-error (SSA:2013-287-04)

Slackware 13.37 / 14.0 : mozilla-thunderbird x86\_64 packages (SSA:2013-136-01)

Slackware 13.37 / current : bind (SSA:2011-189-01)

Slackware 13.37 / current : mozilla-firefox (SSA:2012-166-02)

Slackware 13.37 / current : mozilla-firefox (SSA:2012-200-02)

Slackware 13.37 / current : mozilla-firefox (SSA:2012-244-02)

Slackware 13.37 / current : mozilla-thunderbird (SSA:2012-166-03)

Slackware 13.37 / current : mozilla-thunderbird (SSA:2012-200-03)

Slackware 13.37 / current : mozilla-thunderbird (SSA:2012-244-03)

Slackware 13.37 / current : seamonkey (SSA:2011-195-01)

Slackware 13.37 / current : seamonkey (SSA:2011-249-03)

Slackware 13.37 / current : seamonkey (SSA:2012-166-04)

Slackware 13.37 / current : seamonkey (SSA:2012-200-04)

Slackware 13.37 / current : seamonkey (SSA:2012-244-04)

Slackware 14.0 / 14.1 / 14.2 / current : bind (SSA:2018-192-01)

Slackware 14.0 / 14.1 / 14.2 / current : bind (SSA:2018-222-01)

Slackware 14.0 / 14.1 / 14.2 / current : bind (SSA:2019-116-01)

Slackware 14.0 / 14.1 / 14.2 / current : bind (SSA:2019-171-01)

Slackware 14.0 / 14.1 / 14.2 / current : bind (SSA:2019-324-01)

Slackware 14.0 / 14.1 / 14.2 / current : bind (SSA:2020-106-01)

Slackware 14.0 / 14.1 / 14.2 / current : bzip2 (SSA:2019-195-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2017-279-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2017-297-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2017-333-03)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2018-024-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2018-074-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2018-136-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2018-192-02)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2018-249-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2018-304-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2019-037-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2019-142-01)

Slackware 14.0 / 14.1 / 14.2 / current : curl (SSA:2019-254-01)

Slackware 14.0 / 14.1 / 14.2 / current : expat (SSA:2019-259-01)

Slackware 14.0 / 14.1 / 14.2 / current : file (SSA:2018-212-01)

Slackware 14.0 / 14.1 / 14.2 / current : file (SSA:2019-054-01)

Slackware 14.0 / 14.1 / 14.2 / current : gegl (SSA:2017-270-01)

Slackware 14.0 / 14.1 / 14.2 / current : gimp (SSA:2016-203-01)

Slackware 14.0 / 14.1 / 14.2 / current : git (SSA:2018-283-01)

Slackware 14.0 / 14.1 / 14.2 / current : git (SSA:2020-105-01)

Slackware 14.0 / 14.1 / 14.2 / current : gnutls (SSA:2016-254-01)

Slackware 14.0 / 14.1 / 14.2 / current : gnutls (SSA:2017-011-02)

Slackware 14.0 / 14.1 / 14.2 / current : httpd (SSA:2016-358-01) (httpoxy)

Slackware 14.0 / 14.1 / 14.2 / current : httpd (SSA:2018-199-01)

Slackware 14.0 / 14.1 / 14.2 / current : httpd (SSA:2019-022-01)

Slackware 14.0 / 14.1 / 14.2 / current : httpd (SSA:2019-096-01)

Slackware 14.0 / 14.1 / 14.2 / current : httpd (SSA:2020-091-02) (Internal Data Buffering)

Slackware 14.0 / 14.1 / 14.2 / current : infozip (SSA:2019-060-01)

Slackware 14.0 / 14.1 / 14.2 / current : irssi (SSA:2017-190-01)

Slackware 14.0 / 14.1 / 14.2 / current : irssi (SSA:2017-298-01)

Slackware 14.0 / 14.1 / 14.2 / current : irssi (SSA:2018-008-01)

Slackware 14.0 / 14.1 / 14.2 / current : irssi (SSA:2018-046-01)

Slackware 14.0 / 14.1 / 14.2 / current : irssi (SSA:2019-011-01)

Slackware 14.0 / 14.1 / 14.2 / current : irssi (SSA:2019-180-01)

Slackware 14.0 / 14.1 / 14.2 / current : kernel (SSA:2016-305-01) (Dirty COW)

Slackware 14.0 / 14.1 / 14.2 / current : lftp (SSA:2018-214-01)

Slackware 14.0 / 14.1 / 14.2 / current : libssh (SSA:2018-289-01)

Slackware 14.0 / 14.1 / 14.2 / current : libX11 (SSA:2018-233-01)

Slackware 14.0 / 14.1 / 14.2 / current : libxml2 (SSA:2017-266-01)

Slackware 14.0 / 14.1 / 14.2 / current : mariadb / mysql (SSA:2016-257-01)

Slackware 14.0 / 14.1 / 14.2 / current : mcabber (SSA:2016-347-02)

Slackware 14.0 / 14.1 / 14.2 / current : mcabber (SSA:2017-082-01)

Slackware 14.0 / 14.1 / 14.2 / current : mercurial (SSA:2017-223-03)

Slackware 14.0 / 14.1 / 14.2 / current : mozilla-nss (SSA:2018-337-01)

Slackware 14.0 / 14.1 / 14.2 / current : mutt (SSA:2018-198-01)

Slackware 14.0 / 14.1 / 14.2 / current : netatalk (SSA:2018-355-01)

Slackware 14.0 / 14.1 / 14.2 / current : ntp (SSA:2018-060-02)

Slackware 14.0 / 14.1 / 14.2 / current : ntp (SSA:2018-229-01)

Slackware 14.0 / 14.1 / 14.2 / current : ntp (SSA:2019-067-01)

Slackware 14.0 / 14.1 / 14.2 / current : openssl (SSA:2016-266-01)

Slackware 14.0 / 14.1 / 14.2 / current : openssl (SSA:2018-325-01)

Slackware 14.0 / 14.1 / 14.2 / current : openvpn (SSA:2020-107-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2016-203-02) (httpoxy)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2016-252-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2016-267-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2016-305-04)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2016-347-03)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2017-041-03)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2017-188-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2017-300-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2018-034-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2018-067-02)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2018-090-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2018-201-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2018-257-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2018-341-01)

Slackware 14.0 / 14.1 / 14.2 / current : php (SSA:2019-038-01)

Slackware 14.0 / 14.1 / 14.2 / current : ppp (SSA:2020-064-01)

Slackware 14.0 / 14.1 / 14.2 / current : proftpd (SSA:2020-051-01)

Slackware 14.0 / 14.1 / 14.2 / current : python (SSA:2016-363-01) (httpoxy)

Slackware 14.0 / 14.1 / 14.2 / current : python (SSA:2017-266-02)

Slackware 14.0 / 14.1 / 14.2 / current : python (SSA:2018-124-01)

Slackware 14.0 / 14.1 / 14.2 / current : python (SSA:2019-062-01)

Slackware 14.0 / 14.1 / 14.2 / current : python (SSA:2019-293-01)

Slackware 14.0 / 14.1 / 14.2 / current : rdesktop (SSA:2019-135-01)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2016-189-01)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2017-082-02)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2017-091-01)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2017-195-02) (Orpheus' Lyre)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2017-263-01)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2017-332-01)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2018-072-02)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2018-229-02)

Slackware 14.0 / 14.1 / 14.2 / current : samba (SSA:2018-333-01)

Slackware 14.0 / 14.1 / 14.2 / current : seamonkey (SSA:2018-212-02)

Slackware 14.0 / 14.1 / 14.2 / current : subversion (SSA:2017-223-04)

Slackware 14.0 / 14.1 / 14.2 / current : sudo (SSA:2019-287-01)

Slackware 14.0 / 14.1 / 14.2 / current : sudo (SSA:2020-031-01)

Slackware 14.0 / 14.1 / 14.2 / current : tcpdump (SSA:2019-274-01)

Slackware 14.0 / 14.1 / 14.2 / current : wavpack (SSA:2019-353-01)

Slackware 14.0 / 14.1 / 14.2 / current : wpa\_supplicant (SSA:2017-291-02) (KRACK)

Slackware 14.0 / 14.1 / 14.2 / current : xorg-server (SSA:2017-279-03)

Slackware 14.0 / 14.1 / 14.2 / current : xorg-server (SSA:2017-291-03)

Slackware 14.0 / 14.1 / 14.2 : php (SSA:2018-136-02)

Slackware 14.0 / 14.1 / 14.2 : zsh (SSA:2019-013-01)

Slackware 14.0 / 14.1 / current : gnutls (SSA:2014-050-01)

Slackware 14.0 / 14.1 / current : gnutls (SSA:2015-233-01)

Slackware 14.0 / 14.1 / current : httpd (SSA:2014-086-02)

Slackware 14.0 / 14.1 / current : httpd (SSA:2015-198-01)

Slackware 14.0 / 14.1 / current : imagemagick (SSA:2016-152-01)

Slackware 14.0 / 14.1 / current : libssh (SSA:2015-111-04)

Slackware 14.0 / 14.1 / current : libssh (SSA:2016-057-01)

Slackware 14.0 / 14.1 / current : libtasn1 (SSA:2014-156-02)

Slackware 14.0 / 14.1 / current : libxml2 (SSA:2016-148-01)

Slackware 14.0 / 14.1 / current : libxslt (SSA:2016-148-02)

Slackware 14.0 / 14.1 / current : llvm (SSA:2013-350-03)

Slackware 14.0 / 14.1 / current : mozilla-nss (SSA:2013-339-01)

Slackware 14.0 / 14.1 / current : mozilla-nss (SSA:2014-028-02)

Slackware 14.0 / 14.1 / current : mozilla-nss (SSA:2014-086-04)

Slackware 14.0 / 14.1 / current : mozilla-nss (SSA:2014-267-02)

Slackware 14.0 / 14.1 / current : mozilla-nss (SSA:2015-219-02)

Slackware 14.0 / 14.1 / current : mozilla-nss (SSA:2015-310-02)

Slackware 14.0 / 14.1 / current : mozilla-nss (SSA:2016-069-02)

Slackware 14.0 / 14.1 / current : mozilla-thunderbird (SSA:2016-132-01) (ImageTragick)

Slackware 14.0 / 14.1 / current : openssh (SSA:2014-344-03)

Slackware 14.0 / 14.1 / current : openssl (SSA:2014-013-02)

Slackware 14.0 / 14.1 / current : openssl (SSA:2014-098-01)

Slackware 14.0 / 14.1 / current : openssl (SSA:2015-190-01)

Slackware 14.0 / 14.1 / current : openssl (SSA:2016-034-03)

Slackware 14.0 / 14.1 / current : openssl (SSA:2016-124-01)

Slackware 14.0 / 14.1 / current : php (SSA:2014-013-03)

Slackware 14.0 / 14.1 / current : php (SSA:2014-074-01)

Slackware 14.0 / 14.1 / current : php (SSA:2014-111-02)

Slackware 14.0 / 14.1 / current : php (SSA:2014-192-01)

Slackware 14.0 / 14.1 / current : php (SSA:2014-307-03)

Slackware 14.0 / 14.1 / current : php (SSA:2014-356-02)

Slackware 14.0 / 14.1 / current : php (SSA:2015-111-10)

Slackware 14.0 / 14.1 / current : php (SSA:2015-162-02)

Slackware 14.0 / 14.1 / current : php (SSA:2015-198-02) (BACKRONYM)

Slackware 14.0 / 14.1 / current : php (SSA:2015-274-02)

Slackware 14.0 / 14.1 / current : php (SSA:2016-034-04)

Slackware 14.0 / 14.1 / current : php (SSA:2016-062-03)

Slackware 14.0 / 14.1 / current : php (SSA:2016-067-01)

Slackware 14.0 / 14.1 / current : php (SSA:2016-092-02)

Slackware 14.0 / 14.1 / current : php (SSA:2016-120-02)

Slackware 14.0 / 14.1 / current : php (SSA:2016-148-03)

Slackware 14.0 / 14.1 / current : php (SSA:2016-176-01)

Slackware 14.0 / 14.1 / current : samba (SSA:2013-322-03)

Slackware 14.0 / 14.1 / current : samba (SSA:2014-072-01)

Slackware 14.0 / 14.1 / current : samba (SSA:2014-175-04)

Slackware 14.0 / 14.1 / current : samba (SSA:2016-106-02) (Badlock)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2013-322-04)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2013-339-03)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2013-350-07)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-039-03)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-086-07)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-131-01)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-175-05)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-252-01)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-271-03)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-307-04)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2014-344-06)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2015-016-04)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2015-047-02)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2015-111-14)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2015-246-01)

Slackware 14.0 / 14.1 / current : seamonkey (SSA:2015-274-03)

Slackware 14.0 / 14.1 / current : subversion (SSA:2014-058-01)

Slackware 14.0 / 14.1 / current : subversion (SSA:2016-097-01)

Slackware 14.0 / 14.1 / current : subversion (SSA:2016-121-01)

Slackware 14.0 / 14.1 / current : udisks, udisks2 (SSA:2014-070-01)

Slackware 14.0 / 14.1 / current : wpa\_supplicant (SSA:2015-132-03)

Slackware 14.0 / 14.1 : vim (SSA:2017-100-01)

Slackware 14.0 / 14.2 / current : kernel (SSA:2018-016-01) (Meltdown) (Spectre)

Slackware 14.0 / current : curl (SSA:2013-038-01)

Slackware 14.0 / current : dbus (SSA:2013-191-01)

Slackware 14.0 / current : gnutls (SSA:2013-242-01)

Slackware 14.0 / current : gnutls (SSA:2013-242-03)

Slackware 14.0 / current : libssh (SSA:2012-341-02)

Slackware 14.0 / current : libssh (SSA:2013-087-01)

Slackware 14.0 / current : openssl (SSA:2013-042-01)

Slackware 14.0 / current : php (SSA:2013-242-02)

Slackware 14.0 / current : poppler (SSA:2013-233-03)

Slackware 14.0 / current : seamonkey (SSA:2013-219-03)

Slackware 14.0 / current : seamonkey (SSA:2013-271-01)

Slackware 14.0 / current : subversion (SSA:2013-251-01)

Slackware 14.0 : hplip (SSA:2013-339-04)

Slackware 14.0 : mysql (SSA:2015-132-02)

Slackware 14.0 : Slackware 14.0 kernel (SSA:2017-184-01) (Stack Clash)

Slackware 14.1 / 14.2 / current : gtk+2 (SSA:2016-254-02)

Slackware 14.1 / 14.2 / current : kernel (SSA:2017-258-02) (BlueBorne)

Slackware 14.1 / 14.2 / current : libarchive (SSA:2020-043-01)

Slackware 14.1 / 14.2 / current : libsoup (SSA:2017-223-02)

Slackware 14.1 / 14.2 / current : libXres (SSA:2017-291-01)

Slackware 14.1 / 14.2 / current : mariadb (SSA:2016-305-03)

Slackware 14.1 / 14.2 / current : mariadb (SSA:2017-018-01)

Slackware 14.1 / 14.2 / current : mariadb (SSA:2017-195-01)

Slackware 14.1 / 14.2 / current : mariadb (SSA:2017-306-01)

Slackware 14.1 / 14.2 / current : mariadb (SSA:2018-309-01)

Slackware 14.1 / 14.2 / current : mozilla-firefox (SSA:2016-265-02)

Slackware 14.1 / 14.2 / current : mozilla-firefox (SSA:2016-323-01)

Slackware 14.1 / 14.2 / current : mozilla-firefox (SSA:2016-336-01)

Slackware 14.1 / 14.2 / current : mozilla-firefox (SSA:2016-348-01)

Slackware 14.1 / 14.2 / current : mozilla-firefox (SSA:2017-023-01)

Slackware 14.1 / 14.2 / current : mozilla-firefox (SSA:2017-066-01)

Slackware 14.1 / 14.2 / current : mozilla-thunderbird (SSA:2016-187-01)

Slackware 14.1 / 14.2 / current : mozilla-thunderbird (SSA:2016-244-01)

Slackware 14.1 / 14.2 / current : mozilla-thunderbird (SSA:2016-275-01)

Slackware 14.1 / 14.2 / current : mozilla-thunderbird (SSA:2016-336-02)

Slackware 14.1 / 14.2 / current : mozilla-thunderbird (SSA:2016-365-02)

Slackware 14.1 / 14.2 / current : mozilla-thunderbird (SSA:2017-026-01)

Slackware 14.1 / 14.2 / current : mozilla-thunderbird (SSA:2017-066-02)

Slackware 14.1 / 14.2 / current : seamonkey (SSA:2016-365-03)

Slackware 14.1 / 14.2 : mariadb (SSA:2017-251-02)

Slackware 14.1 / 14.2 : mariadb (SSA:2018-032-01)

Slackware 14.1 / 14.2 : mariadb (SSA:2018-130-01)

Slackware 14.1 / 14.2 : mariadb (SSA:2019-032-01)

Slackware 14.1 / 14.2 : mozilla-firefox (SSA:2016-219-02)

Slackware 14.1 / current : glibc (SSA:2014-296-01)

Slackware 14.1 / current : glibc (SSA:2016-054-02)

Slackware 14.1 / current : grub (SSA:2015-351-01)

Slackware 14.1 / current : libarchive (SSA:2016-145-01)

Slackware 14.1 / current : libarchive (SSA:2016-172-01)

Slackware 14.1 / current : libevent (SSA:2016-085-01)

Slackware 14.1 / current : mariadb (SSA:2014-152-01)

Slackware 14.1 / current : mariadb (SSA:2014-307-01)

Slackware 14.1 / current : mariadb (SSA:2015-132-01)

Slackware 14.1 / current : mariadb (SSA:2019-213-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2013-350-04)

Slackware 14.1 / current : mozilla-firefox (SSA:2014-039-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2014-086-03)

Slackware 14.1 / current : mozilla-firefox (SSA:2014-119-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2014-204-02)

Slackware 14.1 / current : mozilla-firefox (SSA:2014-247-02)

Slackware 14.1 / current : mozilla-firefox (SSA:2014-271-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2014-307-02)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-016-02)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-056-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-111-05)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-132-04)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-188-02)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-219-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-241-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-265-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-310-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2015-349-03)

Slackware 14.1 / current : mozilla-firefox (SSA:2016-034-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2016-042-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2016-068-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2016-077-01)

Slackware 14.1 / current : mozilla-firefox (SSA:2016-117-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2013-350-05)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-039-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-086-05)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-119-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-163-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-204-03)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-247-03)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-271-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2014-337-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-016-03)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-056-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-111-06)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-137-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-192-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-226-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-274-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-337-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2015-357-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2016-045-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2016-078-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2016-085-02)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2016-095-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2016-106-01)

Slackware 14.1 / current : mozilla-thunderbird (SSA:2016-152-02)

Slackware 14.1 / current : openssh (SSA:2013-322-02)

Slackware 14.1 / current : pcre (SSA:2015-328-01)

Slackware 14.1 / current : pcre (SSA:2016-172-02)

Slackware 14.1 / current : qt (SSA:2015-111-13)

Slackware 14.1 / current : samba (SSA:2014-013-04)

Slackware 14.1 / current : samba (SSA:2014-213-01)

Slackware 14.1 / current : samba (SSA:2015-020-01)

Slackware 14.1 / current : samba (SSA:2015-064-01)

Slackware 14.1 / current : samba (SSA:2016-068-02)

Slackware 14.1 / current : seamonkey (SSA:2015-318-01)

Slackware 14.1 / current : seamonkey (SSA:2016-075-02)

Slackware 14.1 / current : xorg-server (SSA:2014-356-03)

Slackware 14.1 : kernel (SSA:2014-050-03)

Slackware 14.1 : kernel (SSA:2016-242-01)

Slackware 14.1 : mozilla-firefox (SSA:2014-157-01)

Slackware 14.1 : mozilla-firefox (SSA:2014-344-02)

Slackware 14.1 : mozilla-firefox (SSA:2015-226-01)

Slackware 14.1 : mozilla-firefox (SSA:2017-112-01)

Slackware 14.1 : mozilla-thunderbird (SSA:2014-320-01)

Slackware 14.1 : Slackware 14.1 kernel (SSA:2017-180-01) (Stack Clash)

Slackware 14.2 / current : blueman (SSA:2018-213-01)

Slackware 14.2 / current : gd (SSA:2017-199-02)

Slackware 14.2 / current : gd (SSA:2018-108-01)

Slackware 14.2 / current : gd (SSA:2020-083-01)

Slackware 14.2 / current : ghostscript (SSA:2018-249-02)

Slackware 14.2 / current : ghostscript (SSA:2018-256-01)

Slackware 14.2 / current : ghostscript (SSA:2019-092-01)

Slackware 14.2 / current : glibc (SSA:2017-181-01) (Stack Clash)

Slackware 14.2 / current : gnutls (SSA:2018-339-01)

Slackware 14.2 / current : gnutls (SSA:2019-086-01)

Slackware 14.2 / current : gnutls (SSA:2020-091-01)

Slackware 14.2 / current : kdelibs (SSA:2019-220-01)

Slackware 14.2 / current : kernel (SSA:2016-347-01)

Slackware 14.2 / current : kernel (SSA:2017-177-01) (Stack Clash)

Slackware 14.2 / current : kernel (SSA:2017-181-02) (Stack Clash)

Slackware 14.2 / current : kernel (SSA:2019-169-01) (SACK Panic) (SACK Slowness)

Slackware 14.2 / current : libgcrypt (SSA:2017-180-04)

Slackware 14.2 / current : libgcrypt (SSA:2017-261-02)

Slackware 14.2 / current : libgcrypt (SSA:2018-164-01)

Slackware 14.2 / current : libplist (SSA:2017-320-01)

Slackware 14.2 / current : libpng (SSA:2019-107-01)

Slackware 14.2 / current : libssh2 (SSA:2019-077-01)

Slackware 14.2 / current : libtiff (SSA:2017-098-01)

Slackware 14.2 / current : libtiff (SSA:2017-324-01)

Slackware 14.2 / current : libtiff (SSA:2018-316-01)

Slackware 14.2 / current : libtiff (SSA:2019-308-01)

Slackware 14.2 / current : libtirpc (SSA:2017-191-01)

Slackware 14.2 / current : libzip (SSA:2017-255-02)

Slackware 14.2 / current : Linux kernel (SSA:2016-236-03)

Slackware 14.2 / current : lxc (SSA:2019-043-01)

Slackware 14.2 / current : mariadb (SSA:2017-087-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2017-114-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2017-221-02)

Slackware 14.2 / current : mozilla-firefox (SSA:2017-271-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2017-320-02)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-072-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-075-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-085-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-120-02)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-129-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-157-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-176-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-249-03)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-265-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-276-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-296-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2018-345-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-029-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-044-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-081-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-141-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-169-02)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-172-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-191-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-226-02)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-295-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2019-337-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2020-006-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2020-009-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2020-042-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2020-070-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2020-094-01)

Slackware 14.2 / current : mozilla-firefox (SSA:2020-098-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2017-356-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2018-025-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2018-082-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2018-142-02)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2018-186-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2018-191-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2019-045-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2019-084-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2019-164-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2019-172-02)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2019-254-02)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2019-268-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2020-010-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2020-024-01)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2020-042-02)

Slackware 14.2 / current : mozilla-thunderbird (SSA:2020-073-01)

Slackware 14.2 / current : nettle (SSA:2018-339-02)

Slackware 14.2 / current : openexr (SSA:2017-274-01)

Slackware 14.2 / current : openjpeg (SSA:2017-279-02)

Slackware 14.2 / current : openjpeg (SSA:2019-095-01)

Slackware 14.2 / current : openssl (SSA:2016-270-01)

Slackware 14.2 / current : openssl (SSA:2017-041-02)

Slackware 14.2 / current : openssl (SSA:2017-306-02)

Slackware 14.2 / current : openssl (SSA:2018-087-01)

Slackware 14.2 / current : openssl (SSA:2018-226-01)

Slackware 14.2 / current : openssl (SSA:2019-254-03)

Slackware 14.2 / current : openssl (SSA:2019-354-01)

Slackware 14.2 / current : procps-ng (SSA:2018-142-03)

Slackware 14.2 / current : rpcbind (SSA:2017-191-02)

Slackware 14.2 / current : ruby (SSA:2017-261-03)

Slackware 14.2 / current : ruby (SSA:2017-353-01)

Slackware 14.2 / current : ruby (SSA:2018-088-01)

Slackware 14.2 / current : samba (SSA:2016-363-02)

Slackware 14.2 / current : seamonkey (SSA:2017-202-01)

Slackware 14.2 / current : seamonkey (SSA:2018-123-01)

Slackware 14.2 / current : seamonkey (SSA:2019-247-01)

Slackware 14.2 / current : seamonkey (SSA:2020-062-01)

Slackware 14.2 / current : Slackware 14.2 mozilla-thunderbird (SSA:2018-249-04)

Slackware 14.2 / current : squashfs-tools (SSA:2017-209-01)

Slackware 14.2 / current : tigervnc (SSA:2019-354-02)

Slackware 14.2 / current : wget (SSA:2019-092-02)

Slackware 14.2 / current : wget (SSA:2019-095-02)

Slackware 14.2 : mozilla-firefox (SSA:2018-020-01)

Slackware 14.2 : openssl (slackware 14.2) (SSA:2019-057-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2018-037-01) (Spectre)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2018-057-01) (Spectre)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2018-142-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2018-208-01) (Spectre)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2018-240-01) (Foreshadow)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2018-264-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2019-030-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2019-202-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2019-226-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2019-238-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2019-311-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2019-320-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2020-008-01)

Slackware 14.2 : Slackware 14.2 kernel (SSA:2020-086-01)

Slackware 8.1 / 9.0 / 9.1 / current : apache (SSA:2004-133-01)

Slackware 8.1 / 9.0 / 9.1 / current : apache security update (SSA:2003-308-01)

Slackware 8.1 / 9.0 / 9.1 / current : cvs (SSA:2004-140-01)

Slackware 8.1 / 9.0 / 9.1 / current : cvs (SSA:2004-161-01)

Slackware 8.1 / 9.0 / 9.1 / current : cvs security update (SSA:2003-345-01)

Slackware 8.1 / 9.0 / 9.1 / current : cvs security update (SSA:2004-108-02)

Slackware 8.1 / 9.0 / 9.1 / current : fetchmail security update (SSA:2003-300-02)

Slackware 8.1 / 9.0 / 9.1 / current : kernel DoS (SSA:2004-167-01)

Slackware 8.1 / 9.0 / 9.1 / current : lftp security update (SSA:2003-346-01)

Slackware 8.1 / 9.0 / 9.1 / current : lha update in bin package (SSA:2004-125-01)

Slackware 8.1 / 9.0 / 9.1 / current : metamail security update (SSA:2004-049-02)

Slackware 8.1 / 9.0 / 9.1 / current : mod\_ssl (SSA:2004-154-01)

Slackware 8.1 / 9.0 / 9.1 / current : mutt security update (SSA:2004-043-01)

Slackware 8.1 / 9.0 / 9.1 / current : OpenSSL security update (SSA:2003-273-01)

Slackware 8.1 / 9.0 / 9.1 / current : OpenSSL security update (SSA:2004-077-01)

Slackware 8.1 / 9.0 / 9.1 / current : PHP local security issue (SSA:2004-154-02)

Slackware 8.1 / 9.0 / 9.1 / current : rsync security update (SSA:2003-337-01)

Slackware 8.1 / 9.0 / 9.1 / current : rsync update (SSA:2004-124-01)

Slackware 8.1 / 9.0 / 9.1 / current : sysklogd update (SSA:2004-124-02)

Slackware 8.1 / 9.0 / 9.1 / current : tcpdump denial of service (SSA:2004-108-01)

Slackware 8.1 / 9.0 / 9.1 / current : XFree86 security update (SSA:2004-043-02)

Slackware 8.1 / 9.0 / 9.1 : PHP packages updated again for 8.1, 9.0, 9.1 (SSA:2005-192-02)

Slackware 8.1 / 9.0 / current : CUPS DoS vulnerability fixed (SSA:2003-149-01)

Slackware 8.1 / 9.0 / current : inetd DoS patched (SSA:2003-251-01)

Slackware 8.1 / 9.0 / current : New OpenSSH packages (SSA:2003-266-01)

Slackware 8.1 / 9.0 / current : nfs-utils off-by-one overflow fixed (SSA:2003-195-01)

Slackware 8.1 / 9.0 / current : nfs-utils packages replaced (SSA:2003-195-01b)

Slackware 8.1 / 9.0 / current : OpenSSH Security Advisory (SSA:2003-259-01)

Slackware 8.1 / 9.0 / current : OpenSSH updated again (SSA:2003-260-01)

Slackware 8.1 / 9.0 / current : ProFTPD Security Advisory (SSA:2003-259-02)

Slackware 8.1 / 9.0 / current : security issues in pine (SSA:2003-253-01)

Slackware 8.1 / 9.0 / current : Sendmail vulnerabilities fixed (SSA:2003-260-02)

Slackware 8.1 / 9.0 : BitchX security fixes (SSA:2003-141-02)

Slackware 8.1 / 9.0 : EPIC4 security fixes (SSA:2003-141-01)

Slackware 8.1 / 9.0 : glibc XDR overflow fix (SSA:2003-141-03)

Slackware 8.1 / 9.0 : Mutt buffer overflow in IMAP support

Slackware 8.1 / 9.0 : Samba security problem fixed

Slackware 8.1 / 9.0 : Sendmail buffer overflow fixed (NEW)

Slackware 8.1 / current : New CVS packages available

Slackware 8.1 / current : New DHCP packages available

Slackware 8.1 / current : New Samba package available

Slackware 8.1 / current : Samba buffer overflow fixed

Slackware 8.1 / current : Sendmail buffer overflow fixed

Slackware 8.1 : Security updates for Slackware 8.1

Slackware 8.1 : Slackware 8.1 kernel security update (SSA:2004-008-01)

Slackware 9.0 / 9.1 / current : GAIM security update (SSA:2004-026-01)

Slackware 9.0 / 9.1 / current : gdm security update (SSA:2003-300-01)

Slackware 9.0 / 9.1 / current : INN security update (SSA:2004-014-02)

Slackware 9.0 / 9.1 / current : kdelibs (SSA:2004-238-01)

Slackware 9.0 / 9.1 / current : kdepim security update (SSA:2004-014-01)

Slackware 9.0 / 9.1 / current : Kernel security update (SSA:2004-006-01)

Slackware 9.0 / 9.1 / current : libpng update (SSA:2004-124-04)

Slackware 9.0 / 9.1 / current : mc (SSA:2004-136-01)

Slackware 9.0 / current : GDM security update (SSA:2003-236-01)

Slackware 9.0 / current : unzip vulnerability patched (SSA:2003-237-01)

Slackware 9.0 / current : WU-FTPD Security Advisory (SSA:2003-259-03)

Slackware 9.0 : 2.4.21 kernels available (SSA:2003-168-01)

Slackware 9.0 : GnuPG key validation fix (SSA:2003-141-04)

Slackware 9.0 : mod\_ssl RSA blinding fixes (SSA:2003-141-05)

Slackware 9.0 : quotacheck security fix in rc.M (SSA:2003-141-06)

Slackware 9.0 : Updated KDE packages available

Slackware 9.1 / current : Kernel security update (SSA:2003-336-01)

Slackware 9.1 / current : Kernel security update (SSA:2004-049-01)

Slackware 9.1 / current : kernel security updates (SSA:2004-119-01)

Slackware 9.1 / current : utempter security update (SSA:2004-110-01)

Slackware 9.1 / current : xine security update (SSA:2004-111-01)

Slackware 9.1 / current : xine-lib update (SSA:2004-124-03)

Slackware current : 64-bit kernel (SSA:2010-265-01)

Slackware current : kernel (SSA:2009-342-01)

Slackware current : mutt remote exploit patched

Slackware current : OpenSSH security problem fixed

Slackware current : slackware-current security updates (SSA:2005-251-03)

Slackware current : sudo upgrade fixes a potential vulnerability

Slackware current : thunderbird (SSA:2007-165-01)

Slackware current : zlib upgrade fixes vulnerability

SSA-2003-141-06a REVISED quotacheck security fix in rc.M

SSA-2003-213-01 Sendmail buffer overflow fixed (NEW)

SSA-2003-336-01b Samba security problem fixed

SSA-2004-222-01b Sendmail buffer overflow fixed (NEW)

SSA-2007-325-01a libpng for Slackware 10.1 and 10.2

SSA-2010-060-01 : seamonkey

# Settings

ADSI Settings

AirWatch API Settings

Amazon Web Services Settings

Apple Profile Manager API Settings

AppSocket & socketAPI Printers - Do Not Scan

Authenticated Check : OS Name and Installed Package Enumeration

Authentication Failure - Local Checks Not Run

Authentication Failure(s) for Provided Credentials

Authentication Success

Authentication Success - Local Checks Not Available

Authentication Success Insufficient Access

Authentication Success with Intermittent Failure

Authentication to Patch Management Failed for Provided Credentials

Blackberry UEM Settings

Cleartext protocols settings

Database Authentication Failure(s) for Provided Credentials

Database settings

Debugging Log Report

Do not scan fragile devices

Do not scan Novell NetWare

Do not scan operational technology devices

Do not scan printers

Do not scan printers (AppSocket)

Exclude top-level domain wildcard hosts

F5 Settings

Global variable settings

Good MDM Settings

Host Fully Qualified Domain Name (FQDN) Resolution (XML tag)

Host Tagging

Host Tagging (Linux)

Host Tagging (Windows)

Hosts File Whitelisted Entries

HTTP cookies import

HTTP login page

IBM iSeries Credentials

Inconsistent Hostname and IP Address

Intune Settings

Kerberos configuration

Local Checks Enabled

Local Checks Not Enabled (info)

Login configurations

MaaS360 Settings

Microsoft Azure Settings

Missing Patch Logging Initialization

MobileIron API Settings

MongoDB Settings

Nessus Internal: Put cgibin() in the KB

Nessus Launched Plugin List

Nessus Product Information

Nessus Scan Information

Nessus Windows Scan Not Performed with Admin Privileges

Netapp API Settings

No Credentials Provided

Office 365 Settings

OpenStack Settings

Oracle Settings

Palo Alto Networks PAN-OS Settings

Patch Management Authentication Success

Patch Management: Dell KACE K1000 Settings

Patch Management: IBM Tivoli Endpoint Manager Server Settings

Patch Management: Patch Schedule From Red Hat Satellite Server

Patch Management: Red Hat Satellite 6 Settings

Patch Management: Red Hat Satellite Get Installed Packages

Patch Management: Red Hat Satellite Server Get Managed Servers

Patch Management: Red Hat Satellite Server Get System Information

Patch Management: Red Hat Satellite Server Settings

Patch Management: SCCM Server Settings

Patch Management: Symantec Altiris Settings

Patch Management: VMware Go Server Settings (deprecated)

Patch Management: WSUS Server Settings

PCI DSS compliance : options settings

PCI Scan Accuracy cannot be verified through Load Balancer with non-identically configured or non-synced systems

Port scanner dependency

Port scanners settings

Post-Scan Rules Application

Post-Scan Status

Rackspace Settings

Report Feed Telemetry

Report Feed Telemtry End

RHEV Settings

Salesforce.com Settings

Set System Name

SMB : Disable the C$ and ADMIN$ shares after the scan (WMI)

SMB : Enable the C$ and ADMIN$ shares during the scan (WMI)

SMB Registry : Start the Registry Service during the scan

SMB Registry : Start the Registry Service during the scan (WMI)

SMB Registry : Starting the Registry Service during the scan failed

SMB Registry : Stop the Registry Service after the scan

SMB Registry : Stop the Registry Service after the scan (WMI)

SMB Registry : Stopping the Registry Service after the scan failed

SMB Scope

SMTP settings

SNMP settings

SSH Combined Host Command Logging (Plugin Debugging)

SSH Commands Ran With Privilege Escalation

SSH Commands Require Privilege Escalation

SSH settings

VMware SOAP API Settings

VMware vCenter SOAP API Settings

Wake-on-LAN

Web Application Tests Settings

# Service detection

.NET NegotiateStream Server Detection

Acronis Agent Detection (TCP)

Acronis Agent Detection (UDP)

ActiveFax Server Detection

Adobe Experience Manager Web Detection

Advanced Message Queuing Protocol Detection

Aeonian Dreams Detection

AFS Client Version Detection

Airport Administrative Traffic Detection (192/UDP)

AJP Connector Detection

Alcatel PABX 4400 Detection

Alert Standard Format / Remote Management and Control Protocol Detection

AlienVault OSSIM REST API Service Detection

Altiris Deployment Server Detection

Altiris Deployment Solution Server DB Manager Detection

AMANDA Client Version

Android Emulator ADB Port on Remote Host

Anon Proxy Server Software Detection

Ansible AWX Installed (Linux/UNIX)

Ansible Installed (Linux/UNIX)

Ansible Tower Installed (Linux/UNIX)

Apache Maven Installed (Linux / Unix)

Apache Zookeeper Server Detection

apcnisd / apcupsd Detection

Apple AirPlay Web Detection

Apple Filing Protocol Server Detection

Apple iOS Lockdown Detection

Apple Profile Manager Detection

Apple Remote Events Service Detection

Apple TV Detection

Apple TV Version Detection

ARCserve Backup for Laptops & Desktops Server Admin Service Detection

ARCserve Backup for Laptops & Desktops Server Detection

Atlassian Jira Installed (Unix / Linux)

avast! Management Server Detection

AXIMilter Detection

Barco/AWiND WePresent Command Port Detection

Beanstalkd Detection

BGP Service Detection

Bitcoin Detection

BitDefender Update Server Detection

BJNP Detection

BNC Detection

CA ARCServe MSSQL Agent Detection

CA ARCServe UniversalAgent Detection

CA BrightStor ARCserve Backup Discovery Service Detection

CA BrightStor HSM Engine Detection (TCP)

CA BrightStor HSM Engine Detection (UDP)

CA DMPrimer Service Detection

CA eTrust Intrusion Detection System Detection

CA InoWeb Detection

CA Message Queuing Service Detection

CA Secure Content Manager HTTP Gateway Service Detection

CA Unicenter Cron Scheduler Detection

Cache' SuperServer Detection

Call Of Duty Server Detection

CDE Subprocess Control Service (dtspcd) Detection

Centennial IP Transfer Agent Detection

Cfengine Detection

Check Point InterSpect Detection

Cheops NG Agent Detection

CISCO ASA SSL VPN Detection

Cisco HyperFlex Web API Detection

Cisco Smart Install Detection

Citrix EdgeSight Load Tester (ESLT) version detection

Citrix Licensing Service Detection

Citrix Server Detection

ColdFusion MX Server Detection

Commvault Web Console Detection

Condor Service Detection

CORBA IIOP Listener Detection

Crestron QM-RMC Service Detection

Crystal Reports Central Management Server Detection

CVS pserver Detection

D-link Click 'n Connect Daemon Detection

D-Link Router Detection

Datagram Transport Layer Security Detection

Daytime Service Detection

DCN HELLO detection

Dell EMC Data Protection Central Web Interface Detected

Derby Network Server Detection

DHCP Server Detection

Discard Service Detection

DiskPulse Server Detection

DistCC Detection

Docker Container File Change Detection

Docker Remote API Detection

Docker Service Detection

Dopewars Server Detection

EA Need For Speed Underground Detection

Echo Service Detection

echoServer Detection

EGP Detection

eIQnetworks Enterprise Security Analyzer License Manager Detection

eIQnetworks Enterprise Security Analyzer Monitoring Agent Detection

eIQnetworks Enterprise Security Analyzer Syslog Server Detection

eIQnetworks Enterprise Security Analyzer Topology Server Detection

Elastic Winlogbeat Installed (Windows)

EMC AlphaStor Device Manager Detection

EMC AlphaStor Library Manager Detection

EMC AutoStart ftAgent Detection

EMC Data Protection Advisor CXML Service Detection

EMC Legato Networker Detection

EMC Replication Manager Client Detection

EMC Replication Manager Server Detection

EMC RepliStor Detection

EMC SMARTS Application Server Detection

eMule Web Server Detection

Enterasys Dragon Enterprise Reporting Detection

Entropy Gathering Daemon (EGD) Detection

ePolicy Orchestrator Detection

Eric Cooperation Server Detection

Erlang Port Mapper Daemon Detection

eScan Agent Detection

Eudora Internet Mail Server Admin Server Detection

eyeMax DVR Server Detection

ezbounce Detection

File Alteration Monitor daemon (famd) Detection

File Transfer (P2P) Detection

Firebird / InterBase Database Server Detection

FlexCast Server Detection

Flexera FlexNet Publisher Detection

FrontBase FBExec Process Detection

FTP Server Detection

GDB Server Detection

Gearman Server Detection

Git Protocol Detection

GNUnet Detection (Client Interface)

GO-Global Server Detection

Goverlan Agent Remote Detection

Grandstream Networking Solutions Device Web Detection

Greenbone Security Assistant detection

H323 Protocol / VoIP Application Detection

H3C / HP Intelligent Management Center Detection

HALO Network Server Detection

Harbor Local Detection

Harbor Web Interface Detection

Hazelcast Memcached Interface Detection

Hazelcast Wire Protocol Detection

HDHomeRun Control Service Detection

HDHomeRun Discovery Service Detection

healthd Detection

HNAP Detection

Hobbit Monitor Daemon Detection

HP Data Protector Detection

HP DesignJet Printer Web Interface Detection

HP iNode Management Center Detection

HP Integrated Lights-Out (iLO) Detection

HP LaserJet Printer Detection

HP LeftHand OS Console Discovery Detection

HP LeftHand OS hydra Detection

HP LeftHand OS Management Protocol Detection

HP Linux Imaging and Printing System HPSSD Daemon Detection

HP LoadRunner Agent Service Detection

HP OfficeJet Printer Detection

HP OpenView BBC Service Detection

HP OpenView NNM Alarm Service Detection

HP OpenView Storage Mirroring Server Detection

HP OpenView Topology Manager Daemon Detection

HP OpenView UI Process Manager Daemon Detection

HP OVCM/Radia Notify Daemon Detection

HP Performance Agent detection - deprecated

HP Printer PJL Interface Detection

HP StorageWorks File Migration Agent Detection

HP Switch Identification

HSQLDB Server Detection

HTTP Backdoor Detection deprecated

HTTP CONNECT Proxy Detection

Hydrogen Detection

Hyper Text Caching Protocol (HTCP) Detection

I Hear U Detection

IBM Domino Detection (uncredentialed check)

IBM iSeries Server Detection

IBM Lotus Notes Detection

IBM Remote Supervisor Adapter Detection (HTTP)

IBM Spectrum Protect / Tivoli Storage Manager Service Detection

IBM Spectrum Protect Mount Detection

IBM Tivoli Storage Manager Client Acceptor Daemon Detection

IBM Tivoli Storage Manager FastBack Server Detection

IBM WebSphere MQ Listener Detection

IDA Pro Disassembler Software Detection

Identd Service Detection

IMAP Service Banner Retrieval

Informix Detection

Ingres Communications Server Detection

Ingres Data Access Server Detection

Inter-Asterisk eXchange Protocol Detection

Internet Cache Protocol (ICP) Version 2 Detection

IPSEC Internet Key Exchange (IKE) Version 1 Detection

IPSEC Internet Key Exchange (IKE) Version 2 Detection

Ipswitch Instant Messaging Client Detection

Ipswitch Instant Messaging Server Detection

IRC Bouncer (BNC) Detection

IRC Daemon Version Detection

iSCSI Target Detection

Isilon OneFS FTP Detection

Isilon OneFS NTP Detection

Isilon OneFS SNMP Detection

Isilon OneFS uname Detection

Isilon OneFS Web Interface Detection

ISS Deployment Manager Detection

Java Debug Wire Protocol Detection

Jenkins Installed (Linux)

JIRA Service Desk Installed (Linux)

Juniper NSM GUI Server Detection

Kerio Mailserver Admin Service Detection

Kerio Personal Firewall Admin Service Detection

Kerio Winroute Firewall Admin Service Detection

KiSS PC-Link Server Detection (TCP)

KiSS PC-Link Server Detection (UDP)

Kubernetes Installed (Linux)

Kubernetes Web API Detection

Kyocera Mita Scanner File Utility Detection

LANDesk Management Agent Detection

LANDesk Ping Discovery Service Detection

LANDesk QIP Server Detection

LANDesk Remote Control Service Detection

LCDproc Detection

LDAP Server Detection

Lexmark Printer Detection

Link-Local Multicast Name Resolution (LLMNR) Detection

LinuxConf Detection

LISa Detection

Logitech Touch Mouse Server Detection

Lotus Domino Console Detection

LPD Detection

McAfee Common Management Agent Detection

McAfee E-Business Administration Agent Detection

McAfee IntruShield Management Console Detection

MDAP Service Detection

mDNS Detection (Local Network)

mDNS Detection (Remote Network)

memcached Detection

Microsoft Dynamics GP Distributed Process Manager Detection

Microsoft Host Integration Server Detection

Microsoft Office Document Conversions Launcher Detection

Microsoft Office Document Conversions Load Balancer Detection

Microsoft SQL Server TCP/IP Listener Detection

MikroTik MAC Telnet Protocol Detection

MikroTik Neighbor Discovery Protocol Detection

MikroTik RouterOS Detection

MikroTik RouterOS Winbox Detection

Milter Detection

MobiLink Server Detection

MongoDB Detection

MS Executable Detection

MSRPC Service Detection

Nagios NRPE Plugin Detect

nagios-statd Daemon Detection

NAT-PMP Detection (local network)

NAT-PMP Detection (remote network)

Nessus Server Detection

NetInfo Daemon Detection

netOctopus Agent Detection (TCP)

netOctopus Agent Detection (UDP)

NetOp Products Detection (TCP)

NetOp Products Detection (UDP)

netsaint-statd Daemon Detection

NetVault Process Manager Service Detection

Network Block Device Server Detection

Network Chemistry Wireless Sensor Detection

Network Notary Server Detection

Network Time Protocol (NTP) Server Detection

Nexpose HTTP Server Detection

NNTP Server Detection

Non-compliant Strict Transport Security (STS)

Novatel MiFi Default Credentials

Novatel MiFi Detection

Novell CLNTRUST Service Detection

Novell Messenger Archive Agent Detection

Novell Messenger Messaging Agent Detection

Novell Privileged User Manager Daemon Detection

Novell ZenWorks Asset Management Server Detection

OEJP Daemon Detection

Open Network Video Interface Forum (ONVIF) Protocol Detection

Open Shortest Path First (OSPF) Agent Detection

OpenBase Detection

OpenGear Web Detection

Openlink Virtuoso Server Detection

OpenSSL Detection

OpenVAS Manager / Administrator Detection

OpenVAS Scanner Detection

OpenVPN Server Detection

Oracle Database Detection

Oracle GoldenGate Manager Version Detection

Oracle MySQL Connectors Installed (Linux)

Oracle WebLogic Server Node Manager Detection

Oracle WebLogic SNMP Detection (TCP)

Oracle WebLogic SNMP Detection (UDP)

Oracle WebLogic T3 Protocol Detection

Oracle WebLogic Web Services Test Client Detection

OSSIM Server Detection

Palo Alto Default Credentials

Palo Alto Demisto Installed (Unix / Linux)

Palo Alto Expedition Cross-Site Scripting

Palo Alto Expedition Web Detection

Panda AdminSecure Communications Agent Detection

Perforce Server Detection

Pervasive PSQL / Btrieve Server Detection

Pgbouncer Service Detection

Poison Ivy Detection

POP Server Detection

Postfix Policyd Protocol Detection

PostgreSQL Server Detection

PowerFolder Server Detection

PPTP Detection

Printer Job Language (PJL) Detection

ProRat Detection

Py2Play Game Engine Detection

Python Flask Installed (Linux)

Python Remote HTTP Detection

QLogic QConvergeConsole GUI Web Interface Detection

QMTP/QMQP Server Detection

QNX pdebug Service Detection

Quote of the Day (QOTD) Service Detection

RADIUS Server Detection

Rancher Docker Container Detection (Linux)

Rancher Web Interface Detection

RAPI Manager Detection

Red Hat Interchange INET Mode Detection

Redis Server Detection

Remote listeners enumeration (Linux / AIX)

Remote PC Access Server detection.

Rendezvous Daemon Detection

RES Workspace Manager Agent Detection

RES Workspace Manager Relay Server Detection

Retrospect Client Detection

rexecd Service Detection

Ricoh Printer Detection

Rio Karma MP3 Player File Upload Service Detection

RIP Detection

rlogin Service Detection

RMI Registry Detection

RMI Remote Object Detection

Rocket Software UniRPC Version Detection

RPC Services Enumeration

rsh Service Detection

RSP Detection

rsync Service Detection

rsync Writeable Module Detection

RTMP Server Detection

RTSP Server Type / Version Detection

Samba Server Detection

Samhain Server (yule) Detection

SAP DB / MaxDB Detection

SAP Dynamic Information and Action Gateway Detection

SAP RMI-P4 Protocol Detection

SAProuter Detection

Scan for UPnP hosts (multicast)

Secure HyperText Transfer Protocol (S-HTTP) Detection

Service Detection

Service Detection (2nd Pass)

Service Detection (GET request)

Service Detection (HELP Request)

Service Detection : SMTP Server on a Well-Known Port

Service Detection: 3 ASCII Digit Code Responses

Session Initiation Protocol Detection

Skinny Server Detection

Skype Detection

Skype Stack Version Detection

slident / fake identd Detection

SLP Server Detection (TCP)

SLP Server Detection (UDP)

SMPP Server Detection

SMTP Server Detection

SOAP Server Detection

sobby Server Detection

SOCKS Server Detection

Solstice Enterprise Agent SNMP (snmpdx) Detection

Sophos XG Firewall Detection

Splashtop Streamer remote detection

SQL Anywhere Broadcast Repeater Detection

Squeezebox Server CLI Detection

Squeezebox Server Detection

SqueezeCenter Discovery Service Detection

SSH (SSF Derivative) Detection

SSH Server Type and Version Information

SSL Anonymous Cipher Suites Supported

SSL Service Requests Client Certificate

SSL Version 2 and 3 Protocol Detection

sslh Detection

StarTeam Server Detection

Strict Transport Security (STS) Detection

STUN Detection

Subversion Server Detection

Sun Java System ASP Server Detection

Sun Secure Global Software / Tarantella Detection

Sybase M-Business Anywhere (AvantGo) SOAP Server Detection

Sybase M-Business Anywhere (AvantGo) Sync Server Detection

Sybase PowerDesigner Repository Proxy Detection

Sybase SQL Anywhere Server Detection

Sybase TCP/IP Listener Service Detection

Symantec Content Analysis Local Detection

Symantec Content Analysis Web Detection

Symantec Ghost Solution Locate Server Detection

Symantec Ghost Solution Status Server Detection

Symantec Management Center Web Detection

Symantec pcAnywhere Access Server Detection

Symantec pcAnywhere Detection (TCP)

Symantec pcAnywhere Status Service Detection (UDP)

Symantec Reporter Web Interface Detection

Symantec SAVCE/Client Security Service Detection

Symantec Storage Foundation Scheduler Service Detection

Symantec Veritas Enterprise Administrator Service (vxsvc) Detection

SynchronEyes Student Detection

SynchronEyes Teacher Detection

Talk Service (talkd, in.talk, ntalk) Detection

TCP Channel Detection

TeamSpeak 3 Server Detection

TeamViewer remote detection

Telnet Server Detection

Telnet Service Detection

Tenable Core Web Interface Detection

Tenable PVS Proxy Detection

Teredo Server Detection

Tetrinet server detection

TFTP Daemon Detection

Thecus NAS Device Detection

Timbuktu Detection (TCP)

Timbuktu Detection (UDP)

Tinc VPN Service Detection

TiVo Detection

TLS Version 1.0 Protocol Detection

TLS Version 1.0 Protocol Detection (PCI DSS)

TLS Version 1.1 Protocol Detection

Tofu Server Detection

Tor Server Detection

Trend Micro Control Manager CmdProcessor.exe Detection

Trend Micro Deep Security Agent Installed (Linux)

Trend Micro Message Routing Framework Detection

Trend Micro OfficeScan Client Detection

Trend Micro OfficeScan Client Version

Trend Micro ServerProtect Detection

UltraVNC w/ DSM Plugin Detection

UltraVNC w/ DSM Plugin Detection (2)

Unauthenticated OpenVPN Server Detection

Unisys Business Information Server Detection

Universal Plug and Play (UPnP) Protocol Detection

Unknown Service Detection: Banner Retrieval

Unprotected QNX qconn Service

Unreal Tournament Server Detection

UPnP Client Detection

Ventrilo Server Detection

VERITAS Backup Agent Detection

VERITAS NetBackup Agent Detection

VERITAS NetBackup Volume Manager Detection

Versant Connection Services Daemon Detection

VLAN Membership Policy Server Detection

VMware ESX/GSX Server detection

VMware vCenter Detect

VMware vSphere Detect

VNC HTTP Server Detection

VNC Server Security Type Detection

VNC Server Unencrypted Communication Detection

VNC Software Detection

VNCviewer in Listen Mode Detection

Vuze Media Server Detection

Web Server Detection (HTTP/1.1)

Web Server UPnP Detection

WinComLPD LPD Monitoring Server Detection

Windows Media Service Server Detection

Windows Server Update Services (WSUS) Detection

WINS Server Detection

writesrv Service Detection

Wyse Device Manager HAgent Service Detection

X Display Manager Control Protocol (XDMCP) Detection

X Font Service Detection

X Server Detection

X-format Communications Protocol (XCP) Detection

XMPP Server Detection

XOT Detection

XSTUNT Server Detection

xtel Detection

xtelw Detection

Yahoo Messenger Detection

YIFF Sound Server Detection

Yosemite Backup Service Driver Detection

Zabbix Server Detection

Zebedee Server Detection

Zebra ZTC Printer Web Interface Detection

Zend Session Clustering Daemon Detection

ZENworks Remote Management Agent Detection

# Scientific Linux Local Security Checks

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20130311)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20130415)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20130730)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20130828)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20140313)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20140807)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20150305)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20161115)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20170411)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20180313)

Scientific Linux Security Update : 389-ds-base on SL6.x i386/x86\_64 (20180509)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20160216)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20170412)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20170905)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20180125)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20180306)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20180515)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20180925)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20190729)

Scientific Linux Security Update : 389-ds-base on SL7.x x86\_64 (20191202)

Scientific Linux Security Update : 4Suite on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : abrt and libreport on SL6.x i386/x86\_64 (20130131)

Scientific Linux Security Update : abrt and libreport on SL7.x x86\_64 (20151123)

Scientific Linux Security Update : abrt on SL6.x i386/x86\_64 (20150707)

Scientific Linux Security Update : abrt on SL7.x x86\_64 (20150609)

Scientific Linux Security Update : abrt, libreport, btparser, and python-meh on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : acpid on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : acpid on SL5.x i386/x86\_64

Scientific Linux Security Update : advancecomp on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : aide on SL5.x i386/x86\_64

Scientific Linux Security Update : apache-commons-beanutils on SL7.x (noarch) (20200121)

Scientific Linux Security Update : apache-commons-collections on SL7.x (noarch) (20151130)

Scientific Linux Security Update : apr and apr-util on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : apr on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : apr on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : apr on SL6.x i386/x86\_64

Scientific Linux Security Update : apr on SL6.x, SL7.x i386/x86\_64 (20171129)

Scientific Linux Security Update : apr-util on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : apr-util on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : atrpms-repo on SL6.x i386/x86\_64

Scientific Linux Security Update : augeas on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : augeas on SL6.x i386/x86\_64 (20140120)

Scientific Linux Security Update : augeas on SL7.x x86\_64 (20170921)

Scientific Linux Security Update : authconfig on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : autofs on SL5.x i386/x86\_64

Scientific Linux Security Update : autofs on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : autofs on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : autofs on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : automake on SL5.x (noarch) (20140916)

Scientific Linux Security Update : automake on SL5.x i386/x86\_64

Scientific Linux Security Update : automake on SL6.x (noarch) (20130221)

Scientific Linux Security Update : avahi on SL5.x i386/x86\_64

Scientific Linux Security Update : avahi on SL5.x i386/x86\_64

Scientific Linux Security Update : avahi on SL5.x i386/x86\_64

Scientific Linux Security Update : avahi on SL6.x i386/x86\_64

Scientific Linux Security Update : axis on SL5.x i386/x86\_64 (20130325)

Scientific Linux Security Update : axis on SL5.x, SL6.x i386/x86\_64 (20140915)

Scientific Linux Security Update : axis on SL6.x (noarch) (20130219)

Scientific Linux Security Update : bash on SL4.x i386/x86\_64

Scientific Linux Security Update : bash on SL5.x i386/x86\_64

Scientific Linux Security Update : bash on SL5.x, SL6.x i386/x86\_64 (20140924) (Shellshock)

Scientific Linux Security Update : bash on SL5.x, SL6.x i386/x86\_64 (20140926) (Shellshock)

Scientific Linux Security Update : bash on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : bash on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : bind for SL 3.0.x on i386/x86\_64

Scientific Linux Security Update : bind for SL 5.x on i386/x86\_64

Scientific Linux Security Update : bind on SL 3.0.x , SL 4.x, SL 5.x

Scientific Linux Security Update : bind on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : bind on SL4.x i386/x86\_64

Scientific Linux Security Update : bind on SL4.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x i386/x86\_64 (20120914)

Scientific Linux Security Update : bind on SL5.x i386/x86\_64 (20150729)

Scientific Linux Security Update : bind on SL5.x i386/x86\_64 (20150903)

Scientific Linux Security Update : bind on SL5.x i386/x86\_64 (20151216)

Scientific Linux Security Update : bind on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : bind on SL5.x, SL6.x i386/x86\_64 (20120607)

Scientific Linux Security Update : bind on SL5.x, SL6.x i386/x86\_64 (20121012)

Scientific Linux Security Update : bind on SL5.x, SL6.x i386/x86\_64 (20161020)

Scientific Linux Security Update : bind on SL5.x, SL6.x i386/x86\_64 (20161102)

Scientific Linux Security Update : bind on SL5.x, SL6.x i386/x86\_64 (20170116)

Scientific Linux Security Update : bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (20141212)

Scientific Linux Security Update : bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160127)

Scientific Linux Security Update : bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160316)

Scientific Linux Security Update : bind on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160928)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20120914)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20121206)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20130328)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20130730)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20140120)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20151216)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20170420)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20170508)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20170705)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20180122)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20180827)

Scientific Linux Security Update : bind on SL6.x i386/x86\_64 (20190617)

Scientific Linux Security Update : bind on SL6.x, SL7.x i386/x86\_64 (20150311)

Scientific Linux Security Update : bind on SL6.x, SL7.x i386/x86\_64 (20150729)

Scientific Linux Security Update : bind on SL6.x, SL7.x i386/x86\_64 (20150903)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20150720)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20170116)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20170215)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20170419)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20170705)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20180122)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20180827)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20190129)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20190529)

Scientific Linux Security Update : bind on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : bind security for SL 4.x on i386/x86\_64

Scientific Linux Security Update : bind-dyndb-ldap on SL6.x i386/x86\_64 (20120521)

Scientific Linux Security Update : bind-dyndb-ldap on SL6.x i386/x86\_64 (20120803)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20120607)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20120914)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20121012)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20130328)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20130730)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20140916)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20141212)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20150729)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20150903)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20151216)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20160127)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20160928)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20161020)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20161102)

Scientific Linux Security Update : bind97 on SL5.x i386/x86\_64 (20170116)

Scientific Linux Security Update : binutils on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : binutils on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : binutils on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : blktrace on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : bluez on SL6.x, SL7.x i386/x86\_64 (20170912) (BlueBorne)

Scientific Linux Security Update : bluez-libs and bluez-utils on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : bluez-utils on SL4.x i386/x86\_64

Scientific Linux Security Update : boost on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : boost on SL5.x, SL6.x i386/x86\_64 (20130321)

Scientific Linux Security Update : brltty on SL5.x i386/x86\_64

Scientific Linux Security Update : busybox on SL4.x i386/x86\_64

Scientific Linux Security Update : busybox on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : busybox on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : busybox on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : bzip2 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : bzip2 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : bzip2 on SL6.x i386/x86\_64

Scientific Linux Security Update : ca-certificates on SL6.x

Scientific Linux Security Update : ca-certificates on SL6.x (noarch) (20131220)

Scientific Linux Security Update : caching-nameserver on SL3.x i386/x86\_64

Scientific Linux Security Update : cairo on SL5.x i386/x86\_64

Scientific Linux Security Update : ccid on SL5.x i386/x86\_64 (20130930)

Scientific Linux Security Update : ccid on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : ccs on SL4.x i386/x86\_64

Scientific Linux Security Update : chrony on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : cifs-utils on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : cloud-init on SL7.x (x86\_64) (20190318)

Scientific Linux Security Update : clutter on SL7.x x86\_64 (20150727)

Scientific Linux Security Update : cman on SL5.x i386/x86\_64

Scientific Linux Security Update : cockpit on SL7.x x86\_64 (20190313)

Scientific Linux Security Update : compat-libtiff3 on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : compiz on SL5.x i386/x86\_64

Scientific Linux Security Update : conga on SL4.x i386/x86\_64

Scientific Linux Security Update : conga on SL5.x i386/x86\_64

Scientific Linux Security Update : conga on SL5.x i386/x86\_64

Scientific Linux Security Update : conga on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : conga on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : conga on SL5.x i386/x86\_64 (20140916)

Scientific Linux Security Update : coolkey on SL5.x i386/x86\_64

Scientific Linux Security Update : Core X11 clients on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : coreutils on SL4.x i386/x86\_64

Scientific Linux Security Update : coreutils on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : coreutils on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : corosync on SL7.x x86\_64 (20180417)

Scientific Linux Security Update : cpio on on SL4 i386/x86\_64

Scientific Linux Security Update : cpio on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cpio on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : cpuspeed on SL5.x i386/x86\_64

Scientific Linux Security Update : cscope on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL3.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL4.x i386/x86\_64

Scientific Linux Security Update : cups on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL5.x i386/x86\_64

Scientific Linux Security Update : cups on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : cups on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : cups on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : cups on SL5.x, SL6.x i386/x86\_64 (20130228)

Scientific Linux Security Update : cups on SL6.x i386/x86\_64

Scientific Linux Security Update : cups on SL6.x i386/x86\_64

Scientific Linux Security Update : cups on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : cups on SL6.x, SL7.x i386/x86\_64 (20150617)

Scientific Linux Security Update : cups-filters on SL7.x x86\_64 (20141103)

Scientific Linux Security Update : cups-filters on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : curl and nss-pem on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : curl on SL3.x i386/x86\_64

Scientific Linux Security Update : curl on SL3.x i386/x86\_64

Scientific Linux Security Update : curl on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : curl on SL4.x i386/x86\_64

Scientific Linux Security Update : curl on SL4.x i386/x86\_64

Scientific Linux Security Update : curl on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : curl on SL5.x i386/x86\_64

Scientific Linux Security Update : curl on SL5.x i386/x86\_64

Scientific Linux Security Update : curl on SL5.x, SL6.x i386/srpm/x86\_64 (20130625)

Scientific Linux Security Update : curl on SL5.x, SL6.x i386/x86\_64 (20130424)

Scientific Linux Security Update : curl on SL6.x i386/x86\_64 (20140527)

Scientific Linux Security Update : curl on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : curl on SL6.x i386/x86\_64 (20170329)

Scientific Linux Security Update : curl on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : curl on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : curl on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : curl on SL7.x x86\_64 (20171127)

Scientific Linux Security Update : curl on SL7.x x86\_64 (20190729)

Scientific Linux Security Update : curl on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : cvs on SL5.x, SL6.x i386/x86\_64 (20120221)

Scientific Linux Security Update : cvs on SL6.x i386/x86\_64

Scientific Linux Security Update : cyrus-imapd on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cyrus-imapd on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : cyrus-imapd on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : cyrus-imapd on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : cyrus-imapd on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : cyrus-sasl on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : dbus on SL5.x i386/x86\_64

Scientific Linux Security Update : dbus on SL5.x i386/x86\_64

Scientific Linux Security Update : dbus on SL5.x i386/x86\_64

Scientific Linux Security Update : dbus on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : dbus on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : dbus on SL6.x i386/x86\_64 (20120913)

Scientific Linux Security Update : dbus on SL6.x i386/x86\_64 (20190710)

Scientific Linux Security Update : dbus-glib on SL5.x i386/x86\_64

Scientific Linux Security Update : dbus-glib on SL5.x, SL6.x i386/x86\_64 (20130226)

Scientific Linux Security Update : device-mapper-multipath on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : dhcp on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : dhcp on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : dhcp on SL4.x,SL5.x,SL6.x i386/x86\_64

Scientific Linux Security Update : dhcp on SL5.x i386/x86\_64 (20120803)

Scientific Linux Security Update : dhcp on SL6.x i386/x86\_64

Scientific Linux Security Update : dhcp on SL6.x i386/x86\_64

Scientific Linux Security Update : dhcp on SL6.x i386/x86\_64 (20120803)

Scientific Linux Security Update : dhcp on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : dhcp on SL6.x i386/x86\_64 (20180308)

Scientific Linux Security Update : dhcp on SL6.x i386/x86\_64 (20180515)

Scientific Linux Security Update : dhcp on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : dhcp on SL7.x x86\_64 (20180125)

Scientific Linux Security Update : dhcp on SL7.x x86\_64 (20180312)

Scientific Linux Security Update : dhcp on SL7.x x86\_64 (20180515)

Scientific Linux Security Update : dhcp on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : dnsmasq on SL5.x i386/x86\_64

Scientific Linux Security Update : dnsmasq on SL5.x i386/x86\_64

Scientific Linux Security Update : dnsmasq on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : dnsmasq on SL6.x i386/x86\_64 (20171002)

Scientific Linux Security Update : dnsmasq on SL7.x x86\_64 (20171002)

Scientific Linux Security Update : dovecot on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : dovecot on SL5.x i386/x86\_64

Scientific Linux Security Update : dovecot on SL5.x i386/x86\_64

Scientific Linux Security Update : dovecot on SL6.x i386/srpm/x86\_64 (20140625)

Scientific Linux Security Update : dovecot on SL6.x i386/x86\_64

Scientific Linux Security Update : dovecot on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : dovecot on SL6.x i386/x86\_64 (20190923)

Scientific Linux Security Update : dovecot on SL7.x x86\_64 (20190920)

Scientific Linux Security Update : dracut on SL6.x (noarch) (20131121)

Scientific Linux Security Update : dstat on SL5.x i386/x86\_64

Scientific Linux Security Update : e2fsprogs on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : eclipse on SL6.x i386/x86\_64

Scientific Linux Security Update : ecryptfs-utils on SL5.x i386/x86\_64

Scientific Linux Security Update : ecryptfs-utils on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : ed on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : elfutils on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : elinks on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : elinks on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : elinks on SL5.x, SL6.x i386/x86\_64 (20130211)

Scientific Linux Security Update : emacs on SL7.x x86\_64 (20170919)

Scientific Linux Security Update : enscript on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : evince on SL6.x i386/x86\_64

Scientific Linux Security Update : evince on SL7.x x86\_64 (20170802)

Scientific Linux Security Update : evolution and evolution-data-server on SL4.x i386/x86\_64

Scientific Linux Security Update : evolution on SL3.x i386/x86\_64

Scientific Linux Security Update : evolution on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : evolution on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : evolution on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : evolution on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : evolution on SL5.x i386/x86\_64

Scientific Linux Security Update : evolution on SL5.x i386/x86\_64

Scientific Linux Security Update : evolution on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : evolution on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : evolution-data-server on SL5.x i386/x86\_64

Scientific Linux Security Update : evolution-data-server on SL5.x i386/x86\_64

Scientific Linux Security Update : evolution28 on SL4.6 i386/x86\_64

Scientific Linux Security Update : evolution28-pango on SL4.x i386/x86\_64

Scientific Linux Security Update : exempi on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : exim on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : exim on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : exiv2 on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : expat on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : expat on SL5.x, SL6.x i386/x86\_64 (20120613)

Scientific Linux Security Update : expat on SL6.x, SL7.x i386/x86\_64 (20161128)

Scientific Linux Security Update : fence on SL4.x i386/x86\_64

Scientific Linux Security Update : fence-agents on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : fetchmail on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : fetchmail on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : file on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : file on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : file on SL6.x i386/x86\_64 (20160510)

Scientific Linux Security Update : file on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : firefox on SL 5.2 i386/x86\_64

Scientific Linux Security Update : firefox on SL3.x i386/x86\_64

Scientific Linux Security Update : firefox on SL3.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x i386/x86\_64 (20120216)

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL4.x, SL5.x, SL6.x i386/x86\_64 (20120131)

Scientific Linux Security Update : firefox on SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/srpm/x86\_64 (20130917)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20120314)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20120424)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20120605)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20120717)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20120829)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20121009)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20121120)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20130108)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20130219)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20130402)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20130514)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20130625)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20130807)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20131029)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20131211)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20140204)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20140318)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20140429)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20140610)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20140722)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20140903)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20151216)

Scientific Linux Security Update : firefox on SL5.x, SL6.x i386/x86\_64 (20170308)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20141015)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20141202)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150113)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150225)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150324)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150401)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150512)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150703)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150807)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150811)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150827)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150922)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20151104)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160127)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160216)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160309)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160426)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160608)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160803)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160921)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161116)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161201)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161214)

Scientific Linux Security Update : firefox on SL5.x, SL6.x, SL7.x i386/x86\_64 (20170125)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20170420)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20180315)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20180410)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20180515)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20180628)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20180912)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20180927)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20181008)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20181025)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20181217)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190130)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190219)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190320)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190327)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190523)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190626)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190711)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20190910)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20191031)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20191205)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20200113)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20200217)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20200316)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20200407)

Scientific Linux Security Update : firefox on SL6.x i386/x86\_64 (20200414)

Scientific Linux Security Update : firefox on SL6.x, SL7.x i386/x86\_64 (20170614)

Scientific Linux Security Update : firefox on SL6.x, SL7.x i386/x86\_64 (20170815)

Scientific Linux Security Update : firefox on SL6.x, SL7.x i386/x86\_64 (20170929)

Scientific Linux Security Update : firefox on SL6.x, SL7.x i386/x86\_64 (20171117)

Scientific Linux Security Update : firefox on SL6.x, SL7.x i386/x86\_64 (20171205)

Scientific Linux Security Update : firefox on SL6.x, SL7.x i386/x86\_64 (20180124)

Scientific Linux Security Update : firefox on SL6.x, SL7.x i386/x86\_64 (20180319)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20170308)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20170317)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20170420)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20180315)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20180515)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20180628)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20180912)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20180927)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20181008)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20181025)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20181217)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190130)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190221)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190320)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190327)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190524)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190626)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190711)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20190911)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20191023)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20191205)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20200113)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20200217)

Scientific Linux Security Update : firefox on SL7.x x86\_64 (20200316)

Scientific Linux Security Update : firewalld on SL7.x (noarch) (20161103)

Scientific Linux Security Update : flac on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : flac on SL6.x, SL7.x i386/x86\_64 (20150401)

Scientific Linux Security Update : flatpak on SL7.x x86\_64 (20180925)

Scientific Linux Security Update : flatpak on SL7.x x86\_64 (20190221)

Scientific Linux Security Update : flatpak on SL7.x x86\_64 (20190508)

Scientific Linux Security Update : fontconfig on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : foomatic on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : foomatic on SL6.x i386/x86\_64

Scientific Linux Security Update : foomatic on SL6.x i386/x86\_64 (20160323)

Scientific Linux Security Update : freeradius on SL3.0.x , SL4.x, SL5.x

Scientific Linux Security Update : freeradius on SL5.x i386/x86\_64

Scientific Linux Security Update : freeradius on SL6.x i386/x86\_64 (20121002)

Scientific Linux Security Update : freeradius on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : freeradius on SL6.x i386/x86\_64 (20170718)

Scientific Linux Security Update : freeradius on SL7.x x86\_64 (20170628)

Scientific Linux Security Update : freeradius on SL7.x x86\_64 (20170802)

Scientific Linux Security Update : freeradius on SL7.x x86\_64 (20190509)

Scientific Linux Security Update : freeradius2 on SL5.x i386/x86\_64 (20121002)

Scientific Linux Security Update : freeradius2 on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : freerdp and vinagre on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : freerdp on SL7.x x86\_64 (20190402)

Scientific Linux Security Update : freetype for SL4 , SL5

Scientific Linux Security Update : freetype on SL3

Scientific Linux Security Update : freetype on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : freetype on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : freetype on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : freetype on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : freetype on SL4.x i386/x86\_64

Scientific Linux Security Update : freetype on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : freetype on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : freetype on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : freetype on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : freetype on SL5.x, SL6.x i386/x86\_64 (20120410)

Scientific Linux Security Update : freetype on SL5.x, SL6.x i386/x86\_64 (20130131)

Scientific Linux Security Update : freetype on SL6.x i386/x86\_64

Scientific Linux Security Update : freetype on SL6.x i386/x86\_64

Scientific Linux Security Update : freetype on SL6.x i386/x86\_64 (20191217)

Scientific Linux Security Update : freetype on SL6.x, SL7.x i386/x86\_64 (20150318)

Scientific Linux Security Update : fribidi on SL7.x x86\_64 (20191219)

Scientific Linux Security Update : frysk on SL4.x i386/x86\_64

Scientific Linux Security Update : fuse on SL6.x i386/x86\_64

Scientific Linux Security Update : fuse on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : gc on SL6.x i386/x86\_64 (20131104)

Scientific Linux Security Update : gcab on SL7.x x86\_64 (20180226)

Scientific Linux Security Update : gcc and gcc4 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : gcc on SL3.x i386/x86\_64

Scientific Linux Security Update : gcc on SL4 i386/x86\_64

Scientific Linux Security Update : gcc on SL5.x i386/x86\_64

Scientific Linux Security Update : gcc on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : gd on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : gd on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : gdb on SL3.x i386/x86\_64

Scientific Linux Security Update : gdb on SL4 i386/x86\_64

Scientific Linux Security Update : gdb on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : gdm and gnome-session on SL7.x x86\_64 (20170802)

Scientific Linux Security Update : gdm on SL4 i386/x86\_64

Scientific Linux Security Update : gdm on SL4.x i386/x86\_64

Scientific Linux Security Update : gdm on SL5.x i386/srpm/x86\_64 (20130905)

Scientific Linux Security Update : gdm on SL5.x i386/x86\_64

Scientific Linux Security Update : gdm on SL5.x i386/x86\_64

Scientific Linux Security Update : gdm on SL6.x i386/x86\_64

Scientific Linux Security Update : gegl on SL6.x i386/x86\_64 (20121112)

Scientific Linux Security Update : GFS on SL3.x i386/x86\_64

Scientific Linux Security Update : GFS on SL3.x i386/x86\_64

Scientific Linux Security Update : gfs-kmod on SL 5.0-5.4 i386/x86\_64

Scientific Linux Security Update : gfs2-utils on SL5.x i386/x86\_64

Scientific Linux Security Update : ghostscript on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ghostscript on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ghostscript on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ghostscript on SL4.x i386/x86\_64 (20120202)

Scientific Linux Security Update : ghostscript on SL5.x, SL6.x i386/x86\_64 (20120202)

Scientific Linux Security Update : ghostscript on SL5.x, SL6.x i386/x86\_64 (20120911)

Scientific Linux Security Update : ghostscript on SL6.x i386/x86\_64 (20170104)

Scientific Linux Security Update : ghostscript on SL6.x i386/x86\_64 (20181204)

Scientific Linux Security Update : ghostscript on SL6.x, SL7.x i386/x86\_64 (20170512)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20170104)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20170802)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20181016)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20181127)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20181204)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20181217)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20190131)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20190321)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20190507)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20190812)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20190903)

Scientific Linux Security Update : ghostscript on SL7.x x86\_64 (20191114)

Scientific Linux Security Update : giflib on SL5.x i386/x86\_64

Scientific Linux Security Update : gimp on SL4.x i386/x86\_64

Scientific Linux Security Update : gimp on SL5.x i386/x86\_64

Scientific Linux Security Update : gimp on SL5.x i386/x86\_64 (20120820)

Scientific Linux Security Update : gimp on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : gimp on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : gimp on SL5.x, SL6.x i386/x86\_64 (20131203)

Scientific Linux Security Update : gimp on SL6.x i386/x86\_64

Scientific Linux Security Update : gimp on SL6.x i386/x86\_64 (20120820)

Scientific Linux Security Update : gimp on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : git on SL6.x i386/x86\_64

Scientific Linux Security Update : git on SL6.x i386/x86\_64 (20130304)

Scientific Linux Security Update : git on SL6.x i386/x86\_64 (20170817)

Scientific Linux Security Update : git on SL6.x i386/x86\_64 (20200203)

Scientific Linux Security Update : git on SL6.x, SL7.x i386/x86\_64 (20160323)

Scientific Linux Security Update : git on SL7.x x86\_64 (20151208)

Scientific Linux Security Update : git on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : git on SL7.x x86\_64 (20170817)

Scientific Linux Security Update : git on SL7.x x86\_64 (20180620)

Scientific Linux Security Update : git on SL7.x x86\_64 (20181031)

Scientific Linux Security Update : git on SL7.x x86\_64 (20200116)

Scientific Linux Security Update : glib2 on SL5.x i386/x86\_64

Scientific Linux Security Update : glibc on SL4.x i386/x86\_64 (20120213)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20120213)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20120319)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20120718)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20120827)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20130424)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20131008)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20150127) (GHOST)

Scientific Linux Security Update : glibc on SL5.x i386/x86\_64 (20150817)

Scientific Linux Security Update : glibc on SL5.x, SL6.x i386/x86\_64 (20140829)

Scientific Linux Security Update : glibc on SL5.x,SL6.x i386/x86\_64

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20120124)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20120315)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20120718)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20120827)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20150107)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20150421)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20160216)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20170619) (Stack Clash)

Scientific Linux Security Update : glibc on SL6.x i386/x86\_64 (20180619)

Scientific Linux Security Update : glibc on SL6.x, SL7.x i386/x86\_64 (20150127) (GHOST)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20141218)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20160216)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20170619) (Stack Clash)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : glibc on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : glibc on SL7.x x86\_64\_important (20151119)

Scientific Linux Security Update : glusterfs on SL6.x x86\_64 (20181009)

Scientific Linux Security Update : glusterfs on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : GNOME on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : GNOME Shell on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : gnome-screensaver on SL5.x i386/x86\_64

Scientific Linux Security Update : gnome-vfs2 on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : gnome-vfs2 on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : gnupg on SL5.x i386/x86\_64 (20131024)

Scientific Linux Security Update : gnupg on SL5.x i386/x86\_64 (20140108)

Scientific Linux Security Update : gnupg2 on SL5.x i386/x86\_64

Scientific Linux Security Update : gnupg2 on SL5.x, SL6.x i386/x86\_64 (20131024)

Scientific Linux Security Update : gnupg2 on SL6.x i386/x86\_64 (20180712)

Scientific Linux Security Update : gnupg2 on SL7.x x86\_64 (20180712)

Scientific Linux Security Update : gnutls on SL4.x i386/x86\_64

Scientific Linux Security Update : gnutls on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : gnutls on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : gnutls on SL5.x i386/x86\_64

Scientific Linux Security Update : gnutls on SL5.x i386/x86\_64

Scientific Linux Security Update : gnutls on SL5.x i386/x86\_64 (20120327)

Scientific Linux Security Update : gnutls on SL5.x i386/x86\_64 (20140303)

Scientific Linux Security Update : gnutls on SL5.x i386/x86\_64 (20140603)

Scientific Linux Security Update : gnutls on SL5.x, SL6.x i386/srpm/x86\_64 (20130530)

Scientific Linux Security Update : gnutls on SL5.x, SL6.x i386/x86\_64 (20130304)

Scientific Linux Security Update : gnutls on SL6.x i386/x86\_64 (20120327)

Scientific Linux Security Update : gnutls on SL6.x i386/x86\_64 (20140303)

Scientific Linux Security Update : gnutls on SL6.x i386/x86\_64 (20140603)

Scientific Linux Security Update : gnutls on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : gnutls on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : gnutls on SL6.x, SL7.x i386/x86\_64 (20160107) (SLOTH)

Scientific Linux Security Update : gnutls on SL7.x x86\_64 (20141112)

Scientific Linux Security Update : gnutls on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : gnutls on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : golang on (20170801)

Scientific Linux Security Update : golang on SL7.x (noarch) (20180410)

Scientific Linux Security Update : golang on SL7.x x86\_64 (20160803) (httpoxy)

Scientific Linux Security Update : gpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : gpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : gpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : gpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : gpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : gpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : gpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : GPG-RPM key on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : graphite2 on SL7.x x86\_64 (20160406)

Scientific Linux Security Update : graphite2 on SL7.x x86\_64 (20170721)

Scientific Linux Security Update : graphviz on SL5.x i386/x86\_64

Scientific Linux Security Update : grep on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : grep on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : groovy on SL7.x (noarch) (20170817)

Scientific Linux Security Update : grub2 on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : grub2 on SL7.x x86\_64 (20151215)

Scientific Linux Security Update : GStreamer on SL7.x x86\_64 (20170802)

Scientific Linux Security Update : gstreamer-plugins on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : gstreamer-plugins on SL4.x i386/x86\_64

Scientific Linux Security Update : gstreamer-plugins on SL4.x i386/x86\_64

Scientific Linux Security Update : gstreamer-plugins-bad-free on SL6.x i386/x86\_64 (20161221)

Scientific Linux Security Update : gstreamer-plugins-bad-free on SL7.x x86\_64 (20170105)

Scientific Linux Security Update : gstreamer-plugins-base on SL5.x i386/x86\_64

Scientific Linux Security Update : gstreamer-plugins-good on SL5.x i386/x86\_64

Scientific Linux Security Update : gstreamer-plugins-good on SL5.x i386/x86\_64

Scientific Linux Security Update : gstreamer-plugins-good on SL6.x i386/x86\_64 (20161221)

Scientific Linux Security Update : gstreamer-plugins-good on SL7.x x86\_64 (20170105)

Scientific Linux Security Update : gstreamer1-plugins-bad-free on SL7.x x86\_64 (20170105)

Scientific Linux Security Update : gstreamer1-plugins-good on SL7.x x86\_64 (20170105)

Scientific Linux Security Update : gtk-vnc on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : gtk2 on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : gvfs on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : gzip on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : haproxy on SL6.x i386/x86\_64 (20130528)

Scientific Linux Security Update : haproxy on SL6.x i386/x86\_64 (20130730)

Scientific Linux Security Update : haproxy on SL6.x, SL7.x i386/x86\_64 (20150908)

Scientific Linux Security Update : HelixPlayer on SL4.x i386/x86\_64

Scientific Linux Security Update : HelixPlayer on SL4.x i386/x86\_64

Scientific Linux Security Update : HelixPlayer on SL4.x i386/x86\_64

Scientific Linux Security Update : hivex on SL6.x x86\_64 (20150722)

Scientific Linux Security Update : hivex on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : hplip on SL5.x i386/x86\_64

Scientific Linux Security Update : hplip on SL5.x i386/x86\_64

Scientific Linux Security Update : hplip on SL5.x i386/x86\_64

Scientific Linux Security Update : hplip on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : hplip on SL6.x i386/x86\_64 (20130919)

Scientific Linux Security Update : hplip3 on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : htdig on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : http-parser on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : http-parser on SL7.x x86\_64 (20200304)

Scientific Linux Security Update : httpd on SL3.x i386/x86\_64

Scientific Linux Security Update : httpd on SL3.x i386/x86\_64

Scientific Linux Security Update : httpd on SL3.x i386/x86\_64

Scientific Linux Security Update : httpd on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL4.x i386/x86\_64

Scientific Linux Security Update : httpd on SL4.x i386/x86\_64

Scientific Linux Security Update : httpd on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : httpd on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : httpd on SL5.x

Scientific Linux Security Update : httpd on SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL5.x i386/x86\_64

Scientific Linux Security Update : httpd on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : httpd on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : httpd on SL5.x i386/x86\_64 (20140403)

Scientific Linux Security Update : httpd on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : httpd on SL5.x, SL6.x i386/x86\_64 (20130513)

Scientific Linux Security Update : httpd on SL5.x, SL6.x i386/x86\_64 (20130813)

Scientific Linux Security Update : httpd on SL5.x, SL6.x i386/x86\_64 (20140723)

Scientific Linux Security Update : httpd on SL5.x, SL6.x i386/x86\_64 (20160718) (httpoxy)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20120213)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20140403)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20150824)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20170711)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20170815)

Scientific Linux Security Update : httpd on SL6.x i386/x86\_64 (20171019) (Optionsbleed)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20150824)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20160718) (httpoxy)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20170412)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20170815)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20171011) (Optionsbleed)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20190729)

Scientific Linux Security Update : httpd on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : hypervkvpd on SL5.x i386/x86\_64 (20130509)

Scientific Linux Security Update : ibutils on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : icedtea-web on SL6.x i386/x86\_64

Scientific Linux Security Update : icedtea-web on SL6.x i386/x86\_64

Scientific Linux Security Update : icedtea-web on SL6.x i386/x86\_64 (20120731)

Scientific Linux Security Update : icedtea-web on SL6.x i386/x86\_64 (20121107)

Scientific Linux Security Update : icedtea-web on SL6.x i386/x86\_64 (20130417)

Scientific Linux Security Update : icedtea-web on SL6.x i386/x86\_64 (20160510)

Scientific Linux Security Update : icoutils on SL7.x x86\_64 (20170322)

Scientific Linux Security Update : icu on SL5.x i386/x86\_64

Scientific Linux Security Update : icu on SL5.x i386/x86\_64

Scientific Linux Security Update : icu on SL5.x i386/x86\_64

Scientific Linux Security Update : icu on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : icu on SL6.x i386/x86\_64 (20200318)

Scientific Linux Security Update : icu on SL7.x x86\_64 (20200318)

Scientific Linux Security Update : ImageMagick on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ImageMagick on SL4.x i386/x86\_64

Scientific Linux Security Update : ImageMagick on SL5.x i386/x86\_64

Scientific Linux Security Update : ImageMagick on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : ImageMagick on SL5.x i386/x86\_64 (20120507)

Scientific Linux Security Update : ImageMagick on SL6.x i386/x86\_64 (20120507)

Scientific Linux Security Update : ImageMagick on SL6.x, SL7.x i386/x86\_64 (20160509) (ImageTragick)

Scientific Linux Security Update : ImageMagick on SL6.x, SL7.x i386/x86\_64 (20160617)

Scientific Linux Security Update : imap on SL3.x i386/x86\_64

Scientific Linux Security Update : Important: 389-Ds-Base Security Update on SL7.x srpm/x86\_64

Scientific Linux Security Update : Important: kernel on SL6.x i386/x86\_64 (20161025) (Dirty COW)

Scientific Linux Security Update : Important: OpenAFS on SL6.x, SL7.x i386/x86\_64 (20191023)

Scientific Linux Security Update : initscripts on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : ipa and slapi-nis on SL7.x x86\_64 (20150326)

Scientific Linux Security Update : ipa on SL6.x i386/x86\_64

Scientific Linux Security Update : ipa on SL6.x i386/x86\_64 (20130123)

Scientific Linux Security Update : ipa on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : ipa on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : ipa on SL6.x, SL7.x i386/x86\_64 (20160901)

Scientific Linux Security Update : ipa on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : ipa on SL7.x x86\_64 (20170102)

Scientific Linux Security Update : ipa on SL7.x x86\_64 (20170302)

Scientific Linux Security Update : ipa on SL7.x x86\_64 (20200205)

Scientific Linux Security Update : ipa-client on SL5.x i386/x86\_64 (20130123)

Scientific Linux Security Update : ipmitool on SL6.x i386/x86\_64

Scientific Linux Security Update : ipmitool on SL6.x i386/x86\_64 (20200406)

Scientific Linux Security Update : ipmitool on SL7.x x86\_64 (20200327)

Scientific Linux Security Update : ipsec-tools on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ipsec-tools on SL5.x i386/x86\_64

Scientific Linux Security Update : ipsec-tools on SL5.x i386/x86\_64

Scientific Linux Security Update : ipw3945 on SL5.x i386/x86\_64

Scientific Linux Security Update : iscsi-initiator-utils on SL5.x i386/x86\_64

Scientific Linux Security Update : jakarta-commons-collections on SL5.x i386/x86\_64 (20151221)

Scientific Linux Security Update : jakarta-commons-collections on SL6.x (noarch) (20151130)

Scientific Linux Security Update : jakarta-commons-httpclient on SL5.x, SL6.x i386/x86\_64 (20130219)

Scientific Linux Security Update : jasper on SL6.x i386/x86\_64

Scientific Linux Security Update : jasper on SL6.x, SL7.x i386/x86\_64 (20141218)

Scientific Linux Security Update : jasper on SL6.x, SL7.x i386/x86\_64 (20150122)

Scientific Linux Security Update : jasper on SL6.x, SL7.x i386/x86\_64 (20170509)

Scientific Linux Security Update : jasper on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : java (jdk 1.5.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java (jdk 1.6.0) on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.3 i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64 (20120613)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64 (20120903)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64 (20121017) (ROBOT)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64 (20130208)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x i386/x86\_64 (20130306)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x i386/srpm/x86\_64 (20140721)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20130424)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20130703)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20131105)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20140127)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20140416)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x i386/x86\_64 (BEAST)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/srpm/x86\_64 (20150415)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20141015)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150126) (POODLE)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150730) (Bar Mitzvah) (Logjam)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20151118)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160126)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160509)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160826)

Scientific Linux Security Update : java-1.6.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20170113)

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64 (20120214)

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64 (20120613)

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64 (20120903)

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64 (20121017) (ROBOT)

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64 (20130208)

Scientific Linux Security Update : java-1.6.0-openjdk on SL6.x i386/x86\_64 (20130306)

Scientific Linux Security Update : java-1.6.0-sun on SL4.x, SL5.x i386/x86\_64 (20120216)

Scientific Linux Security Update : java-1.6.0-sun on SL5.x i386/x86\_64 (20120613)

Scientific Linux Security Update : java-1.6.0-sun on SL5.x i386/x86\_64 (20120904)

Scientific Linux Security Update : java-1.6.0-sun on SL5.x i386/x86\_64 (20121018) (ROBOT)

Scientific Linux Security Update : java-1.6.0-sun on SL5.x i386/x86\_64 (BEAST)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20130306)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20130417)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20130620)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20131021)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20140115)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20140416)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20140716)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20141015)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20150121) (POODLE)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20150415)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20150715) (Bar Mitzvah) (Logjam)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x i386/x86\_64 (20151021)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20130116)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20130208)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL6.x i386/x86\_64 (20161107)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160727)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL6.x, SL7.x i386/x86\_64 (20170213)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL7.x i386/x86\_64 (20160121) (SLOTH)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL7.x i386/x86\_64 (20160325)

Scientific Linux Security Update : java-1.7.0-openjdk on SL5.x, SL7.x i386/x86\_64 (20160421)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20120903)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20121017) (ROBOT)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20130306)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20130417)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20130620)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20131022)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20140115)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20140416)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20140716)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20160121) (SLOTH)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20160325)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20160421)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20180430)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20180521) (Spectre)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20180730)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20181031)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20190305)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20190422)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20190723)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20191022)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x i386/x86\_64 (20200227)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/srpm/x86\_64 (20150415)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20141015)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20150121) (POODLE)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20150715) (Bar Mitzvah) (Logjam)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20151021)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20170509)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20170807)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20171206)

Scientific Linux Security Update : java-1.7.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20180226)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20180502)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20180730)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20190305)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20190422)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20190724)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20191022)

Scientific Linux Security Update : java-1.7.0-openjdk on SL7.x x86\_64 (20200218)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20141015)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20150121) (POODLE)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20160120) (SLOTH)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20160325)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20160420)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20170421)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20180419)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20180723)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20181018)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20190226)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20190417)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20190722)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20191018)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x i386/x86\_64 (20200121)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/srpm/x86\_64 (20150415)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20150715) (Bar Mitzvah) (Logjam)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20151021)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20160720)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20161019)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20170120)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20170720)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20171020)

Scientific Linux Security Update : java-1.8.0-openjdk on SL6.x, SL7.x i386/x86\_64 (20180117)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20160120) (SLOTH)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20160325)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20160420)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20170421)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20180419)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20180723)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20181018)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20190228)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20190417)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20190722)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20191016)

Scientific Linux Security Update : java-1.8.0-openjdk on SL7.x x86\_64 (20200122)

Scientific Linux Security Update : java-11-openjdk on SL7.x x86\_64 (20181107)

Scientific Linux Security Update : java-11-openjdk on SL7.x x86\_64 (20190228)

Scientific Linux Security Update : java-11-openjdk on SL7.x x86\_64 (20190417)

Scientific Linux Security Update : java-11-openjdk on SL7.x x86\_64 (20190722)

Scientific Linux Security Update : java-11-openjdk on SL7.x x86\_64 (20191016)

Scientific Linux Security Update : java-11-openjdk on SL7.x x86\_64 (20200116)

Scientific Linux Security Update : jdk (java) on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : jdk (java) on SL5.x i386/x86\_64

Scientific Linux Security Update : jdk-1.6.0 on SL 5.0 - 5.8 (i386 x86\_64) (20130205)

Scientific Linux Security Update : jss on SL7.x x86\_64 (20191016)

Scientific Linux Security Update : kde-workspace on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : kdebase on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : kdebase on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : kdebase on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL4.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL4.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL5.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : kdegraphics on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : kdelibs and kde-settings on SL7.x x86\_64 (20190903)

Scientific Linux Security Update : kdelibs and kdelibs3 on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : kdelibs on SL3.x i386/x86\_64

Scientific Linux Security Update : kdelibs on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : kdelibs on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : kdelibs on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : kdelibs on SL6.x i386/x86\_64

Scientific Linux Security Update : kdelibs on SL6.x i386/x86\_64

Scientific Linux Security Update : kdelibs on SL6.x i386/x86\_64 (20121030)

Scientific Linux Security Update : kdelibs on SL7.x x86\_64 (20170522)

Scientific Linux Security Update : kdenetwork on SL6.x i386/x86\_64

Scientific Linux Security Update : kdenetwork on SL7.x x86\_64 (20141111)

Scientific Linux Security Update : keepalived on SL7.x x86\_64 (20190103)

Scientific Linux Security Update : keepalived on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : kernel for SL 5.x on i386/x86\_64

Scientific Linux Security Update : kernel on SL 5.0-5.4 i386/x86\_64

Scientific Linux Security Update : kernel on SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL4.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20120110)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20120209)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20120417)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20120529)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20120612)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20120710)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20120821)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20121002)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20121113)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20121204)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130122)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130305)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130311)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130416)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130521)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130710)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130820)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20130926)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20131022)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20131205)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20140129)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20140312)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20140424)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20140610)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20140723)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20140903)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20141204)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20141217)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20150210)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20150407)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20150602)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20160119)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20160315)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20161028) (Dirty COW)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20161220)

Scientific Linux Security Update : kernel on SL5.x i386/x86\_64 (20170224)

Scientific Linux Security Update : kernel on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/srpm/x86\_64 (20131016)

Scientific Linux Security Update : kernel on SL6.x i386/srpm/x86\_64 (20150127)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120123)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120306)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120417)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120515)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120618)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120710)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120814)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20120925)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20121016)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20121106)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20121218)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20130205)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20130312)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20130423)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20130516)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20130610)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20130716)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20130827)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20131212)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20140211)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20140325)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20140507)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20140619)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20140723)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20140909)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20141216)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20150311)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20150421)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20150609)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20150714)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20150813)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20151215)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20160323)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20160504)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20160510)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20160712)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20160823)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20161004)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20161115)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170110)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170222)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170223)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170411)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170531)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170619) (Stack Clash)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170711)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170912) (BlueBorne)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20170926)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20171006)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20171115)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180103) (Meltdown) (Spectre)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180125)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180313) (Meltdown) (Spectre)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180508) (Meltdown)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180619) (Spectre)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180710) (Spectre)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20180814) (Foreshadow)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20181009)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20190226)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20190409)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20190514) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20190617) (SACK Panic) (SACK Slowness)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20190813)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20190912)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20190923)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20191113)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20191114)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20191217)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (20200311)

Scientific Linux Security Update : kernel on SL6.x i386/x86\_64 (SACK Panic) (SACK Slowness)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20141028)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20141209)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20150128)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20150512)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20150623)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20150805)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20150915)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20151103)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20151208)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20160125)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20160216)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20160512)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20160623)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20160802)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20160818)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20160915)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20161010)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20161024) (Dirty COW)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170117)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170222)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170302)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170412)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170525)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170619) (Stack Clash)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170628)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170815)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20170912) (BlueBorne)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20171019)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20171130)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180103) (Meltdown) (Spectre)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180125) (Meltdown) (Spectre)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180306)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180410) (Meltdown)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180508)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180614)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180626) (Spectre)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180814) (Foreshadow)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20180925)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20181127)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190129)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190314)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190423)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190514) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190617) (SACK Panic) (SACK Slowness)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190729)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190903)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20190920)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20191016)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20191113)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20191114)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20191205)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20200205)

Scientific Linux Security Update : kernel on SL7.x x86\_64 (20200317)

Scientific Linux Security Update : kexec-tools on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : kexec-tools on SL6.x i386/x86\_64

Scientific Linux Security Update : kexec-tools on SL7.x x86\_64 (20150512)

Scientific Linux Security Update : keycloak-httpd-client-install on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : krb5 on SL3.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL3.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL5.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : krb5 on SL5.x i386/x86\_64 (20140916)

Scientific Linux Security Update : krb5 on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL5.x, SL6.x i386/x86\_64 (20130612)

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64 (20120731)

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64 (20130318)

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64 (20130416)

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64 (20150409)

Scientific Linux Security Update : krb5 on SL6.x i386/x86\_64 (20160323)

Scientific Linux Security Update : krb5 on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : krb5 on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : krb5 on SL7.x x86\_64 (20160404)

Scientific Linux Security Update : krb5 on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : krb5 on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : krb5 on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : krb5-appl on SL6.x i386/x86\_64

Scientific Linux Security Update : krb5-appl on SL6.x i386/x86\_64

Scientific Linux Security Update : krb5-appl on SL6.x i386/x86\_64 (20200407)

Scientific Linux Security Update : ksh on SL6.x i386/x86\_64 (20200217)

Scientific Linux Security Update : ksh on SL7.x x86\_64 (20200224)

Scientific Linux Security Update : kvm on SL 5.4 x86\_64

Scientific Linux Security Update : kvm on SL5.4 i386/x86\_64

Scientific Linux Security Update : kvm on SL5.4 x86\_64

Scientific Linux Security Update : kvm on SL5.4 x86\_64

Scientific Linux Security Update : kvm on SL5.x x86\_64

Scientific Linux Security Update : kvm on SL5.x x86\_64

Scientific Linux Security Update : kvm on SL5.x x86\_64

Scientific Linux Security Update : kvm on SL5.x x86\_64

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20120123)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20120221)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20120521)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20120905)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20130307)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20130409)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20140212)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20150422)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20150513) (Venom)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20150625)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20151022)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20160927)

Scientific Linux Security Update : kvm on SL5.x x86\_64 (20170307)

Scientific Linux Security Update : lcms on SL5.x i386/x86\_64

Scientific Linux Security Update : lcms on SL5.x i386/x86\_64

Scientific Linux Security Update : lftp for SL 5

Scientific Linux Security Update : lftp on SL5.x i386/x86\_64

Scientific Linux Security Update : libarchive on SL6.x i386/x86\_64

Scientific Linux Security Update : libarchive on SL6.x i386/x86\_64 (20160912)

Scientific Linux Security Update : libarchive on SL7.x x86\_64 (20160912)

Scientific Linux Security Update : libarchive on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libarchive on SL7.x x86\_64 (20200122)

Scientific Linux Security Update : libcap on SL6.x i386/x86\_64

Scientific Linux Security Update : libcdio on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : libcgroup on SL6.x i386/x86\_64

Scientific Linux Security Update : libcgroup on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libexif on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : libexif on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : libexif on SL5.x, SL6.x i386/x86\_64 (20120911)

Scientific Linux Security Update : libgcrypt on SL5.0 - 5.3 i386/x86\_64

Scientific Linux Security Update : libgcrypt on SL5.x, SL6.x i386/x86\_64 (20131024)

Scientific Linux Security Update : libgcrypt on SL6.x i386/x86\_64 (20161108)

Scientific Linux Security Update : libgtop2 on SL4.x i386/x86\_64

Scientific Linux Security Update : libguestfs and virt-p2v on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : libguestfs on SL6.x x86\_64

Scientific Linux Security Update : libguestfs on SL6.x x86\_64 (20120620)

Scientific Linux Security Update : libguestfs on SL6.x x86\_64 (20131121)

Scientific Linux Security Update : libguestfs on SL6.x x86\_64 (20170321)

Scientific Linux Security Update : libguestfs-winsupport on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libjpeg on SL5.x i386/x86\_64 (20131210)

Scientific Linux Security Update : libjpeg-turbo on SL6.x i386/x86\_64 (20131210)

Scientific Linux Security Update : libjpeg-turbo on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libkdcraw on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : libldb on SL6.x, SL7.x i386/x86\_64 (20160107)

Scientific Linux Security Update : liblouis on SL7.x x86\_64 (20171102)

Scientific Linux Security Update : liblouis on SL7.x x86\_64 (20171205)

Scientific Linux Security Update : libmspack on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : libmspack on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libndp on SL7.x x86\_64 (20160517)

Scientific Linux Security Update : libpng on SL3.x i386/x86\_64

Scientific Linux Security Update : libpng on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libpng on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libpng on SL4.x i386/x86\_64

Scientific Linux Security Update : libpng on SL4.x, SL5.x, SL6.x i386/x86\_64 (20120220)

Scientific Linux Security Update : libpng on SL5.x i386/x86\_64

Scientific Linux Security Update : libpng on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : libpng on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : libpng on SL5.x, SL6.x i386/x86\_64 (20120320)

Scientific Linux Security Update : libpng on SL5.x, SL6.x i386/x86\_64 (20120425)

Scientific Linux Security Update : libpng on SL6.x i386/x86\_64

Scientific Linux Security Update : libpng on SL6.x i386/x86\_64 (20151209)

Scientific Linux Security Update : libpng on SL7.x x86\_64 (20151209)

Scientific Linux Security Update : libpng12 on SL7.x x86\_64 (20151209)

Scientific Linux Security Update : libproxy on SL6.x i386/x86\_64 (20121114)

Scientific Linux Security Update : librelp on SL6.x i386/x86\_64 (20180424)

Scientific Linux Security Update : librelp on SL7.x x86\_64 (20180424)

Scientific Linux Security Update : libreoffice on SL6.x i386/x86\_64 (20120801)

Scientific Linux Security Update : libreoffice on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : libreoffice on SL6.x i386/x86\_64 (20151214)

Scientific Linux Security Update : libreoffice on SL6.x i386/x86\_64 (20170418)

Scientific Linux Security Update : libreoffice on SL6.x i386/x86\_64 (20180313)

Scientific Linux Security Update : libreoffice on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : libreoffice on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : libreoffice on SL7.x x86\_64 (20170412)

Scientific Linux Security Update : libreoffice on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : libreoffice on SL7.x x86\_64 (20180306)

Scientific Linux Security Update : libreoffice on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : libreoffice on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libreport on SL6.x i386/x86\_64 (20151123)

Scientific Linux Security Update : libreswan on SL7.x x86\_64 (20150623)

Scientific Linux Security Update : libreswan on SL7.x x86\_64 (20151104)

Scientific Linux Security Update : libreswan on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : librsvg2 on SL6.x i386/x86\_64

Scientific Linux Security Update : librsvg2 on SL6.x i386/x86\_64 (20140203)

Scientific Linux Security Update : libsndfile on SL6.x i386/x86\_64

Scientific Linux Security Update : libsolv on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libsoup on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libsoup on SL6.x i386/x86\_64

Scientific Linux Security Update : libsoup on SL7.x x86\_64 (20170815)

Scientific Linux Security Update : libssh2 on SL6.x i386/x86\_64 (20190702)

Scientific Linux Security Update : libssh2 on SL6.x, SL7.x i386/x86\_64 (20160310)

Scientific Linux Security Update : libssh2 on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : libssh2 on SL7.x x86\_64 (20190328)

Scientific Linux Security Update : libssh2 on SL7.x x86\_64 (20190729)

Scientific Linux Security Update : libssh2 on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libtar on SL6.x i386/x86\_64 (20131010)

Scientific Linux Security Update : libtasn1 on SL6.x i386/x86\_64 (20120327)

Scientific Linux Security Update : libtasn1 on SL6.x i386/x86\_64 (20140603)

Scientific Linux Security Update : libtasn1 on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : libtiff for SL3.0.x, SL 4.x, SL 5.x on i386/x86\_64

Scientific Linux Security Update : libtiff on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libtiff on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libtiff on SL4.x i386/x86\_64

Scientific Linux Security Update : libtiff on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libtiff on SL5.x i386/x86\_64

Scientific Linux Security Update : libtiff on SL5.x i386/x86\_64 (20140227)

Scientific Linux Security Update : libtiff on SL5.x, SL6.x i386/x86\_64 (20120410)

Scientific Linux Security Update : libtiff on SL5.x, SL6.x i386/x86\_64 (20120703)

Scientific Linux Security Update : libtiff on SL5.x, SL6.x i386/x86\_64 (20121218)

Scientific Linux Security Update : libtiff on SL6.x i386/x86\_64

Scientific Linux Security Update : libtiff on SL6.x i386/x86\_64

Scientific Linux Security Update : libtiff on SL6.x i386/x86\_64 (20140227)

Scientific Linux Security Update : libtiff on SL6.x i386/x86\_64 (20160802)

Scientific Linux Security Update : libtiff on SL6.x, SL7.x i386/x86\_64 (20170201)

Scientific Linux Security Update : libtiff on SL7.x x86\_64 (20160802)

Scientific Linux Security Update : libtiff on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libtirpc on SL6.x i386/srpm/x86\_64 (20130530)

Scientific Linux Security Update : libtirpc on SL6.x i386/x86\_64 (20170523)

Scientific Linux Security Update : libtirpc on SL7.x x86\_64 (20170521)

Scientific Linux Security Update : libtool on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libuser on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libuser on SL6.x i386/x86\_64 (20150723)

Scientific Linux Security Update : libuser on SL7.x x86\_64 (20150723)

Scientific Linux Security Update : libvirt on SL5.x i386/x86\_64

Scientific Linux Security Update : libvirt on SL5.x i386/x86\_64

Scientific Linux Security Update : libvirt on SL5.x i386/x86\_64

Scientific Linux Security Update : libvirt on SL5.x i386/x86\_64

Scientific Linux Security Update : libvirt on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : libvirt on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20120823)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20121011)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20130128)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20130516)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20130919)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20140128)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20140527)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20141118)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20180104) (Spectre)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20180619)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20190514) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Scientific Linux Security Update : libvirt on SL6.x i386/x86\_64 (20190620)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20150105)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20180104) (Spectre)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20180515)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20180626) (Spectre)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20190514) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20190523)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20190620)

Scientific Linux Security Update : libvirt on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libvncserver on SL6.x, SL7.x i386/x86\_64 (20141111)

Scientific Linux Security Update : libvncserver on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : libvncserver on SL7.x x86\_64 (20190115)

Scientific Linux Security Update : libvncserver on SL7.x x86\_64 (20200323)

Scientific Linux Security Update : libvorbis on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libvorbis on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libvorbis on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libvorbis on SL4.x, SL5.x, SL6.x i386/x86\_64 (20120215)

Scientific Linux Security Update : libvorbis on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : libvorbis on SL6.x i386/x86\_64 (20180405)

Scientific Linux Security Update : libvorbis on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : libvpx on SL6.x i386/x86\_64

Scientific Linux Security Update : libwmf on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libwmf on SL6.x, SL7.x i386/x86\_64 (20151020)

Scientific Linux Security Update : libwpd on SL5.x i386/x86\_64 (20120626)

Scientific Linux Security Update : libwpd on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : libXfont on SL5.x i386/x86\_64

Scientific Linux Security Update : libXfont on SL5.x i386/x86\_64 (20141124)

Scientific Linux Security Update : libXfont on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : libXfont on SL5.x, SL6.x i386/x86\_64 (20140110)

Scientific Linux Security Update : libXfont on SL6.x, SL7.x i386/srpm/x86\_64 (20141118)

Scientific Linux Security Update : libXfont on SL6.x, SL7.x i386/x86\_64 (20150903)

Scientific Linux Security Update : libxml and libxml2 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libxml2 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libxml2 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libxml2 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libxml2 on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libxml2 on SL4.x i386/x86\_64 (20120111)

Scientific Linux Security Update : libxml2 on SL5.x i386/x86\_64 (20120111)

Scientific Linux Security Update : libxml2 on SL5.x i386/x86\_64 (20141120)

Scientific Linux Security Update : libxml2 on SL5.x, SL6.x i386/x86\_64 (20120221)

Scientific Linux Security Update : libxml2 on SL5.x, SL6.x i386/x86\_64 (20120918)

Scientific Linux Security Update : libxml2 on SL5.x, SL6.x i386/x86\_64 (20121129)

Scientific Linux Security Update : libxml2 on SL5.x, SL6.x i386/x86\_64 (20130228)

Scientific Linux Security Update : libxml2 on SL6.x i386/x86\_64

Scientific Linux Security Update : libxml2 on SL6.x i386/x86\_64 (20120111)

Scientific Linux Security Update : libxml2 on SL6.x i386/x86\_64 (20140519)

Scientific Linux Security Update : libxml2 on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : libxml2 on SL6.x i386/x86\_64 (20151207)

Scientific Linux Security Update : libxml2 on SL6.x, SL7.x i386/x86\_64 (20141016)

Scientific Linux Security Update : libxml2 on SL6.x, SL7.x i386/x86\_64 (20160623)

Scientific Linux Security Update : libxml2 on SL7.x x86\_64 (20150330)

Scientific Linux Security Update : libxml2 on SL7.x x86\_64 (20151207)

Scientific Linux Security Update : libxslt on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libxslt on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : libxslt on SL5.x, SL6.x i386/x86\_64 (20120913)

Scientific Linux Security Update : libyaml on SL6.x, SL7.x i386/x86\_64 (20150128)

Scientific Linux Security Update : linux-firmware on SL7.x (noarch) (20180104) (Spectre)

Scientific Linux Security Update : linux-firmware on SL7.x (noarch) (20180116) (Spectre)

Scientific Linux Security Update : linux-firmware on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : log4j on SL7.x (noarch) (20170807)

Scientific Linux Security Update : logrotate on SL6.x i386/x86\_64

Scientific Linux Security Update : logwatch on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : luci on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : luci on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : lvm2-cluster,lvm2 for SL5

Scientific Linux Security Update : lynx on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : lzo on SL6.x i386/srpm/x86\_64 (20140709)

Scientific Linux Security Update : madwifi on SL5.x i386/x86\_64

Scientific Linux Security Update : madwifi on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : mailman on SL4.x i386/x86\_64

Scientific Linux Security Update : mailman on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : mailman on SL6.x i386/x86\_64

Scientific Linux Security Update : mailman on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : mailman on SL6.x i386/x86\_64 (20180313)

Scientific Linux Security Update : mailman on SL7.x x86\_64 (20150623)

Scientific Linux Security Update : mailman on SL7.x x86\_64 (20180313)

Scientific Linux Security Update : mailx on SL6.x, SL7.x i386/x86\_64 (20141216)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20141117)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20150203)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20150824) (BACKRONYM)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20160404)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20160811)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20180816)

Scientific Linux Security Update : mariadb on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : mcstrans on SL5.x i386/x86\_64

Scientific Linux Security Update : memcached on SL6.x i386/x86\_64 (20161123)

Scientific Linux Security Update : memcached on SL7.x x86\_64 (20161123)

Scientific Linux Security Update : mercurial on SL6.x, SL7.x i386/x86\_64 (20170627)

Scientific Linux Security Update : mercurial on SL7.x x86\_64 (20160502)

Scientific Linux Security Update : mercurial on SL7.x x86\_64 (20170817)

Scientific Linux Security Update : mercurial on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : mesa on SL5.x i386/x86\_64 (20130603)

Scientific Linux Security Update : mesa on SL6.x i386/x86\_64 (20130603)

Scientific Linux Security Update : microcode\_ctl on SL6.x i386/x86\_64 (20180103) (Spectre)

Scientific Linux Security Update : microcode\_ctl on SL6.x, SL7.x i386/x86\_64 (20180116) (Spectre)

Scientific Linux Security Update : microcode\_ctl on SL7.x x86\_64 (20180103) (Spectre)

Scientific Linux Security Update : mikmod on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : mingw32-libxml2 on SL6.x (x86\_64) (20130131)

Scientific Linux Security Update : mod\_auth\_mellon on SL6.x i386/x86\_64 (20141105)

Scientific Linux Security Update : mod\_auth\_mellon on SL7.x x86\_64 (20190416)

Scientific Linux Security Update : mod\_auth\_mysql on SL5.x i386/x86\_64

Scientific Linux Security Update : mod\_auth\_mysql on SL6.x i386/x86\_64

Scientific Linux Security Update : mod\_auth\_openidc on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : mod\_nss on SL5.x, SL6.x i386/x86\_64 (20131203)

Scientific Linux Security Update : mod\_nss on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : mod\_perl on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : mod\_perl on SL6.x i386/x86\_64 (20180924)

Scientific Linux Security Update : mod\_wsgi on SL6.x i386/srpm/x86\_64 (20140625)

Scientific Linux Security Update : Moderate: OpenAFS on SL6.x, SL7.x i386/x86\_64 (20180911)

Scientific Linux Security Update : mutt on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : mutt on SL6.x i386/x86\_64

Scientific Linux Security Update : mutt on SL6.x i386/x86\_64 (20140317)

Scientific Linux Security Update : mutt on SL6.x, SL7.x i386/x86\_64 (20180821)

Scientific Linux Security Update : mysql on SL4.x i386/x86\_64

Scientific Linux Security Update : mysql on SL4.x i386/x86\_64

Scientific Linux Security Update : mysql on SL4.x i386/x86\_64

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64 (20120213)

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : mysql on SL5.x i386/x86\_64 (20130122)

Scientific Linux Security Update : mysql on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : mysql on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20120208)

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20121114)

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20121207)

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20130131)

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20130425)

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20140212)

Scientific Linux Security Update : mysql on SL6.x i386/x86\_64 (20170124)

Scientific Linux Security Update : mysql55-mysql on SL5.x i386/x86\_64 (20140218)

Scientific Linux Security Update : mysql55-mysql on SL5.x i386/x86\_64 (20140522)

Scientific Linux Security Update : mysql55-mysql on SL5.x i386/x86\_64 (20141117)

Scientific Linux Security Update : mysql55-mysql on SL5.x i386/x86\_64 (20150817)

Scientific Linux Security Update : nautilus on SL7.x x86\_64 (20180125)

Scientific Linux Security Update : ndiswrapper on SL5.x i386/x86\_64

Scientific Linux Security Update : ndiswrapper on SL5.x i386/x86\_64

Scientific Linux Security Update : neon on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : net-snmp on SL3.x i386/x86\_64

Scientific Linux Security Update : net-snmp on SL3.x i386/x86\_64

Scientific Linux Security Update : net-snmp on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : net-snmp on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : net-snmp on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : net-snmp on SL5.x i386/x86\_64 (20140324)

Scientific Linux Security Update : net-snmp on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : net-snmp on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : net-snmp on SL6.x i386/x86\_64 (20140324)

Scientific Linux Security Update : net-snmp on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : net-snmp on SL6.x, SL7.x i386/x86\_64 (20150817)

Scientific Linux Security Update : net-snmp on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : netcf on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : netpbm on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : netpbm on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : netpbm on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : nettle on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : NetworkManager and libnl3 on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : NetworkManager on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : NetworkManager on SL5.x i386/x86\_64

Scientific Linux Security Update : NetworkManager on SL6.x i386/x86\_64

Scientific Linux Security Update : NetworkManager on SL6.x i386/x86\_64

Scientific Linux Security Update : NetworkManager on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : NetworkManager on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : NetworkManager on SL7.x x86\_64 (20181127)

Scientific Linux Security Update : newt on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : nfs-utils on SL5.x i386/x86\_64

Scientific Linux Security Update : nfs-utils on SL5.x i386/x86\_64

Scientific Linux Security Update : nfs-utils on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : nfs-utils on SL6.x i386/x86\_64

Scientific Linux Security Update : nfs-utils-lib on SL4.x i386/x86\_64

Scientific Linux Security Update : nfs-utils-lib on SL5.x i386/x86\_64

Scientific Linux Security Update : nspluginwrapper on SL6.x i386/x86\_64 (20121113)

Scientific Linux Security Update : nspr and nss for SL 4.x on i386/x86\_64

Scientific Linux Security Update : nspr and nss for SL 5.x on i386/x86\_64

Scientific Linux Security Update : nss and nspr on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20120717)

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20130131)

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20130805)

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20131205)

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20140722)

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20140916)

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20151104)

Scientific Linux Security Update : nss and nspr on SL5.x i386/x86\_64 (20160425)

Scientific Linux Security Update : nss and nspr on SL6.x i386/x86\_64 (20140722)

Scientific Linux Security Update : nss and nss-util on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161116)

Scientific Linux Security Update : nss and nss-util on SL6.x, SL7.x i386/x86\_64 (20170420)

Scientific Linux Security Update : nss on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : nss on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : nss on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : nss on SL5.x i386/x86\_64 (20150824)

Scientific Linux Security Update : nss on SL5.x i386/x86\_64 (20160309)

Scientific Linux Security Update : nss on SL5.x, SL6.x i386/x86\_64 (20131219)

Scientific Linux Security Update : nss on SL5.x, SL6.x i386/x86\_64 (20140926)

Scientific Linux Security Update : nss on SL6.x i386/x86\_64

Scientific Linux Security Update : nss on SL6.x i386/x86\_64 (20170530)

Scientific Linux Security Update : nss on SL6.x i386/x86\_64 (20181009)

Scientific Linux Security Update : nss on SL6.x, SL7.x i386/x86\_64 (20150625) (Logjam)

Scientific Linux Security Update : nss on SL6.x, SL7.x i386/x86\_64 (20160107) (SLOTH)

Scientific Linux Security Update : nss on SL6.x, SL7.x i386/x86\_64 (20170929)

Scientific Linux Security Update : nss on SL7.x x86\_64 (20170530)

Scientific Linux Security Update : nss on SL7.x x86\_64 (20180925)

Scientific Linux Security Update : nss, nspr, and nss-util on SL6.x i386/x86\_64 (20120717)

Scientific Linux Security Update : nss, nspr, and nss-util on SL6.x i386/x86\_64 (20131212)

Scientific Linux Security Update : nss, nspr, nss-softokn, and nss-util on SL7.x x86\_64 (20160425)

Scientific Linux Security Update : nss, nss-softokn, nss-util on SL7.x x86\_64 (20191210)

Scientific Linux Security Update : nss, nss-softokn, nss-util, and nspr on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : nss, nss-util, and nspr on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : nss, nss-util, and nspr on SL6.x i386/x86\_64 (20130131)

Scientific Linux Security Update : nss, nss-util, and nspr on SL6.x i386/x86\_64 (20160405)

Scientific Linux Security Update : nss, nss-util, and nspr on SL6.x, SL7.x i386/x86\_64 (20151104)

Scientific Linux Security Update : nss, nss-util, and nss-softokn on SL5.x, SL6.x, SL7.x i386/x86\_64 (20141202) (POODLE)

Scientific Linux Security Update : nss, nss-util, nss-softokn, and nspr on SL6.x i386/x86\_64 (20130807)

Scientific Linux Security Update : nss-pam-ldapd on SL6.x i386/x86\_64 (20130304)

Scientific Linux Security Update : nss-softokn on SL6.x i386/x86\_64 (20191210)

Scientific Linux Security Update : nss-softokn on SL6.x, SL7.x i386/x86\_64 (20150901)

Scientific Linux Security Update : nss-util on SL6.x, SL7.x i386/x86\_64 (20160309)

Scientific Linux Security Update : nss-util on SL6.x, SL7.x x86\_64 (20170420)

Scientific Linux Security Update : nss\_db on SL5.x i386/x86\_64

Scientific Linux Security Update : nss\_ldap on SL3.x i386/x86\_64

Scientific Linux Security Update : nss\_ldap on SL4.x i386/x86\_64

Scientific Linux Security Update : nss\_ldap on SL5.x i386/x86\_64

Scientific Linux Security Update : ntp on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ntp on SL4.x i386/x86\_64

Scientific Linux Security Update : ntp on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ntp on SL5.x i386/x86\_64

Scientific Linux Security Update : ntp on SL5.x i386/x86\_64 (20141220)

Scientific Linux Security Update : ntp on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : ntp on SL6.x i386/x86\_64 (20160510)

Scientific Linux Security Update : ntp on SL6.x i386/x86\_64 (20171026)

Scientific Linux Security Update : ntp on SL6.x i386/x86\_64 (20181220)

Scientific Linux Security Update : ntp on SL6.x, SL7.x i386/x86\_64 (20141220)

Scientific Linux Security Update : ntp on SL6.x, SL7.x i386/x86\_64 (20151026)

Scientific Linux Security Update : ntp on SL6.x, SL7.x i386/x86\_64 (20160125)

Scientific Linux Security Update : ntp on SL6.x, SL7.x i386/x86\_64 (20160531)

Scientific Linux Security Update : ntp on SL6.x, SL7.x i386/x86\_64 (20170206)

Scientific Linux Security Update : ntp on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : ntp on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : ntp on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : ntp on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : ocaml on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : ocaml on SL7.x x86\_64 (20160623)

Scientific Linux Security Update : opal on SL5.x i386/x86\_64

Scientific Linux Security Update : openafs on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openafs on SL4.x i386/x86\_64

Scientific Linux Security Update : openafs on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openafs on SL41-45 i386/x86\_64

Scientific Linux Security Update : openafs on SL5.0 i386/x86\_64

Scientific Linux Security Update : openafs on SL5.x i386/x86\_64

Scientific Linux Security Update : openafs on SL5.x i386/x86\_64

Scientific Linux Security Update : openafs on SL5.x i386/x86\_64

Scientific Linux Security Update : openafs on SL5.x SL6.x i386/x86\_64 (20130304)

Scientific Linux Security Update : openafs on SL5.x, SL6.x i386/x86\_64 (20130724)

Scientific Linux Security Update : openafs on SL5.x, SL6.x i386/x86\_64 (20140411)

Scientific Linux Security Update : openafs on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150730)

Scientific Linux Security Update : openafs on SL5.x, SL6.x, SL7.x i386/x86\_64 (20151021)

Scientific Linux Security Update : OpenAFS on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160317)

Scientific Linux Security Update : Openafs Security Update on SL6.x, SL7.x i386/x86\_64 (20171206)

Scientific Linux Security Update : openchange on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : openhpi on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : OpenIPMI on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : openjpeg on SL6.x i386/x86\_64 (20120711)

Scientific Linux Security Update : openjpeg on SL6.x i386/x86\_64 (20120917)

Scientific Linux Security Update : openjpeg on SL6.x i386/x86\_64 (20131217)

Scientific Linux Security Update : openjpeg on SL6.x i386/x86\_64 (20170319)

Scientific Linux Security Update : openjpeg on SL7.x x86\_64 (20170322)

Scientific Linux Security Update : openjpeg2 on SL7.x x86\_64 (20200128)

Scientific Linux Security Update : openjpeg2 on SL7.x x86\_64 (20200219)

Scientific Linux Security Update : openldap on SL3.x i386/x86\_64

Scientific Linux Security Update : openldap on SL4.x i386/x86\_64

Scientific Linux Security Update : openldap on SL4.x i386/x86\_64

Scientific Linux Security Update : openldap on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openldap on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openldap on SL5.x i386/x86\_64

Scientific Linux Security Update : openldap on SL5.x i386/x86\_64

Scientific Linux Security Update : openldap on SL5.x i386/x86\_64

Scientific Linux Security Update : openldap on SL5.x i386/x86\_64

Scientific Linux Security Update : openldap on SL5.x i386/x86\_64 (20140224)

Scientific Linux Security Update : openldap on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150929)

Scientific Linux Security Update : openldap on SL6.x i386/x86\_64

Scientific Linux Security Update : openldap on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : openldap on SL6.x i386/x86\_64 (20120808)

Scientific Linux Security Update : openldap on SL6.x i386/x86\_64 (20140203)

Scientific Linux Security Update : openldap on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : openldap on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : openoffice.org and openoffice.org2 on SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL3.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL3.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL3.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL4.x, i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64 (20120322)

Scientific Linux Security Update : openoffice.org on SL5.x i386/x86\_64 (20120801)

Scientific Linux Security Update : openoffice.org on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : openoffice.org on SL5.x, SL6.x i386/x86\_64 (20120604)

Scientific Linux Security Update : openoffice.org on SL6.x i386/x86\_64

Scientific Linux Security Update : openoffice.org, hsqldb on SL5.x i386/x86\_64

Scientific Linux Security Update : openoffice.org2 on SL4.5 and 4.6 i386/x86\_64

Scientific Linux Security Update : openoffice.org2 on SL4.5 i386/x86\_64

Scientific Linux Security Update : openoffice.org2 on SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org2 on SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org2 on SL4.x i386/x86\_64

Scientific Linux Security Update : openoffice.org2 on SL45, 46, 47 i386/x86\_64

Scientific Linux Security Update : opensc on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : openslp on SL6.x i386/x86\_64 (20180802)

Scientific Linux Security Update : openslp on SL6.x i386/x86\_64 (20200122)

Scientific Linux Security Update : openslp on SL7.x x86\_64 (20180723)

Scientific Linux Security Update : openslp on SL7.x x86\_64 (20191216)

Scientific Linux Security Update : openssh on SL4.x i386/x86\_64

Scientific Linux Security Update : openssh on SL4.x i386/x86\_64

Scientific Linux Security Update : openssh on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openssh on SL5.x

Scientific Linux Security Update : openssh on SL5.x i386/x86\_64

Scientific Linux Security Update : openssh on SL5.x i386/x86\_64

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20160321)

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20160510)

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : openssh on SL6.x i386/x86\_64 (20190409)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20160114)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20160321)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : openssh on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : openssl on SL3.x i386/x86\_64

Scientific Linux Security Update : openssl on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : openssl on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openssl on SL4.x i386/x86\_64

Scientific Linux Security Update : openssl on SL4.x i386/x86\_64 (20120201)

Scientific Linux Security Update : openssl on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20120124)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20140605)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20140813)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20141016) (POODLE)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20150413) (FREAK)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20150630) (Logjam)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20151214)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20160301) (DROWN)

Scientific Linux Security Update : openssl on SL5.x i386/x86\_64 (20160531)

Scientific Linux Security Update : openssl on SL5.x, SL6.x i386/x86\_64 (20120327)

Scientific Linux Security Update : openssl on SL5.x, SL6.x i386/x86\_64 (20120424)

Scientific Linux Security Update : openssl on SL5.x, SL6.x i386/x86\_64 (20120529)

Scientific Linux Security Update : openssl on SL5.x, SL6.x i386/x86\_64 (20130304)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20120124)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20140108)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20140605)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20140813)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20150324)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20151214)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20160510)

Scientific Linux Security Update : openssl on SL6.x i386/x86\_64 (20190813)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20141016) (POODLE)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20150121) (FREAK)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20150604) (Logjam)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20150615)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20160107) (SLOTH)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20160301) (DROWN)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20160927)

Scientific Linux Security Update : openssl on SL6.x, SL7.x i386/x86\_64 (20170220)

Scientific Linux Security Update : openssl on SL7.x x86\_64 (20150324)

Scientific Linux Security Update : openssl on SL7.x x86\_64 (20160509)

Scientific Linux Security Update : openssl on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : openssl on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : openssl on SL7.x x86\_64 (20190313)

Scientific Linux Security Update : openssl on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : openssl096b on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : openssl097a and openssl098e on SL5.x, SL6.x i386/x86\_64 (20140605)

Scientific Linux Security Update : openssl097a on SL5.x i386/x86\_64

Scientific Linux Security Update : openssl098e on SL6.x, SL7.x i386/x86\_64 (20160309) (DROWN)

Scientific Linux Security Update : openswan on SL5.x i386/x86\_64

Scientific Linux Security Update : openswan on SL5.x i386/x86\_64

Scientific Linux Security Update : openswan on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : openswan on SL5.x, SL6.x i386/x86\_64 (20130515)

Scientific Linux Security Update : openswan on SL5.x, SL6.x i386/x86\_64 (20140218)

Scientific Linux Security Update : openswan on SL6.x i386/x86\_64

Scientific Linux Security Update : openswan on SL6.x i386/x86\_64

Scientific Linux Security Update : openwsman on SL7.x x86\_64 (20190326)

Scientific Linux Security Update : ovmf on (20190423)

Scientific Linux Security Update : ovmf on on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : ovmf on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : pacemaker on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : pacemaker on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : pacemaker on SL6.x i386/x86\_64 (20161108)

Scientific Linux Security Update : pacemaker on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : pacemaker on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : pacemaker on SL7.x x86\_64 (20161104)

Scientific Linux Security Update : pacemaker on SL7.x x86\_64 (20190528)

Scientific Linux Security Update : PackageKit on SL7.x x86\_64 (20180424)

Scientific Linux Security Update : pam on SL3.x i386/x86\_64

Scientific Linux Security Update : pam on SL4.x i386/x86\_64

Scientific Linux Security Update : pam on SL5.x

Scientific Linux Security Update : pam on SL5.x i386/x86\_64

Scientific Linux Security Update : pam on SL6.x i386/x86\_64

Scientific Linux Security Update : pam on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : pam on SL6.x, SL7.x i386/x86\_64 (20150818)

Scientific Linux Security Update : pam\_krb5 on SL3.x i386/x86\_64

Scientific Linux Security Update : pam\_krb5 on SL5.x i386/x86\_64

Scientific Linux Security Update : pam\_krb5/krb5 on SL5.x i386/x86\_64

Scientific Linux Security Update : pango on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pango on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pango on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pango on SL5.x i386/x86\_64

Scientific Linux Security Update : pango on SL6.x i386/x86\_64

Scientific Linux Security Update : pango on SL7.x x86\_64 (20190828)

Scientific Linux Security Update : patch on SL6.x i386/x86\_64 (20180423)

Scientific Linux Security Update : patch on SL7.x x86\_64 (20180423)

Scientific Linux Security Update : patch on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : patch on SL7.x x86\_64 (20191003)

Scientific Linux Security Update : pcre on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : pcre on SL5.x i386/x86\_64

Scientific Linux Security Update : pcre on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : pcre on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : pcre on SL7.x x86\_64 (20160511)

Scientific Linux Security Update : pcs on SL6.x i386/srpm/x86\_64 (20150512)

Scientific Linux Security Update : pcs on SL6.x i386/x86\_64 (20180619)

Scientific Linux Security Update : pcs on SL6.x, SL7.x i386/x86\_64 (20150901)

Scientific Linux Security Update : pcs on SL7.x x86\_64 (20150512)

Scientific Linux Security Update : pcs on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : pcs on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : pcs on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : pcsc-lite on SL5.x i386/x86\_64

Scientific Linux Security Update : pcsc-lite on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : perl on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : perl on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : perl on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : perl on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : perl on SL5.x i386/x86\_64

Scientific Linux Security Update : perl on SL5.x i386/x86\_64

Scientific Linux Security Update : perl on SL5.x, SL6.x i386/x86\_64 (20130326)

Scientific Linux Security Update : perl on SL6.x i386/x86\_64

Scientific Linux Security Update : perl on SL6.x i386/x86\_64

Scientific Linux Security Update : perl on SL7.x x86\_64 (20190122)

Scientific Linux Security Update : perl-Archive-Tar on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : perl-Archive-Tar on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : perl-DBD-Pg on SL5.x i386/x86\_64

Scientific Linux Security Update : perl-DBD-Pg on SL5.x, SL6.x i386/x86\_64 (20120725)

Scientific Linux Security Update : perl-Net-DNS on SL3.0.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : php on SL3.x i386/x86\_64

Scientific Linux Security Update : php on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : php on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : php on SL4.x i386/x86\_64

Scientific Linux Security Update : php on SL4.x i386/x86\_64 (20120130)

Scientific Linux Security Update : php on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : php on SL4.x, SL5.x, SL6.x i386/x86\_64 (20120202)

Scientific Linux Security Update : php on SL5.x i386/x86\_64

Scientific Linux Security Update : php on SL5.x i386/x86\_64 (20120118)

Scientific Linux Security Update : php on SL5.x i386/x86\_64 (20120627)

Scientific Linux Security Update : php on SL5.x i386/x86\_64 (20131211)

Scientific Linux Security Update : php on SL5.x i386/x86\_64 (20140318)

Scientific Linux Security Update : php on SL5.x i386/x86\_64 (20141106)

Scientific Linux Security Update : php on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : php on SL5.x, SL6.x i386/x86\_64 (20120507)

Scientific Linux Security Update : php on SL5.x, SL6.x i386/x86\_64 (20130712)

Scientific Linux Security Update : php on SL6.x i386/x86\_64

Scientific Linux Security Update : php on SL6.x i386/x86\_64 (20120627)

Scientific Linux Security Update : php on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : php on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : php on SL6.x i386/x86\_64 (20150709)

Scientific Linux Security Update : php on SL6.x i386/x86\_64 (20160811) (httpoxy)

Scientific Linux Security Update : php on SL6.x i386/x86\_64 (20191031)

Scientific Linux Security Update : php on SL6.x, SL7.x i386/x86\_64 (20141030)

Scientific Linux Security Update : php on SL7.x x86\_64 (20150623)

Scientific Linux Security Update : php on SL7.x x86\_64 (20160811) (httpoxy)

Scientific Linux Security Update : php on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : php on SL7.x x86\_64 (20171115)

Scientific Linux Security Update : php on SL7.x x86\_64 (20180306)

Scientific Linux Security Update : php on SL7.x x86\_64 (20191031)

Scientific Linux Security Update : php-pear on SL6.x

Scientific Linux Security Update : php-pecl-apc on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : php53 and php on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : php53 and php on SL5.x, SL6.x i386/x86\_64 (20120111)

Scientific Linux Security Update : php53 and php on SL5.x, SL6.x i386/x86\_64 (20131211)

Scientific Linux Security Update : php53 and php on SL5.x, SL6.x i386/x86\_64 (20140806)

Scientific Linux Security Update : php53 and php on SL5.x, SL6.x i386/x86\_64 (20140930)

Scientific Linux Security Update : php53 on SL5.x i386/x86\_64

Scientific Linux Security Update : php53 on SL5.x i386/x86\_64 (20120202)

Scientific Linux Security Update : php53 on SL5.x i386/x86\_64 (20120507)

Scientific Linux Security Update : php53 on SL5.x i386/x86\_64 (20120627)

Scientific Linux Security Update : php53 on SL5.x i386/x86\_64 (20130712)

Scientific Linux Security Update : php53 on SL5.x i386/x86\_64 (20130930)

Scientific Linux Security Update : php53 on SL5.x i386/x86\_64 (20141030)

Scientific Linux Security Update : pidgin on SL 3.0.x , SL 4.x , SL 5.x

Scientific Linux Security Update : pidgin on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL5.x, SL6.x i386/x86\_64 (20120719)

Scientific Linux Security Update : pidgin on SL5.x, SL6.x i386/x86\_64 (20130314)

Scientific Linux Security Update : pidgin on SL5.x, SL6.x i386/x86\_64 (20140205)

Scientific Linux Security Update : pidgin on SL6.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL6.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL6.x i386/x86\_64

Scientific Linux Security Update : pidgin on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : piranha on SL5.x i386/x86\_64 (20140213)

Scientific Linux Security Update : piranha on SL6.x i386/x86\_64 (20140213)

Scientific Linux Security Update : pixman on SL5.x, SL6.x i386/x86\_64 (20131220)

Scientific Linux Security Update : pixman on SL6.x i386/x86\_64 (20130327)

Scientific Linux Security Update : pki-core on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : pki-core on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : pki-core on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : pki-core on SL7.x x86\_64 (20180626)

Scientific Linux Security Update : plexus-archiver on SL7.x (noarch) (20180612)

Scientific Linux Security Update : policycoreutils on SL6.x i386/x86\_64

Scientific Linux Security Update : policycoreutils on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : polkit on SL6.x i386/x86\_64

Scientific Linux Security Update : polkit on SL6.x i386/x86\_64 (20130919)

Scientific Linux Security Update : polkit on SL6.x i386/x86\_64 (20190226)

Scientific Linux Security Update : polkit on SL7.x x86\_64 (20160216)

Scientific Linux Security Update : polkit on SL7.x x86\_64 (20190131)

Scientific Linux Security Update : polkit on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : poppler on SL5.x i386/x86\_64

Scientific Linux Security Update : poppler on SL5.x i386/x86\_64

Scientific Linux Security Update : poppler on SL5.x i386/x86\_64

Scientific Linux Security Update : poppler on SL5.x i386/x86\_64

Scientific Linux Security Update : poppler on SL5.x i386/x86\_64

Scientific Linux Security Update : poppler on SL5.x i386/x86\_64

Scientific Linux Security Update : poppler on SL6.x i386/x86\_64

Scientific Linux Security Update : poppler on SL6.x i386/x86\_64 (20170830)

Scientific Linux Security Update : poppler on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : poppler on SL7.x x86\_64 (20170830)

Scientific Linux Security Update : poppler on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : postfix on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postfix on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postfix on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postfix on SL6.x i386/x86\_64

Scientific Linux Security Update : postgresql and postgresql84 on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postgresql and postgresql84 on SL5.x i386/x86\_64 (20120625)

Scientific Linux Security Update : postgresql and postgresql84 on SL5.x, SL6.x i386/x86\_64 (20120521)

Scientific Linux Security Update : postgresql and postgresql84 on SL5.x, SL6.x i386/x86\_64 (20120913)

Scientific Linux Security Update : postgresql and postgresql84 on SL5.x, SL6.x i386/x86\_64 (20131029)

Scientific Linux Security Update : postgresql and postgresql84 on SL6.x i386/x86\_64 (20120625)

Scientific Linux Security Update : postgresql on on SL3.0.x i386/x86\_64

Scientific Linux Security Update : postgresql on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postgresql on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postgresql on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postgresql on SL4 i386,x86\_64, SL5 i386

Scientific Linux Security Update : postgresql on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : postgresql on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : postgresql on SL5.x i386/x86\_64 (20120521)

Scientific Linux Security Update : postgresql on SL5.x i386/x86\_64 (20120625)

Scientific Linux Security Update : postgresql on SL5.x i386/x86\_64 (20120913)

Scientific Linux Security Update : postgresql on SL5.x i386/x86\_64 (20140304)

Scientific Linux Security Update : postgresql on SL6.x i386/x86\_64

Scientific Linux Security Update : postgresql on SL6.x i386/x86\_64 (20151118)

Scientific Linux Security Update : postgresql on SL6.x i386/x86\_64 (20160302)

Scientific Linux Security Update : postgresql on SL6.x i386/x86\_64 (20171005)

Scientific Linux Security Update : postgresql on SL6.x, SL7.x i386/x86\_64 (20150330)

Scientific Linux Security Update : postgresql on SL6.x, SL7.x i386/x86\_64 (20150629)

Scientific Linux Security Update : postgresql on SL7.x srpm/x86\_64 (20151119)

Scientific Linux Security Update : postgresql on SL7.x x86\_64 (20160302)

Scientific Linux Security Update : postgresql on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : postgresql on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : postgresql on SL7.x x86\_64 (20170914)

Scientific Linux Security Update : postgresql on SL7.x x86\_64 (20171219)

Scientific Linux Security Update : postgresql on SL7.x x86\_64 (20180823)

Scientific Linux Security Update : postgresql84 and postgresql on SL5.x, SL6.x i386/x86\_64 (20140225)

Scientific Linux Security Update : postgresql84 on SL5.x i386/x86\_64

Scientific Linux Security Update : postgresql84 on SL5.x i386/x86\_64

Scientific Linux Security Update : postgresql84 on SL5.x i386/x86\_64

Scientific Linux Security Update : ppp on SL6.x i386/x86\_64 (20200227)

Scientific Linux Security Update : ppp on SL7.x x86\_64 (20200227)

Scientific Linux Security Update : procmail on SL5.x, SL6.x i386/x86\_64 (20140910)

Scientific Linux Security Update : procmail on SL7.x x86\_64 (20171129)

Scientific Linux Security Update : procps on SL6.x i386/x86\_64 (20180531)

Scientific Linux Security Update : procps-ng on SL7.x x86\_64 (20180523)

Scientific Linux Security Update : procps-ng on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : pwlib on SL5.x i386/x86\_64

Scientific Linux Security Update : python for SL 3.0.x on i386/x86\_64

Scientific Linux Security Update : python for SL 4.x on i386/x86\_64

Scientific Linux Security Update : python for SL5.x i386/x86\_64

Scientific Linux Security Update : python on SL4.x i386/x86\_64

Scientific Linux Security Update : python on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : python on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : python on SL5.x i386/x86\_64

Scientific Linux Security Update : python on SL5.x i386/x86\_64 (20120618)

Scientific Linux Security Update : python on SL6.x i386/x86\_64

Scientific Linux Security Update : python on SL6.x i386/x86\_64 (20120618)

Scientific Linux Security Update : python on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : python on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : python on SL6.x i386/x86\_64 (20190613)

Scientific Linux Security Update : python on SL6.x, SL7.x i386/x86\_64 (20160818) (httpoxy)

Scientific Linux Security Update : python on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : python on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : python on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : python on SL7.x x86\_64 (20180703)

Scientific Linux Security Update : python on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : python on SL7.x x86\_64 (20190408)

Scientific Linux Security Update : python on SL7.x x86\_64 (20190620)

Scientific Linux Security Update : python on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : python-imaging on SL6.x i386/x86\_64 (20200318)

Scientific Linux Security Update : python-jinja2 on SL6.x i386/x86\_64 (20140611)

Scientific Linux Security Update : python-jinja2 on SL7.x (noarch) (20190507)

Scientific Linux Security Update : python-paramiko on SL6.x (noarch) (20180412)

Scientific Linux Security Update : python-paramiko on SL6.x (noarch) (20181031)

Scientific Linux Security Update : python-paramiko on SL7.x (noarch) (20181030)

Scientific Linux Security Update : python-paste-script on SL6.x i386/x86\_64 (20120827)

Scientific Linux Security Update : python-pillow on SL7.x x86\_64 (20200224)

Scientific Linux Security Update : python-pip on SL7.x (noarch) (20200317)

Scientific Linux Security Update : python-reportlab on SL6.x i386/x86\_64 (20200121)

Scientific Linux Security Update : python-reportlab on SL7.x x86\_64 (20200122)

Scientific Linux Security Update : python-requests on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : python-sqlalchemy on SL6.x (20120307)

Scientific Linux Security Update : python-urllib3 on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : python-virtualenv on SL7.x (noarch) (20200317)

Scientific Linux Security Update : PyXML on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : qemu-kvm on SL6.x i386/srpm/x86\_64 (20130722)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20130307)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20130603)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20140422)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20140610)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20140819)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20150421)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20150513) (Venom)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20150610)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20150922)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20151022)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20151222)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20160128)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20160510)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20160809)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20170223)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20170301)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20170509)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20180104) (Spectre)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20180313)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20180521) (Spectre)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20180710) (Spectre)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20190514) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20190702)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20190924)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20200310)

Scientific Linux Security Update : qemu-kvm on SL6.x i386/x86\_64 (20200408)

Scientific Linux Security Update : qemu-kvm on SL6.x x86\_64

Scientific Linux Security Update : qemu-kvm on SL6.x x86\_64

Scientific Linux Security Update : qemu-kvm on SL6.x x86\_64

Scientific Linux Security Update : qemu-kvm on SL6.x x86\_64 (20120905)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20141020)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20150305)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20150513) (Venom)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20150727)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20150915)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20151027)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20160128)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20160509)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20160811)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20170117)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20170302)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20170418)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20170613)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20170705)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20170815)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20171130)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20180104) (Spectre)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20180515)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20180522) (Spectre)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20180626) (Spectre)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20180816)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20190514) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20190729)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20190903)

Scientific Linux Security Update : qemu-kvm on SL7.x x86\_64 (20200205)

Scientific Linux Security Update : qpid on SL6.x i386/x86\_64 (20120919)

Scientific Linux Security Update : qspice on SL5.x x86\_64

Scientific Linux Security Update : qspice on SL5.x x86\_64 (20131029)

Scientific Linux Security Update : qspice-client on SL5.x i386/x86\_64

Scientific Linux Security Update : qt on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : qt on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : qt on SL6.x i386/x86\_64

Scientific Linux Security Update : qt on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : qt on SL6.x i386/x86\_64 (20130321)

Scientific Linux Security Update : qt4 on SL5.x i386/x86\_64

Scientific Linux Security Update : qt5 on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : quagga on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : quagga on SL5.x i386/x86\_64 (20120912)

Scientific Linux Security Update : quagga on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : quagga on SL6.x i386/x86\_64

Scientific Linux Security Update : quagga on SL6.x i386/x86\_64

Scientific Linux Security Update : quagga on SL6.x i386/x86\_64 (20120912)

Scientific Linux Security Update : quagga on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : quagga on SL7.x x86\_64 (20180228)

Scientific Linux Security Update : quota on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : raptor on SL6.x i386/x86\_64 (20120322)

Scientific Linux Security Update : rdesktop on SL3.x i386/x86\_64

Scientific Linux Security Update : rdesktop on SL4.x i386/x86\_64

Scientific Linux Security Update : rdesktop on SL5.x i386/x86\_64

Scientific Linux Security Update : rdesktop on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : rdma on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : RDMA stack on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : realmd on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : Red Hat Enterprise Linux 5 kernel update on SL5.x i386/x86\_64 (20130930)

Scientific Linux Security Update : resource-agents on SL6.x i386/x86\_64

Scientific Linux Security Update : rest on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : resteasy-base on SL7.x (noarch) (20161103)

Scientific Linux Security Update : rgmanager on SL4.x i386/x86\_64

Scientific Linux Security Update : rgmanager on SL5.x i386/x86\_64

Scientific Linux Security Update : rgmanager on SL5.x i386/x86\_64

Scientific Linux Security Update : rhn-client-tools on SL5.x i386/x86\_64

Scientific Linux Security Update : rpcbind on SL6.x i386/x86\_64 (20170523)

Scientific Linux Security Update : rpcbind on SL6.x, SL7.x i386/x86\_64 (20160107)

Scientific Linux Security Update : rpcbind on SL7.x x86\_64 (20170521)

Scientific Linux Security Update : rpm on SL4.x i386/x86\_64

Scientific Linux Security Update : rpm on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : rpm on SL5.x i386/x86\_64

Scientific Linux Security Update : rpm on SL5.x, SL6.x i386/x86\_64 (20120403)

Scientific Linux Security Update : rpm on SL5.x, SL6.x i386/x86\_64 (20141209)

Scientific Linux Security Update : rpm on SL7.x x86\_64 (20141209)

Scientific Linux Security Update : rsync on SL5.x i386/x86\_64

Scientific Linux Security Update : rsync on SL5.x i386/x86\_64

Scientific Linux Security Update : rsync on SL6.x i386/x86\_64

Scientific Linux Security Update : rsyslog on SL6.x i386/x86\_64

Scientific Linux Security Update : rsyslog on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : rsyslog on SL7.x x86\_64 (20141013)

Scientific Linux Security Update : rsyslog on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : rsyslog5 and rsyslog on SL5.x, SL6.x i386/x86\_64 (20141020)

Scientific Linux Security Update : rtkit on SL6.x i386/x86\_64 (20130924)

Scientific Linux Security Update : ruby on SL3.x i386/x86\_64

Scientific Linux Security Update : ruby on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ruby on SL4.x i386/x86\_64

Scientific Linux Security Update : ruby on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ruby on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ruby on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : ruby on SL4.x, SL5.x i386/x86\_64 (20120130)

Scientific Linux Security Update : ruby on SL5.x i386/x86\_64

Scientific Linux Security Update : ruby on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : ruby on SL5.x i386/x86\_64 (20130307)

Scientific Linux Security Update : ruby on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : ruby on SL5.x, SL6.x i386/srpm/x86\_64 (20130717)

Scientific Linux Security Update : ruby on SL6.x i386/x86\_64

Scientific Linux Security Update : ruby on SL6.x i386/x86\_64

Scientific Linux Security Update : ruby on SL6.x i386/x86\_64 (20120130)

Scientific Linux Security Update : ruby on SL6.x i386/x86\_64 (20130307)

Scientific Linux Security Update : ruby on SL6.x i386/x86\_64 (20131125)

Scientific Linux Security Update : ruby on SL6.x i386/x86\_64 (20141126)

Scientific Linux Security Update : ruby on SL7.x x86\_64 (20141126)

Scientific Linux Security Update : ruby on SL7.x x86\_64 (20180228)

Scientific Linux Security Update : ruby on SL7.x x86\_64 (20181130)

Scientific Linux Security Update : ruby on SL7.x x86\_64 (20190515)

Scientific Linux Security Update : ruby on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : rubygem-bundler and rubygem-thor on SL7.x (noarch) (20151119)

Scientific Linux Security Update : rubygems on SL6.x (noarch) (20131017)

Scientific Linux Security Update : samba and cifs-utils on SL6.x i386/x86\_64

Scientific Linux Security Update : samba and samba3x on SL5.x i386/x86\_64

Scientific Linux Security Update : samba and samba3x on SL5.x, SL6.x i386/srpm/x86\_64 (20140325)

Scientific Linux Security Update : samba and samba3x on SL5.x, SL6.x i386/srpm/x86\_64 (20140709)

Scientific Linux Security Update : samba and samba3x on SL5.x, SL6.x i386/x86\_64 (20120430)

Scientific Linux Security Update : samba and samba3x on SL5.x, SL6.x i386/x86\_64 (20131210)

Scientific Linux Security Update : samba and samba4 on SL6.x, SL7.x i386/x86\_64 (20160412) (Badlock)

Scientific Linux Security Update : samba on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : samba on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : samba on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : samba on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : samba on SL4.x i386/x86\_64 (20120223)

Scientific Linux Security Update : samba on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : samba on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : samba on SL5.x i386 (20150223)

Scientific Linux Security Update : samba on SL5.x i386/x86\_64

Scientific Linux Security Update : samba on SL5.x i386/x86\_64 (20120223)

Scientific Linux Security Update : samba on SL5.x i386/x86\_64 (20140317)

Scientific Linux Security Update : samba on SL5.x i386/x86\_64 (20160412) (Badlock)

Scientific Linux Security Update : samba on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : samba on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : samba on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : samba on SL5.x, SL6.x i386/x86\_64 (20120410)

Scientific Linux Security Update : samba on SL6.x i386/x86\_64

Scientific Linux Security Update : samba on SL6.x i386/x86\_64

Scientific Linux Security Update : samba on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : samba on SL6.x i386/x86\_64 (20160107)

Scientific Linux Security Update : samba on SL6.x i386/x86\_64 (20160412) (Badlock)

Scientific Linux Security Update : samba on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : samba on SL6.x i386/x86\_64 (20170921)

Scientific Linux Security Update : samba on SL6.x i386/x86\_64 (20180619)

Scientific Linux Security Update : samba on SL6.x, SL7.x i386/x86\_64 (20150223)

Scientific Linux Security Update : samba on SL6.x, SL7.x i386/x86\_64 (20160315)

Scientific Linux Security Update : samba on SL6.x, SL7.x i386/x86\_64 (20170524) (SambaCry)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20150223)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20160107)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20160726)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20170522)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20170921)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20171127)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : samba on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : samba3x on SL5.x i386/x86\_64

Scientific Linux Security Update : samba3x on SL5.x i386/x86\_64

Scientific Linux Security Update : samba3x on SL5.x i386/x86\_64

Scientific Linux Security Update : samba3x on SL5.x i386/x86\_64 (20120410)

Scientific Linux Security Update : samba3x on SL5.x i386/x86\_64 (20130930)

Scientific Linux Security Update : samba3x on SL5.x i386/x86\_64 (20160412) (Badlock)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20131210)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20140409)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20140805)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20150223)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20160107)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20160315)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20160726)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20170524) (SambaCry)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20170921)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20171129)

Scientific Linux Security Update : samba4 on SL6.x i386/x86\_64 (20180619)

Scientific Linux Security Update : sblim on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : sblim-cim-client2 on SL6.x (20120620)

Scientific Linux Security Update : Scientific Linux 6 kernel on SL6.x i386/x86\_64

Scientific Linux Security Update : scsi-target-utils on SL5.x i386/x86\_64

Scientific Linux Security Update : scsi-target-utils on SL5.x i386/x86\_64

Scientific Linux Security Update : scsi-target-utils on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : SDL on SL7.x x86\_64 (20191202)

Scientific Linux Security Update : seamonkey on SL3.0.9 i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64 (20120201)

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64 (fwd)

Scientific Linux Security Update : seamonkey on SL4.x i386/x86\_64 (fwd)

Scientific Linux Security Update : seamonkey on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : seamonkey on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : selinux-policy bug fix update on SL6.x i386/x86\_64 (20130612)

Scientific Linux Security Update : selinux-policy enhancement update on SL5.x, SL6.x i386/x86\_64 (20120911)

Scientific Linux Security Update : selinux-policy enhancement update on SL5.x, SL6.x i386/x86\_64 (20121119)

Scientific Linux Security Update : selinux-policy enhancement update on SL6.x i386/x86\_64 (20121112)

Scientific Linux Security Update : selinux-policy enhancement update on SL6.x i386/x86\_64 (20121218)

Scientific Linux Security Update : selinux-policy enhancement update on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : selinux-policy enhancement update on SL6.x i386/x86\_64 (20130603)

Scientific Linux Security Update : selinux-policy enhancement update on SL6.x i386/x86\_64 (20131104)

Scientific Linux Security Update : selinux-policy on SL5.x i386/x86\_64

Scientific Linux Security Update : selinux-policy on SL5.x i386/x86\_64

Scientific Linux Security Update : selinux-policy on SL5.x i386/x86\_64

Scientific Linux Security Update : selinux-policy on SL5.x i386/x86\_64 (20120209)

Scientific Linux Security Update : selinux-policy on SL6.x i386/x86\_64

Scientific Linux Security Update : selinux-policy on SL6.x i386/x86\_64

Scientific Linux Security Update : selinux-policy on SL6.x i386/x86\_64 (20120213)

Scientific Linux Security Update : selinux-policy on SL6.x i386/x86\_64 (20120307)

Scientific Linux Security Update : selinux-policy on SL6.x i386/x86\_64 (20120709)

Scientific Linux Security Update : sendmail on SL4.x i386/x86\_64

Scientific Linux Security Update : sendmail on SL4.x i386/x86\_64

Scientific Linux Security Update : sendmail on SL5.x i386/x86\_64

Scientific Linux Security Update : setroubleshoot and setroubleshoot-plugins on SL6.x i386/x86\_64 (20160621)

Scientific Linux Security Update : setroubleshoot and setroubleshoot-plugins on SL7.x x86\_64 (20160623)

Scientific Linux Security Update : setroubleshoot on SL5.x i386/x86\_64

Scientific Linux Security Update : setroubleshoot on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150326)

Scientific Linux Security Update : setup on SL7.x (noarch) (20181030)

Scientific Linux Security Update : shadow-utils on SL3.x i386/x86\_64

Scientific Linux Security Update : shadow-utils on SL4.x i386/x86\_64

Scientific Linux Security Update : shim on SL7.x x86\_64 (20141104)

Scientific Linux Security Update : sl-release on SL5.1 i386/x86\_64

Scientific Linux Security Update : SL\_desktop\_tweaks on SL5.x i386/x86\_64

Scientific Linux Security Update : slf4j on SL7.x (noarch) (20180326)

Scientific Linux Security Update : sos on SL5.x (20120221)

Scientific Linux Security Update : sos on SL5.x (noarch) (20130730)

Scientific Linux Security Update : sos on SL6.x

Scientific Linux Security Update : sos on SL6.x (20120620)

Scientific Linux Security Update : sos on SL6.x (noarch) (20160209)

Scientific Linux Security Update : sos on SL7.x (noarch) (20160216)

Scientific Linux Security Update : sos-collector on SL7.x (noarch) (20181127)

Scientific Linux Security Update : sox on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : spamassassin on SL5.x, SL4.x i386/x86\_64 (fwd)

Scientific Linux Security Update : spamassassin on SL7.x x86\_64 (20181011)

Scientific Linux Security Update : speex on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : spice and spice-gtk on SL7.x x86\_64 (20180920)

Scientific Linux Security Update : spice on SL7.x x86\_64 (20151012)

Scientific Linux Security Update : spice on SL7.x x86\_64 (20160606)

Scientific Linux Security Update : spice on SL7.x x86\_64 (20170205)

Scientific Linux Security Update : spice on SL7.x x86\_64 (20170815)

Scientific Linux Security Update : spice on SL7.x x86\_64 (20190131)

Scientific Linux Security Update : spice-gtk and spice-server on SL6.x i386/x86\_64 (20180920)

Scientific Linux Security Update : spice-gtk on SL6.x i386/x86\_64 (20120917)

Scientific Linux Security Update : spice-gtk on SL6.x i386/x86\_64 (20130919)

Scientific Linux Security Update : spice-gtk on SL6.x i386/x86\_64 (20200211)

Scientific Linux Security Update : spice-gtk on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20130903)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20131029)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20150903)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20151012)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20160606)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20170205)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20181108)

Scientific Linux Security Update : spice-server on SL6.x x86\_64 (20190131)

Scientific Linux Security Update : spice-server on SL7.x x86\_64 (20150903)

Scientific Linux Security Update : spice-xpi on SL5.x i386/x86\_64

Scientific Linux Security Update : spice-xpi on SL5.x,SL6.x i386/x86\_64

Scientific Linux Security Update : sqlite on SL6.x i386/x86\_64 (20150817)

Scientific Linux Security Update : sqlite on SL7.x x86\_64 (20150817)

Scientific Linux Security Update : sqlite on SL7.x x86\_64 (20200127)

Scientific Linux Security Update : squid on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : squid on SL5.x i386/x86\_64

Scientific Linux Security Update : squid on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : squid on SL5.x, SL6.x i386/x86\_64 (20140903)

Scientific Linux Security Update : squid on SL6.x i386/x86\_64

Scientific Linux Security Update : squid on SL6.x i386/x86\_64

Scientific Linux Security Update : squid on SL6.x i386/x86\_64

Scientific Linux Security Update : squid on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : squid on SL6.x i386/x86\_64 (20140603)

Scientific Linux Security Update : squid on SL6.x i386/x86\_64 (20160531)

Scientific Linux Security Update : squid on SL6.x i386/x86\_64 (20160804)

Scientific Linux Security Update : squid on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : squid on SL7.x x86\_64 (20160531)

Scientific Linux Security Update : squid on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : squid on SL7.x x86\_64 (20170124)

Scientific Linux Security Update : squid34 on SL6.x i386/x86\_64 (20160531)

Scientific Linux Security Update : squid34 on SL6.x i386/x86\_64 (20170124)

Scientific Linux Security Update : squirrelmail on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : squirrelmail on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : squirrelmail on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : squirrelmail on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : squirrelmail on SL4.x, SL5.x (20120208)

Scientific Linux Security Update : squirrelmail on SL5.x (noarch) (20130108)

Scientific Linux Security Update : squirrelmail on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : sssd and ding-libs on SL6.x i386/x86\_64 (20180619)

Scientific Linux Security Update : sssd on SL5.x i386/x86\_64

Scientific Linux Security Update : sssd on SL5.x i386/x86\_64 (20130930)

Scientific Linux Security Update : sssd on SL6.x i386/x86\_64

Scientific Linux Security Update : sssd on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : sssd on SL6.x i386/x86\_64 (20130319)

Scientific Linux Security Update : sssd on SL6.x i386/x86\_64 (20151110)

Scientific Linux Security Update : sssd on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : sssd on SL7.x x86\_64 (20171205)

Scientific Linux Security Update : sssd on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : sssd on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : star on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : struts on SL5.x i386/x86\_64 (20140507)

Scientific Linux Security Update : stunnel on SL6.x i386/x86\_64 (20130408)

Scientific Linux Security Update : subscription-manager on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : subscription-manager on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : subversion on SL4.x i386/x86\_64

Scientific Linux Security Update : subversion on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : subversion on SL5.x i386/x86\_64

Scientific Linux Security Update : subversion on SL5.x i386/x86\_64

Scientific Linux Security Update : subversion on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : subversion on SL5.x, SL6.x i386/x86\_64 (20130411)

Scientific Linux Security Update : subversion on SL5.x, SL6.x i386/x86\_64 (20140305)

Scientific Linux Security Update : subversion on SL6.x i386/x86\_64

Scientific Linux Security Update : subversion on SL6.x i386/x86\_64 (20150210)

Scientific Linux Security Update : subversion on SL6.x i386/x86\_64 (20150817)

Scientific Linux Security Update : subversion on SL7.x x86\_64 (20150210)

Scientific Linux Security Update : subversion on SL7.x x86\_64 (20150908)

Scientific Linux Security Update : subversion on SL7.x x86\_64 (20170816)

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64 (20120808)

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64 (20130930)

Scientific Linux Security Update : sudo on SL5.x i386/x86\_64 (20140310)

Scientific Linux Security Update : sudo on SL5.x, SL6.x i386/x86\_64 (20120716)

Scientific Linux Security Update : sudo on SL6.x i386/x86\_64

Scientific Linux Security Update : sudo on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : sudo on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : sudo on SL6.x i386/x86\_64 (20191106)

Scientific Linux Security Update : sudo on SL6.x i386/x86\_64 (20200305)

Scientific Linux Security Update : sudo on SL6.x, SL7.x i386/x86\_64 (20161206)

Scientific Linux Security Update : sudo on SL6.x, SL7.x i386/x86\_64 (20170530)

Scientific Linux Security Update : sudo on SL6.x, SL7.x i386/x86\_64 (20170623)

Scientific Linux Security Update : sudo on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : sudo on SL7.x x86\_64 (20191024)

Scientific Linux Security Update : sudo on SL7.x x86\_64 (20200218)

Scientific Linux Security Update : sysreport on SL3.x i386/x86\_64

Scientific Linux Security Update : sysstat on SL5.x i386/x86\_64

Scientific Linux Security Update : system-config-firewall on SL6.x i386/x86\_64

Scientific Linux Security Update : system-config-printer on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : systemd on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : systemd on SL7.x x86\_64 (20180131)

Scientific Linux Security Update : systemd on SL7.x x86\_64 (20190114)

Scientific Linux Security Update : systemd on SL7.x x86\_64 (20190129)

Scientific Linux Security Update : systemd on SL7.x x86\_64 (20190221)

Scientific Linux Security Update : systemd on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : systemtap on SL4.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL4.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL5.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL5.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL5.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL5.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL5.x, SL6.x i386/x86\_64 (20120308)

Scientific Linux Security Update : systemtap on SL6.x i386/x86\_64

Scientific Linux Security Update : systemtap on SL6.x i386/x86\_64

Scientific Linux Security Update : t1lib on SL6.x i386/x86\_64 (20120124)

Scientific Linux Security Update : tar on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tar on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : tcl on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : tcltk on SL3.x i386/x86\_64

Scientific Linux Security Update : tcpdump on SL4.x i386/x86\_64

Scientific Linux Security Update : tcpdump on SL5.x i386/x86\_64

Scientific Linux Security Update : tcpdump on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : tcpdump on SL7.x x86\_64 (20191202)

Scientific Linux Security Update : telnet on SL6.x i386/x86\_64 (20200406)

Scientific Linux Security Update : tetex on SL3.x i386/x86\_64

Scientific Linux Security Update : tetex on SL4.x i386/x86\_64

Scientific Linux Security Update : tetex on SL5.x i386/x86\_64

Scientific Linux Security Update : tetex on SL5.x i386/x86\_64 (20120823)

Scientific Linux Security Update : tetex on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : tetex on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : texlive on SL6.x i386/x86\_64 (20120215)

Scientific Linux Security Update : thunderbird on SL3.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x i386/x86\_64 (20120201)

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL4.x,SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL5.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : Thunderbird on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/srpm/x86\_64 (20130917)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20120314)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20120424)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20120606)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20120717)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20120829)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20121009)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20121029)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20121120)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20130108)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20130219)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20130311)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20130402)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20130514)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20130625)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20130807)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20131030)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20131211)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20140204)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20140319)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20140429)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20140610)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20140722)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20140903)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20150113)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x i386/x86\_64 (20150225)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150401)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150518)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150720)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20150825)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20151001)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20151126)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160105)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160218)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160316)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160711)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20160905)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161003)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161129)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161205)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20161221)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20170202)

Scientific Linux Security Update : thunderbird on SL5.x, SL6.x, SL7.x i386/x86\_64 (20170314)

Scientific Linux Security Update : thunderbird on SL5.x, SL7.x i386/x86\_64 (20160512)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20120131)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20141015)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20141202)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20160512)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20180405)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20180524)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20180725)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20181031)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20181109)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20190125)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20190204)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20190328)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20190604)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20190627)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20190715)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20190919)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20191106)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20191211)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20200116)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20200224)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20200323)

Scientific Linux Security Update : thunderbird on SL6.x i386/x86\_64 (20200416)

Scientific Linux Security Update : thunderbird on SL6.x, SL7.x i386/x86\_64 (20170508)

Scientific Linux Security Update : thunderbird on SL6.x, SL7.x i386/x86\_64 (20170621)

Scientific Linux Security Update : thunderbird on SL6.x, SL7.x i386/x86\_64 (20170824)

Scientific Linux Security Update : thunderbird on SL6.x, SL7.x i386/x86\_64 (20171012)

Scientific Linux Security Update : thunderbird on SL6.x, SL7.x i386/x86\_64 (20171204)

Scientific Linux Security Update : thunderbird on SL6.x, SL7.x i386/x86\_64 (20180107)

Scientific Linux Security Update : thunderbird on SL6.x, SL7.x i386/x86\_64 (20180201)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20180405)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20180524)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20180725)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20181105)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20181109)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20190125)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20190204)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20190328)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20190604)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20190627)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20190715)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20190918)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20191029)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20191210)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20200116)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20200224)

Scientific Linux Security Update : thunderbird on SL7.x x86\_64 (20200319)

Scientific Linux Security Update : tigervnc and fltk on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : tigervnc on SL6.x i386/x86\_64

Scientific Linux Security Update : tigervnc on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : tigervnc on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : tk on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tog-pegasus on SL5.x i386/x86\_64

Scientific Linux Security Update : tog-pegasus on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : tomcat on SL5.x i386/x86\_64

Scientific Linux Security Update : tomcat on SL5.x i386/x86\_64

Scientific Linux Security Update : tomcat on SL5.x i386/x86\_64

Scientific Linux Security Update : tomcat on SL5.x i386/x86\_64

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20150512)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20161010) (httpoxy)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20161103)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20170412)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20170727)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20170802)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20171030)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20181016)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20190313)

Scientific Linux Security Update : tomcat on SL7.x (noarch) (20200317)

Scientific Linux Security Update : tomcat on SL7.x (x86\_64) (20190318)

Scientific Linux Security Update : tomcat on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : tomcat5 on SL5.x i386/x86\_64

Scientific Linux Security Update : tomcat5 on SL5.x i386/x86\_64

Scientific Linux Security Update : tomcat5 on SL5.x i386/x86\_64

Scientific Linux Security Update : tomcat5 on SL5.x i386/x86\_64 (20120411)

Scientific Linux Security Update : tomcat5 on SL5.x i386/x86\_64 (20130312)

Scientific Linux Security Update : tomcat5 on SL5.x i386/x86\_64 (20130528)

Scientific Linux Security Update : tomcat6 on SL6.x

Scientific Linux Security Update : tomcat6 on SL6.x (20120411)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20130311)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20130528)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20130620)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20140423)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20140811)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20161010) (httpoxy)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20170315)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20171030)

Scientific Linux Security Update : tomcat6 on SL6.x (noarch) (20200323)

Scientific Linux Security Update : tomcat6 on SL6.x i386/srpm/x86\_64 (20140709)

Scientific Linux Security Update : tomcat6 on SL6.x i386/srpm/x86\_64 (20150512)

Scientific Linux Security Update : tomcat6 on SL6.x i386/x86\_64

Scientific Linux Security Update : tomcat6 on SL6.x i386/x86\_64

Scientific Linux Security Update : tomcat6 on SL6.x i386/x86\_64 (20160323)

Scientific Linux Security Update : trousers on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : tzdata bug fix update on SL5.x, SL6.x i386/x86\_64 (20160621)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20120719)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20121004)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20121126)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20130123)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20130308)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20130709)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20131223)

Scientific Linux Security Update : tzdata enhancement update on SL5.x, SL6.x i386/x86\_64 (20140623)

Scientific Linux Security Update : tzdata on SL3.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL5.x, SL4.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : tzdata on SL5.x, SL6.x i386/x86\_64 (20120323)

Scientific Linux Security Update : tzdata on SL5.x, SL6.x i386/x86\_64 (20120523)

Scientific Linux Security Update : udev on SL5.x i386/x86\_64

Scientific Linux Security Update : udisks on SL6.x i386/x86\_64 (20140313)

Scientific Linux Security Update : udisks2 on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : unbound on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : unixODBC on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : unzip on SL3.x i386/x86\_64

Scientific Linux Security Update : unzip on SL4.x i386/x86\_64

Scientific Linux Security Update : unzip on SL6.x, SL7.x i386/x86\_64 (20150318)

Scientific Linux Security Update : unzip on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : up2date on SL3.x i386/x86\_64

Scientific Linux Security Update : uriparser on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : util-linux for SL4.x i386/x86\_64

Scientific Linux Security Update : util-linux on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : util-linux on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : util-linux on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : util-linux on SL7.x x86\_64 (20170412)

Scientific Linux Security Update : util-linux-ng on SL6.x i386/x86\_64

Scientific Linux Security Update : util-linux-ng on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : vim on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : vim on SL6.x i386/x86\_64 (20190715)

Scientific Linux Security Update : vim on SL6.x, SL7.x i386/x86\_64 (20161221)

Scientific Linux Security Update : vim on SL7.x x86\_64 (20190701)

Scientific Linux Security Update : vino on SL5.x, SL6.x i386/x86\_64 (20131022)

Scientific Linux Security Update : vino on SL6.x i386/x86\_64 (20130121)

Scientific Linux Security Update : virt-v2v on SL6.x x86\_64

Scientific Linux Security Update : virt-who on SL7.x (noarch) (20150305)

Scientific Linux Security Update : Virtio on SL3.x i386/x86\_64

Scientific Linux Security Update : vixie-cron on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : vixie-cron on SL5.x, SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : vnc on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : vsftpd on SL3.x i386/x86\_64

Scientific Linux Security Update : vsftpd on SL4.x i386/x86\_64

Scientific Linux Security Update : vsftpd on SL4.x, SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : vsftpd on SL5.x i386/x86\_64

Scientific Linux Security Update : w3c-libwww on SL4 i386/x86\_64

Scientific Linux Security Update : w3m on SL5.x i386/x86\_64

Scientific Linux Security Update : webkitgtk on SL6.x i386/x86\_64

Scientific Linux Security Update : wget on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wget on SL6.x i386/x86\_64 (20140210)

Scientific Linux Security Update : wget on SL6.x, SL7.x i386/x86\_64 (20141030)

Scientific Linux Security Update : wget on SL7.x x86\_64 (20161103)

Scientific Linux Security Update : wget on SL7.x x86\_64 (20171026)

Scientific Linux Security Update : wget on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : wget on SL7.x x86\_64 (20190514)

Scientific Linux Security Update : wireshark on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL4.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL5.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL5.x i386/x86\_64 (20130108)

Scientific Linux Security Update : wireshark on SL5.x i386/x86\_64 (20140331)

Scientific Linux Security Update : wireshark on SL5.x i386/x86\_64 (20141021)

Scientific Linux Security Update : wireshark on SL6.x i386/x86\_64

Scientific Linux Security Update : wireshark on SL6.x i386/x86\_64 (20120423)

Scientific Linux Security Update : wireshark on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : wireshark on SL6.x i386/x86\_64 (20140331)

Scientific Linux Security Update : wireshark on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : wireshark on SL6.x i386/x86\_64 (20170321)

Scientific Linux Security Update : wireshark on SL6.x, SL7.x i386/x86\_64 (20141021)

Scientific Linux Security Update : wireshark on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : wpa\_supplicant on SL6.x i386/x86\_64 (20150722)

Scientific Linux Security Update : wpa\_supplicant on SL6.x i386/x86\_64 (20171018) (KRACK)

Scientific Linux Security Update : wpa\_supplicant on SL7.x x86\_64 (20141203)

Scientific Linux Security Update : wpa\_supplicant on SL7.x x86\_64 (20150611)

Scientific Linux Security Update : wpa\_supplicant on SL7.x x86\_64 (20171018) (KRACK)

Scientific Linux Security Update : wpa\_supplicant on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : X.org X11 libraries on SL7.x x86\_64 (20170801)

Scientific Linux Security Update : X.org X11 on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : X11 client libraries on SL6.x i386/x86\_64 (20141014)

Scientific Linux Security Update : xalan-j2 on SL5.x, SL6.x i386/x86\_64 (20140401)

Scientific Linux Security Update : xdg-user-dirs on SL7.x x86\_64 (20180410)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64

Scientific Linux Security Update : xen on SL5.x i386/x86\_64

Scientific Linux Security Update : xen on SL5.x i386/x86\_64

Scientific Linux Security Update : xen on SL5.x i386/x86\_64

Scientific Linux Security Update : xen on SL5.x i386/x86\_64

Scientific Linux Security Update : xen on SL5.x i386/x86\_64

Scientific Linux Security Update : xen on SL5.x i386/x86\_64

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20120307)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20120731)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20120905)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20130207)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20130306)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20150513) (Venom)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20151116)

Scientific Linux Security Update : xen on SL5.x i386/x86\_64 (20161220)

Scientific Linux Security Update : xen/libvirt on SL5.0 i386/x86\_64

Scientific Linux Security Update : xerces-c on SL6.x i386/x86\_64 (20200304)

Scientific Linux Security Update : xerces-c on SL7.x x86\_64 (20150629)

Scientific Linux Security Update : xerces-c on SL7.x x86\_64 (20160310)

Scientific Linux Security Update : xerces-c on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : xerces-c on SL7.x x86\_64 (20200304)

Scientific Linux Security Update : xerces-j2 on SL5.x i386/x86\_64

Scientific Linux Security Update : xerces-j2 on SL6.x i386/x86\_64

Scientific Linux Security Update : xerces-j2 on SL6.x i386/x86\_64 (20140929)

Scientific Linux Security Update : XFree86 on SL3.x i386/x86\_64

Scientific Linux Security Update : XFree86 on SL3.x i386/x86\_64

Scientific Linux Security Update : xfsprogs on SL7.x x86\_64 (20151119)

Scientific Linux Security Update : xinetd on SL5.x i386/x86\_64 (20130930)

Scientific Linux Security Update : xinetd on SL5.x, SL6.x i386/x86\_64 (20131007)

Scientific Linux Security Update : xinetd on SL6.x i386/x86\_64 (20130221)

Scientific Linux Security Update : xmlrpc on SL7.x (noarch) (20180531)

Scientific Linux Security Update : xmlrpc3 on SL6.x (noarch) (20180531)

Scientific Linux Security Update : xmlsec1 on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : xmlsec1 on SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : xmlsec1 on SL7.x x86\_64 (20170821)

Scientific Linux Security Update : Xorg on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : xorg-x11 on SL4.x i386/x86\_64

Scientific Linux Security Update : xorg-x11 on SL4.x i386/x86\_64

Scientific Linux Security Update : xorg-x11 on SL4.x i386/x86\_64

Scientific Linux Security Update : xorg-x11 on SL4.x i386/x86\_64

Scientific Linux Security Update : xorg-x11 on SL4.x i386/x86\_64

Scientific Linux Security Update : xorg-x11 on SL4.x i386/x86\_64

Scientific Linux Security Update : xorg-x11 on SL4.x i386/x86\_64

Scientific Linux Security Update : xorg-x11-drv-qxl on SL6.x i386/x86\_64 (20130131)

Scientific Linux Security Update : xorg-x11-server on SL5.x i386/x86\_64

Scientific Linux Security Update : xorg-x11-server on SL5.x i386/x86\_64

Scientific Linux Security Update : xorg-x11-server on SL5.x i386/x86\_64

Scientific Linux Security Update : xorg-x11-server on SL5.x i386/x86\_64 (20120221)

Scientific Linux Security Update : xorg-x11-server on SL5.x i386/x86\_64 (20141211)

Scientific Linux Security Update : xorg-x11-server on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : xorg-x11-server on SL5.x, SL6.x i386/x86\_64 (20131015)

Scientific Linux Security Update : xorg-x11-server on SL5.x, SL6.x i386/x86\_64 (20131220)

Scientific Linux Security Update : xorg-x11-server on SL6.x i386/x86\_64 (20120620)

Scientific Linux Security Update : xorg-x11-server on SL6.x i386/x86\_64 (20131121)

Scientific Linux Security Update : xorg-x11-server on SL6.x, SL7.x i386/x86\_64 (20141211)

Scientific Linux Security Update : xorg-x11-server on SL6.x, SL7.x i386/x86\_64 (20150410)

Scientific Linux Security Update : xorg-x11-server on SL7.x x86\_64 (20181031)

Scientific Linux Security Update : xorg-x11-server-utils on SL5.x, SL6.x i386/x86\_64

Scientific Linux Security Update : xorg-x11-xfs on SL5.x i386/x86\_64

Scientific Linux Security Update : xpdf on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : xpdf on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : xpdf on SL3.x, SL4.x i386/x86\_64

Scientific Linux Security Update : xpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : xpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : xpdf on SL4.x i386/x86\_64

Scientific Linux Security Update : xpdf on SL4.x, SL3.x i386/x86\_64

Scientific Linux Security Update : xscreensaver on SL3.0.x i386/x86\_64

Scientific Linux Security Update : xscreensaver on SL4 i386/x86\_64

Scientific Linux Security Update : xterm on SL3.x, SL4.x, SL5.x i386/x86\_64

Scientific Linux Security Update : xterm on SL4.x i386/x86\_64

Scientific Linux Security Update : xulrunner on SL5.x i386/x86\_64

Scientific Linux Security Update : xulrunner on SL5.x, SL6.x i386/x86\_64 (20120216)

Scientific Linux Security Update : xulrunner on SL5.x, SL6.x i386/x86\_64 (20121012)

Scientific Linux Security Update : xulrunner on SL5.x, SL6.x i386/x86\_64 (20130308)

Scientific Linux Security Update : ypbind on SL3.x i386/x86\_64

Scientific Linux Security Update : yum on SL4.x i386/x86\_64

Scientific Linux Security Update : yum on SL5.x i386/x86\_64

Scientific Linux Security Update : yum on SL5.x i386/x86\_64

Scientific Linux Security Update : yum-autoupdate update on SL5.x, SL6.x i386/x86\_64 (20120925)

Scientific Linux Security Update : yum-conf on SL3.x i386/x86\_64

Scientific Linux Security Update : yum-rhn-plugin on SL5.x i386/x86\_64

Scientific Linux Security Update : yum-updatesd on SL5.x (noarch) (20140805)

Scientific Linux Security Update : yum-utils on SL6.x (noarch) (20180730)

Scientific Linux Security Update : yum-utils on SL7.x (noarch) (20180730)

Scientific Linux Security Update : zsh on SL6.x i386/x86\_64 (20180619)

Scientific Linux Security Update : zsh on SL6.x i386/x86\_64 (20200318)

Scientific Linux Security Update : zsh on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : zsh on SL7.x x86\_64 (20190806)

Scientific Linux Security Update : zsh on SL7.x x86\_64 (20200317)

Scientific Linux Security Update : zziplib on SL7.x x86\_64 (20181030)

Scientific Linux Security Update : zziplib on SL7.x x86\_64 (20190806)

Scientific Linux Update Level

# SCADA

3S CODESYS 2.x Development System Detection (credentialed check)

3S CODESYS CmpWebServerHandlerV3 Heap-based Buffer Overflow

3S CODESYS Runtime 3.x < 3.5.14.0 Insufficient Access Control Vulnerability

3S CODESYS Runtime 3.x < 3.5.14.20 Multiple Vulnerabilities

3S CODESYS Runtime Toolkit < 2.4.7.48 PLCWinNT DoS

3S CODESYS Runtime Toolkit < 2.4.7.48 PLCWinNT DoS (credentialed check)

3S CoDeSys Runtime Toolkit NULL Pointer Dereference (credentialed check)

3S CoDeSys Runtime Toolkit NULL Pointer Dereference (uncredentialed check)

3S CODESYS V3 CmpUserMgr 3.x < 3.5.16.0 Password Transmission Vulnerability

3S CODESYS V3 CmpWebServer Multiple Vulnerabilities

7-Technologies / Schneider-Electric IGSS Data Collector Detection

7-Technologies / Schneider-Electric IGSS Detection

7-Technologies / Schneider-Electric IGSS ODBC Service Detection

7-Technologies / Schneider-Electric IGSS ODBC Version Identification

7-Technologies AQUIS Detection

7-Technologies AQUIS Unspecified Path Subversion Arbitrary DLL Injection Code Execution

7-Technologies IGSS < 10.0.0 ODBC Buffer Overflow RCE

7-Technologies IGSS < 9.0.0.11129 Multiple DoS Vulnerabilities

7-Technologies IGSS < 9.0.0.11143 ODBC Invalid Structure RCE

7-Technologies IGSS < 9.0.0.11143 ODBC Remote Memory Corruption

7-Technologies IGSS < 9.0.0.11291 DLL Loading Arbitrary Code Execution

7-Technologies TERMIS Detection

7-Technologies TERMIS Unspecified Path Subversion Arbitrary DLL Injection Code Execution

Advantech / BroadWin WebAccess Client 'bwocxrun.ocx ' Multiple Remote Vulnerabilities

Advantech / BroadWin WebAccess webvrpcs.exe Service Remote Code Execution (credentialed check)

Advantech / BroadWin WebAccess webvrpcs.exe Service Remote Code Execution (uncredentialed check) (deprecated)

Advantech ADAMView Installation Detection

Advantech ADAMView Multiple Buffer Overflow Vulnerabilities

Advantech Studio Detection

Advantech Studio ISSymbol ActiveX Control Multiple Buffer Overflow Vulnerabilities

Advantech WebAccess 7.2 < 7.2-2014.07.30 Multiple ActiveX RCE

Advantech WebAccess < 7.0-2009.06.29 Multiple Vulnerabilities

Advantech WebAccess < 7.0-2011.08.27 Multiple ActiveX RCE

Advantech WebAccess < 7.0-2011.12.20 Multiple Vulnerabilities

Advantech WebAccess < 7.2-2013.11.14 Multiple Vulnerabilities

Advantech WebAccess < 7.2-2014.06.06 Multiple Vulnerabilities

Advantech WebAccess < 8.0.2015.08.16 Unspecified DLL String Handling Arbitrary Code Execution

Advantech WebAccess < 8.1-2015.12.30 Multiple Vulnerabilities

Advantech WebAccess < 8.2\_20170817 Multiple Vulnerabilities

Advantech WebAccess Authentication Bypass

Advantech WebAccess Default Credential Check

Advantech WebAccess Multiple BWOCXRUN.OCX ActiveX Vulnerabilities

Advantech WebAccess openWidget Script Path Traversal Remote File Disclosure

Advantech WebAccess SQLi

Advantech WebAccess Stored Cross-Site Scripting

Advantech WebAccess Web Administration Interface Detection

Advantech WebAccess Webeye ActiveX Control Stack Based Buffer Overflow Vulnerability

Advantech WebAccess webvact ActiveX Multiple Buffer Overflow Vulnerabilities

Advantech WebAccess webvprcs IOCTL 10012 Stack Overflow

Advantech WebAccess webvprcs IOCTL 70603 Stack Overflow

Advantech WebAccess webvrpcs.exe 0x138bd IOCTL RCE

Advantech WebAccess webvrpcs.exe Arbitrary File Download

Advantech WebAccess webvrpcs.exe IOCTL 70022 Stack Overflow

Advantech WebAccess webvrpcs.exe Path Traversal RCE

Advantech WebAccess/SCADA Network Service Detection

Allen-Bradley MicroLogix 1400 Multiple Vulnerabilities

Areva/Alstom Energy Management System Detection

Automated Solutions Modbus Slave MiniHMI.exe ActiveX Modbus/TCP Diagnostic Function Arbitrary Code Execution

Automated Solutions Modbus/TCP OPC Server Detection

AVEVA InduSoft Web Studio / InTouch Edge HMI Command 66 RCE

AVEVA InduSoft Web Studio / InTouch Edge HMI TCP/IP Server Detection

AVEVA InduSoft Web Studio / InTouch Edge HMI UniSoft.dll wcscpy() Stack Overflow

AVEVA InduSoft Web Studio / InTouch Machine Edition Command 81 mbstowcs() Stack Overflow

BACnet OPC Client < 1.0.25 Buffer Overflow

BACnet Protocol Detection

CitectSCADA Detection

CitectSCADA ODBC Server Remote Buffer Overflow

ClearSCADA Web Server Detection

ClearSCADA Web Server Remote Denial of Service

Clorius Controls ISC SCADA Detection

Clorius Controls ISC SCADA Information Disclosure

CoDeSys Authentication Bypass Directory Traversal

CODESYS ENI Server < 3.2.2.25 Stack Overflow (credentialed check)

CoDeSys Gateway Service < 2.3.9.27 Multiple Vulnerabilities

CoDeSys Gateway Service < 2.3.9.28 Use-After-Free

CoDeSys Gateway Service Detection

CODESYS Gateway V3 Detection

CODESYS Gateway V3 DoS

CODESYS PLC Runtime Service Detection

CoDeSys Unauthenticated Command-line Access

CoDeSys Unprotected Gateway Service

CODESYS V3 Runtime Service Detection

CODESYS WAGO WebVisu Detection

CODESYS WAGO WebVisu Password Information Disclosure Vulnerability

Cogent DataHub < 6.4.3 OPC Client Reconnection Saturation Remote DoS

Cogent DataHub < 6.4.5Beta OPC Connection Failure DoS

Cogent DataHub < 6.4.7 Incoming DDE Connection Handling Remote DoS

Cogent DataHub < 7.3.0 Multiple Vulnerabilities

Cogent DataHub < 7.3.4 Malformed POST Request Buffer Overflow RCE

Cogent DataHub < 7.3.5 Multiple Vulnerabilities

Cogent DataHub Tunnel/Mirror Service Detection

Detect PROFINET targets listening on the Network Layer.

DNP3 Binary Inputs Access Remote Information Disclosure

DNP3 Detection of Device attributes

DNP3 Link Layer Brute Force Addressing Disclosure

DNP3 Outstation Unsolicited Messaging Support

Ecava IntegraXor 5.0.413.0 getdata Requests Handling Multiple SQLi

Ecava IntegraXor < 3.60.4050 Unspecified SQL Injection

Ecava IntegraXor < 3.60.4080 XSS

Ecava IntegraXor < 4.00.4283 ActiveX Remote Buffer Overflow

Ecava IntegraXor < 4.1.4369 Project Directory Information Disclosure

Ecava IntegraXor < 4.1.4390 Buffer Overflow

Ecava IntegraXor < 4.1.4410 Information Disclosure

Ecava IntegraXor < 4.2.4458 Multiple Vulnerabilities

Ecava IntegraXor < 4.2.4488 Privilege Escalation

Ecava IntegraXor ActiveX save Method Buffer Overflow

Ecava IntegraXor Detection

Ecava IntegraXor igcom.dll Traversal Arbitrary File Overwrite

Ecava IntegraXor Path Subversion Arbitrary DLL Injection Code Execution

Emerson SM-Ethernet FTP Server Default Credentials

Emerson SM-Ethernet Web Interface Default Credentials

Emerson SM-Ethernet Web Interface Detection

EtherNet/IP CIP Device Identification

EtherNet/IP CIP EDS Metadata

EtherNet/IP CIP List of Active Object Classes

Fuji Electric V-Server Detection

GE D20 Default Credentials

GE Multilin UR / URPlus / B95Plus Protection Relay Cryptographic Algorithm Weakness Information Disclosure (UR-2017-0001)

GE Multilin UR / URPlus / B95Plus Relay Web Interface Detection

Honeywell Excel (XL) Web Controller Detection

Honeywell FALCON XL Web Controller Multiple Vulnerabilities

Honeywell Multiple Products HscRemoteDepoy.dll ActiveX Control Arbitrary Code Execution

Honeywell OPOS Suite Stack Buffer Overflow

Honeywell XL Web Controller FTP Directory Traversal

ICCP/COTP (ISO 8073) Protocol Detection

ICCP/COTP TSAP Addressing Weakness

ICONICS Dialog Wrapper Module ActiveX (DlgWrapper.dll) DoModal Function Overflow

IGSS Data Server Directory Traversal Arbitrary File Access

Induction Automation Ignition

Induction Automation Ignition Multiple Vulnerabilities

iniNet SpiderControl PLC Editor Beckhoff 6.30.04 Local Privilege Escalation

iniNet SpiderControl PLC Editor Beckhoff Detection

iniNet SpiderControl PLC Editor Simatic 6.30.04 Local Privilege Escalation

iniNet SpiderControl PLC Editor Simatic Detection

iniNet SpiderControl SCADA Editor 6.30.01 Local Privilege Escalation

iniNet SpiderControl SCADA Editor Detection

iniNet SpiderControl SCADA Web Server 2.02 Local Privilege Escalation

iniNet SpiderControl SCADA Web Server Detection

IOServer Detection

IOServer XML Server URI Directory Traversal Arbitrary File Access

Janitza Multiple UMG Devices Remote Debug Interface RCE

KEPServerEX < 5.12.140.0 Denial of Service

KEPServerEX Detection

LiveData ICCP Server Detection

LiveData Server Multiple Remote Vulnerabilities

Magnum MNS-6K Hardcoded Admin Account

Matrikon OPC Explorer Detection

Matrikon OPC Server for ControlLogix Detection

Matrikon OPC Server for Modbus Detection

MatrikonOPC Server for DNP3 < 1.2.3.1 Message Handling Remote DoS

MatrikonOPC Server for DNP3 Detection

Measuresoft ScadaPro < 4.0.1.0 service.exe Multiple Vulnerabilities (credentialed check)

Measuresoft ScadaPro < 4.0.1.0 service.exe RF Command Arbitrary File Disclosure

Measuresoft ScadaPro Detection

Measuresoft ScadaPro Path Subversion Arbitrary DLL Injection Code Execution

Meinberg LANTIME Web Interface Unspecified XSS

MicroLogix 1100 PLC Default Credentials

MicroLogix 1400 PLC Web Server Multiple Vulnerabilities

MicroLogix 1400 PLC Web Server Request Handling RCE

Microsys PROMOTIC < 8.1.5 Multiple Vulnerabilities

Microsys PROMOTIC Detection

Microsys PROMOTIC Project File Handling Use-after-free Remote Code Execution

Mitsubishi Electric Automation MC-WorX 8.x ActiveX Control Remote Code Execution

Mitsubishi Electric Automation MC-WorX Suite Detection

Mitsubishi MX Component ActiveX Remote Code Execution

Modbus/TCP Coil Access

Modbus/TCP Device Identification

Modbus/TCP Discrete Input Access

Modbus/TCP Master OPC Server MODBUS Protocol Response Packet Remote Overflow

Modbus/TCP Report Slave ID

Modicon Modbus/TCP Programming Function Code Access

Modicon Modbus/TCP UnityPro Programming Function Code Access

Modicon PLC CPU Type SNMP Request Model Type Remote Disclosure

Modicon PLC Embedded HTTP Server Detection

Modicon PLC IO Scan Status SNMP Request Scan Status Remote Disclosure

Modicon PLC Modbus Slave Mode SNMP Request Modbus Mode Remote Disclosure

Modicon PLC Web Password Status Disclosure SNMP Request Password Status Remote Disclosure

Modicon Quantum HTTP Server 'formTest' 'name' Parameter XSS

Modicon Quantum HTTP Server Default Credentials

Modicon Quantum Telnet Server Default Credentials

Modicon Quantum TFTP Arbitrary File Upload

Movicon < 11.2 Build 1084 Multiple Vulnerabilities

Movicon SCADA/HMI Software Detection

Movicon TcpUploadServer Data Leakage (remote check)

Movicon TcpUploadServer Detection

Moxa Device Manager Gateway Detection

Moxa Device Manager Tool MDM2\_Gateway Response Remote Overflow

Moxa NPort Serial-to-Ethernet Server Detection

Moxa NPort Serial-to-Ethernet Server Multiple Vulnerabilities

National Instruments Lookout Detection

Netbiter Config NetbiterConfig.exe Device Hostname Remote Overflow

OMRON FINS TCP Protocol Detection

OMRON FINS UDP Protocol Detection

OPC Application Components Detection

OPC Data Access (DA) Server Detection

OPC Historical Data Access (HDA) Server Detection

PACTware 4.1 SP3 (4.1.0.42) File Processing Error Handling DoS

PACTware Detection

PACTware Unsupported Version Detection

Panasonic Control FPWIN Pro Detection

Panasonic FPWIN Pro 5.x < 7.130 Multiple Vulnerabilities

ProSoft RadioLinx ControlScape Install Detection

ProSoft RadioLinx ControlScape PRNG Weakness

RealFlex Technologies RealWin Detection

RealWin < 2.1.10 Multiple Packet Type Processing Overflows

RealWin < 2.1.12 Multiple Buffer Overflows

RedLion Crimson Protocol Detection

Rockwell Automation MicroLogix 1100 PLC < FRN 10.0 Authentication Mechanism DoS

Rockwell Automation MicroLogix 1100 PLC < Series B FRN 12.0 MitM Replay Authentication Bypass

Rockwell Automation MicroLogix 1100 PLC < Series B FRN 13.0 Multiple Vulnerabilities

Rockwell Automation MicroLogix 1100 PLC Default Credentials

Rockwell Automation MicroLogix 1100 PLC Web Server Detection

Rockwell Automation MicroLogix 1100/1400 and CompactLogix 5370 Controllers Open Redirection Vulnerability

Rockwell Automation MicroLogix 1400 PLC Default Credentials

Rockwell Automation MicroLogix 1400 PLC Web Server Detection

Rockwell Automation RSLinx Classic < 3.73.00 Buffer Overflow

Rockwell Automation RSLinx Classic < 4.00.01 Local Privilege Escalation

Rockwell Automation RSLinx Classic < 4.11.00 Local Privilege Escalation

Rockwell Automation RSLinx Classic <= 4.00.01 Multiple Vulnerabilities

Rockwell Automation RSLinx Classic Detection

Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow

Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow (CVE-2019-6553)

RuggedCom RuggedOS (ROS) Web-Based Admin Interface Detection

RuggedCom RuggedOS < 3.12.1 Web UI Multiple Security Vulnerabilities

RuggedCom RuggedOS < 3.12.2 Multiple Vulnerabilities

RuggedCom RuggedOS Default 'factory' Account Backdoor

RuggedCom RuggedOS HTTP Traffic Handling Remote DoS

RuggedCom RuggedOS SNMP Protocol Unspecified DoS

RuggedCom RuggedOS Web-Based Admin Interface Default Credentials

Samsung Data Management Server < 1.4.3 verifyUser Method SQL Injection

Samsung Data Management Server Default Password (rkwjsdusrnth) for 'root' Account

SCADA Engine BACnet OPC Server < 2.1.371.24 Multiple Vulnerabilities

Schneider Electric Accutech Manager 'RFManagerService' SQL Injection

Schneider Electric Accutech Manager Detection

Schneider Electric Accutech Manager RFManagerService Heap Overflow

Schneider Electric FTP Server Default Credentials

Schneider Electric InduSoft Web Studio / InTouch Machine Edition < 8.1 RCE

Schneider Electric InduSoft Web Studio / InTouch Machine Edition Opcode 50 mbstowcs() Stack Overflow

Schneider Electric InduSoft Web Studio < 7.1.3.4 Multiple Information Disclosures (SEVD-2015-054-01)

Schneider Electric InduSoft Web Studio < 7.1.3.5 Local Plaintext Password Information Disclosure (SEVD-2015-100-01)

Schneider Electric InduSoft Web Studio < 8.0 SP2 Patch 1 Unspecified Remote Command Execution (LFSEC00000121)

Schneider Electric InduSoft Web Studio Arbitrary Script Execution

Schneider Electric InduSoft Web Studio Detection

Schneider Electric InduSoft Web Studio Detection

Schneider Electric Interactive Graphical SCADA System (IGSS) Unsupported Version

Schneider Electric Interactive Graphical SCADA System dc.exe Unspecified Buffer Overflow

Schneider Electric InTouch Machine Edition Detection

Schneider Electric Multiple Products Buffer Overflow

Schneider Electric OPC Factory Server (OFS) < 3.5 SP1 ActiveX Object Multiple Buffer Overflows DoS

SEL Controller Default Credentials

Sensitive information can be obtained from the GE D20 Remote Terminal Unit via TFTP

Sielco Sistemi Winlog < 2.07.17 Multiple Vulnerabilities

Sielco Sistemi Winlog < 2.07.18 Multiple Vulnerabilities

Sielco Sistemi Winlog Arbitrary File Disclosure

Sielco Sistemi Winlog Detection

Sielco Sistemi Winlog Pro < 2.07.01 TCP/IP Server Runtime.exe Packet Handling Remote Overflow

Siemens Automation License Manager 'almaxcx.dll' ActiveX Arbitrary File Overwrite Vulnerability

Siemens Automation License Manager 5.x < 5.3.4.4 Multiple Vulnerabilities

Siemens Automation License Manager 6.x < 6.0.1 Directory Traversal

Siemens Automation License Manager CVE-2012-4691 Denial of Service

Siemens Automation License Manager Detection

Siemens Automation License Manager Multiple Vulnerabilities

Siemens S7 Protocol Support Detection

Siemens S7-SCL Development Tools Detection

Siemens SCALANCE S612 Firewall > 2.1 and < 2.3.0.3 Multiple Vulnerabilities (SSA-268149)

Siemens SCALANCE S612 Firewall Detection

Siemens SCALANCE X-200 Authentication Bypass

Siemens SCALANCE X-200 Web Session Hijacking

Siemens SCALANCE X-200IRT < 5.2.0 Session Hijacking

Siemens SIMATIC Logon Authentication Bypass

Siemens SIMATIC Logon Detection

Siemens SIMATIC PDM Detection

Siemens SIMATIC ProSave < 1300.100.2201.15 Untrusted Path Arbitrary Code Execution (SSA-451236)

Siemens SIMATIC ProSave Detection

Siemens SIMATIC RF-MANAGER Detection

Siemens SIMATIC RF-MANAGER KeyHelp.ocx Buffer Overflow

Siemens SIMATIC S7-1200 PLC < 4.1 Open Redirection

Siemens SIMATIC S7-1200 PLC < 4.1.3 XSRF

Siemens SIMATIC S7-1200 PLC Firmware Detection

Siemens SIMATIC S7-1200 PLC UDP Denial of Service (CVE-2019-10936)

Siemens SIMATIC S7-1200 PLC Web Server Detection

Siemens SIMATIC STEP 7 (TIA Portal) < 1300.100.2501.1 Multiple Vulnerabilities (SSA-315836)

Siemens SIMATIC STEP 7 (TIA Portal) < 14 Unquoted Service Path Local Privilege Escalation (SSA-701708)

Siemens SIMATIC STEP 7 (TIA Portal) Detection

Siemens SIMATIC STEP 7 Local Privilege Escalation Vulnerability in TIA Portal (SSA-629512)

Siemens SIMATIC TIA Portal 13.x < 13 Upd6 Remote Code Execution

Siemens SIMATIC TIA Portal Detection

Siemens SIMATIC WinCC (TIA Portal) 10.x < 14 SP1 Upd6 Multiple Vulnerabilities (SSA-979106)

Siemens SIMATIC WinCC (TIA Portal) 13 < 13 SP1 Multiple Vulnerabilities (SSA-543623)

Siemens SIMATIC WinCC (TIA Portal) 13 < 13 SP2 / 14 < 14 SP1 Multiple DoS

Siemens SIMATIC WinCC (TIA Portal) 13.x < 13 SP1 Upd2 Multiple Vulnerabilities (SSA-487246)

Siemens SIMATIC WinCC (TIA Portal) < 14 SP1 XXE Vulnerability

Siemens SIMATIC WinCC (TIA Portal) < 14 Unquoted Service Path Local Privilege Escalation (SSA-701708)

Siemens SIMATIC WinCC (TIA Portal) < 15 Update 4 Multiple Vulnerabilities (SSA-233109)

Siemens SIMATIC WinCC (TIA Portal) Code Upload Vulnerability (SSA-121293)

Siemens SIMATIC WinCC (TIA Portal) Detection

Siemens SIMATIC WinCC Default Password Authentication Bypass

Siemens SINEMA Remote Connect Server Detection

Siemens SINEMA Remote Connect Server Multiple Vulnerabilities (SSA-884497)

Siemens SINEMA Server < 13 SP2 Unquoted Service Path Local Privilege Escalation (SSA-701708)

Siemens SINEMA Server Installed

Siemens-Telegyr ICCP Gateway Detection

SISCO OSI Stack Malformed Packet Remote DoS

SISCO OSI Stack Vulnerability Scan Remote DoS

SISCO OSI/ICCP Stack Detection

StruxureWare SCADA Expert ClearSCADA < 2013 R2 Remote DoS

StruxureWare SCADA Expert ClearSCADA Detection

StruxureWare SCADA Expert ClearSCADA Remote Security Bypass

StruxureWare SCADA Expert ClearSCADA Unspecified Vulnerability

StruxureWare SCADA Expert ClearSCADA Weak Hashing Algorithm

Takebishi Electric DeviceXPlorer OPC Server Multiple Vulnerabilities

Tamarack IEC 61850 Server Detection

Telvent OASyS System Detection

Triangle MicroWorks SCADA Data Gateway < 3.0.635 Multiple DoS Vulnerabilities

Triangle MicroWorks SCADA Data Gateway < 3.3.729 Heartbeat Information Disclosure (Heartbleed)

Triangle MicroWorks SCADA Data Gateway Detection (credentialed check)

Tridium Niagara AX Web Server Detection

Tridium Niagara AX Web Server Directory Traversal 'config.bog' Disclosure Remote Compromise

Tridium Niagara AX Web Server Multiple Vulnerabilities

Trihedral VTScada 6.5.x < 9.1.20 / 10.x < 10.2.22 / 11.x < 11.1.09 HTTP Server DoS

Trihedral VTScada 8.x < 11.2.02 Multiple Vulnerabilities

Trihedral VTScada Detection

Trihedral VTScada Detection

TURCK BL20/BL67 Hardcoded Admin Account

WellinTech KingHistorian Detection

WellinTech KingOPCServer Detection

WellinTech KingSCADA 3.1 < 2012-04-16 user.db Base-64 Encoding Local Credentials Disclosure

WellinTech KingSCADA < 3.1.2.13-EN 'kxClientDownload.ocx' ActiveX RCE

WellinTech KingSCADA < 3.1.2.13-EN 'kxNetDispose.dll' Buffer Overflow RCE

WellinTech KingSCADA < 3.1.2.13-EN KAEClientManager Console Remote Authentication Credential Disclosure

WellinTech KingSCADA Detection

WellinTech KingView 6.53 < 2010-12-15 HistorySvr.exe TCP Request Remote Overflow

WellinTech KingView 6.53 < 2011-11-20 HistoryServer.exe nettransdll.dll Module Op-code 3 Packet Parsing Remote Overflow

WellinTech KingView 6.53 < 2012-03-22 Multiple Vulnerabilities

WellinTech KingView < 6.53 (2012-10-09) User Credentials Not Securely Hashed

WellinTech KingView ActiveX Multiple Arbitrary File Overwrite Vulnerabilities

WellinTech KingView Detection

WellinTech KingView History Server Detection

# RPC

3270 Mapper Service Detection

CDE RPC tooltalk Service Multiple Overflows

Detect RPC over TCP

Detect RPC over UDP

IRIX rpc.yppasswdd Unspecified Remote Overflow

JetBrains TeamCity Agent XML-RPC Port RCE

Linux Multiple statd Packages Remote Format String

Linux NFS utils package (nfs-utils) mountd xlog Function Off-by-one Remote Overflow

Multiple Vendor NFS CD Command Arbitrary File/Directory Access

Multiple Vendor NIS rpc.ypupdated YP Map Update Arbitrary Remote Command Execution

Multiple Vendor RPC portmapper Access Restriction Bypass

Multiple Vendor rpc.nisd Long NIS+ Argument Remote Overflow

NFS Exported Share Information Disclosure

NFS portmapper localhost Mount Request Restricted Host Access

NFS Predictable Filehandles Filesystem Access

NFS Server Superfluous

NFS Share Export List

NFS Share User Mountable

NFS Shares World Readable

NIS passwd.byname Map Disclosure

NIS Server Detection

RPC alis Service Detection

RPC bootparamd NIS Domain Name Disclosure

RPC bootparamd Service Information Disclosure (Deprecated)

RPC database Service Detection

RPC etherstatd Service Detection

RPC nibindd Service Detection

RPC portmapper (TCP)

RPC portmapper Service Detection

RPC rpcbind Non-standard Port Assignment Filter Bypass

RPC rstatd Service Detection

RPC rusers Remote Information Disclosure

rquotad Service Detection

Solaris rpc.rwalld Remote Format String Arbitrary Code Execution

Solaris XDR RPC Request Handling RCE (April 2017 CPU) (EBBISLAND / EBBSHAVE)

Sun RPC XDR xdrmem\_getbytes Function Remote Overflow

Sun rpc.cmsd Remote Overflow

VxWorks WDB Debug Service Detection

# Red Hat Local Security Checks

HP Network Node Manager i (NNMi) 8.x / 9.0x / 9.1x / 9.20 Unspecified XSS

HP Network Node Manager i (NNMi) XSS (HPSBMU03035)

HP Network Node Manager i Remote Code Execution (HPSBMU03075)

HP SNMP Agents < 9.0.0 Multiple Vulnerabilities (HPSBMU02771 SSRT100558) (Red Hat)

HP Version Control Agent (VCA) < 7.3.3 Multiple SSL Vulnerabilities

HP Version Control Agent (VCA) Heartbeat Information Disclosure (Heartbleed)

HPE Network Node Manager i (NNMi) Multiple Vulnerabilities (HPESBGN03762)

IBM General Parallel File System 3.4 < 3.4.0.27 / 3.5 < 3.5.0.16 DoS (RHEL)

JBoss Enterprise Application Platform 6.1.0 Update (RHSA-2013:0833)

JBoss Enterprise Application Platform 6.1.1 Update (RHSA-2013:1209)

JBoss Enterprise Portal Platform 5.2.2 Security Update (RHSA-2013-0141)

JBoss Enterprise Portal Platform GateIn Portal Security Update (RHSA-2013-0613)

JBoss Portal 6.1.0 Update (RHSA-2013:1437)

Red Hat Enterprise Linux fixes

Red Hat JBoss Enterprise Application Platform 6.1.0 Security Update (RHSA-2013:1152)

Red Hat JBoss Enterprise Application Platform 6.1.0 Security Update (RHSA-2013:1843)

Red Hat Single User Mode

Red Hat Update Level

Remote host has a compromised Red Hat OpenSSH package intalled

RHEL 2.1 / 3 / 4 / 5 : bind (RHSA-2007:0740)

RHEL 2.1 / 3 / 4 / 5 : bind (RHSA-2008:0533)

RHEL 2.1 / 3 / 4 / 5 : bind (RHSA-2009:0020)

RHEL 2.1 / 3 / 4 / 5 : bzip2 (RHSA-2008:0893)

RHEL 2.1 / 3 / 4 / 5 : curl (RHSA-2009:0341)

RHEL 2.1 / 3 / 4 / 5 : e2fsprogs (RHSA-2008:0003)

RHEL 2.1 / 3 / 4 / 5 : ed (RHSA-2008:0946)

RHEL 2.1 / 3 / 4 / 5 : fetchmail (RHSA-2007:0385)

RHEL 2.1 / 3 / 4 / 5 : freetype (RHSA-2007:0403)

RHEL 2.1 / 3 / 4 / 5 : gimp (RHSA-2007:0343)

RHEL 2.1 / 3 / 4 / 5 : gimp (RHSA-2007:0513)

RHEL 2.1 / 3 / 4 / 5 : krb5 (RHSA-2007:0095)

RHEL 2.1 / 3 / 4 / 5 : libpng (RHSA-2007:0356)

RHEL 2.1 / 3 / 4 / 5 : libpng (RHSA-2007:0992)

RHEL 2.1 / 3 / 4 / 5 : libxml2 (RHSA-2008:0032)

RHEL 2.1 / 3 / 4 / 5 : libxml2 (RHSA-2008:0836)

RHEL 2.1 / 3 / 4 / 5 : libxml2 (RHSA-2008:0988)

RHEL 2.1 / 3 / 4 / 5 : libxslt (RHSA-2008:0287)

RHEL 2.1 / 3 / 4 / 5 : lynx (RHSA-2008:0965)

RHEL 2.1 / 3 / 4 / 5 : openssl (RHSA-2009:0004)

RHEL 2.1 / 3 / 4 / 5 : qt (RHSA-2007:0883)

RHEL 2.1 / 3 / 4 / 5 : samba (RHSA-2007:0354)

RHEL 2.1 / 3 / 4 / 5 : samba (RHSA-2007:1114)

RHEL 2.1 / 3 / 4 / 5 : squid (RHSA-2007:1130)

RHEL 2.1 / 3 / 4 / 5 : squid (RHSA-2008:0214)

RHEL 2.1 / 3 / 4 / 5 : tetex (RHSA-2007:0731)

RHEL 2.1 / 3 / 4 / 5 : wireshark (RHSA-2007:0066)

RHEL 2.1 / 3 / 4 : bind (RHSA-2007:0044)

RHEL 2.1 / 3 / 4 : bzip2 (RHSA-2005:474)

RHEL 2.1 / 3 / 4 : curl (RHSA-2005:340)

RHEL 2.1 / 3 / 4 : cvs (RHSA-2005:387)

RHEL 2.1 / 3 / 4 : cvs (RHSA-2005:756)

RHEL 2.1 / 3 / 4 : enscript (RHSA-2008:1021)

RHEL 2.1 / 3 / 4 : ethereal (RHSA-2005:306)

RHEL 2.1 / 3 / 4 : ethereal (RHSA-2005:427)

RHEL 2.1 / 3 / 4 : ethereal (RHSA-2005:687)

RHEL 2.1 / 3 / 4 : ethereal (RHSA-2005:809)

RHEL 2.1 / 3 / 4 : ethereal (RHSA-2006:0156)

RHEL 2.1 / 3 / 4 : ethereal (RHSA-2006:0420)

RHEL 2.1 / 3 / 4 : fetchmail (RHSA-2005:640)

RHEL 2.1 / 3 / 4 : fetchmail (RHSA-2007:0018)

RHEL 2.1 / 3 / 4 : freetype (RHSA-2006:0500)

RHEL 2.1 / 3 / 4 : gdk-pixbuf (RHSA-2005:343)

RHEL 2.1 / 3 / 4 : gdk-pixbuf (RHSA-2005:810)

RHEL 2.1 / 3 / 4 : gftp (RHSA-2005:410)

RHEL 2.1 / 3 / 4 : gnome-vfs, gnome-vfs2 (RHSA-2009:0005)

RHEL 2.1 / 3 / 4 : gnupg (RHSA-2006:0266)

RHEL 2.1 / 3 / 4 : gnupg (RHSA-2006:0571)

RHEL 2.1 / 3 / 4 : gnupg (RHSA-2006:0615)

RHEL 2.1 / 3 / 4 : gnupg (RHSA-2006:0754)

RHEL 2.1 / 3 / 4 : gnupg (RHSA-2007:0106)

RHEL 2.1 / 3 / 4 : gzip (RHSA-2005:357)

RHEL 2.1 / 3 / 4 : gzip (RHSA-2006:0667)

RHEL 2.1 / 3 / 4 : ImageMagick (RHSA-2005:480)

RHEL 2.1 / 3 / 4 : ImageMagick (RHSA-2006:0178)

RHEL 2.1 / 3 / 4 : ImageMagick (RHSA-2006:0633)

RHEL 2.1 / 3 / 4 : ImageMagick (RHSA-2007:0015)

RHEL 2.1 / 3 / 4 : kdelibs (RHSA-2006:0720)

RHEL 2.1 / 3 / 4 : krb5 (RHSA-2005:330)

RHEL 2.1 / 3 / 4 : libtiff (RHSA-2006:0425)

RHEL 2.1 / 3 / 4 : libtiff (RHSA-2006:0603)

RHEL 2.1 / 3 / 4 : libungif (RHSA-2005:828)

RHEL 2.1 / 3 / 4 : lynx (RHSA-2005:803)

RHEL 2.1 / 3 / 4 : lynx (RHSA-2005:839)

RHEL 2.1 / 3 / 4 : mikmod (RHSA-2005:506)

RHEL 2.1 / 3 / 4 : mozilla (RHSA-2005:435)

RHEL 2.1 / 3 / 4 : mozilla (RHSA-2005:587)

RHEL 2.1 / 3 / 4 : mozilla (RHSA-2005:769)

RHEL 2.1 / 3 / 4 : mozilla (RHSA-2005:789)

RHEL 2.1 / 3 / 4 : mozilla (RHSA-2006:0199)

RHEL 2.1 / 3 / 4 : mozilla (RHSA-2006:0329)

RHEL 2.1 / 3 / 4 : mutt (RHSA-2006:0577)

RHEL 2.1 / 3 / 4 : mysql (RHSA-2005:334)

RHEL 2.1 / 3 / 4 : nasm (RHSA-2005:381)

RHEL 2.1 / 3 / 4 : ncompress (RHSA-2006:0663)

RHEL 2.1 / 3 / 4 : netpbm (RHSA-2005:743)

RHEL 2.1 / 3 / 4 : netpbm (RHSA-2008:0131)

RHEL 2.1 / 3 / 4 : openmotif (RHSA-2005:412)

RHEL 2.1 / 3 / 4 : openmotif (RHSA-2006:0272)

RHEL 2.1 / 3 / 4 : openssl (RHSA-2005:476)

RHEL 2.1 / 3 / 4 : openssl (RHSA-2005:800)

RHEL 2.1 / 3 / 4 : openssl (RHSA-2006:0661)

RHEL 2.1 / 3 / 4 : openssl (RHSA-2006:0695)

RHEL 2.1 / 3 / 4 : pcre (RHSA-2005:761)

RHEL 2.1 / 3 / 4 : php (RHSA-2006:0730)

RHEL 2.1 / 3 / 4 : python (RHSA-2006:0197)

RHEL 2.1 / 3 / 4 : qt (RHSA-2006:0725)

RHEL 2.1 / 3 / 4 : ruby (RHSA-2005:799)

RHEL 2.1 / 3 / 4 : ruby (RHSA-2006:0604)

RHEL 2.1 / 3 / 4 : ruby (RHSA-2006:0729)

RHEL 2.1 / 3 / 4 : samba (RHSA-2006:0591)

RHEL 2.1 / 3 / 4 : samba (RHSA-2008:0288)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2006:0676)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2006:0734)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2006:0759)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2007:0077)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2007:0402)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2007:0722)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2007:0980)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2007:1084)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:0104)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:0208)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:0223)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:0547)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:0599)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:0882)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:0977)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2008:1037)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2009:0257)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2009:0325)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2009:0398)

RHEL 2.1 / 3 / 4 : seamonkey (RHSA-2009:0437)

RHEL 2.1 / 3 / 4 : sendmail (RHSA-2006:0515)

RHEL 2.1 / 3 / 4 : sharutils (RHSA-2005:377)

RHEL 2.1 / 3 / 4 : squid (RHSA-2005:766)

RHEL 2.1 / 3 / 4 : sudo (RHSA-2005:535)

RHEL 2.1 / 3 / 4 : sysreport (RHSA-2005:502)

RHEL 2.1 / 3 / 4 : sysreport (RHSA-2005:598)

RHEL 2.1 / 3 / 4 : tar (RHSA-2006:0749)

RHEL 2.1 / 3 / 4 : telnet (RHSA-2005:327)

RHEL 2.1 / 3 / 4 : telnet (RHSA-2005:504)

RHEL 2.1 / 3 / 4 : tetex (RHSA-2006:0160)

RHEL 2.1 / 3 / 4 : texinfo (RHSA-2006:0727)

RHEL 2.1 / 3 / 4 : util-linux and mount (RHSA-2005:782)

RHEL 2.1 / 3 / 4 : vim (RHSA-2005:745)

RHEL 2.1 / 3 / 4 : wget (RHSA-2005:771)

RHEL 2.1 / 3 / 4 : wget (RHSA-2005:812)

RHEL 2.1 / 3 / 4 : wireshark (RHSA-2006:0602)

RHEL 2.1 / 3 / 4 : wireshark (RHSA-2006:0658)

RHEL 2.1 / 3 / 4 : wireshark (RHSA-2006:0726)

RHEL 2.1 / 3 / 4 : xloadimage (RHSA-2005:332)

RHEL 2.1 / 3 / 4 : xloadimage (RHSA-2005:802)

RHEL 2.1 / 3 / 4 : xpdf (RHSA-2005:840)

RHEL 2.1 / 3 / 4 : xpdf (RHSA-2007:0735)

RHEL 2.1 / 3 / 4 : xscreensaver (RHSA-2007:0322)

RHEL 2.1 / 3 : cvs (RHSA-2004:004)

RHEL 2.1 / 3 : cvs (RHSA-2004:153)

RHEL 2.1 / 3 : cvs (RHSA-2004:190)

RHEL 2.1 / 3 : cvs (RHSA-2004:233)

RHEL 2.1 / 3 : cyrus-sasl (RHSA-2004:546)

RHEL 2.1 / 3 : emacs (RHSA-2005:112)

RHEL 2.1 / 3 : enscript (RHSA-2005:039)

RHEL 2.1 / 3 : ethereal (RHSA-2003:324)

RHEL 2.1 / 3 : ethereal (RHSA-2004:002)

RHEL 2.1 / 3 : ethereal (RHSA-2004:136)

RHEL 2.1 / 3 : ethereal (RHSA-2004:234)

RHEL 2.1 / 3 : ethereal (RHSA-2004:378)

RHEL 2.1 / 3 : ethereal (RHSA-2005:011)

RHEL 2.1 / 3 : gd (RHSA-2004:638)

RHEL 2.1 / 3 : gdk-pixbuf (RHSA-2004:103)

RHEL 2.1 / 3 : gdk-pixbuf (RHSA-2004:447)

RHEL 2.1 / 3 : gnome-vfs (RHSA-2004:373)

RHEL 2.1 / 3 : gnupg (RHSA-2003:395)

RHEL 2.1 / 3 : ImageMagick (RHSA-2004:636)

RHEL 2.1 / 3 : ImageMagick (RHSA-2005:070)

RHEL 2.1 / 3 : imap (RHSA-2005:850)

RHEL 2.1 / 3 : imlib (RHSA-2004:465)

RHEL 2.1 / 3 : imlib (RHSA-2004:651)

RHEL 2.1 / 3 : iproute (RHSA-2003:317)

RHEL 2.1 / 3 : kdegraphics (RHSA-2005:021)

RHEL 2.1 / 3 : kdegraphics (RHSA-2006:0648)

RHEL 2.1 / 3 : kdelibs (RHSA-2004:222)

RHEL 2.1 / 3 : kdelibs (RHSA-2005:307)

RHEL 2.1 / 3 : kdelibs, kdebase (RHSA-2004:412)

RHEL 2.1 / 3 : kdelibs, kdebase (RHSA-2005:009)

RHEL 2.1 / 3 : kdenetwork (RHSA-2005:175)

RHEL 2.1 / 3 : krb5 (RHSA-2004:236)

RHEL 2.1 / 3 : krb5 (RHSA-2005:012)

RHEL 2.1 / 3 : krb5 (RHSA-2005:562)

RHEL 2.1 / 3 : krb5 (RHSA-2007:0384)

RHEL 2.1 / 3 : krb5 (RHSA-2008:0181)

RHEL 2.1 / 3 : krb5 (RHSA-2009:0410)

RHEL 2.1 / 3 : lftp (RHSA-2003:404)

RHEL 2.1 / 3 : lha (RHSA-2004:178)

RHEL 2.1 / 3 : libpng (RHSA-2004:180)

RHEL 2.1 / 3 : libpng (RHSA-2004:402)

RHEL 2.1 / 3 : libtiff (RHSA-2004:577)

RHEL 2.1 / 3 : libtiff (RHSA-2005:019)

RHEL 2.1 / 3 : libtiff (RHSA-2008:0863)

RHEL 2.1 / 3 : libxml (RHSA-2004:650)

RHEL 2.1 / 3 : libxml2 (RHSA-2004:090)

RHEL 2.1 / 3 : libxml2 (RHSA-2004:615)

RHEL 2.1 / 3 : mailman (RHSA-2005:136)

RHEL 2.1 / 3 : mod\_python (RHSA-2004:058)

RHEL 2.1 / 3 : mod\_python (RHSA-2005:104)

RHEL 2.1 / 3 : mozilla (RHSA-2004:110)

RHEL 2.1 / 3 : mozilla (RHSA-2004:421)

RHEL 2.1 / 3 : mozilla (RHSA-2004:486)

RHEL 2.1 / 3 : mozilla (RHSA-2005:038)

RHEL 2.1 / 3 : mozilla (RHSA-2005:323)

RHEL 2.1 / 3 : Mozilla (RHSA-2005:384)

RHEL 2.1 / 3 : netpbm (RHSA-2004:031)

RHEL 2.1 / 3 : netpbm (RHSA-2005:843)

RHEL 2.1 / 3 : openldap and nss\_ldap (RHSA-2005:751)

RHEL 2.1 / 3 : openmotif (RHSA-2004:537)

RHEL 2.1 / 3 : openssl (RHSA-2007:0813)

RHEL 2.1 / 3 : perl (RHSA-2005:069)

RHEL 2.1 / 3 : qt (RHSA-2004:414)

RHEL 2.1 / 3 : rsync (RHSA-2003:399)

RHEL 2.1 / 3 : rsync (RHSA-2004:192)

RHEL 2.1 / 3 : rsync (RHSA-2004:436)

RHEL 2.1 / 3 : ruby (RHSA-2004:441)

RHEL 2.1 / 3 : ruby (RHSA-2004:635)

RHEL 2.1 / 3 : ruby (RHSA-2008:0562)

RHEL 2.1 / 3 : samba (RHSA-2004:632)

RHEL 2.1 / 3 : samba (RHSA-2007:1013)

RHEL 2.1 / 3 : slocate (RHSA-2004:041)

RHEL 2.1 / 3 : squid (RHSA-2004:133)

RHEL 2.1 / 3 : squid (RHSA-2004:591)

RHEL 2.1 / 3 : squid (RHSA-2005:061)

RHEL 2.1 / 3 : squid (RHSA-2005:173)

RHEL 2.1 / 3 : sysstat (RHSA-2004:053)

RHEL 2.1 / 3 : tar (RHSA-2006:0195)

RHEL 2.1 / 3 : tcltk (RHSA-2008:0134)

RHEL 2.1 / 3 : tcpdump (RHSA-2004:008)

RHEL 2.1 / 3 : tcpdump (RHSA-2004:219)

RHEL 2.1 / 3 : tetex (RHSA-2005:354)

RHEL 2.1 / 3 : tetex (RHSA-2007:1028)

RHEL 2.1 / 3 : unzip (RHSA-2008:0196)

RHEL 2.1 / 3 : utempter (RHSA-2004:174)

RHEL 2.1 / 3 : vim (RHSA-2005:010)

RHEL 2.1 / 3 : vim (RHSA-2005:122)

RHEL 2.1 / 3 : xchat (RHSA-2004:585)

RHEL 2.1 / 3 : xemacs (RHSA-2005:134)

RHEL 2.1 / 3 : XFree86 (RHSA-2006:0635)

RHEL 2.1 / 3 : XFree86 (RHSA-2006:0666)

RHEL 2.1 / 3 : XFree86 (RHSA-2007:0002)

RHEL 2.1 / 3 : XFree86 (RHSA-2007:0125)

RHEL 2.1 / 3 : XFree86 (RHSA-2008:0029)

RHEL 2.1 / 3 : xpdf (RHSA-2004:592)

RHEL 2.1 / 3 : xpdf (RHSA-2005:213)

RHEL 2.1 / 3 : xscreensaver (RHSA-2006:0498)

RHEL 2.1 / 3 : zip (RHSA-2004:634)

RHEL 2.1 / 4 / 5 : libpng (RHSA-2009:0333)

RHEL 2.1 / 4 : dia (RHSA-2006:0280)

RHEL 2.1 : apache (RHSA-2002:126)

RHEL 2.1 : apache (RHSA-2002:251)

RHEL 2.1 : apache (RHSA-2003:244)

RHEL 2.1 : apache (RHSA-2003:360)

RHEL 2.1 : apache (RHSA-2006:0158)

RHEL 2.1 : apache (RHSA-2006:0618)

RHEL 2.1 : apache (RHSA-2007:0532)

RHEL 2.1 : apache (RHSA-2008:0004)

RHEL 2.1 : apache, mod\_ssl (RHSA-2004:245)

RHEL 2.1 : apache, mod\_ssl (RHSA-2004:600)

RHEL 2.1 : auth\_ldap (RHSA-2006:0179)

RHEL 2.1 : balsa (RHSA-2003:111)

RHEL 2.1 : bind (RHSA-2002:119)

RHEL 2.1 : binutils (RHSA-2005:763)

RHEL 2.1 : cadaver (RHSA-2004:157)

RHEL 2.1 : cadaver (RHSA-2004:191)

RHEL 2.1 : Canna (RHSA-2002:261)

RHEL 2.1 : cpio (RHSA-2005:806)

RHEL 2.1 : cvs (RHSA-2003:013)

RHEL 2.1 : ddskk (RHSA-2003:242)

RHEL 2.1 : dhcp (RHSA-2005:212)

RHEL 2.1 : dhcp (RHSA-2007:0970)

RHEL 2.1 : dhcpcd (RHSA-2005:603)

RHEL 2.1 : dump (RHSA-2005:583)

RHEL 2.1 : elm (RHSA-2004:009)

RHEL 2.1 : elm (RHSA-2005:755)

RHEL 2.1 : ethereal (RHSA-2002:170)

RHEL 2.1 : ethereal (RHSA-2002:291)

RHEL 2.1 : ethereal (RHSA-2003:077)

RHEL 2.1 : fam (RHSA-2005:005)

RHEL 2.1 : fetchmail (RHSA-2002:216)

RHEL 2.1 : fetchmail (RHSA-2002:294)

RHEL 2.1 : fetchmail (RHSA-2005:823)

RHEL 2.1 : file (RHSA-2003:087)

RHEL 2.1 : fileutils (RHSA-2003:016)

RHEL 2.1 : fileutils (RHSA-2003:310)

RHEL 2.1 : freetype (RHSA-2008:0558)

RHEL 2.1 : freetype (RHSA-2009:1062)

RHEL 2.1 : gaim (RHSA-2002:122)

RHEL 2.1 : gaim (RHSA-2002:191)

RHEL 2.1 : gaim (RHSA-2004:045)

RHEL 2.1 : gaim (RHSA-2005:432)

RHEL 2.1 : gaim (RHSA-2005:589)

RHEL 2.1 : gdb (RHSA-2005:801)

RHEL 2.1 : gdm (RHSA-2003:259)

RHEL 2.1 : ggv (RHSA-2002:211)

RHEL 2.1 : ghostscript (RHSA-2002:123)

RHEL 2.1 : ghostscript (RHSA-2003:182)

RHEL 2.1 : glibc (RHSA-2002:167)

RHEL 2.1 : glibc (RHSA-2003:022)

RHEL 2.1 : glibc (RHSA-2003:090)

RHEL 2.1 : glibc (RHSA-2003:249)

RHEL 2.1 : glibc (RHSA-2004:383)

RHEL 2.1 : glibc (RHSA-2005:261)

RHEL 2.1 : gnupg (RHSA-2003:176)

RHEL 2.1 : grip (RHSA-2005:304)

RHEL 2.1 : hanterm-xf (RHSA-2003:071)

RHEL 2.1 : hanterm-xf (RHSA-2009:0019)

RHEL 2.1 : IBMJava2 (RHSA-2007:0072)

RHEL 2.1 : IBMJava2 (RHSA-2008:0133)

RHEL 2.1 : im (RHSA-2003:038)

RHEL 2.1 : ImageMagick (RHSA-2004:494)

RHEL 2.1 : ImageMagick (RHSA-2008:0165)

RHEL 2.1 : imap (RHSA-2005:114)

RHEL 2.1 : kdbg (RHSA-2005:416)

RHEL 2.1 : kdebase (RHSA-2003:146)

RHEL 2.1 : kdebase (RHSA-2003:270)

RHEL 2.1 : kdelibs (RHSA-2002:221)

RHEL 2.1 : kdelibs (RHSA-2003:003)

RHEL 2.1 : kdelibs (RHSA-2003:193)

RHEL 2.1 : kdelibs (RHSA-2003:236)

RHEL 2.1 : kdelibs (RHSA-2004:074)

RHEL 2.1 : kernel (RHSA-2002:128)

RHEL 2.1 : kernel (RHSA-2002:227)

RHEL 2.1 : kernel (RHSA-2002:263)

RHEL 2.1 : kernel (RHSA-2003:103)

RHEL 2.1 : kernel (RHSA-2003:147)

RHEL 2.1 : kernel (RHSA-2003:195)

RHEL 2.1 : kernel (RHSA-2003:239)

RHEL 2.1 : kernel (RHSA-2003:389)

RHEL 2.1 : kernel (RHSA-2003:408)

RHEL 2.1 : kernel (RHSA-2003:419)

RHEL 2.1 : kernel (RHSA-2004:044)

RHEL 2.1 : kernel (RHSA-2004:069)

RHEL 2.1 : kernel (RHSA-2004:105)

RHEL 2.1 : kernel (RHSA-2004:260)

RHEL 2.1 : kernel (RHSA-2004:354)

RHEL 2.1 : kernel (RHSA-2004:418)

RHEL 2.1 : kernel (RHSA-2004:437)

RHEL 2.1 : kernel (RHSA-2004:505)

RHEL 2.1 : kernel (RHSA-2005:016)

RHEL 2.1 : kernel (RHSA-2005:283)

RHEL 2.1 : kernel (RHSA-2005:529)

RHEL 2.1 : kernel (RHSA-2006:0191)

RHEL 2.1 : kernel (RHSA-2006:0579)

RHEL 2.1 : kernel (RHSA-2007:0013)

RHEL 2.1 : kernel (RHSA-2007:0672)

RHEL 2.1 : kernel (RHSA-2009:0001)

RHEL 2.1 : koffice (RHSA-2007:0010)

RHEL 2.1 : kon2 (RHSA-2003:050)

RHEL 2.1 : krb5 (RHSA-2002:173)

RHEL 2.1 : krb5 (RHSA-2002:250)

RHEL 2.1 : krb5 (RHSA-2003:021)

RHEL 2.1 : krb5 (RHSA-2003:052)

RHEL 2.1 : krb5 (RHSA-2004:448)

RHEL 2.1 : lesstif (RHSA-2005:004)

RHEL 2.1 : lesstif (RHSA-2005:473)

RHEL 2.1 : lha (RHSA-2004:440)

RHEL 2.1 : libpng (RHSA-2002:152)

RHEL 2.1 : libpng (RHSA-2003:007)

RHEL 2.1 : libuser (RHSA-2005:770)

RHEL 2.1 : libvorbis (RHSA-2007:0912)

RHEL 2.1 : libvorbis (RHSA-2008:0271)

RHEL 2.1 : libxml2 (RHSA-2008:0886)

RHEL 2.1 : logwatch (RHSA-2005:364)

RHEL 2.1 : LPRng (RHSA-2002:120)

RHEL 2.1 : LPRng (RHSA-2003:150)

RHEL 2.1 : lv (RHSA-2003:167)

RHEL 2.1 : lynx (RHSA-2003:030)

RHEL 2.1 : mailman (RHSA-2002:125)

RHEL 2.1 : mailman (RHSA-2002:181)

RHEL 2.1 : mailman (RHSA-2004:019)

RHEL 2.1 : mailman (RHSA-2004:156)

RHEL 2.1 : man (RHSA-2003:134)

RHEL 2.1 : mc (RHSA-2004:035)

RHEL 2.1 : mc (RHSA-2004:172)

RHEL 2.1 : mc (RHSA-2004:464)

RHEL 2.1 : mc (RHSA-2005:217)

RHEL 2.1 : mc (RHSA-2005:512)

RHEL 2.1 : metamail (RHSA-2004:073)

RHEL 2.1 : metamail (RHSA-2006:0217)

RHEL 2.1 : mgetty (RHSA-2003:008)

RHEL 2.1 : micq (RHSA-2003:119)

RHEL 2.1 : mm (RHSA-2002:154)

RHEL 2.1 : mod\_auth\_any (RHSA-2003:114)

RHEL 2.1 : mod\_perl (RHSA-2007:0486)

RHEL 2.1 : mod\_ssl (RHSA-2002:136)

RHEL 2.1 : mod\_ssl (RHSA-2004:408)

RHEL 2.1 : mod\_ssl (RHSA-2005:773)

RHEL 2.1 : mozilla (RHSA-2003:046)

RHEL 2.1 : mozilla (RHSA-2003:163)

RHEL 2.1 : mysql (RHSA-2002:289)

RHEL 2.1 : mysql (RHSA-2003:094)

RHEL 2.1 : mysql (RHSA-2003:282)

RHEL 2.1 : mysql (RHSA-2004:597)

RHEL 2.1 : ncompress (RHSA-2004:536)

RHEL 2.1 : ncpfs (RHSA-2005:371)

RHEL 2.1 : netpbm (RHSA-2003:061)

RHEL 2.1 : netscape (RHSA-2003:027)

RHEL 2.1 : nfs-utils (RHSA-2003:207)

RHEL 2.1 : nfs-utils (RHSA-2005:014)

RHEL 2.1 : nss\_ldap (RHSA-2002:180)

RHEL 2.1 : openldap (RHSA-2002:312)

RHEL 2.1 : openssh (RHSA-2002:131)

RHEL 2.1 : openssh (RHSA-2003:224)

RHEL 2.1 : openssh (RHSA-2003:280)

RHEL 2.1 : openssh (RHSA-2005:481)

RHEL 2.1 : openssh (RHSA-2006:0698)

RHEL 2.1 : openssl (RHSA-2002:157)

RHEL 2.1 : openssl (RHSA-2002:161)

RHEL 2.1 : openssl (RHSA-2003:063)

RHEL 2.1 : openssl (RHSA-2003:102)

RHEL 2.1 : openssl (RHSA-2003:293)

RHEL 2.1 : openssl (RHSA-2004:119)

RHEL 2.1 : openssl (RHSA-2005:829)

RHEL 2.1 : pam (RHSA-2003:028)

RHEL 2.1 : pam (RHSA-2004:304)

RHEL 2.1 : pam\_smb (RHSA-2003:262)

RHEL 2.1 : pan (RHSA-2003:312)

RHEL 2.1 : pcre (RHSA-2007:1065)

RHEL 2.1 : perl (RHSA-2003:257)

RHEL 2.1 : php (RHSA-2002:129)

RHEL 2.1 : php (RHSA-2002:214)

RHEL 2.1 : php (RHSA-2004:395)

RHEL 2.1 : php (RHSA-2005:031)

RHEL 2.1 : php (RHSA-2005:838)

RHEL 2.1 : php (RHSA-2006:0501)

RHEL 2.1 : php (RHSA-2006:0567)

RHEL 2.1 : php (RHSA-2006:0682)

RHEL 2.1 : php (RHSA-2006:0708)

RHEL 2.1 : php (RHSA-2007:0081)

RHEL 2.1 : php (RHSA-2007:0154)

RHEL 2.1 : php (RHSA-2007:0888)

RHEL 2.1 : php (RHSA-2008:0546)

RHEL 2.1 : pine (RHSA-2002:271)

RHEL 2.1 : pine (RHSA-2003:274)

RHEL 2.1 : pine (RHSA-2005:015)

RHEL 2.1 : postgresql (RHSA-2002:301)

RHEL 2.1 : postgresql (RHSA-2003:314)

RHEL 2.1 : postgresql (RHSA-2005:150)

RHEL 2.1 : pxe (RHSA-2002:165)

RHEL 2.1 : python (RHSA-2003:048)

RHEL 2.1 : python (RHSA-2007:1077)

RHEL 2.1 : redhat-release (EOL Notice) (RHSA-2008:0521)

RHEL 2.1 : redhat-release (EOL Notice) (RHSA-2009:0297)

RHEL 2.1 : redhat-release (EOL Notice) (RHSA-2009:1076)

RHEL 2.1 : rsh (RHSA-2005:495)

RHEL 2.1 : ruby (RHSA-2008:0895)

RHEL 2.1 : rxvt (RHSA-2003:055)

RHEL 2.1 : samba (RHSA-2003:096)

RHEL 2.1 : samba (RHSA-2003:138)

RHEL 2.1 : samba (RHSA-2004:404)

RHEL 2.1 : samba (RHSA-2004:498)

RHEL 2.1 : samba (RHSA-2004:681)

RHEL 2.1 : samba (RHSA-2005:020)

RHEL 2.1 : sane-backends (RHSA-2003:285)

RHEL 2.1 : seamonkey (RHSA-2006:0594)

RHEL 2.1 : semi (RHSA-2003:231)

RHEL 2.1 : semi (RHSA-2004:344)

RHEL 2.1 : sendmail (RHSA-2002:259)

RHEL 2.1 : sendmail (RHSA-2003:074)

RHEL 2.1 : sendmail (RHSA-2003:121)

RHEL 2.1 : sendmail (RHSA-2003:284)

RHEL 2.1 : sendmail (RHSA-2006:0265)

RHEL 2.1 : shadow-utils (RHSA-2003:058)

RHEL 2.1 : sharutils (RHSA-2003:180)

RHEL 2.1 : slocate (RHSA-2005:747)

RHEL 2.1 : squid (RHSA-2002:130)

RHEL 2.1 : squid (RHSA-2005:489)

RHEL 2.1 : stunnel (RHSA-2003:223)

RHEL 2.1 : stunnel (RHSA-2003:297)

RHEL 2.1 : sylpheed (RHSA-2005:303)

RHEL 2.1 : tcpdump (RHSA-2002:121)

RHEL 2.1 : tcpdump (RHSA-2003:033)

RHEL 2.1 : tcpdump (RHSA-2003:085)

RHEL 2.1 : tcpdump (RHSA-2003:151)

RHEL 2.1 : tetex (RHSA-2002:195)

RHEL 2.1 : tripwire (RHSA-2004:244)

RHEL 2.1 : ucd-snmp (RHSA-2005:720)

RHEL 2.1 : ucd-snmp (RHSA-2008:0528)

RHEL 2.1 : unarj (RHSA-2005:007)

RHEL 2.1 : unzip (RHSA-2002:138)

RHEL 2.1 : unzip (RHSA-2003:200)

RHEL 2.1 : up2date (RHSA-2003:177)

RHEL 2.1 : up2date (RHSA-2003:268)

RHEL 2.1 : util-linux (RHSA-2002:137)

RHEL 2.1 : util-linux (RHSA-2004:056)

RHEL 2.1 : vim (RHSA-2002:302)

RHEL 2.1 : vim (RHSA-2008:0618)

RHEL 2.1 : vnc (RHSA-2002:287)

RHEL 2.1 : vnc (RHSA-2003:068)

RHEL 2.1 : w3m (RHSA-2003:045)

RHEL 2.1 : webalizer (RHSA-2002:255)

RHEL 2.1 : wget (RHSA-2002:256)

RHEL 2.1 : wget (RHSA-2003:372)

RHEL 2.1 : WindowMaker (RHSA-2003:009)

RHEL 2.1 : wu-ftpd (RHSA-2003:246)

RHEL 2.1 : wu-ftpd (RHSA-2004:096)

RHEL 2.1 : xchat (RHSA-2002:124)

RHEL 2.1 : XFree86 (RHSA-2003:065)

RHEL 2.1 : XFree86 (RHSA-2003:289)

RHEL 2.1 : XFree86 (RHSA-2004:060)

RHEL 2.1 : XFree86 (RHSA-2004:152)

RHEL 2.1 : XFree86 (RHSA-2004:479)

RHEL 2.1 : XFree86 (RHSA-2004:610)

RHEL 2.1 : XFree86 (RHSA-2005:044)

RHEL 2.1 : XFree86 (RHSA-2005:329)

RHEL 2.1 : XFree86 (RHSA-2008:0512)

RHEL 2.1 : xinetd (RHSA-2003:161)

RHEL 2.1 : xpdf (RHSA-2002:307)

RHEL 2.1 : xpdf (RHSA-2003:197)

RHEL 2.1 : xpdf (RHSA-2007:1031)

RHEL 2.1 : ypserv (RHSA-2002:224)

RHEL 2.1 : ypserv (RHSA-2003:201)

RHEL 2.1 : zebra (RHSA-2003:305)

RHEL 2.1 : zebra (RHSA-2006:0533)

RHEL 2.1 : zlib (RHSA-2003:081)

RHEL 3 / 4 / 5 : acpid (RHSA-2009:0474)

RHEL 3 / 4 / 5 : acroread (RHSA-2008:0144)

RHEL 3 / 4 / 5 : acroread (RHSA-2008:0641)

RHEL 3 / 4 / 5 : acroread (RHSA-2008:0974)

RHEL 3 / 4 / 5 : acroread (RHSA-2009:0376)

RHEL 3 / 4 / 5 : acroread (RHSA-2009:0478)

RHEL 3 / 4 / 5 : acroread (RHSA-2009:1109)

RHEL 3 / 4 / 5 : acroread (RHSA-2009:1499)

RHEL 3 / 4 / 5 : bzip2 (RHSA-2010:0703)

RHEL 3 / 4 / 5 : cups (RHSA-2007:0123)

RHEL 3 / 4 / 5 : cups (RHSA-2007:0720)

RHEL 3 / 4 / 5 : cups (RHSA-2008:0498)

RHEL 3 / 4 / 5 : cups (RHSA-2008:0937)

RHEL 3 / 4 / 5 : cups (RHSA-2010:0490)

RHEL 3 / 4 / 5 : curl (RHSA-2009:1209)

RHEL 3 / 4 / 5 : expat (RHSA-2009:1625)

RHEL 3 / 4 / 5 : fetchmail (RHSA-2009:1427)

RHEL 3 / 4 / 5 : flash-plugin (RHSA-2007:0696)

RHEL 3 / 4 / 5 : flash-plugin (RHSA-2007:1126)

RHEL 3 / 4 / 5 : flash-plugin (RHSA-2008:0221)

RHEL 3 / 4 / 5 : flash-plugin (RHSA-2008:1047)

RHEL 3 / 4 / 5 : flash-plugin (RHSA-2010:0706)

RHEL 3 / 4 / 5 : freeradius (RHSA-2007:0338)

RHEL 3 / 4 / 5 : freetype (RHSA-2007:0150)

RHEL 3 / 4 / 5 : freetype (RHSA-2008:0556)

RHEL 3 / 4 / 5 : freetype (RHSA-2010:0607)

RHEL 3 / 4 / 5 : gcc and gcc4 (RHSA-2010:0039)

RHEL 3 / 4 / 5 : ghostscript (RHSA-2008:0155)

RHEL 3 / 4 / 5 : ghostscript (RHSA-2009:0345)

RHEL 3 / 4 / 5 : gzip (RHSA-2010:0061)

RHEL 3 / 4 / 5 : httpd (RHSA-2008:0967)

RHEL 3 / 4 / 5 : ImageMagick (RHSA-2008:0145)

RHEL 3 / 4 / 5 : ipsec-tools (RHSA-2008:0849)

RHEL 3 / 4 / 5 : java-1.4.2-bea (RHSA-2008:0100)

RHEL 3 / 4 / 5 : java-1.4.2-bea (RHSA-2008:0243)

RHEL 3 / 4 / 5 : java-1.4.2-bea (RHSA-2008:1043)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2007:0166)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2007:0817)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2008:0132)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2008:0555)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2008:0955)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2009:0445)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2009:1505)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2009:1643)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2010:0155)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2010:0574)

RHEL 3 / 4 / 5 : java-1.4.2-ibm (RHSA-2010:0786)

RHEL 3 / 4 / 5 : kdebase (RHSA-2007:0494)

RHEL 3 / 4 / 5 : krb5 (RHSA-2010:0029)

RHEL 3 / 4 / 5 : krb5 (RHSA-2010:0423)

RHEL 3 / 4 / 5 : libpng (RHSA-2010:0534)

RHEL 3 / 4 / 5 : libtiff (RHSA-2009:1159)

RHEL 3 / 4 / 5 : libtool (RHSA-2009:1646)

RHEL 3 / 4 / 5 : libvorbis (RHSA-2007:0845)

RHEL 3 / 4 / 5 : libvorbis (RHSA-2008:0270)

RHEL 3 / 4 / 5 : libvorbis (RHSA-2009:1219)

RHEL 3 / 4 / 5 : libvorbis (RHSA-2009:1561)

RHEL 3 / 4 / 5 : libxml and libxml2 (RHSA-2009:1206)

RHEL 3 / 4 / 5 : libxml2 (RHSA-2008:0884)

RHEL 3 / 4 / 5 : mikmod (RHSA-2010:0720)

RHEL 3 / 4 / 5 : mod\_perl (RHSA-2007:0395)

RHEL 3 / 4 / 5 : mutt (RHSA-2007:0386)

RHEL 3 / 4 / 5 : net-snmp (RHSA-2007:1045)

RHEL 3 / 4 / 5 : net-snmp (RHSA-2008:0529)

RHEL 3 / 4 / 5 : net-snmp (RHSA-2008:0971)

RHEL 3 / 4 / 5 : newt (RHSA-2009:1463)

RHEL 3 / 4 / 5 : openoffice.org (RHSA-2007:0406)

RHEL 3 / 4 / 5 : openoffice.org (RHSA-2007:0848)

RHEL 3 / 4 / 5 : openoffice.org (RHSA-2008:0939)

RHEL 3 / 4 / 5 : openoffice.org (RHSA-2009:1426)

RHEL 3 / 4 / 5 : openoffice.org (RHSA-2010:0101)

RHEL 3 / 4 / 5 : pango (RHSA-2009:0476)

RHEL 3 / 4 / 5 : pango (RHSA-2010:0140)

RHEL 3 / 4 / 5 : perl (RHSA-2007:0966)

RHEL 3 / 4 / 5 : perl (RHSA-2008:0522)

RHEL 3 / 4 / 5 : php (RHSA-2010:0040)

RHEL 3 / 4 / 5 : pidgin (RHSA-2008:0584)

RHEL 3 / 4 / 5 : pidgin (RHSA-2009:1218)

RHEL 3 / 4 / 5 : postfix (RHSA-2008:0839)

RHEL 3 / 4 / 5 : postgresql (RHSA-2007:0336)

RHEL 3 / 4 / 5 : qt (RHSA-2007:0721)

RHEL 3 / 4 / 5 : quagga (RHSA-2007:0389)

RHEL 3 / 4 / 5 : RealPlayer (RHSA-2007:0841)

RHEL 3 / 4 / 5 : RealPlayer (RHSA-2008:0812)

RHEL 3 / 4 / 5 : samba (RHSA-2010:0697)

RHEL 3 / 4 / 5 : samba and samba3x (RHSA-2010:0488)

RHEL 3 / 4 / 5 : squirrelmail (RHSA-2007:0358)

RHEL 3 / 4 / 5 : squirrelmail (RHSA-2009:0010)

RHEL 3 / 4 / 5 : squirrelmail (RHSA-2009:0057)

RHEL 3 / 4 / 5 : squirrelmail (RHSA-2009:1066)

RHEL 3 / 4 / 5 : squirrelmail (RHSA-2009:1490)

RHEL 3 / 4 / 5 : star (RHSA-2007:0873)

RHEL 3 / 4 / 5 : util-linux (RHSA-2007:0969)

RHEL 3 / 4 / 5 : vixie-cron (RHSA-2007:0345)

RHEL 3 / 4 / 5 : vnc (RHSA-2009:0261)

RHEL 3 / 4 / 5 : wget (RHSA-2009:1549)

RHEL 3 / 4 / 5 : wireshark (RHSA-2008:0890)

RHEL 3 / 4 / 5 : wireshark (RHSA-2009:0313)

RHEL 3 / 4 / 5 : wireshark (RHSA-2009:1100)

RHEL 3 / 4 / 5 : wireshark (RHSA-2010:0360)

RHEL 3 / 4 / 5 : wireshark (RHSA-2010:0625)

RHEL 3 / 4 / 5 : xterm (RHSA-2009:0018)

RHEL 3 / 4 : 4Suite (RHSA-2009:1572)

RHEL 3 / 4 : Adobe Acrobat Reader (RHSA-2005:575)

RHEL 3 / 4 : Adobe Acrobat Reader (RHSA-2005:750)

RHEL 3 / 4 : cpio (RHSA-2005:378)

RHEL 3 / 4 : cscope (RHSA-2009:1101)

RHEL 3 / 4 : cups (RHSA-2005:706)

RHEL 3 / 4 : cups (RHSA-2005:878)

RHEL 3 / 4 : cups (RHSA-2006:0163)

RHEL 3 / 4 : cups (RHSA-2008:0206)

RHEL 3 / 4 : cups (RHSA-2009:1083)

RHEL 3 / 4 : curl (RHSA-2005:807)

RHEL 3 / 4 : curl (RHSA-2010:0329)

RHEL 3 / 4 : Evolution (RHSA-2005:267)

RHEL 3 / 4 : evolution (RHSA-2007:0353)

RHEL 3 / 4 : evolution (RHSA-2007:0509)

RHEL 3 / 4 : evolution (RHSA-2008:0516)

RHEL 3 / 4 : flash-plugin (RHSA-2005:835)

RHEL 3 / 4 : flash-plugin (RHSA-2006:0268)

RHEL 3 / 4 : flash-plugin (RHSA-2006:0674)

RHEL 3 / 4 : flash-plugin (RHSA-2007:0009)

RHEL 3 / 4 : flash-plugin (RHSA-2008:0980)

RHEL 3 / 4 : flash-plugin (RHSA-2009:0334)

RHEL 3 / 4 : flash-plugin (RHSA-2009:1189)

RHEL 3 / 4 : flash-plugin (RHSA-2009:1658)

RHEL 3 / 4 : flash-plugin (RHSA-2010:0103)

RHEL 3 / 4 : flash-plugin (RHSA-2010:0470)

RHEL 3 / 4 : flash-plugin (RHSA-2010:0624)

RHEL 3 / 4 : freeradius (RHSA-2005:524)

RHEL 3 / 4 : freeradius (RHSA-2006:0271)

RHEL 3 / 4 : freetype (RHSA-2009:0329)

RHEL 3 / 4 : gaim (RHSA-2005:215)

RHEL 3 / 4 : gaim (RHSA-2005:365)

RHEL 3 / 4 : gaim (RHSA-2005:429)

RHEL 3 / 4 : gaim (RHSA-2005:518)

RHEL 3 / 4 : gaim (RHSA-2005:627)

RHEL 3 / 4 : gedit (RHSA-2005:499)

RHEL 3 / 4 : ghostscript (RHSA-2009:0420)

RHEL 3 / 4 : gnomemeeting (RHSA-2007:0086)

RHEL 3 / 4 : gtk2 (RHSA-2005:344)

RHEL 3 / 4 : gtk2 (RHSA-2005:811)

RHEL 3 / 4 : httpd (RHSA-2005:582)

RHEL 3 / 4 : httpd (RHSA-2005:608)

RHEL 3 / 4 : httpd (RHSA-2006:0159)

RHEL 3 / 4 : httpd (RHSA-2006:0619)

RHEL 3 / 4 : httpd (RHSA-2007:0662)

RHEL 3 / 4 : ImageMagick (RHSA-2005:413)

RHEL 3 / 4 : ipsec-tools (RHSA-2005:232)

RHEL 3 / 4 : ipsec-tools (RHSA-2006:0267)

RHEL 3 / 4 : java-1.4.2-ibm (RHSA-2007:0062)

RHEL 3 / 4 : libgsf (RHSA-2007:0011)

RHEL 3 / 4 : mailman (RHSA-2005:235)

RHEL 3 / 4 : mailman (RHSA-2006:0204)

RHEL 3 / 4 : mailman (RHSA-2006:0486)

RHEL 3 / 4 : mailman (RHSA-2006:0600)

RHEL 3 / 4 : mod\_auth\_pgsql (RHSA-2006:0164)

RHEL 3 / 4 : openoffice.org (RHSA-2005:375)

RHEL 3 / 4 : openoffice.org (RHSA-2006:0573)

RHEL 3 / 4 : openoffice.org (RHSA-2007:0001)

RHEL 3 / 4 : openoffice.org (RHSA-2007:0033)

RHEL 3 / 4 : openoffice.org (RHSA-2008:0176)

RHEL 3 / 4 : openoffice.org (RHSA-2008:0538)

RHEL 3 / 4 : openoffice.org (RHSA-2010:0643)

RHEL 3 / 4 : openssh (RHSA-2006:0697)

RHEL 3 / 4 : openssh (RHSA-2006:0738)

RHEL 3 / 4 : openssl (RHSA-2010:0163)

RHEL 3 / 4 : openssl096b (RHSA-2005:830)

RHEL 3 / 4 : openssl096b (RHSA-2010:0173)

RHEL 3 / 4 : perl (RHSA-2010:0457)

RHEL 3 / 4 : php (RHSA-2005:564)

RHEL 3 / 4 : php (RHSA-2005:748)

RHEL 3 / 4 : php (RHSA-2005:831)

RHEL 3 / 4 : php (RHSA-2006:0276)

RHEL 3 / 4 : php (RHSA-2006:0568)

RHEL 3 / 4 : php (RHSA-2006:0669)

RHEL 3 / 4 : php (RHSA-2007:0076)

RHEL 3 / 4 : php (RHSA-2007:0155)

RHEL 3 / 4 : php (RHSA-2009:0337)

RHEL 3 / 4 : postgresql (RHSA-2005:433)

RHEL 3 / 4 : postgresql (RHSA-2006:0526)

RHEL 3 / 4 : postgresql (RHSA-2007:0064)

RHEL 3 / 4 : Proxy Server (RHSA-2008:0523)

RHEL 3 / 4 : python (RHSA-2006:0713)

RHEL 3 / 4 : python (RHSA-2007:1076)

RHEL 3 / 4 : quagga (RHSA-2006:0525)

RHEL 3 / 4 : RealPlayer (RHSA-2005:523)

RHEL 3 / 4 : RealPlayer (RHSA-2005:762)

RHEL 3 / 4 : RealPlayer (RHSA-2006:0257)

RHEL 3 / 4 : redhat-release (EOL Notice) (RHSA-2011:0001)

RHEL 3 / 4 : redhat-release (EOL Notice) (RHSA-2011:0002)

RHEL 3 / 4 : samba (RHSA-2007:0060)

RHEL 3 / 4 : Satellite Server (RHSA-2008:0524)

RHEL 3 / 4 : seamonkey (RHSA-2009:1096)

RHEL 3 / 4 : seamonkey (RHSA-2009:1134)

RHEL 3 / 4 : seamonkey (RHSA-2009:1163)

RHEL 3 / 4 : seamonkey (RHSA-2009:1531)

RHEL 3 / 4 : seamonkey (RHSA-2009:1673)

RHEL 3 / 4 : seamonkey (RHSA-2010:0113)

RHEL 3 / 4 : seamonkey (RHSA-2010:0333)

RHEL 3 / 4 : seamonkey (RHSA-2010:0499)

RHEL 3 / 4 : seamonkey (RHSA-2010:0546)

RHEL 3 / 4 : seamonkey (RHSA-2010:0557)

RHEL 3 / 4 : seamonkey (RHSA-2010:0680)

RHEL 3 / 4 : seamonkey (RHSA-2010:0781)

RHEL 3 / 4 : seamonkey (RHSA-2010:0810)

RHEL 3 / 4 : sendmail (RHSA-2006:0264)

RHEL 3 / 4 : Solaris client in Satellite Server (RHSA-2008:0525)

RHEL 3 / 4 : squid (RHSA-2005:415)

RHEL 3 / 4 : squirrelmail (RHSA-2005:595)

RHEL 3 / 4 : squirrelmail (RHSA-2006:0283)

RHEL 3 / 4 : squirrelmail (RHSA-2006:0547)

RHEL 3 / 4 : squirrelmail (RHSA-2006:0668)

RHEL 3 / 4 : squirrelmail (RHSA-2007:0022)

RHEL 3 / 4 : tomcat in Satellite Server (RHSA-2007:1069)

RHEL 3 / 4 : vim (RHSA-2008:0617)

RHEL 3 / 4 : xpdf (RHSA-2009:0430)

RHEL 3 / 5 : httpd (RHSA-2009:1579)

RHEL 3 / 5 : perl-Net-DNS (RHSA-2007:0674)

RHEL 3 / 5 : php (RHSA-2008:0544)

RHEL 3 : acroread (RHSA-2004:432)

RHEL 3 : acroread (RHSA-2004:674)

RHEL 3 : acroread (RHSA-2010:0060)

RHEL 3 : Adobe Acrobat Reader (RHSA-2007:0021)

RHEL 3 : bind (RHSA-2009:1181)

RHEL 3 : binutils (RHSA-2005:659)

RHEL 3 : cpio (RHSA-2005:080)

RHEL 3 : cpio (RHSA-2010:0145)

RHEL 3 : cups (RHSA-2004:449)

RHEL 3 : cups (RHSA-2004:543)

RHEL 3 : cups (RHSA-2005:013)

RHEL 3 : cups (RHSA-2005:049)

RHEL 3 : cups (RHSA-2005:132)

RHEL 3 : cups (RHSA-2005:571)

RHEL 3 : cups (RHSA-2007:1023)

RHEL 3 : cups (RHSA-2008:0153)

RHEL 3 : cups (RHSA-2008:1028)

RHEL 3 : cups (RHSA-2009:0308)

RHEL 3 : cups (RHSA-2009:0428)

RHEL 3 : cups (RHSA-2010:0754)

RHEL 3 : cyrus-sasl (RHSA-2007:0878)

RHEL 3 : dhcp (RHSA-2009:1154)

RHEL 3 : elfutils (RHSA-2006:0368)

RHEL 3 : evolution (RHSA-2005:238)

RHEL 3 : evolution (RHSA-2009:0358)

RHEL 3 : freeradius (RHSA-2003:386)

RHEL 3 : freeradius (RHSA-2004:609)

RHEL 3 : freetype (RHSA-2010:0577)

RHEL 3 : freetype (RHSA-2010:0736)

RHEL 3 : gaim (RHSA-2004:033)

RHEL 3 : gaim (RHSA-2004:400)

RHEL 3 : gaim (RHSA-2004:604)

RHEL 3 : gcc (RHSA-2007:0473)

RHEL 3 : gdb (RHSA-2007:0469)

RHEL 3 : ghostscript (RHSA-2005:081)

RHEL 3 : glibc (RHSA-2003:334)

RHEL 3 : glibc (RHSA-2004:586)

RHEL 3 : glibc (RHSA-2005:256)

RHEL 3 : gstreamer-plugins (RHSA-2009:0269)

RHEL 3 : gtk2 (RHSA-2004:466)

RHEL 3 : httpd (RHSA-2004:015)

RHEL 3 : httpd (RHSA-2004:084)

RHEL 3 : httpd (RHSA-2004:342)

RHEL 3 : httpd (RHSA-2004:349)

RHEL 3 : httpd (RHSA-2004:463)

RHEL 3 : httpd (RHSA-2004:562)

RHEL 3 : httpd (RHSA-2007:0533)

RHEL 3 : httpd (RHSA-2008:0005)

RHEL 3 : httpd (RHSA-2009:1108)

RHEL 3 : httpd (RHSA-2009:1205)

RHEL 3 : ImageMagick (RHSA-2004:480)

RHEL 3 : imap (RHSA-2005:128)

RHEL 3 : imap (RHSA-2009:0275)

RHEL 3 : initscripts (RHSA-2006:0015)

RHEL 3 : ipsec-tools (RHSA-2004:165)

RHEL 3 : ipsec-tools (RHSA-2004:308)

RHEL 3 : kdebase (RHSA-2006:0576)

RHEL 3 : kdelibs (RHSA-2009:1128)

RHEL 3 : kdepim (RHSA-2004:005)

RHEL 3 : kernel (RHSA-2003:416)

RHEL 3 : kernel (RHSA-2004:017)

RHEL 3 : kernel (RHSA-2004:066)

RHEL 3 : kernel (RHSA-2004:183)

RHEL 3 : kernel (RHSA-2004:188)

RHEL 3 : kernel (RHSA-2004:255)

RHEL 3 : kernel (RHSA-2004:360)

RHEL 3 : kernel (RHSA-2004:413)

RHEL 3 : kernel (RHSA-2004:549)

RHEL 3 : kernel (RHSA-2004:689)

RHEL 3 : kernel (RHSA-2005:043)

RHEL 3 : kernel (RHSA-2005:293)

RHEL 3 : kernel (RHSA-2005:294)

RHEL 3 : kernel (RHSA-2005:472)

RHEL 3 : kernel (RHSA-2005:663)

RHEL 3 : kernel (RHSA-2006:0140)

RHEL 3 : kernel (RHSA-2006:0144)

RHEL 3 : kernel (RHSA-2006:0437)

RHEL 3 : kernel (RHSA-2006:0710)

RHEL 3 : kernel (RHSA-2007:0436)

RHEL 3 : kernel (RHSA-2007:0671)

RHEL 3 : kernel (RHSA-2007:0938)

RHEL 3 : kernel (RHSA-2007:1049)

RHEL 3 : kernel (RHSA-2008:0211)

RHEL 3 : kernel (RHSA-2008:0973)

RHEL 3 : kernel (RHSA-2009:1233)

RHEL 3 : kernel (RHSA-2009:1550)

RHEL 3 : krb5 (RHSA-2004:350)

RHEL 3 : less (RHSA-2005:068)

RHEL 3 : lha (RHSA-2004:323)

RHEL 3 : libpng (RHSA-2004:249)

RHEL 3 : libpng (RHSA-2009:0340)

RHEL 3 : libtiff (RHSA-2010:0520)

RHEL 3 : mutt (RHSA-2004:050)

RHEL 3 : mysql (RHSA-2004:569)

RHEL 3 : mysql-server (RHSA-2004:611)

RHEL 3 : mysql-server (RHSA-2005:348)

RHEL 3 : net-snmp (RHSA-2004:023)

RHEL 3 : net-snmp (RHSA-2005:373)

RHEL 3 : net-snmp (RHSA-2009:0295)

RHEL 3 : net-snmp (RHSA-2009:1124)

RHEL 3 : nfs-utils (RHSA-2004:072)

RHEL 3 : nfs-utils (RHSA-2004:583)

RHEL 3 : ntp (RHSA-2009:1651)

RHEL 3 : openldap (RHSA-2007:0430)

RHEL 3 : openoffice.org (RHSA-2004:160)

RHEL 3 : openoffice.org (RHSA-2004:446)

RHEL 3 : openssh (RHSA-2005:106)

RHEL 3 : openssh (RHSA-2005:550)

RHEL 3 : openssh (RHSA-2006:0298)

RHEL 3 : openssl (RHSA-2004:120)

RHEL 3 : pam (RHSA-2007:0465)

RHEL 3 : pcre (RHSA-2007:1063)

RHEL 3 : perl (RHSA-2005:105)

RHEL 3 : perl (RHSA-2005:881)

RHEL 3 : php (RHSA-2004:392)

RHEL 3 : php (RHSA-2004:687)

RHEL 3 : PHP (RHSA-2005:405)

RHEL 3 : php (RHSA-2007:0889)

RHEL 3 : pidgin (RHSA-2009:1059)

RHEL 3 : pidgin (RHSA-2009:1535)

RHEL 3 : postgresql (RHSA-2008:0039)

RHEL 3 : postgresql (RHSA-2009:1485)

RHEL 3 : postgresql (RHSA-2010:0427)

RHEL 3 : pwlib (RHSA-2004:047)

RHEL 3 : python (RHSA-2005:109)

RHEL 3 : python (RHSA-2009:1178)

RHEL 3 : quagga (RHSA-2003:315)

RHEL 3 : rdesktop (RHSA-2008:0576)

RHEL 3 : realplayer (RHSA-2005:299)

RHEL 3 : RealPlayer (RHSA-2005:394)

RHEL 3 : redhat-config-nfs (RHSA-2004:434)

RHEL 3 : redhat-release (EOL Notice) (RHSA-2009:1526)

RHEL 3 : redhat-release (EOL Notice) (RHSA-2010:0386)

RHEL 3 : redhat-release (EOL Notice) (RHSA-2010:0576)

RHEL 3 : redhat-release (EOL Notice) (RHSA-2010:0734)

RHEL 3 : redhat-release (EOL Notice) (RHSA-2010:0817)

RHEL 3 : rh-postgresql (RHSA-2004:489)

RHEL 3 : rh-postgresql (RHSA-2005:141)

RHEL 3 : rsh (RHSA-2005:074)

RHEL 3 : ruby (RHSA-2008:0896)

RHEL 3 : samba (RHSA-2004:064)

RHEL 3 : samba (RHSA-2004:259)

RHEL 3 : samba (RHSA-2004:467)

RHEL 3 : samba (RHSA-2004:670)

RHEL 3 : samba (RHSA-2009:1528)

RHEL 3 : seamonkey (RHSA-2006:0578)

RHEL 3 : seamonkey (RHSA-2006:0608)

RHEL 3 : seamonkey (RHSA-2009:1185)

RHEL 3 : seamonkey (RHSA-2009:1432)

RHEL 3 : shadow-utils (RHSA-2007:0431)

RHEL 3 : slocate (RHSA-2005:345)

RHEL 3 : sox (RHSA-2004:409)

RHEL 3 : spamassassin (RHSA-2004:451)

RHEL 3 : squid (RHSA-2004:242)

RHEL 3 : squid (RHSA-2004:462)

RHEL 3 : squid (RHSA-2006:0045)

RHEL 3 : squirrelmail (RHSA-2004:240)

RHEL 3 : squirrelmail (RHSA-2004:654)

RHEL 3 : squirrelmail (RHSA-2005:135)

RHEL 3 : tar (RHSA-2010:0142)

RHEL 3 : tcpdump (RHSA-2005:421)

RHEL 3 : tetex (RHSA-2010:0401)

RHEL 3 : vixie-cron (RHSA-2006:0117)

RHEL 3 : vsftpd (RHSA-2008:0579)

RHEL 3 : wireshark (RHSA-2008:0059)

RHEL 3 : XFree86 (RHSA-2004:061)

RHEL 3 : XFree86 (RHSA-2004:478)

RHEL 3 : XFree86 (RHSA-2004:612)

RHEL 3 : XFree86 (RHSA-2005:331)

RHEL 3 : XFree86 (RHSA-2005:501)

RHEL 3 : XFree86 (RHSA-2008:0502)

RHEL 3 : xpdf (RHSA-2005:018)

RHEL 3 : xpdf (RHSA-2005:059)

RHEL 3 : xpdf (RHSA-2007:1030)

RHEL 3 : xpdf (RHSA-2009:1500)

RHEL 3 : xpdf (RHSA-2010:0750)

RHEL 4 / 5 / 6 : acroread (RHSA-2010:0934)

RHEL 4 / 5 / 6 : acroread (RHSA-2011:0301)

RHEL 4 / 5 / 6 : acroread (RHSA-2011:1434)

RHEL 4 / 5 / 6 : apr (RHSA-2011:0507)

RHEL 4 / 5 / 6 : apr (RHSA-2011:0844)

RHEL 4 / 5 / 6 : apr-util (RHSA-2010:0950)

RHEL 4 / 5 / 6 : bash (RHSA-2014:1294) (Shellshock)

RHEL 4 / 5 / 6 : bash (RHSA-2014:1311)

RHEL 4 / 5 / 6 : curl (RHSA-2011:0918)

RHEL 4 / 5 / 6 : cyrus-imapd (RHSA-2011:0859)

RHEL 4 / 5 / 6 : cyrus-imapd (RHSA-2011:1317)

RHEL 4 / 5 / 6 : cyrus-imapd (RHSA-2011:1508)

RHEL 4 / 5 / 6 : dhcp (RHSA-2011:0428)

RHEL 4 / 5 / 6 : dhcp (RHSA-2011:1160)

RHEL 4 / 5 / 6 : dovecot (RHSA-2011:1187)

RHEL 4 / 5 / 6 : firefox (RHSA-2010:0966)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:0310)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:0373)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:0471)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:0885)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:1164)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:1242)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:1268)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:1341)

RHEL 4 / 5 / 6 : firefox (RHSA-2011:1437)

RHEL 4 / 5 / 6 : firefox (RHSA-2012:0079)

RHEL 4 / 5 / 6 : freetype (RHSA-2010:0889)

RHEL 4 / 5 / 6 : freetype (RHSA-2011:1402)

RHEL 4 / 5 / 6 : freetype (RHSA-2011:1455)

RHEL 4 / 5 / 6 : gnutls (RHSA-2014:0288)

RHEL 4 / 5 / 6 : httpd (RHSA-2011:1245)

RHEL 4 / 5 / 6 : java-1.5.0-ibm (RHSA-2011:0169)

RHEL 4 / 5 / 6 : java-1.5.0-ibm (RHSA-2011:0291)

RHEL 4 / 5 / 6 : java-1.5.0-ibm (RHSA-2011:0364)

RHEL 4 / 5 / 6 : java-1.5.0-ibm (RHSA-2011:1087)

RHEL 4 / 5 / 6 : java-1.5.0-ibm (RHSA-2011:1478)

RHEL 4 / 5 / 6 : java-1.6.0-ibm (RHSA-2010:0987)

RHEL 4 / 5 / 6 : java-1.6.0-ibm (RHSA-2011:0290)

RHEL 4 / 5 / 6 : java-1.6.0-ibm (RHSA-2011:0357)

RHEL 4 / 5 / 6 : java-1.6.0-ibm (RHSA-2011:0938)

RHEL 4 / 5 / 6 : java-1.6.0-sun (RHSA-2011:0282)

RHEL 4 / 5 / 6 : java-1.6.0-sun (RHSA-2011:0860)

RHEL 4 / 5 / 6 : java-1.6.0-sun (RHSA-2011:1384) (BEAST)

RHEL 4 / 5 / 6 : java-1.6.0-sun (RHSA-2012:0139)

RHEL 4 / 5 / 6 : JBoss EAP (RHSA-2014:1321)

RHEL 4 / 5 / 6 : JBoss EWP (RHSA-2014:0792)

RHEL 4 / 5 / 6 : JBoss EWP (RHSA-2014:0898)

RHEL 4 / 5 / 6 : JBoss EWP (RHSA-2014:1320)

RHEL 4 / 5 / 6 : jboss-remoting (RHSA-2013:1369)

RHEL 4 / 5 / 6 : jbossws-common (RHSA-2011:1301)

RHEL 4 / 5 / 6 : kdelibs and kdelibs3 (RHSA-2011:1385)

RHEL 4 / 5 / 6 : libpng (RHSA-2012:0317)

RHEL 4 / 5 / 6 : libtiff (RHSA-2011:0318)

RHEL 4 / 5 / 6 : libtiff (RHSA-2011:0392)

RHEL 4 / 5 / 6 : libuser (RHSA-2011:0170)

RHEL 4 / 5 / 6 : libvorbis (RHSA-2012:0136)

RHEL 4 / 5 / 6 : nss (RHSA-2011:0472)

RHEL 4 / 5 / 6 : nss (RHSA-2011:1444)

RHEL 4 / 5 / 6 : nss (RHSA-2014:1371)

RHEL 4 / 5 / 6 : nss and nspr (RHSA-2011:1282)

RHEL 4 / 5 / 6 : openssl (RHSA-2012:0522)

RHEL 4 / 5 / 6 : openssl (RHSA-2014:0627)

RHEL 4 / 5 / 6 : pango (RHSA-2011:0180)

RHEL 4 / 5 / 6 : php (RHSA-2012:0093)

RHEL 4 / 5 / 6 : postfix (RHSA-2011:0843)

RHEL 4 / 5 / 6 : postgresql (RHSA-2011:0197)

RHEL 4 / 5 / 6 : postgresql (RHSA-2011:1377)

RHEL 4 / 5 / 6 : rpm (RHSA-2011:1349)

RHEL 4 / 5 / 6 : rpm (RHSA-2012:0451)

RHEL 4 / 5 / 6 : samba (RHSA-2011:0305)

RHEL 4 / 5 / 6 : thunderbird (RHSA-2011:0374)

RHEL 4 / 5 / 6 : thunderbird (RHSA-2011:1243)

RHEL 4 / 5 / 6 : thunderbird (RHSA-2011:1267)

RHEL 4 / 5 / 6 : vsftpd (RHSA-2011:0337)

RHEL 4 / 5 / 6 : wireshark (RHSA-2011:0013)

RHEL 4 / 5 : acroread (RHSA-2010:0114)

RHEL 4 / 5 : acroread (RHSA-2010:0349)

RHEL 4 / 5 : acroread (RHSA-2010:0503)

RHEL 4 / 5 : acroread (RHSA-2010:0636)

RHEL 4 / 5 : acroread (RHSA-2010:0743)

RHEL 4 / 5 : apr and apr-util (RHSA-2009:1204)

RHEL 4 / 5 : apr-util (RHSA-2009:1107)

RHEL 4 / 5 : bluez-libs and bluez-utils (RHSA-2008:0581)

RHEL 4 / 5 : cobbler (RHSA-2010:0775)

RHEL 4 / 5 : cups (RHSA-2009:0429)

RHEL 4 / 5 : cyrus-imapd (RHSA-2009:1116)

RHEL 4 / 5 : cyrus-imapd (RHSA-2009:1459)

RHEL 4 / 5 : device-mapper-multipath (RHSA-2009:0411)

RHEL 4 / 5 : elinks (RHSA-2007:0933)

RHEL 4 / 5 : elinks (RHSA-2009:1471)

RHEL 4 / 5 : evolution (RHSA-2008:0177)

RHEL 4 / 5 : evolution-data-server (RHSA-2009:0354)

RHEL 4 / 5 : exim (RHSA-2010:0970)

RHEL 4 / 5 : exim (RHSA-2011:0153)

RHEL 4 / 5 : file (RHSA-2007:0124)

RHEL 4 / 5 : file (RHSA-2007:0391)

RHEL 4 / 5 : firefox (RHSA-2007:0400)

RHEL 4 / 5 : firefox (RHSA-2007:0724)

RHEL 4 / 5 : firefox (RHSA-2007:0979)

RHEL 4 / 5 : firefox (RHSA-2007:1082)

RHEL 4 / 5 : firefox (RHSA-2008:0103)

RHEL 4 / 5 : firefox (RHSA-2008:0207)

RHEL 4 / 5 : firefox (RHSA-2008:0222)

RHEL 4 / 5 : firefox (RHSA-2008:0879)

RHEL 4 / 5 : firefox (RHSA-2008:0978)

RHEL 4 / 5 : firefox (RHSA-2008:1036)

RHEL 4 / 5 : firefox (RHSA-2009:0256)

RHEL 4 / 5 : firefox (RHSA-2009:0315)

RHEL 4 / 5 : firefox (RHSA-2009:0397)

RHEL 4 / 5 : firefox (RHSA-2009:0436)

RHEL 4 / 5 : firefox (RHSA-2009:0449)

RHEL 4 / 5 : firefox (RHSA-2009:1095)

RHEL 4 / 5 : firefox (RHSA-2009:1162)

RHEL 4 / 5 : firefox (RHSA-2009:1430)

RHEL 4 / 5 : firefox (RHSA-2009:1530)

RHEL 4 / 5 : firefox (RHSA-2009:1674)

RHEL 4 / 5 : firefox (RHSA-2010:0112)

RHEL 4 / 5 : firefox (RHSA-2010:0332)

RHEL 4 / 5 : firefox (RHSA-2010:0547)

RHEL 4 / 5 : firefox (RHSA-2010:0681)

RHEL 4 / 5 : firefox (RHSA-2010:0782)

RHEL 4 / 5 : flac (RHSA-2007:0975)

RHEL 4 / 5 : foomatic (RHSA-2011:1109)

RHEL 4 / 5 : freetype (RHSA-2010:0578)

RHEL 4 / 5 : freetype (RHSA-2010:0737)

RHEL 4 / 5 : gd (RHSA-2008:0146)

RHEL 4 / 5 : gd (RHSA-2010:0003)

RHEL 4 / 5 : gnutls (RHSA-2009:1232)

RHEL 4 / 5 : htdig (RHSA-2007:1095)

RHEL 4 / 5 : httpd (RHSA-2011:1392)

RHEL 4 / 5 : IBM Java Runtime in Satellite Server (RHSA-2010:0043)

RHEL 4 / 5 : IBM Java Runtime in Satellite Server (RHSA-2010:0471)

RHEL 4 / 5 : java-1.4.2-ibm (RHSA-2010:0935)

RHEL 4 / 5 : java-1.4.2-ibm (RHSA-2011:0152)

RHEL 4 / 5 : java-1.4.2-ibm (RHSA-2011:0292)

RHEL 4 / 5 : java-1.4.2-ibm (RHSA-2011:0490)

RHEL 4 / 5 : java-1.4.2-ibm (RHSA-2011:1159)

RHEL 4 / 5 : java-1.5.0-bea (RHSA-2007:0956)

RHEL 4 / 5 : java-1.5.0-bea (RHSA-2008:0156)

RHEL 4 / 5 : java-1.5.0-bea (RHSA-2008:0244)

RHEL 4 / 5 : java-1.5.0-bea (RHSA-2008:1044)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2007:0167)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2007:0829)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2007:1041)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2008:0210)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2008:0790)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2008:0891)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2009:0016)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2009:0466)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2009:1038)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2009:1236)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2009:1647)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2010:0130)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2010:0489)

RHEL 4 / 5 : java-1.5.0-ibm (RHSA-2010:0807)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2007:0963)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2008:0123)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2008:0186)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2008:0595)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2008:1025)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2009:0394)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2009:1199)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2009:1571)

RHEL 4 / 5 : java-1.5.0-sun (RHSA-2010:0338)

RHEL 4 / 5 : java-1.6.0-bea (RHSA-2008:1045)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2008:0906)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2009:0015)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2009:0369)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2009:1198)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2009:1582)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2009:1694)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2010:0383)

RHEL 4 / 5 : java-1.6.0-ibm (RHSA-2010:0549)

RHEL 4 / 5 : java-1.6.0-sun (RHSA-2008:1018)

RHEL 4 / 5 : java-1.6.0-sun (RHSA-2009:0392)

RHEL 4 / 5 : java-1.6.0-sun (RHSA-2009:1200)

RHEL 4 / 5 : java-1.6.0-sun (RHSA-2009:1560)

RHEL 4 / 5 : java-1.6.0-sun (RHSA-2010:0337)

RHEL 4 / 5 : java-1.6.0-sun (RHSA-2010:0356)

RHEL 4 / 5 : java-1.6.0-sun (RHSA-2010:0770)

RHEL 4 / 5 : jboss-remoting (RHSA-2010:0964)

RHEL 4 / 5 : jboss-seam2 (RHSA-2010:0564)

RHEL 4 / 5 : jboss-seam2 (RHSA-2011:0460)

RHEL 4 / 5 : jboss-seam2 (RHSA-2011:0461)

RHEL 4 / 5 : jboss-seam2 (RHSA-2011:0950)

RHEL 4 / 5 : jbossas (RHSA-2011:1309)

RHEL 4 / 5 : jbossweb (RHSA-2008:0877)

RHEL 4 / 5 : jbossweb (RHSA-2010:0584)

RHEL 4 / 5 : jbossws-common (RHSA-2011:1306)

RHEL 4 / 5 : kdebase (RHSA-2007:0905)

RHEL 4 / 5 : kdebase (RHSA-2010:0348)

RHEL 4 / 5 : kdegraphics (RHSA-2007:0729)

RHEL 4 / 5 : kdegraphics (RHSA-2009:0431)

RHEL 4 / 5 : kdegraphics (RHSA-2010:0753)

RHEL 4 / 5 : kdelibs (RHSA-2007:0909)

RHEL 4 / 5 : kdelibs (RHSA-2009:1127)

RHEL 4 / 5 : kdelibs (RHSA-2009:1601)

RHEL 4 / 5 : krb5 (RHSA-2007:0562)

RHEL 4 / 5 : krb5 (RHSA-2010:0926)

RHEL 4 / 5 : krb5 (RHSA-2011:1851)

RHEL 4 / 5 : libexif (RHSA-2007:0501)

RHEL 4 / 5 : libsoup (RHSA-2009:0344)

RHEL 4 / 5 : libtiff (RHSA-2010:0519)

RHEL 4 / 5 : libwmf (RHSA-2009:0457)

RHEL 4 / 5 : libxslt (RHSA-2008:0649)

RHEL 4 / 5 : mailman (RHSA-2011:0307)

RHEL 4 / 5 : mysql (RHSA-2007:0875)

RHEL 4 / 5 : mysql (RHSA-2007:1155)

RHEL 4 / 5 : neon (RHSA-2009:1452)

RHEL 4 / 5 : netpbm (RHSA-2009:0012)

RHEL 4 / 5 : netpbm (RHSA-2011:1811)

RHEL 4 / 5 : nss (RHSA-2010:0165)

RHEL 4 / 5 : ntp (RHSA-2009:0046)

RHEL 4 / 5 : ntp (RHSA-2009:1648)

RHEL 4 / 5 : openldap (RHSA-2008:0110)

RHEL 4 / 5 : openldap (RHSA-2008:0583)

RHEL 4 / 5 : openoffice.org (RHSA-2008:0175)

RHEL 4 / 5 : openoffice.org (RHSA-2008:0537)

RHEL 4 / 5 : openoffice.org (RHSA-2010:0459)

RHEL 4 / 5 : openssh (RHSA-2008:0855)

RHEL 4 / 5 : pcre (RHSA-2007:1052)

RHEL 4 / 5 : perl (RHSA-2011:1797)

RHEL 4 / 5 : perl-Archive-Tar (RHSA-2010:0505)

RHEL 4 / 5 : php (RHSA-2007:0890)

RHEL 4 / 5 : php (RHSA-2010:0919)

RHEL 4 / 5 : pidgin (RHSA-2008:1023)

RHEL 4 / 5 : pidgin (RHSA-2009:1060)

RHEL 4 / 5 : pidgin (RHSA-2009:1139)

RHEL 4 / 5 : pidgin (RHSA-2009:1453)

RHEL 4 / 5 : pidgin (RHSA-2009:1536)

RHEL 4 / 5 : pidgin (RHSA-2010:0044)

RHEL 4 / 5 : pidgin (RHSA-2010:0115)

RHEL 4 / 5 : pidgin (RHSA-2010:0788)

RHEL 4 / 5 : pidgin (RHSA-2011:1371)

RHEL 4 / 5 : pidgin (RHSA-2011:1820)

RHEL 4 / 5 : postfix (RHSA-2011:0422)

RHEL 4 / 5 : postgresql (RHSA-2008:0038)

RHEL 4 / 5 : postgresql (RHSA-2009:1484)

RHEL 4 / 5 : postgresql and postgresql84 (RHSA-2010:0742)

RHEL 4 / 5 : PyXML (RHSA-2010:0002)

RHEL 4 / 5 : quagga (RHSA-2010:0785)

RHEL 4 / 5 : ruby (RHSA-2008:0561)

RHEL 4 / 5 : ruby (RHSA-2008:0897)

RHEL 4 / 5 : ruby (RHSA-2008:0981)

RHEL 4 / 5 : ruby (RHSA-2009:1140)

RHEL 4 / 5 : ruby (RHSA-2012:0070)

RHEL 4 / 5 : samba (RHSA-2009:1529)

RHEL 4 / 5 : samba (RHSA-2011:1219)

RHEL 4 / 5 : samba (RHSA-2012:0332)

RHEL 4 / 5 : sblim (RHSA-2008:0497)

RHEL 4 / 5 : spamassassin (RHSA-2007:0492)

RHEL 4 / 5 : speex (RHSA-2008:0235)

RHEL 4 / 5 : squirrelmail (RHSA-2012:0103)

RHEL 4 / 5 : subversion (RHSA-2009:1203)

RHEL 4 / 5 : system-config-printer (RHSA-2011:1196)

RHEL 4 / 5 : systemtap (RHSA-2009:0373)

RHEL 4 / 5 : tar (RHSA-2007:0860)

RHEL 4 / 5 : tar (RHSA-2010:0141)

RHEL 4 / 5 : tetex (RHSA-2007:1027)

RHEL 4 / 5 : thunderbird (RHSA-2007:0401)

RHEL 4 / 5 : thunderbird (RHSA-2007:0723)

RHEL 4 / 5 : thunderbird (RHSA-2007:0981)

RHEL 4 / 5 : thunderbird (RHSA-2007:1083)

RHEL 4 / 5 : thunderbird (RHSA-2008:0105)

RHEL 4 / 5 : thunderbird (RHSA-2008:0209)

RHEL 4 / 5 : thunderbird (RHSA-2008:0224)

RHEL 4 / 5 : thunderbird (RHSA-2008:0616)

RHEL 4 / 5 : thunderbird (RHSA-2008:0908)

RHEL 4 / 5 : thunderbird (RHSA-2008:0976)

RHEL 4 / 5 : thunderbird (RHSA-2009:0002)

RHEL 4 / 5 : thunderbird (RHSA-2009:0258)

RHEL 4 / 5 : thunderbird (RHSA-2010:0682)

RHEL 4 / 5 : thunderbird (RHSA-2010:0780)

RHEL 4 / 5 : thunderbird (RHSA-2010:0812)

RHEL 4 / 5 : thunderbird (RHSA-2010:0968)

RHEL 4 / 5 : thunderbird (RHSA-2011:0312)

RHEL 4 / 5 : thunderbird (RHSA-2011:0474)

RHEL 4 / 5 : thunderbird (RHSA-2011:0887)

RHEL 4 / 5 : thunderbird (RHSA-2011:1165)

RHEL 4 / 5 : thunderbird (RHSA-2011:1343)

RHEL 4 / 5 : thunderbird (RHSA-2011:1438)

RHEL 4 / 5 : thunderbird (RHSA-2012:0085)

RHEL 4 / 5 : tog-pegasus (RHSA-2008:0002)

RHEL 4 / 5 : wireshark (RHSA-2008:0058)

RHEL 4 / 5 : wireshark (RHSA-2011:0370)

RHEL 4 / 5 : xmlsec1 (RHSA-2009:1428)

RHEL 4 / 5 : xmlsec1 (RHSA-2011:0486)

RHEL 4 : acroread (RHSA-2010:0038)

RHEL 4 : Adobe Acrobat Reader (RHSA-2007:0017)

RHEL 4 : alsa-lib (RHSA-2005:033)

RHEL 4 : autofs5 (RHSA-2007:1129)

RHEL 4 : autofs5 (RHSA-2007:1177)

RHEL 4 : bash (RHSA-2011:0261)

RHEL 4 : bind (RHSA-2009:1180)

RHEL 4 : bind (RHSA-2010:1000)

RHEL 4 : bind (RHSA-2011:1496)

RHEL 4 : binutils (RHSA-2005:673)

RHEL 4 : bluez-utils (RHSA-2007:0065)

RHEL 4 : busybox (RHSA-2007:0244)

RHEL 4 : coreutils (RHSA-2008:0780)

RHEL 4 : cpio (RHSA-2005:073)

RHEL 4 : cpio (RHSA-2007:0245)

RHEL 4 : cpio (RHSA-2010:0143)

RHEL 4 : CUPS (RHSA-2005:053)

RHEL 4 : cups (RHSA-2005:772)

RHEL 4 : cups (RHSA-2007:1022)

RHEL 4 : cups (RHSA-2008:0161)

RHEL 4 : cups (RHSA-2010:0755)

RHEL 4 : curl (RHSA-2005:875)

RHEL 4 : cyrus-imapd (RHSA-2005:408)

RHEL 4 : cyrus-sasl (RHSA-2007:0795)

RHEL 4 : dbus (RHSA-2005:102)

RHEL 4 : dbus (RHSA-2007:0008)

RHEL 4 : dhcp (RHSA-2009:1136)

RHEL 4 : dia (RHSA-2006:0541)

RHEL 4 : elfutils (RHSA-2006:0354)

RHEL 4 : elinks (RHSA-2006:0742)

RHEL 4 : emacs (RHSA-2005:110)

RHEL 4 : enscript (RHSA-2005:040)

RHEL 4 : ethereal (RHSA-2005:037)

RHEL 4 : evolution (RHSA-2005:397)

RHEL 4 : evolution (RHSA-2008:0178)

RHEL 4 : evolution (RHSA-2008:0517)

RHEL 4 : evolution and evolution-data-server (RHSA-2009:0355)

RHEL 4 : evolution28 (RHSA-2008:0515)

RHEL 4 : evolution28-pango (RHSA-2011:1325)

RHEL 4 : exim (RHSA-2005:025)

RHEL 4 : exim (RHSA-2005:358)

RHEL 4 : firefox (RHSA-2005:176)

RHEL 4 : firefox (RHSA-2005:336)

RHEL 4 : firefox (RHSA-2005:383)

RHEL 4 : firefox (RHSA-2005:434)

RHEL 4 : firefox (RHSA-2005:586)

RHEL 4 : firefox (RHSA-2005:768)

RHEL 4 : firefox (RHSA-2005:785)

RHEL 4 : firefox (RHSA-2006:0200)

RHEL 4 : firefox (RHSA-2006:0328)

RHEL 4 : firefox (RHSA-2006:0610)

RHEL 4 : firefox (RHSA-2006:0675)

RHEL 4 : firefox (RHSA-2006:0733)

RHEL 4 : firefox (RHSA-2006:0758)

RHEL 4 : Firefox (RHSA-2007:0079)

RHEL 4 : firefox (RHSA-2008:0549)

RHEL 4 : firefox (RHSA-2008:0598)

RHEL 4 : firefox (RHSA-2010:0500)

RHEL 4 : firefox (RHSA-2010:0558)

RHEL 4 : firefox (RHSA-2010:0808)

RHEL 4 : firefox (RHSA-2012:0142)

RHEL 4 : flash-plugin (RHSA-2010:0834)

RHEL 4 : freetype (RHSA-2011:1161)

RHEL 4 : frysk (RHSA-2011:1327)

RHEL 4 : gcc (RHSA-2007:0220)

RHEL 4 : gd (RHSA-2006:0194)

RHEL 4 : gdb (RHSA-2005:709)

RHEL 4 : gdb (RHSA-2007:0229)

RHEL 4 : gdm (RHSA-2007:0286)

RHEL 4 : gdm (RHSA-2010:0657)

RHEL 4 : ghostscript (RHSA-2012:0096)

RHEL 4 : gimp (RHSA-2006:0598)

RHEL 4 : gimp (RHSA-2011:0837)

RHEL 4 : glibc (RHSA-2012:0125)

RHEL 4 : glibc (RHSA-2015:0101) (GHOST)

RHEL 4 : gnutls (RHSA-2005:430)

RHEL 4 : gnutls (RHSA-2006:0207)

RHEL 4 : gnutls (RHSA-2006:0680)

RHEL 4 : gnutls (RHSA-2008:0492)

RHEL 4 : gnutls (RHSA-2010:0167)

RHEL 4 : gpdf (RHSA-2005:057)

RHEL 4 : gpdf (RHSA-2005:708)

RHEL 4 : gpdf (RHSA-2005:867)

RHEL 4 : gpdf (RHSA-2006:0177)

RHEL 4 : gpdf (RHSA-2007:0730)

RHEL 4 : gpdf (RHSA-2007:1025)

RHEL 4 : gpdf (RHSA-2008:0262)

RHEL 4 : gpdf (RHSA-2009:0458)

RHEL 4 : gpdf (RHSA-2009:1503)

RHEL 4 : gpdf (RHSA-2009:1681)

RHEL 4 : gpdf (RHSA-2010:0752)

RHEL 4 : gstreamer-plugins (RHSA-2009:0270)

RHEL 4 : gstreamer-plugins (RHSA-2011:0477)

RHEL 4 : gstreamer-plugins (RHSA-2011:1264)

RHEL 4 : gtk2 (RHSA-2007:0019)

RHEL 4 : HelixPlayer (RHSA-2005:271)

RHEL 4 : HelixPlayer (RHSA-2005:392)

RHEL 4 : HelixPlayer (RHSA-2005:517)

RHEL 4 : HelixPlayer (RHSA-2005:788)

RHEL 4 : HelixPlayer (RHSA-2007:0605)

RHEL 4 : HelixPlayer (RHSA-2010:0094)

RHEL 4 : HelixPlayer (RHSA-2010:0981)

RHEL 4 : htdig (RHSA-2005:090)

RHEL 4 : httpd (RHSA-2007:0534)

RHEL 4 : httpd (RHSA-2007:0747)

RHEL 4 : httpd (RHSA-2008:0006)

RHEL 4 : httpd (RHSA-2009:1580)

RHEL 4 : httpd (RHSA-2010:0175)

RHEL 4 : ImageMagick (RHSA-2005:071)

RHEL 4 : ImageMagick (RHSA-2005:320)

RHEL 4 : ImageMagick (RHSA-2010:0653)

RHEL 4 : initscripts (RHSA-2006:0016)

RHEL 4 : java-1.4.2-bea (RHSA-2007:1086)

RHEL 4 : java-1.5.0-ibm (RHSA-2007:0073)

RHEL 4 : java-1.5.0-sun (RHSA-2007:0818)

RHEL 4 : JBoss EAP (RHSA-2008:0151)

RHEL 4 : JBoss EAP (RHSA-2008:0825)

RHEL 4 : JBoss EAP (RHSA-2008:0826)

RHEL 4 : JBoss EAP (RHSA-2008:0831)

RHEL 4 : JBoss EAP (RHSA-2008:0833)

RHEL 4 : JBoss EAP (RHSA-2009:0346)

RHEL 4 : JBoss EAP (RHSA-2009:0347)

RHEL 4 : JBoss EAP (RHSA-2009:1144)

RHEL 4 : JBoss EAP (RHSA-2009:1146)

RHEL 4 : JBoss EAP (RHSA-2009:1636)

RHEL 4 : JBoss EAP (RHSA-2009:1637)

RHEL 4 : JBoss EAP (RHSA-2010:0376)

RHEL 4 : JBoss EAP (RHSA-2010:0377)

RHEL 4 : JBoss EAP (RHSA-2010:0937)

RHEL 4 : JBoss EAP (RHSA-2010:0959)

RHEL 4 : JBoss EAP (RHSA-2011:0947)

RHEL 4 : JBoss EAP (RHSA-2011:1800)

RHEL 4 : JBoss EAP (RHSA-2013:0193)

RHEL 4 : JBoss EWP (RHSA-2013:0197)

RHEL 4 : kdebase (RHSA-2006:0548)

RHEL 4 : kdebase (RHSA-2006:0582)

RHEL 4 : kdegraphics (RHSA-2005:066)

RHEL 4 : kdegraphics (RHSA-2005:671)

RHEL 4 : kdegraphics (RHSA-2005:868)

RHEL 4 : kdegraphics (RHSA-2006:0206)

RHEL 4 : kdegraphics (RHSA-2006:0262)

RHEL 4 : kdegraphics (RHSA-2007:1024)

RHEL 4 : kdegraphics (RHSA-2008:0238)

RHEL 4 : kdegraphics (RHSA-2009:1512)

RHEL 4 : kdegraphics (RHSA-2009:1682)

RHEL 4 : kdelibs (RHSA-2005:065)

RHEL 4 : kdelibs (RHSA-2005:325)

RHEL 4 : kdelibs (RHSA-2005:393)

RHEL 4 : kdelibs (RHSA-2005:612)

RHEL 4 : kdelibs (RHSA-2006:0184)

RHEL 4 : kdenetwork (RHSA-2005:639)

RHEL 4 : kernel (RHSA-2005:092)

RHEL 4 : kernel (RHSA-2005:366)

RHEL 4 : kernel (RHSA-2005:420)

RHEL 4 : kernel (RHSA-2005:514)

RHEL 4 : kernel (RHSA-2005:808)

RHEL 4 : kernel (RHSA-2006:0101)

RHEL 4 : kernel (RHSA-2006:0132)

RHEL 4 : kernel (RHSA-2006:0493)

RHEL 4 : kernel (RHSA-2006:0574)

RHEL 4 : kernel (RHSA-2006:0575)

RHEL 4 : kernel (RHSA-2006:0617)

RHEL 4 : kernel (RHSA-2006:0689)

RHEL 4 : kernel (RHSA-2007:0014)

RHEL 4 : kernel (RHSA-2007:0085)

RHEL 4 : kernel (RHSA-2007:0488)

RHEL 4 : kernel (RHSA-2007:0774)

RHEL 4 : kernel (RHSA-2007:0937)

RHEL 4 : kernel (RHSA-2007:0939)

RHEL 4 : kernel (RHSA-2007:1104)

RHEL 4 : kernel (RHSA-2008:0055)

RHEL 4 : kernel (RHSA-2008:0167)

RHEL 4 : kernel (RHSA-2008:0237)

RHEL 4 : kernel (RHSA-2008:0508)

RHEL 4 : kernel (RHSA-2008:0607)

RHEL 4 : kernel (RHSA-2008:0665)

RHEL 4 : kernel (RHSA-2008:0972)

RHEL 4 : kernel (RHSA-2009:0014)

RHEL 4 : kernel (RHSA-2009:0331)

RHEL 4 : kernel (RHSA-2009:0459)

RHEL 4 : kernel (RHSA-2009:1024)

RHEL 4 : kernel (RHSA-2009:1077)

RHEL 4 : kernel (RHSA-2009:1132)

RHEL 4 : kernel (RHSA-2009:1211)

RHEL 4 : kernel (RHSA-2009:1223)

RHEL 4 : kernel (RHSA-2009:1438)

RHEL 4 : kernel (RHSA-2009:1469)

RHEL 4 : kernel (RHSA-2009:1522)

RHEL 4 : kernel (RHSA-2009:1541)

RHEL 4 : kernel (RHSA-2009:1588)

RHEL 4 : kernel (RHSA-2009:1671)

RHEL 4 : kernel (RHSA-2010:0020)

RHEL 4 : kernel (RHSA-2010:0076)

RHEL 4 : kernel (RHSA-2010:0111)

RHEL 4 : kernel (RHSA-2010:0146)

RHEL 4 : kernel (RHSA-2010:0342)

RHEL 4 : kernel (RHSA-2010:0394)

RHEL 4 : kernel (RHSA-2010:0424)

RHEL 4 : kernel (RHSA-2010:0474)

RHEL 4 : kernel (RHSA-2010:0606)

RHEL 4 : kernel (RHSA-2010:0676)

RHEL 4 : kernel (RHSA-2010:0677)

RHEL 4 : kernel (RHSA-2010:0718)

RHEL 4 : kernel (RHSA-2010:0719)

RHEL 4 : kernel (RHSA-2010:0779)

RHEL 4 : kernel (RHSA-2010:0936)

RHEL 4 : kernel (RHSA-2011:0162)

RHEL 4 : kernel (RHSA-2011:0263)

RHEL 4 : kernel (RHSA-2015:0009)

RHEL 4 : krb5 (RHSA-2005:045)

RHEL 4 : krb5 (RHSA-2005:567)

RHEL 4 : krb5 (RHSA-2006:0612)

RHEL 4 : krb5 (RHSA-2008:0180)

RHEL 4 : krb5 (RHSA-2008:0182)

RHEL 4 : krb5 (RHSA-2009:0409)

RHEL 4 : libc-client (RHSA-2005:848)

RHEL 4 : libexif (RHSA-2005:300)

RHEL 4 : libexif (RHSA-2007:1166)

RHEL 4 : libgtop2 (RHSA-2007:0765)

RHEL 4 : libpng (RHSA-2006:0205)

RHEL 4 : libpng (RHSA-2011:1103)

RHEL 4 : libtiff (RHSA-2005:035)

RHEL 4 : libtiff (RHSA-2008:0848)

RHEL 4 : libwmf (RHSA-2006:0597)

RHEL 4 : libxml2 (RHSA-2012:0016)

RHEL 4 : lm\_sensors (RHSA-2005:825)

RHEL 4 : mailman (RHSA-2005:137)

RHEL 4 : mailman (RHSA-2007:0779)

RHEL 4 : mod\_auth\_kerb (RHSA-2006:0746)

RHEL 4 : mod\_jk in Satellite Server (RHSA-2009:1618)

RHEL 4 : mod\_python (RHSA-2005:100)

RHEL 4 : mozilla (RHSA-2005:277)

RHEL 4 : mozilla (RHSA-2005:335)

RHEL 4 : Mozilla (RHSA-2005:386)

RHEL 4 : mysql (RHSA-2005:685)

RHEL 4 : mysql (RHSA-2006:0544)

RHEL 4 : mysql (RHSA-2007:0152)

RHEL 4 : mysql (RHSA-2008:0768)

RHEL 4 : mysql (RHSA-2010:0110)

RHEL 4 : mysql (RHSA-2010:0824)

RHEL 4 : net-snmp (RHSA-2005:395)

RHEL 4 : netpbm (RHSA-2005:793)

RHEL 4 : NetworkManager (RHSA-2009:0362)

RHEL 4 : nfs-utils (RHSA-2009:0955)

RHEL 4 : nfs-utils-lib (RHSA-2007:0913)

RHEL 4 : nspr and nss (RHSA-2009:1184)

RHEL 4 : nspr and nss (RHSA-2009:1190)

RHEL 4 : nss (RHSA-2014:1165)

RHEL 4 : nss\_ldap (RHSA-2006:0719)

RHEL 4 : nss\_ldap (RHSA-2008:0715)

RHEL 4 : ntp (RHSA-2006:0393)

RHEL 4 : ntp (RHSA-2009:1040)

RHEL 4 : openldap (RHSA-2007:0310)

RHEL 4 : openldap (RHSA-2007:1038)

RHEL 4 : openldap (RHSA-2010:0543)

RHEL 4 : openldap and nss\_ldap (RHSA-2005:767)

RHEL 4 : openoffice.org and openoffice.org2 (RHSA-2011:0181)

RHEL 4 : openoffice.org2 (RHSA-2007:1090)

RHEL 4 : openssh (RHSA-2005:527)

RHEL 4 : openssh (RHSA-2006:0044)

RHEL 4 : openssh (RHSA-2007:0257)

RHEL 4 : openssh (RHSA-2007:0703)

RHEL 4 : openssl (RHSA-2007:1003)

RHEL 4 : openssl (RHSA-2010:0977)

RHEL 4 : openssl (RHSA-2012:0086)

RHEL 4 : pam (RHSA-2005:805)

RHEL 4 : pam (RHSA-2007:0737)

RHEL 4 : pcre (RHSA-2007:0968)

RHEL 4 : pcre (RHSA-2007:1068)

RHEL 4 : perl (RHSA-2005:103)

RHEL 4 : perl (RHSA-2005:674)

RHEL 4 : perl (RHSA-2005:880)

RHEL 4 : perl (RHSA-2006:0605)

RHEL 4 : perl-DBI (RHSA-2005:072)

RHEL 4 : perl-Net-DNS (RHSA-2007:0675)

RHEL 4 : php (RHSA-2005:032)

RHEL 4 : PHP (RHSA-2005:406)

RHEL 4 : php (RHSA-2007:0349)

RHEL 4 : php (RHSA-2008:0545)

RHEL 4 : php (RHSA-2012:0071)

RHEL 4 : postfix (RHSA-2005:152)

RHEL 4 : postgresql (RHSA-2005:138)

RHEL 4 : postgresql (RHSA-2010:0428)

RHEL 4 : Proxy Server (RHSA-2008:0263)

RHEL 4 : Proxy Server (RHSA-2008:0627)

RHEL 4 : python (RHSA-2005:108)

RHEL 4 : python (RHSA-2009:1177)

RHEL 4 : python (RHSA-2011:0260)

RHEL 4 : python (RHSA-2011:0491)

RHEL 4 : rdesktop (RHSA-2008:0725)

RHEL 4 : RealPlayer (RHSA-2005:265)

RHEL 4 : RealPlayer (RHSA-2005:363)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2011:0219)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2011:0259)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2011:0279)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2011:1239)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2011:1240)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2011:1506)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2012:0073)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2012:0349)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2012:1546)

RHEL 4 : redhat-release (EOL Notice) (RHSA-2012:1547)

RHEL 4 : rpm (RHSA-2010:0678)

RHEL 4 : rsh (RHSA-2005:165)

RHEL 4 : ruby (RHSA-2005:543)

RHEL 4 : ruby (RHSA-2006:0427)

RHEL 4 : ruby (RHSA-2007:0961)

RHEL 4 : ruby (RHSA-2011:0908)

RHEL 4 : samba (RHSA-2007:1016)

RHEL 4 : samba (RHSA-2007:1034)

RHEL 4 : samba (RHSA-2007:1117)

RHEL 4 : samba (RHSA-2008:0289)

RHEL 4 : Satellite Server (RHSA-2007:0868)

RHEL 4 : Satellite Server (RHSA-2008:0261)

RHEL 4 : Satellite Server (RHSA-2008:0630)

RHEL 4 : seamonkey (RHSA-2006:0609)

RHEL 4 : seamonkey (RHSA-2009:1431)

RHEL 4 : seamonkey (RHSA-2010:0967)

RHEL 4 : seamonkey (RHSA-2011:0313)

RHEL 4 : seamonkey (RHSA-2011:0375)

RHEL 4 : seamonkey (RHSA-2011:0473)

RHEL 4 : seamonkey (RHSA-2011:0888)

RHEL 4 : seamonkey (RHSA-2011:1167)

RHEL 4 : seamonkey (RHSA-2011:1244)

RHEL 4 : seamonkey (RHSA-2011:1266)

RHEL 4 : seamonkey (RHSA-2011:1344)

RHEL 4 : seamonkey (RHSA-2011:1440)

RHEL 4 : seamonkey (RHSA-2012:0084)

RHEL 4 : seamonkey (RHSA-2012:0141)

RHEL 4 : sendmail (RHSA-2007:0252)

RHEL 4 : sendmail (RHSA-2011:0262)

RHEL 4 : shadow-utils (RHSA-2007:0276)

RHEL 4 : slocate (RHSA-2005:346)

RHEL 4 : Solaris client in Satellite Server (RHSA-2008:0264)

RHEL 4 : Solaris client in Satellite Server (RHSA-2008:0629)

RHEL 4 : spamassassin (RHSA-2005:498)

RHEL 4 : spamassassin (RHSA-2006:0129)

RHEL 4 : spamassassin (RHSA-2006:0543)

RHEL 4 : spamassassin (RHSA-2007:0074)

RHEL 4 : squid (RHSA-2005:060)

RHEL 4 : squid (RHSA-2005:201)

RHEL 4 : squid (RHSA-2006:0052)

RHEL 4 : squirrelmail (RHSA-2005:099)

RHEL 4 : subversion (RHSA-2011:0861)

RHEL 4 : Sun Java Runtime in Satellite Server (RHSA-2008:0636)

RHEL 4 : Sun Java Runtime in Satellite Server (RHSA-2009:1662)

RHEL 4 : systemtap (RHSA-2010:0125)

RHEL 4 : systemtap (RHSA-2010:0895)

RHEL 4 : tar (RHSA-2006:0232)

RHEL 4 : tcpdump (RHSA-2005:417)

RHEL 4 : tcpdump (RHSA-2005:505)

RHEL 4 : tcpdump (RHSA-2007:0387)

RHEL 4 : tetex (RHSA-2005:026)

RHEL 4 : tetex (RHSA-2010:0399)

RHEL 4 : thunderbird (RHSA-2005:094)

RHEL 4 : thunderbird (RHSA-2005:337)

RHEL 4 : thunderbird (RHSA-2005:601)

RHEL 4 : thunderbird (RHSA-2005:791)

RHEL 4 : thunderbird (RHSA-2006:0330)

RHEL 4 : thunderbird (RHSA-2006:0611)

RHEL 4 : thunderbird (RHSA-2006:0677)

RHEL 4 : thunderbird (RHSA-2006:0735)

RHEL 4 : thunderbird (RHSA-2006:0760)

RHEL 4 : thunderbird (RHSA-2007:0078)

RHEL 4 : thunderbird (RHSA-2009:1125)

RHEL 4 : thunderbird (RHSA-2010:0154)

RHEL 4 : thunderbird (RHSA-2010:0544)

RHEL 4 : tk (RHSA-2008:0135)

RHEL 4 : tomcat in Satellite Server (RHSA-2008:1007)

RHEL 4 : tomcat in Satellite Server (RHSA-2009:1616)

RHEL 4 : tomcat in Satellite Server (RHSA-2009:1617)

RHEL 4 : udev (RHSA-2005:864)

RHEL 4 : unzip (RHSA-2007:0203)

RHEL 4 : util-linux (RHSA-2007:0235)

RHEL 4 : util-linux (RHSA-2009:0981)

RHEL 4 : vim (RHSA-2005:036)

RHEL 4 : vixie-cron (RHSA-2005:361)

RHEL 4 : vixie-cron (RHSA-2006:0539)

RHEL 4 : vsftpd (RHSA-2008:0680)

RHEL 4 : w3c-libwww (RHSA-2007:0208)

RHEL 4 : wireshark (RHSA-2007:0709)

RHEL 4 : xemacs (RHSA-2005:133)

RHEL 4 : xorg-x11 (RHSA-2005:198)

RHEL 4 : xorg-x11 (RHSA-2005:396)

RHEL 4 : xorg-x11 (RHSA-2006:0451)

RHEL 4 : xorg-x11 (RHSA-2006:0634)

RHEL 4 : xorg-x11 (RHSA-2006:0665)

RHEL 4 : xorg-x11 (RHSA-2007:0003)

RHEL 4 : xorg-x11 (RHSA-2007:0126)

RHEL 4 : xorg-x11 (RHSA-2007:0519)

RHEL 4 : xorg-x11 (RHSA-2007:0898)

RHEL 4 : xorg-x11 (RHSA-2008:0030)

RHEL 4 : xorg-x11 (RHSA-2008:0503)

RHEL 4 : xorg-x11 (RHSA-2011:0432)

RHEL 4 : xorg-x11 (RHSA-2011:1155)

RHEL 4 : xorg-x11 (RHSA-2011:1360)

RHEL 4 : xpdf (RHSA-2005:034)

RHEL 4 : xpdf (RHSA-2005:670)

RHEL 4 : xpdf (RHSA-2006:0201)

RHEL 4 : xpdf (RHSA-2007:1029)

RHEL 4 : xpdf (RHSA-2008:0240)

RHEL 4 : xpdf (RHSA-2009:1501)

RHEL 4 : xpdf (RHSA-2009:1680)

RHEL 4 : xpdf (RHSA-2010:0751)

RHEL 4 : xterm (RHSA-2007:0701)

RHEL 4 : zlib (RHSA-2005:569)

RHEL 4 : zlib (RHSA-2005:584)

RHEL 5 / 6 / 7 : bash (RHSA-2014:1293) (Shellshock)

RHEL 5 / 6 / 7 : bash (RHSA-2014:1306)

RHEL 5 / 6 / 7 : bind (RHSA-2014:1984)

RHEL 5 / 6 / 7 : bind (RHSA-2016:0073)

RHEL 5 / 6 / 7 : bind (RHSA-2016:0459)

RHEL 5 / 6 / 7 : bind (RHSA-2016:1944)

RHEL 5 / 6 / 7 : firefox (RHSA-2014:0741)

RHEL 5 / 6 / 7 : firefox (RHSA-2014:0919)

RHEL 5 / 6 / 7 : firefox (RHSA-2014:1144)

RHEL 5 / 6 / 7 : firefox (RHSA-2014:1635)

RHEL 5 / 6 / 7 : firefox (RHSA-2014:1919)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:0046)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:0265)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:0718)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:0766)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:0988)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:1207)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:1581)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:1586)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:1693)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:1834)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:1982)

RHEL 5 / 6 / 7 : firefox (RHSA-2015:2657)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:0071)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:0197)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:0373)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:0695)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:1217)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:1551)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:1912)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:2780)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:2843)

RHEL 5 / 6 / 7 : firefox (RHSA-2016:2946)

RHEL 5 / 6 / 7 : firefox (RHSA-2017:0190)

RHEL 5 / 6 / 7 : glibc (CVE-2014-9402)

RHEL 5 / 6 / 7 : glibc (RHSA-2014:1110)

RHEL 5 / 6 / 7 : jakarta-commons-httpclient (RHSA-2014:1166)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2014:0907)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2014:1634)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2015:0085) (POODLE)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2015:0808)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2015:1526) (Bar Mitzvah) (Logjam)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2015:2086)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2016:0067)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2016:0723)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2016:1776)

RHEL 5 / 6 / 7 : java-1.6.0-openjdk (RHSA-2017:0061)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2014:0908)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2014:1658)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2015:0086) (POODLE)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2015:0858)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2015:1243) (Bar Mitzvah) (Logjam)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2015:1928)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2016:0057)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2016:0679)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2016:1477)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2016:2090)

RHEL 5 / 6 / 7 : java-1.6.0-sun (RHSA-2017:0177)

RHEL 5 / 6 / 7 : java-1.7.0-openjdk (RHSA-2016:1504)

RHEL 5 / 6 / 7 : java-1.7.0-openjdk (RHSA-2016:2658)

RHEL 5 / 6 / 7 : java-1.7.0-openjdk (RHSA-2017:0269)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2014:0902)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2014:1657)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2015:0079) (POODLE)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2015:0857)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2015:1242) (Bar Mitzvah) (Logjam)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2015:1927)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2016:0056) (SLOTH)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2016:0515)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2016:0678)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2016:1476)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2016:2089)

RHEL 5 / 6 / 7 : java-1.7.0-oracle (RHSA-2017:0176)

RHEL 5 / 6 / 7 : JBoss EAP (RHSA-2014:1040)

RHEL 5 / 6 / 7 : JBoss EAP (RHSA-2014:1162)

RHEL 5 / 6 / 7 : JBoss EAP (RHSA-2014:2019)

RHEL 5 / 6 / 7 : JBoss EAP (RHSA-2015:2500)

RHEL 5 / 6 / 7 : JBoss EAP (RHSA-2015:2536)

RHEL 5 / 6 / 7 : JBoss EAP (RHSA-2016:1330)

RHEL 5 / 6 / 7 : JBoss Web Server (RHSA-2015:1622)

RHEL 5 / 6 / 7 : JBoss Web Server (RHSA-2015:1642)

RHEL 5 / 6 / 7 : JBoss Web Server (RHSA-2016:0061)

RHEL 5 / 6 / 7 : nss (RHSA-2014:1307)

RHEL 5 / 6 / 7 : nss and nss-util (RHSA-2016:2779)

RHEL 5 / 6 / 7 : nss, nss-util, and nss-softokn (RHSA-2014:1948) (POODLE)

RHEL 5 / 6 / 7 : openldap (RHSA-2015:1840)

RHEL 5 / 6 / 7 : procmail (RHSA-2014:1172)

RHEL 5 / 6 / 7 : Red Hat JBoss Enterprise Application Platform 6.4 (RHSA-2020:1478)

RHEL 5 / 6 / 7 : setroubleshoot (RHSA-2015:0729)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2015:0771)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2015:1012)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2015:1455)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2015:1682)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2015:1852)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2015:2519)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:0001)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:0258)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:0460)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:1041)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:1392)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:1809)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:1985)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:2825)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:2850)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2016:2973)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2017:0238)

RHEL 5 / 6 / 7 : thunderbird (RHSA-2017:0498)

RHEL 5 / 6 : acroread (RHSA-2012:0011)

RHEL 5 / 6 : acroread (RHSA-2012:0469)

RHEL 5 / 6 : acroread (RHSA-2013:0150)

RHEL 5 / 6 : acroread (RHSA-2013:0551)

RHEL 5 / 6 : acroread (RHSA-2013:0826)

RHEL 5 / 6 : Adobe Reader (RHSA-2013:1402)

RHEL 5 / 6 : apache-cxf (RHSA-2013:0644)

RHEL 5 / 6 : axis (RHSA-2014:1193)

RHEL 5 / 6 : bind (RHSA-2011:0845)

RHEL 5 / 6 : bind (RHSA-2011:0926)

RHEL 5 / 6 : bind (RHSA-2011:1458)

RHEL 5 / 6 : bind (RHSA-2012:0716)

RHEL 5 / 6 : bind (RHSA-2012:1123)

RHEL 5 / 6 : bind (RHSA-2012:1363)

RHEL 5 / 6 : bind (RHSA-2016:2093)

RHEL 5 / 6 : bind (RHSA-2016:2141)

RHEL 5 / 6 : bind (RHSA-2017:0063)

RHEL 5 / 6 : boost (RHSA-2013:0668)

RHEL 5 / 6 : cobbler (RHSA-2012:1060)

RHEL 5 / 6 : cups (RHSA-2013:0580)

RHEL 5 / 6 : curl (RHSA-2013:0771)

RHEL 5 / 6 : curl (RHSA-2013:0983)

RHEL 5 / 6 : cvs (RHSA-2012:0321)

RHEL 5 / 6 : dbus (RHSA-2011:0376)

RHEL 5 / 6 : dbus (RHSA-2011:1132)

RHEL 5 / 6 : dbus-glib (RHSA-2013:0568)

RHEL 5 / 6 : ecryptfs-utils (RHSA-2011:1241)

RHEL 5 / 6 : elinks (RHSA-2013:0250)

RHEL 5 / 6 : expat (RHSA-2012:0731)

RHEL 5 / 6 : firefox (RHSA-2012:0387)

RHEL 5 / 6 : firefox (RHSA-2012:0515)

RHEL 5 / 6 : firefox (RHSA-2012:0710)

RHEL 5 / 6 : firefox (RHSA-2012:1088)

RHEL 5 / 6 : firefox (RHSA-2012:1210)

RHEL 5 / 6 : firefox (RHSA-2012:1350)

RHEL 5 / 6 : firefox (RHSA-2012:1407)

RHEL 5 / 6 : firefox (RHSA-2012:1482)

RHEL 5 / 6 : firefox (RHSA-2013:0144)

RHEL 5 / 6 : firefox (RHSA-2013:0271)

RHEL 5 / 6 : firefox (RHSA-2013:0696)

RHEL 5 / 6 : firefox (RHSA-2013:0820)

RHEL 5 / 6 : firefox (RHSA-2013:0981)

RHEL 5 / 6 : firefox (RHSA-2013:1140)

RHEL 5 / 6 : firefox (RHSA-2013:1268)

RHEL 5 / 6 : firefox (RHSA-2013:1476)

RHEL 5 / 6 : firefox (RHSA-2013:1812)

RHEL 5 / 6 : firefox (RHSA-2014:0132)

RHEL 5 / 6 : firefox (RHSA-2014:0310)

RHEL 5 / 6 : firefox (RHSA-2014:0448)

RHEL 5 / 6 : firefox (RHSA-2017:0459)

RHEL 5 / 6 : flash-plugin (RHSA-2011:0206)

RHEL 5 / 6 : flash-plugin (RHSA-2011:0372)

RHEL 5 / 6 : flash-plugin (RHSA-2011:0451)

RHEL 5 / 6 : flash-plugin (RHSA-2011:0511)

RHEL 5 / 6 : flash-plugin (RHSA-2011:0850)

RHEL 5 / 6 : flash-plugin (RHSA-2011:0869)

RHEL 5 / 6 : flash-plugin (RHSA-2011:1144)

RHEL 5 / 6 : flash-plugin (RHSA-2011:1333)

RHEL 5 / 6 : flash-plugin (RHSA-2011:1445)

RHEL 5 / 6 : flash-plugin (RHSA-2012:0144)

RHEL 5 / 6 : flash-plugin (RHSA-2012:0359)

RHEL 5 / 6 : flash-plugin (RHSA-2012:0434)

RHEL 5 / 6 : flash-plugin (RHSA-2012:0688)

RHEL 5 / 6 : flash-plugin (RHSA-2012:0722)

RHEL 5 / 6 : flash-plugin (RHSA-2012:1346)

RHEL 5 / 6 : flash-plugin (RHSA-2012:1431)

RHEL 5 / 6 : flash-plugin (RHSA-2012:1569)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0149)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0243)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0254)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0574)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0643)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0730)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0825)

RHEL 5 / 6 : flash-plugin (RHSA-2013:0941)

RHEL 5 / 6 : flash-plugin (RHSA-2013:1035)

RHEL 5 / 6 : flash-plugin (RHSA-2013:1256)

RHEL 5 / 6 : flash-plugin (RHSA-2013:1518)

RHEL 5 / 6 : flash-plugin (RHSA-2013:1818)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0028)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0137)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0196)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0289)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0380)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0447)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0496)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0745)

RHEL 5 / 6 : flash-plugin (RHSA-2014:0860)

RHEL 5 / 6 : flash-plugin (RHSA-2014:1051)

RHEL 5 / 6 : flash-plugin (RHSA-2014:1173)

RHEL 5 / 6 : flash-plugin (RHSA-2014:1648)

RHEL 5 / 6 : flash-plugin (RHSA-2014:1852)

RHEL 5 / 6 : flash-plugin (RHSA-2014:1915)

RHEL 5 / 6 : flash-plugin (RHSA-2014:1981)

RHEL 5 / 6 : flash-plugin (RHSA-2015:0052)

RHEL 5 / 6 : flash-plugin (RHSA-2015:0094)

RHEL 5 / 6 : flash-plugin (RHSA-2015:0140)

RHEL 5 / 6 : flash-plugin (RHSA-2015:0697)

RHEL 5 / 6 : flash-plugin (RHSA-2015:0813)

RHEL 5 / 6 : flash-plugin (RHSA-2015:1005)

RHEL 5 / 6 : flash-plugin (RHSA-2015:1086)

RHEL 5 / 6 : flash-plugin (RHSA-2015:1184)

RHEL 5 / 6 : flash-plugin (RHSA-2015:1214) (Underminer)

RHEL 5 / 6 : flash-plugin (RHSA-2015:1235)

RHEL 5 / 6 : flash-plugin (RHSA-2015:1603)

RHEL 5 / 6 : flash-plugin (RHSA-2015:1814)

RHEL 5 / 6 : flash-plugin (RHSA-2015:2593)

RHEL 5 / 6 : flash-plugin (RHSA-2015:2697)

RHEL 5 / 6 : flash-plugin (RHSA-2016:0166)

RHEL 5 / 6 : flash-plugin (RHSA-2016:0438)

RHEL 5 / 6 : flash-plugin (RHSA-2016:0610)

RHEL 5 / 6 : flash-plugin (RHSA-2016:1079)

RHEL 5 / 6 : flash-plugin (RHSA-2016:1238)

RHEL 5 / 6 : flash-plugin (RHSA-2016:1423)

RHEL 5 / 6 : flash-plugin (RHSA-2016:1865)

RHEL 5 / 6 : flash-plugin (RHSA-2016:2057)

RHEL 5 / 6 : flash-plugin (RHSA-2016:2119)

RHEL 5 / 6 : flash-plugin (RHSA-2016:2676)

RHEL 5 / 6 : freetype (RHSA-2012:0467)

RHEL 5 / 6 : freetype (RHSA-2013:0216)

RHEL 5 / 6 : ghostscript (RHSA-2012:0095)

RHEL 5 / 6 : ghostscript (RHSA-2012:1256)

RHEL 5 / 6 : gimp (RHSA-2013:1778)

RHEL 5 / 6 : glibc (RHSA-2014:1118)

RHEL 5 / 6 : glibc (RHSA-2015:0099) (GHOST)

RHEL 5 / 6 : gnupg2 (RHSA-2013:1459)

RHEL 5 / 6 : gnutls (RHSA-2013:0588)

RHEL 5 / 6 : gnutls (RHSA-2013:0883)

RHEL 5 / 6 : hplip (RHSA-2011:0154)

RHEL 5 / 6 : httpd (RHSA-2011:1294)

RHEL 5 / 6 : httpd (RHSA-2013:0815)

RHEL 5 / 6 : httpd (RHSA-2013:1156)

RHEL 5 / 6 : httpd (RHSA-2014:0920)

RHEL 5 / 6 : httpd (RHSA-2016:1421) (httpoxy)

RHEL 5 / 6 : IBM Java Runtime in Satellite Server (RHSA-2013:1455) (BEAST) (ROBOT)

RHEL 5 / 6 : IBM Java Runtime in Satellite Server (RHSA-2013:1456) (ROBOT)

RHEL 5 / 6 : IBM Java Runtime in Satellite Server (RHSA-2013:1793)

RHEL 5 / 6 : IBM Java Runtime in Satellite Server (RHSA-2014:0982)

RHEL 5 / 6 : icu (RHSA-2011:1815)

RHEL 5 / 6 : jabberd (RHSA-2012:1539)

RHEL 5 / 6 : jabberd in Satellite Server (RHSA-2012:1538)

RHEL 5 / 6 : jakarta-commons-httpclient (RHSA-2013:0270)

RHEL 5 / 6 : jakarta-commons-httpclient (RHSA-2013:0680)

RHEL 5 / 6 : java-1.4.2-ibm-sap (RHSA-2012:1080)

RHEL 5 / 6 : java-1.4.2-ibm-sap (RHSA-2012:1332)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2012:0508) (BEAST)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2012:1245)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2012:1465) (ROBOT)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2013:0624)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2013:0855)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2013:1081)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2013:1509)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2014:0136)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2014:0509)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2014:1036)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2014:1881) (POODLE)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2015:0136)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2015:1021) (Bar Mitzvah)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2015:1544) (Logjam)

RHEL 5 / 6 : java-1.5.0-ibm (RHSA-2015:2518)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2012:0034) (BEAST)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2012:0514)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2012:1238)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2012:1466) (ROBOT)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2013:0625)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2013:0823)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2013:1059)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2013:1508)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2014:0135)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2014:0508)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2014:1033)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2014:1877) (POODLE)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2015:0135)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2015:1006) (Bar Mitzvah)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2015:1486) (Logjam)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2015:2508)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2016:0101) (SLOTH)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2016:0708)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2016:2659)

RHEL 5 / 6 : java-1.6.0-ibm (RHSA-2017:0338)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2011:0214)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2011:0281)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2011:1380) (BEAST)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2013:0770)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2013:1014)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2013:1505)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2014:0097)

RHEL 5 / 6 : java-1.6.0-openjdk (RHSA-2014:0408)

RHEL 5 / 6 : java-1.6.0-sun (RHSA-2012:0734)

RHEL 5 / 6 : java-1.6.0-sun (RHSA-2012:1392)

RHEL 5 / 6 : java-1.6.0-sun (RHSA-2013:0236)

RHEL 5 / 6 : java-1.6.0-sun (RHSA-2013:0531)

RHEL 5 / 6 : java-1.6.0-sun (RHSA-2013:0601)

RHEL 5 / 6 : java-1.6.0-sun (RHSA-2013:0758)

RHEL 5 / 6 : java-1.6.0-sun (RHSA-2014:0414)

RHEL 5 / 6 : java-1.7.0-ibm (RHSA-2013:0626)

RHEL 5 / 6 : java-1.7.0-ibm (RHSA-2013:0822)

RHEL 5 / 6 : java-1.7.0-ibm (RHSA-2013:1060)

RHEL 5 / 6 : java-1.7.0-ibm (RHSA-2013:1507)

RHEL 5 / 6 : java-1.7.0-ibm (RHSA-2014:0134)

RHEL 5 / 6 : java-1.7.0-ibm (RHSA-2014:0486)

RHEL 5 / 6 : java-1.7.0-ibm (RHSA-2014:1041)

RHEL 5 / 6 : java-1.7.0-ibm and java-1.7.1-ibm (RHSA-2016:1430) (SLOTH)

RHEL 5 / 6 : java-1.7.0-openjdk (RHSA-2013:0165)

RHEL 5 / 6 : java-1.7.0-openjdk (RHSA-2013:0247)

RHEL 5 / 6 : java-1.7.0-openjdk (RHSA-2013:0275)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2013:0156)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2013:0237)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2013:0532)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2013:0600)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2013:0757)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2013:0963)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2013:1440)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2014:0030)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2014:0412)

RHEL 5 / 6 : java-1.7.0-oracle (RHSA-2014:0413)

RHEL 5 / 6 : JBoss EAP (RHSA-2013:0229)

RHEL 5 / 6 : JBoss EAP (RHSA-2013:0231)

RHEL 5 / 6 : JBoss EAP (RHSA-2013:0257)

RHEL 5 / 6 : JBoss EAP (RHSA-2013:0873)

RHEL 5 / 6 : JBoss EAP (RHSA-2013:1151)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0204)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0253)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0453)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0591)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0793)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0826)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0843)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0883)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:0885)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:1726)

RHEL 5 / 6 : JBoss EAP (RHSA-2014:1834)

RHEL 5 / 6 : JBoss EAP (RHSA-2015:2535)

RHEL 5 / 6 : JBoss EAP (RHSA-2016:1328)

RHEL 5 / 6 : JBoss EAP (RHSA-2018:2664)

RHEL 5 / 6 : JBoss EWP (RHSA-2014:1728)

RHEL 5 / 6 : JBoss EWP (RHSA-2014:1833)

RHEL 5 / 6 : JBoss Web Server (RHSA-2012:0542)

RHEL 5 / 6 : JBoss Web Server (RHSA-2012:0680)

RHEL 5 / 6 : JBoss Web Server (RHSA-2012:0682)

RHEL 5 / 6 : JBoss Web Server (RHSA-2012:1166)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:0005)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:0158)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:0266)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:0268)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:0641)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:0871)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:1133)

RHEL 5 / 6 : JBoss Web Server (RHSA-2013:1428)

RHEL 5 / 6 : JBoss Web Server (RHSA-2014:0525)

RHEL 5 / 6 : JBoss Web Server (RHSA-2014:0526)

RHEL 5 / 6 : JBoss Web Server (RHSA-2014:0783)

RHEL 5 / 6 : JBoss Web Server (RHSA-2014:0834)

RHEL 5 / 6 : JBoss Web Server (RHSA-2014:0835)

RHEL 5 / 6 : jboss-remoting in JBoss EWP (RHSA-2013:1370)

RHEL 5 / 6 : jbossas and jboss-naming (RHSA-2012:1026)

RHEL 5 / 6 : jbossweb (RHSA-2012:0074)

RHEL 5 / 6 : jbossweb (RHSA-2013:0164)

RHEL 5 / 6 : jbossweb (RHSA-2013:0629)

RHEL 5 / 6 : jbossweb (RHSA-2013:0647)

RHEL 5 / 6 : jbossweb (RHSA-2013:1193)

RHEL 5 / 6 : krb5 (RHSA-2013:0942)

RHEL 5 / 6 : libexif (RHSA-2012:1255)

RHEL 5 / 6 : libgcrypt (RHSA-2013:1457)

RHEL 5 / 6 : libpng (RHSA-2012:0407)

RHEL 5 / 6 : libpng (RHSA-2012:0523)

RHEL 5 / 6 : libtiff (RHSA-2012:0468)

RHEL 5 / 6 : libtiff (RHSA-2012:1054)

RHEL 5 / 6 : libtiff (RHSA-2012:1590)

RHEL 5 / 6 : libvirt (RHSA-2011:0391)

RHEL 5 / 6 : libXfont (RHSA-2011:1154)

RHEL 5 / 6 : libXfont (RHSA-2014:0018)

RHEL 5 / 6 : libxml2 (RHSA-2012:0324)

RHEL 5 / 6 : libxml2 (RHSA-2012:1288)

RHEL 5 / 6 : libxml2 (RHSA-2012:1512)

RHEL 5 / 6 : libxml2 (RHSA-2013:0581)

RHEL 5 / 6 : libxslt (RHSA-2012:1265)

RHEL 5 / 6 : logwatch (RHSA-2011:0324)

RHEL 5 / 6 : mod\_cluster (RHSA-2012:1052)

RHEL 5 / 6 : mod\_cluster-native (RHSA-2012:0037)

RHEL 5 / 6 : mod\_nss (RHSA-2013:1779)

RHEL 5 / 6 : nss (RHSA-2013:1861)

RHEL 5 / 6 : nss (RHSA-2014:0915)

RHEL 5 / 6 : openoffice.org (RHSA-2012:0705)

RHEL 5 / 6 : openssl (RHSA-2012:0426)

RHEL 5 / 6 : openssl (RHSA-2012:0518)

RHEL 5 / 6 : openssl (RHSA-2012:0699)

RHEL 5 / 6 : openssl (RHSA-2013:0587)

RHEL 5 / 6 : openssl097a and openssl098e (RHSA-2014:0626)

RHEL 5 / 6 : openswan (RHSA-2011:1422)

RHEL 5 / 6 : openswan (RHSA-2013:0827)

RHEL 5 / 6 : openswan (RHSA-2014:0185)

RHEL 5 / 6 : Oracle Java SE (RHSA-2013:0666)

RHEL 5 / 6 : perl (RHSA-2013:0685)

RHEL 5 / 6 : perl-DBD-Pg (RHSA-2012:1116)

RHEL 5 / 6 : php (RHSA-2012:0546)

RHEL 5 / 6 : php (RHSA-2012:0568)

RHEL 5 / 6 : php (RHSA-2013:1049)

RHEL 5 / 6 : php (RHSA-2013:1061)

RHEL 5 / 6 : php (RHSA-2013:1824)

RHEL 5 / 6 : php53 and php (RHSA-2011:1423)

RHEL 5 / 6 : php53 and php (RHSA-2012:0019)

RHEL 5 / 6 : php53 and php (RHSA-2013:1813)

RHEL 5 / 6 : php53 and php (RHSA-2014:1012)

RHEL 5 / 6 : php53 and php (RHSA-2014:1326)

RHEL 5 / 6 : pidgin (RHSA-2012:1102)

RHEL 5 / 6 : pidgin (RHSA-2013:0646)

RHEL 5 / 6 : pidgin (RHSA-2014:0139)

RHEL 5 / 6 : pixman (RHSA-2013:1869)

RHEL 5 / 6 : postgresql and postgresql84 (RHSA-2012:0678)

RHEL 5 / 6 : postgresql and postgresql84 (RHSA-2012:1037)

RHEL 5 / 6 : postgresql and postgresql84 (RHSA-2012:1263)

RHEL 5 / 6 : postgresql and postgresql84 (RHSA-2013:1475)

RHEL 5 / 6 : postgresql84 and postgresql (RHSA-2014:0211)

RHEL 5 / 6 : rdesktop (RHSA-2011:0506)

RHEL 5 / 6 : Red Hat Satellite IBM Java Runtime (RHSA-2015:0264) (POODLE)

RHEL 5 / 6 : Red Hat Satellite IBM Java Runtime (RHSA-2015:1091) (Bar Mitzvah)

RHEL 5 / 6 : Red Hat Satellite IBM Java Runtime (RHSA-2015:1604) (Logjam)

RHEL 5 / 6 : resteasy (RHSA-2012:1059)

RHEL 5 / 6 : rhncfg (RHSA-2012:1369)

RHEL 5 / 6 : richfaces (RHSA-2013:1042)

RHEL 5 / 6 : richfaces in JBoss EWP (RHSA-2013:1043)

RHEL 5 / 6 : rpm (RHSA-2014:1974)

RHEL 5 / 6 : rpm (RHSA-2014:1975)

RHEL 5 / 6 : rsyslog5 and rsyslog (RHSA-2014:1671)

RHEL 5 / 6 : ruby (RHSA-2013:1090)

RHEL 5 / 6 : samba (RHSA-2012:0465)

RHEL 5 / 6 : samba and samba3x (RHSA-2012:0533)

RHEL 5 / 6 : samba and samba3x (RHSA-2013:1806)

RHEL 5 / 6 : samba and samba3x (RHSA-2014:0330)

RHEL 5 / 6 : samba and samba3x (RHSA-2014:0866)

RHEL 5 / 6 : Satellite Server (RHSA-2011:1299)

RHEL 5 / 6 : Satellite Server (RHSA-2011:1794)

RHEL 5 / 6 : scsi-target-utils (RHSA-2011:0332)

RHEL 5 / 6 : spacewalk-backend (RHSA-2012:0101)

RHEL 5 / 6 : spacewalk-backend (RHSA-2012:0102)

RHEL 5 / 6 : spacewalk-backend (RHSA-2017:1259)

RHEL 5 / 6 : spacewalk-backend in Satellite Server (RHSA-2013:0848)

RHEL 5 / 6 : spacewalk-java (RHSA-2014:1762)

RHEL 5 / 6 : spacewalk-java in Satellite Server (RHSA-2013:1514)

RHEL 5 / 6 : spacewalk-java, spacewalk-web and satellite-branding (RHSA-2014:0148)

RHEL 5 / 6 : squid (RHSA-2014:1148)

RHEL 5 / 6 : subscription-manager (RHSA-2013:0788)

RHEL 5 / 6 : subversion (RHSA-2011:0862)

RHEL 5 / 6 : subversion (RHSA-2013:0737)

RHEL 5 / 6 : subversion (RHSA-2014:0255)

RHEL 5 / 6 : sudo (RHSA-2012:1081)

RHEL 5 / 6 : systemtap (RHSA-2010:0894)

RHEL 5 / 6 : systemtap (RHSA-2012:0376)

RHEL 5 / 6 : thunderbird (RHSA-2012:0388)

RHEL 5 / 6 : thunderbird (RHSA-2012:0516)

RHEL 5 / 6 : thunderbird (RHSA-2012:0715)

RHEL 5 / 6 : thunderbird (RHSA-2012:1089)

RHEL 5 / 6 : thunderbird (RHSA-2012:1211)

RHEL 5 / 6 : thunderbird (RHSA-2012:1351)

RHEL 5 / 6 : thunderbird (RHSA-2012:1362)

RHEL 5 / 6 : thunderbird (RHSA-2012:1413)

RHEL 5 / 6 : thunderbird (RHSA-2012:1483)

RHEL 5 / 6 : thunderbird (RHSA-2013:0145)

RHEL 5 / 6 : thunderbird (RHSA-2013:0272)

RHEL 5 / 6 : thunderbird (RHSA-2013:0627)

RHEL 5 / 6 : thunderbird (RHSA-2013:0697)

RHEL 5 / 6 : thunderbird (RHSA-2013:0821)

RHEL 5 / 6 : thunderbird (RHSA-2013:0982)

RHEL 5 / 6 : thunderbird (RHSA-2013:1142)

RHEL 5 / 6 : thunderbird (RHSA-2013:1269)

RHEL 5 / 6 : thunderbird (RHSA-2013:1480)

RHEL 5 / 6 : thunderbird (RHSA-2013:1823)

RHEL 5 / 6 : thunderbird (RHSA-2014:0133)

RHEL 5 / 6 : thunderbird (RHSA-2014:0316)

RHEL 5 / 6 : thunderbird (RHSA-2014:0449)

RHEL 5 / 6 : thunderbird (RHSA-2014:0742)

RHEL 5 / 6 : thunderbird (RHSA-2014:0918)

RHEL 5 / 6 : thunderbird (RHSA-2014:1145)

RHEL 5 / 6 : thunderbird (RHSA-2014:1647)

RHEL 5 / 6 : thunderbird (RHSA-2014:1924)

RHEL 5 / 6 : thunderbird (RHSA-2015:0047)

RHEL 5 / 6 : thunderbird (RHSA-2015:0266)

RHEL 5 / 6 : tomcat5 and tomcat6 (RHSA-2013:0872)

RHEL 5 / 6 : vino (RHSA-2013:1452)

RHEL 5 / 6 : xalan-j2 (RHSA-2014:0348)

RHEL 5 / 6 : xinetd (RHSA-2013:1409)

RHEL 5 / 6 : xml-security (RHSA-2013:1217)

RHEL 5 / 6 : xml-security in JBoss EWP (RHSA-2013:1219)

RHEL 5 / 6 : xorg-x11-server (RHSA-2011:1359)

RHEL 5 / 6 : xorg-x11-server (RHSA-2013:1426)

RHEL 5 / 6 : xorg-x11-server (RHSA-2013:1868)

RHEL 5 / 6 : xorg-x11-server-utils (RHSA-2011:0433)

RHEL 5 / 6 : xulrunner (RHSA-2012:0143)

RHEL 5 / 6 : xulrunner (RHSA-2012:1361)

RHEL 5 / 6 : xulrunner (RHSA-2013:0614)

RHEL 5 / 7 : java-1.7.0-openjdk (RHSA-2016:0054) (SLOTH)

RHEL 5 / 7 : java-1.7.0-openjdk (RHSA-2016:0512)

RHEL 5 / 7 : java-1.7.0-openjdk (RHSA-2016:0676)

RHEL 5 / 7 : nss and nspr (RHSA-2014:0916)

RHEL 5 : acpid (RHSA-2009:1642)

RHEL 5 : acroread (RHSA-2010:0037)

RHEL 5 : aide (RHSA-2007:0539)

RHEL 5 : autofs (RHSA-2007:1128)

RHEL 5 : autofs (RHSA-2007:1176)

RHEL 5 : autofs (RHSA-2013:0132)

RHEL 5 : automake (RHSA-2010:0321)

RHEL 5 : automake (RHSA-2014:1243)

RHEL 5 : avahi (RHSA-2009:0013)

RHEL 5 : avahi (RHSA-2010:0528)

RHEL 5 : avahi (RHSA-2011:0436)

RHEL 5 : axis (RHSA-2013:0683)

RHEL 5 : bash (RHSA-2011:1073)

RHEL 5 : bind (RHSA-2007:0057)

RHEL 5 : bind (RHSA-2008:0300)

RHEL 5 : bind (RHSA-2009:1179)

RHEL 5 : bind (RHSA-2009:1620)

RHEL 5 : bind (RHSA-2010:0062)

RHEL 5 : bind (RHSA-2010:0976)

RHEL 5 : bind (RHSA-2012:1267)

RHEL 5 : bind (RHSA-2015:1514)

RHEL 5 : bind (RHSA-2015:1706)

RHEL 5 : bind (RHSA-2015:2656)

RHEL 5 : bind97 (RHSA-2011:1459)

RHEL 5 : bind97 (RHSA-2012:0717)

RHEL 5 : bind97 (RHSA-2012:1122)

RHEL 5 : bind97 (RHSA-2012:1266)

RHEL 5 : bind97 (RHSA-2012:1364)

RHEL 5 : bind97 (RHSA-2013:0690)

RHEL 5 : bind97 (RHSA-2013:1115)

RHEL 5 : bind97 (RHSA-2014:1244)

RHEL 5 : bind97 (RHSA-2014:1985)

RHEL 5 : bind97 (RHSA-2015:1515)

RHEL 5 : bind97 (RHSA-2015:1707)

RHEL 5 : bind97 (RHSA-2015:2658)

RHEL 5 : bind97 (RHSA-2016:0074)

RHEL 5 : bind97 (RHSA-2016:0458)

RHEL 5 : bind97 (RHSA-2016:1945)

RHEL 5 : bind97 (RHSA-2016:2094)

RHEL 5 : bind97 (RHSA-2016:2142)

RHEL 5 : bind97 (RHSA-2017:0064)

RHEL 5 : boost (RHSA-2012:0305)

RHEL 5 : brltty (RHSA-2010:0181)

RHEL 5 : busybox (RHSA-2012:0308)

RHEL 5 : cairo (RHSA-2007:1078)

RHEL 5 : ccid (RHSA-2013:1323)

RHEL 5 : cman (RHSA-2007:0559)

RHEL 5 : cman (RHSA-2009:1341)

RHEL 5 : compiz (RHSA-2008:0485)

RHEL 5 : condor (RHSA-2012:1168)

RHEL 5 : condor (RHSA-2015:0036)

RHEL 5 : conga (RHSA-2007:0640)

RHEL 5 : conga (RHSA-2011:0394)

RHEL 5 : conga (RHSA-2012:0151)

RHEL 5 : conga (RHSA-2013:0128)

RHEL 5 : conga (RHSA-2014:1194)

RHEL 5 : coolkey (RHSA-2007:0631)

RHEL 5 : cpio (RHSA-2010:0144)

RHEL 5 : cscope (RHSA-2009:1102)

RHEL 5 : cups (RHSA-2007:1020)

RHEL 5 : cups (RHSA-2007:1021)

RHEL 5 : cups (RHSA-2008:0157)

RHEL 5 : cups (RHSA-2008:0192)

RHEL 5 : cups (RHSA-2008:1029)

RHEL 5 : cups (RHSA-2009:1082)

RHEL 5 : cups (RHSA-2009:1513)

RHEL 5 : cups (RHSA-2009:1595)

RHEL 5 : cups (RHSA-2010:0129)

RHEL 5 : cups (RHSA-2010:0811)

RHEL 5 : cups (RHSA-2012:0302)

RHEL 5 : curl (RHSA-2010:0273)

RHEL 5 : dbus (RHSA-2008:0159)

RHEL 5 : dbus (RHSA-2009:0008)

RHEL 5 : dbus (RHSA-2010:0018)

RHEL 5 : dbus-glib (RHSA-2010:0616)

RHEL 5 : dhcp (RHSA-2012:1140)

RHEL 5 : dnsmasq (RHSA-2008:0789)

RHEL 5 : dnsmasq (RHSA-2009:1238)

RHEL 5 : dnsmasq (RHSA-2017:2840)

RHEL 5 : dnsmasq (RHSA-2017:2841)

RHEL 5 : dovecot (RHSA-2008:0297)

RHEL 5 : dovecot (RHSA-2009:0205)

RHEL 5 : dstat (RHSA-2009:1619)

RHEL 5 : ecryptfs-utils (RHSA-2009:1307)

RHEL 5 : ekiga (RHSA-2007:0087)

RHEL 5 : enscript (RHSA-2008:1016)

RHEL 5 : evolution (RHSA-2007:0158)

RHEL 5 : evolution (RHSA-2008:0514)

RHEL 5 : evolution-data-server (RHSA-2007:0344)

RHEL 5 : evolution-data-server (RHSA-2007:0510)

RHEL 5 : firefox (RHSA-2007:0097)

RHEL 5 : firefox (RHSA-2008:0569)

RHEL 5 : firefox (RHSA-2008:0597)

RHEL 5 : firefox (RHSA-2010:0501)

RHEL 5 : firefox (RHSA-2010:0556)

RHEL 5 : flash-plugin (RHSA-2008:0945)

RHEL 5 : flash-plugin (RHSA-2009:0332)

RHEL 5 : flash-plugin (RHSA-2009:1188)

RHEL 5 : flash-plugin (RHSA-2009:1657)

RHEL 5 : flash-plugin (RHSA-2010:0102)

RHEL 5 : flash-plugin (RHSA-2010:0464)

RHEL 5 : flash-plugin (RHSA-2010:0623)

RHEL 5 : flash-plugin (RHSA-2010:0829)

RHEL 5 : flash-plugin (RHSA-2012:1203)

RHEL 5 : flash-plugin (RHSA-2015:2024)

RHEL 5 : freeradius (RHSA-2009:1451)

RHEL 5 : freeradius2 (RHSA-2012:1327)

RHEL 5 : freeradius2 (RHSA-2013:0134)

RHEL 5 : freetype (RHSA-2009:1061)

RHEL 5 : freetype (RHSA-2012:0094)

RHEL 5 : gc in Satellite Server (RHSA-2014:0150)

RHEL 5 : gcc (RHSA-2011:0025)

RHEL 5 : gdm (RHSA-2007:0777)

RHEL 5 : gdm (RHSA-2009:1364)

RHEL 5 : gdm (RHSA-2013:1213)

RHEL 5 : gfs-kmod (RHSA-2010:0291)

RHEL 5 : gfs-kmod (RHSA-2010:0521)

RHEL 5 : gfs2-utils (RHSA-2009:1337)

RHEL 5 : ghostscript (RHSA-2009:0421)

RHEL 5 : giflib (RHSA-2009:0444)

RHEL 5 : gimp (RHSA-2011:0838)

RHEL 5 : gimp (RHSA-2012:1181)

RHEL 5 : glib2 (RHSA-2009:0336)

RHEL 5 : glibc (RHSA-2010:0787)

RHEL 5 : glibc (RHSA-2010:0793)

RHEL 5 : glibc (RHSA-2011:0412)

RHEL 5 : glibc (RHSA-2012:0126)

RHEL 5 : glibc (RHSA-2012:0397)

RHEL 5 : glibc (RHSA-2012:1097)

RHEL 5 : glibc (RHSA-2012:1207)

RHEL 5 : glibc (RHSA-2013:0769)

RHEL 5 : glibc (RHSA-2013:1411)

RHEL 5 : glibc (RHSA-2015:0090) (GHOST)

RHEL 5 : glibc (RHSA-2015:1627)

RHEL 5 : gnome-screensaver (RHSA-2008:0197)

RHEL 5 : gnome-screensaver (RHSA-2008:0218)

RHEL 5 : gnome-vfs2 (RHSA-2013:0131)

RHEL 5 : gnupg (RHSA-2007:0107)

RHEL 5 : gnupg (RHSA-2013:1458)

RHEL 5 : gnupg (RHSA-2014:0016)

RHEL 5 : gnupg2 (RHSA-2010:0603)

RHEL 5 : gnutls (RHSA-2008:0489)

RHEL 5 : gnutls (RHSA-2008:0982)

RHEL 5 : gnutls (RHSA-2010:0166)

RHEL 5 : gnutls (RHSA-2012:0428)

RHEL 5 : gnutls (RHSA-2014:0247)

RHEL 5 : gnutls (RHSA-2014:0594)

RHEL 5 : gstreamer-plugins-base (RHSA-2009:0352)

RHEL 5 : gstreamer-plugins-good (RHSA-2009:0271)

RHEL 5 : gstreamer-plugins-good (RHSA-2009:1123)

RHEL 5 : gtk2 (RHSA-2013:0135)

RHEL 5 : hplip (RHSA-2007:0960)

RHEL 5 : hplip (RHSA-2008:0818)

RHEL 5 : hplip3 (RHSA-2013:0133)

RHEL 5 : httpd (RHSA-2007:0556)

RHEL 5 : httpd (RHSA-2007:0746)

RHEL 5 : httpd (RHSA-2008:0008)

RHEL 5 : httpd (RHSA-2009:1075)

RHEL 5 : httpd (RHSA-2009:1148)

RHEL 5 : httpd (RHSA-2010:0168)

RHEL 5 : httpd (RHSA-2010:0659)

RHEL 5 : httpd (RHSA-2012:0323)

RHEL 5 : httpd (RHSA-2013:0130)

RHEL 5 : httpd (RHSA-2014:0369)

RHEL 5 : hypervkvpd (RHSA-2013:0807)

RHEL 5 : IBM Java Runtime (RHSA-2011:0880)

RHEL 5 : ibutils (RHSA-2012:0311)

RHEL 5 : icu (RHSA-2008:0090)

RHEL 5 : icu (RHSA-2009:0296)

RHEL 5 : icu (RHSA-2009:1122)

RHEL 5 : ImageMagick (RHSA-2010:0652)

RHEL 5 : ImageMagick (RHSA-2012:0301)

RHEL 5 : ImageMagick (RHSA-2012:0545)

RHEL 5 : initscripts (RHSA-2012:0312)

RHEL 5 : ipa-client (RHSA-2013:0189)

RHEL 5 : ipsec-tools (RHSA-2007:0342)

RHEL 5 : ipsec-tools (RHSA-2009:1036)

RHEL 5 : iscsi-initiator-utils (RHSA-2007:0497)

RHEL 5 : jabberd (RHSA-2011:0881)

RHEL 5 : jabberd (RHSA-2011:0882)

RHEL 5 : jakarta-commons-collections (RHSA-2015:2671)

RHEL 5 : java-1.4.2-ibm (RHSA-2012:0006) (BEAST)

RHEL 5 : java-1.4.2-ibm (RHSA-2012:0702)

RHEL 5 : java-1.4.2-ibm (RHSA-2012:1243)

RHEL 5 : java-1.4.2-ibm (RHSA-2012:1485) (ROBOT)

RHEL 5 : java-1.6.0-bea (RHSA-2008:0245)

RHEL 5 : java-1.6.0-ibm (RHSA-2008:0267)

RHEL 5 : java-1.6.0-openjdk (RHSA-2009:0377)

RHEL 5 : java-1.6.0-openjdk (RHSA-2009:1201)

RHEL 5 : java-1.6.0-openjdk (RHSA-2009:1584)

RHEL 5 : java-1.6.0-openjdk (RHSA-2010:0339)

RHEL 5 : java-1.6.0-openjdk (RHSA-2010:0768)

RHEL 5 : java-1.6.0-openjdk (RHSA-2011:0176)

RHEL 5 : java-1.6.0-openjdk (RHSA-2011:0857)

RHEL 5 : java-1.6.0-openjdk (RHSA-2012:0322)

RHEL 5 : java-1.6.0-openjdk (RHSA-2012:0730)

RHEL 5 : java-1.6.0-openjdk (RHSA-2012:1222)

RHEL 5 : java-1.6.0-openjdk (RHSA-2012:1385) (ROBOT)

RHEL 5 : java-1.6.0-openjdk (RHSA-2013:0246)

RHEL 5 : java-1.6.0-openjdk (RHSA-2013:0274)

RHEL 5 : java-1.6.0-openjdk (RHSA-2013:0604)

RHEL 5 : java-1.6.0-sun (RHSA-2008:0594)

RHEL 5 : java-1.7.0-ibm (RHSA-2014:1876) (POODLE)

RHEL 5 : java-1.7.0-ibm (RHSA-2015:0134)

RHEL 5 : java-1.7.0-ibm (RHSA-2015:1007) (Bar Mitzvah)

RHEL 5 : java-1.7.0-ibm (RHSA-2015:1488) (Logjam)

RHEL 5 : java-1.7.0-ibm (RHSA-2015:2507)

RHEL 5 : java-1.7.0-ibm (RHSA-2016:0100) (SLOTH)

RHEL 5 : java-1.7.0-ibm (RHSA-2016:0702)

RHEL 5 : java-1.7.0-ibm (RHSA-2016:1589)

RHEL 5 : java-1.7.0-ibm (RHSA-2016:2138)

RHEL 5 : java-1.7.0-ibm (RHSA-2017:0337)

RHEL 5 : java-1.7.0-openjdk (RHSA-2013:0603)

RHEL 5 : java-1.7.0-openjdk (RHSA-2013:0752)

RHEL 5 : java-1.7.0-openjdk (RHSA-2013:0958)

RHEL 5 : java-1.7.0-openjdk (RHSA-2013:1447)

RHEL 5 : java-1.7.0-openjdk (RHSA-2014:0027)

RHEL 5 : java-1.7.0-openjdk (RHSA-2014:0407)

RHEL 5 : java-1.7.0-openjdk (RHSA-2014:0890)

RHEL 5 : java-1.7.0-openjdk (RHSA-2014:1633)

RHEL 5 : java-1.7.0-openjdk (RHSA-2015:0068) (POODLE)

RHEL 5 : java-1.7.0-openjdk (RHSA-2015:0807)

RHEL 5 : java-1.7.0-openjdk (RHSA-2015:1230) (Bar Mitzvah) (Logjam)

RHEL 5 : java-1.7.0-openjdk (RHSA-2015:1921)

RHEL 5 : JBoss EAP (RHSA-2008:0213)

RHEL 5 : JBoss EAP (RHSA-2008:0827)

RHEL 5 : JBoss EAP (RHSA-2008:0828)

RHEL 5 : JBoss EAP (RHSA-2008:0832)

RHEL 5 : JBoss EAP (RHSA-2008:0834)

RHEL 5 : JBoss EAP (RHSA-2009:0348)

RHEL 5 : JBoss EAP (RHSA-2009:0349)

RHEL 5 : JBoss EAP (RHSA-2009:1143)

RHEL 5 : JBoss EAP (RHSA-2009:1145)

RHEL 5 : JBoss EAP (RHSA-2009:1649)

RHEL 5 : JBoss EAP (RHSA-2009:1650)

RHEL 5 : JBoss EAP (RHSA-2010:0378)

RHEL 5 : JBoss EAP (RHSA-2010:0379)

RHEL 5 : JBoss EAP (RHSA-2010:0938)

RHEL 5 : JBoss EAP (RHSA-2010:0960)

RHEL 5 : JBoss EAP (RHSA-2011:0948)

RHEL 5 : JBoss EAP (RHSA-2011:1799)

RHEL 5 : JBoss EAP (RHSA-2012:1591)

RHEL 5 : JBoss EAP (RHSA-2013:0192)

RHEL 5 : JBoss EAP (RHSA-2013:0249)

RHEL 5 : JBoss EAP (RHSA-2013:0839)

RHEL 5 : JBoss EAP (RHSA-2013:1207)

RHEL 5 : JBoss EAP (RHSA-2013:1784)

RHEL 5 : JBoss EAP (RHSA-2013:1785)

RHEL 5 : JBoss EAP (RHSA-2014:0170)

RHEL 5 : JBoss EAP (RHSA-2014:0343)

RHEL 5 : JBoss EAP (RHSA-2014:0564)

RHEL 5 : JBoss EAP (RHSA-2014:0798)

RHEL 5 : JBoss EAP (RHSA-2014:1019)

RHEL 5 : JBoss EAP (RHSA-2014:1286)

RHEL 5 : JBoss EAP (RHSA-2014:1821)

RHEL 5 : JBoss EAP (RHSA-2015:0216)

RHEL 5 : JBoss EAP (RHSA-2015:0846)

RHEL 5 : JBoss EAP (RHSA-2015:1669)

RHEL 5 : JBoss EAP (RHSA-2015:1904)

RHEL 5 : JBoss EAP (RHSA-2015:2538)

RHEL 5 : JBoss EAP (RHSA-2016:0121)

RHEL 5 : JBoss EAP (RHSA-2016:0595)

RHEL 5 : JBoss EAP (RHSA-2017:0246)

RHEL 5 : JBoss EAP (RHSA-2017:0826)

RHEL 5 : JBoss EAP (RHSA-2017:1256)

RHEL 5 : JBoss EAP (RHSA-2017:1550)

RHEL 5 : JBoss EAP (RHSA-2017:2637)

RHEL 5 : JBoss EWP (RHSA-2013:0196)

RHEL 5 : JBoss Web Server (RHSA-2013:1011)

RHEL 5 : JBoss Web Server (RHSA-2014:1088)

RHEL 5 : jboss-seam2 (RHSA-2013:1044)

RHEL 5 : jbossas (RHSA-2012:1025)

RHEL 5 : jbossas (RHSA-2013:0147)

RHEL 5 : kdegraphics (RHSA-2007:1051)

RHEL 5 : kdegraphics (RHSA-2009:1130)

RHEL 5 : kdegraphics (RHSA-2009:1502)

RHEL 5 : kernel (RHSA-2007:0099)

RHEL 5 : kernel (RHSA-2007:0169)

RHEL 5 : kernel (RHSA-2007:0347)

RHEL 5 : kernel (RHSA-2007:0376)

RHEL 5 : kernel (RHSA-2007:0595)

RHEL 5 : kernel (RHSA-2007:0705)

RHEL 5 : kernel (RHSA-2007:0936)

RHEL 5 : kernel (RHSA-2007:0940)

RHEL 5 : kernel (RHSA-2007:0993)

RHEL 5 : kernel (RHSA-2008:0089)

RHEL 5 : kernel (RHSA-2008:0129)

RHEL 5 : kernel (RHSA-2008:0154)

RHEL 5 : kernel (RHSA-2008:0233)

RHEL 5 : kernel (RHSA-2008:0275)

RHEL 5 : kernel (RHSA-2008:0519)

RHEL 5 : kernel (RHSA-2008:0612)

RHEL 5 : kernel (RHSA-2008:0885)

RHEL 5 : kernel (RHSA-2008:0957)

RHEL 5 : kernel (RHSA-2008:1017)

RHEL 5 : kernel (RHSA-2009:0021)

RHEL 5 : kernel (RHSA-2009:0225)

RHEL 5 : kernel (RHSA-2009:0264)

RHEL 5 : kernel (RHSA-2009:0326)

RHEL 5 : kernel (RHSA-2009:0473)

RHEL 5 : kernel (RHSA-2009:1055)

RHEL 5 : kernel (RHSA-2009:1106)

RHEL 5 : kernel (RHSA-2009:1193)

RHEL 5 : kernel (RHSA-2009:1222)

RHEL 5 : kernel (RHSA-2009:1243)

RHEL 5 : kernel (RHSA-2009:1455)

RHEL 5 : kernel (RHSA-2009:1457)

RHEL 5 : kernel (RHSA-2009:1466)

RHEL 5 : kernel (RHSA-2009:1548)

RHEL 5 : kernel (RHSA-2009:1587)

RHEL 5 : kernel (RHSA-2009:1670)

RHEL 5 : kernel (RHSA-2009:1672)

RHEL 5 : kernel (RHSA-2010:0019)

RHEL 5 : kernel (RHSA-2010:0046)

RHEL 5 : kernel (RHSA-2010:0053)

RHEL 5 : kernel (RHSA-2010:0079)

RHEL 5 : kernel (RHSA-2010:0147)

RHEL 5 : kernel (RHSA-2010:0148)

RHEL 5 : kernel (RHSA-2010:0149)

RHEL 5 : kernel (RHSA-2010:0178)

RHEL 5 : kernel (RHSA-2010:0380)

RHEL 5 : kernel (RHSA-2010:0398)

RHEL 5 : kernel (RHSA-2010:0439)

RHEL 5 : kernel (RHSA-2010:0504)

RHEL 5 : kernel (RHSA-2010:0610)

RHEL 5 : kernel (RHSA-2010:0660)

RHEL 5 : kernel (RHSA-2010:0661)

RHEL 5 : kernel (RHSA-2010:0670)

RHEL 5 : kernel (RHSA-2010:0704)

RHEL 5 : kernel (RHSA-2010:0705)

RHEL 5 : kernel (RHSA-2010:0711)

RHEL 5 : kernel (RHSA-2010:0723)

RHEL 5 : kernel (RHSA-2010:0792)

RHEL 5 : kernel (RHSA-2010:0839)

RHEL 5 : kernel (RHSA-2010:0893)

RHEL 5 : kernel (RHSA-2010:0907)

RHEL 5 : kernel (RHSA-2011:0004)

RHEL 5 : kernel (RHSA-2011:0017)

RHEL 5 : kernel (RHSA-2011:0163)

RHEL 5 : kernel (RHSA-2011:0303)

RHEL 5 : kernel (RHSA-2011:0429)

RHEL 5 : kernel (RHSA-2011:0833)

RHEL 5 : kernel (RHSA-2011:0927)

RHEL 5 : kernel (RHSA-2011:1065)

RHEL 5 : kernel (RHSA-2011:1163)

RHEL 5 : kernel (RHSA-2011:1212)

RHEL 5 : kernel (RHSA-2011:1321)

RHEL 5 : kernel (RHSA-2011:1386)

RHEL 5 : kernel (RHSA-2011:1418)

RHEL 5 : kernel (RHSA-2011:1419)

RHEL 5 : kernel (RHSA-2011:1479)

RHEL 5 : kernel (RHSA-2011:1813)

RHEL 5 : kernel (RHSA-2012:0007)

RHEL 5 : kernel (RHSA-2012:0107)

RHEL 5 : kernel (RHSA-2012:0150)

RHEL 5 : kernel (RHSA-2012:0358)

RHEL 5 : kernel (RHSA-2012:0480)

RHEL 5 : kernel (RHSA-2012:0517)

RHEL 5 : kernel (RHSA-2012:0690)

RHEL 5 : kernel (RHSA-2012:0720)

RHEL 5 : kernel (RHSA-2012:0721)

RHEL 5 : kernel (RHSA-2012:1061)

RHEL 5 : kernel (RHSA-2012:1087)

RHEL 5 : kernel (RHSA-2012:1174)

RHEL 5 : kernel (RHSA-2012:1323)

RHEL 5 : kernel (RHSA-2012:1347)

RHEL 5 : kernel (RHSA-2012:1445)

RHEL 5 : kernel (RHSA-2012:1481)

RHEL 5 : kernel (RHSA-2012:1540)

RHEL 5 : kernel (RHSA-2013:0168)

RHEL 5 : kernel (RHSA-2013:0594)

RHEL 5 : kernel (RHSA-2013:0621)

RHEL 5 : kernel (RHSA-2013:0695)

RHEL 5 : kernel (RHSA-2013:0747)

RHEL 5 : kernel (RHSA-2013:0847)

RHEL 5 : kernel (RHSA-2013:1034)

RHEL 5 : kernel (RHSA-2013:1166)

RHEL 5 : kernel (RHSA-2013:1292)

RHEL 5 : kernel (RHSA-2013:1348)

RHEL 5 : kernel (RHSA-2013:1449)

RHEL 5 : kernel (RHSA-2013:1790)

RHEL 5 : kernel (RHSA-2013:1860)

RHEL 5 : kernel (RHSA-2014:0108)

RHEL 5 : kernel (RHSA-2014:0285)

RHEL 5 : kernel (RHSA-2014:0433)

RHEL 5 : kernel (RHSA-2014:0476)

RHEL 5 : kernel (RHSA-2014:0740)

RHEL 5 : kernel (RHSA-2014:0772)

RHEL 5 : kernel (RHSA-2014:0801)

RHEL 5 : kernel (RHSA-2014:0926)

RHEL 5 : kernel (RHSA-2014:1143)

RHEL 5 : kernel (RHSA-2014:1959)

RHEL 5 : kernel (RHSA-2014:2008)

RHEL 5 : kernel (RHSA-2014:2029)

RHEL 5 : kernel (RHSA-2014:2031)

RHEL 5 : kernel (RHSA-2015:0164)

RHEL 5 : kernel (RHSA-2015:0783)

RHEL 5 : kernel (RHSA-2015:0870)

RHEL 5 : kernel (RHSA-2015:0919)

RHEL 5 : kernel (RHSA-2015:1042)

RHEL 5 : kernel (RHSA-2015:1120)

RHEL 5 : kernel (RHSA-2015:1190)

RHEL 5 : kernel (RHSA-2016:0045)

RHEL 5 : kernel (RHSA-2016:0450)

RHEL 5 : kernel (RHSA-2016:2124) (Dirty COW)

RHEL 5 : kernel (RHSA-2016:2126) (Dirty COW)

RHEL 5 : kernel (RHSA-2016:2127) (Dirty COW)

RHEL 5 : kernel (RHSA-2016:2962)

RHEL 5 : kernel (RHSA-2017:0323)

RHEL 5 : kernel (RHSA-2017:0346)

RHEL 5 : kernel (RHSA-2017:0347)

RHEL 5 : kernel (RHSA-2017:1482) (Stack Clash)

RHEL 5 : kernel (RHSA-2017:1483) (Stack Clash)

RHEL 5 : kernel (RHSA-2017:2412)

RHEL 5 : kernel (RHSA-2018:0292) (Meltdown) (Spectre)

RHEL 5 : kexec-tools (RHSA-2012:0152)

RHEL 5 : krb5 (RHSA-2007:0858)

RHEL 5 : krb5 (RHSA-2007:0892)

RHEL 5 : krb5 (RHSA-2008:0164)

RHEL 5 : krb5 (RHSA-2009:0408)

RHEL 5 : krb5 (RHSA-2010:0343)

RHEL 5 : krb5 (RHSA-2011:0199)

RHEL 5 : krb5 (RHSA-2011:1853)

RHEL 5 : krb5 (RHSA-2012:0306)

RHEL 5 : krb5 (RHSA-2014:1245)

RHEL 5 : krb5 (RHSA-2014:1255)

RHEL 5 : kvm (RHSA-2009:1465)

RHEL 5 : kvm (RHSA-2009:1659)

RHEL 5 : kvm (RHSA-2010:0088)

RHEL 5 : kvm (RHSA-2010:0126)

RHEL 5 : kvm (RHSA-2010:0271)

RHEL 5 : kvm (RHSA-2010:0627)

RHEL 5 : kvm (RHSA-2010:0898)

RHEL 5 : kvm (RHSA-2010:0998)

RHEL 5 : kvm (RHSA-2011:0028)

RHEL 5 : kvm (RHSA-2012:0051)

RHEL 5 : kvm (RHSA-2012:0149)

RHEL 5 : kvm (RHSA-2012:0676)

RHEL 5 : kvm (RHSA-2012:1235)

RHEL 5 : kvm (RHSA-2013:0608)

RHEL 5 : kvm (RHSA-2013:0727)

RHEL 5 : kvm (RHSA-2014:0163)

RHEL 5 : kvm (RHSA-2015:0869)

RHEL 5 : kvm (RHSA-2015:1003) (Venom)

RHEL 5 : kvm (RHSA-2015:1189)

RHEL 5 : kvm (RHSA-2015:1925)

RHEL 5 : kvm (RHSA-2016:1943)

RHEL 5 : kvm (RHSA-2017:0454)

RHEL 5 : lcms (RHSA-2009:0011)

RHEL 5 : lcms (RHSA-2009:0339)

RHEL 5 : lftp (RHSA-2009:1278)

RHEL 5 : lftp (RHSA-2010:0585)

RHEL 5 : libexif (RHSA-2007:1165)

RHEL 5 : libjpeg (RHSA-2013:1804)

RHEL 5 : libpng (RHSA-2011:1104)

RHEL 5 : libtiff (RHSA-2008:0847)

RHEL 5 : libtiff (RHSA-2014:0223)

RHEL 5 : libvirt (RHSA-2009:0382)

RHEL 5 : libvirt (RHSA-2010:0615)

RHEL 5 : libvirt (RHSA-2011:0478)

RHEL 5 : libvirt (RHSA-2011:1019)

RHEL 5 : libvirt (RHSA-2013:0127)

RHEL 5 : libwpd (RHSA-2007:0055)

RHEL 5 : libwpd (RHSA-2012:1043)

RHEL 5 : libXfont (RHSA-2007:0132)

RHEL 5 : libXfont (RHSA-2008:0064)

RHEL 5 : libXfont (RHSA-2011:1834)

RHEL 5 : libXfont (RHSA-2014:1893)

RHEL 5 : libxml2 (RHSA-2012:0017)

RHEL 5 : libxml2 (RHSA-2012:0104)

RHEL 5 : libxml2 (RHSA-2014:1885)

RHEL 5 : lvm2-cluster (RHSA-2010:0567)

RHEL 5 : mcstrans (RHSA-2007:0542)

RHEL 5 : mesa (RHSA-2013:0898)

RHEL 5 : mod\_auth\_mysql (RHSA-2009:0259)

RHEL 5 : MRG (RHSA-2011:1249)

RHEL 5 : MRG (RHSA-2012:0100)

RHEL 5 : MRG (RHSA-2012:0476)

RHEL 5 : MRG (RHSA-2012:0529)

RHEL 5 : MRG (RHSA-2012:1278)

RHEL 5 : MRG (RHSA-2013:0561)

RHEL 5 : MRG (RHSA-2013:0564)

RHEL 5 : MRG (RHSA-2013:1171)

RHEL 5 : MRG (RHSA-2013:1295)

RHEL 5 : MRG (RHSA-2013:1851)

RHEL 5 : MRG (RHSA-2014:0261)

RHEL 5 : MRG (RHSA-2014:0350)

RHEL 5 : MRG (RHSA-2014:0441)

RHEL 5 : MRG (RHSA-2014:0859)

RHEL 5 : MRG (RHSA-2015:0662)

RHEL 5 : MRG Messaging (RHSA-2012:1277)

RHEL 5 : mysql (RHSA-2008:0364)

RHEL 5 : mysql (RHSA-2009:1289)

RHEL 5 : mysql (RHSA-2010:0109)

RHEL 5 : mysql (RHSA-2010:0442)

RHEL 5 : mysql (RHSA-2010:0825)

RHEL 5 : mysql (RHSA-2012:0127)

RHEL 5 : mysql (RHSA-2013:0121)

RHEL 5 : mysql (RHSA-2013:0180)

RHEL 5 : mysql55-mysql (RHSA-2014:0186)

RHEL 5 : mysql55-mysql (RHSA-2014:0536)

RHEL 5 : mysql55-mysql (RHSA-2014:1859)

RHEL 5 : mysql55-mysql (RHSA-2015:1628)

RHEL 5 : net-snmp (RHSA-2013:0124)

RHEL 5 : net-snmp (RHSA-2014:0322)

RHEL 5 : NetworkManager (RHSA-2009:0361)

RHEL 5 : NetworkManager (RHSA-2010:0108)

RHEL 5 : nfs-utils (RHSA-2008:0486)

RHEL 5 : nfs-utils (RHSA-2009:1321)

RHEL 5 : nfs-utils (RHSA-2012:0310)

RHEL 5 : nfs-utils-lib (RHSA-2007:0951)

RHEL 5 : nspr and nss (RHSA-2009:1186)

RHEL 5 : nspr and nss (RHSA-2009:1207)

RHEL 5 : nss (RHSA-2012:0532)

RHEL 5 : nss (RHSA-2013:1841)

RHEL 5 : nss (RHSA-2015:1664)

RHEL 5 : nss (RHSA-2016:0371)

RHEL 5 : nss (RHSA-2017:1101)

RHEL 5 : nss (RHSA-2017:1103)

RHEL 5 : nss and nspr (RHSA-2012:1090)

RHEL 5 : nss and nspr (RHSA-2013:0214)

RHEL 5 : nss and nspr (RHSA-2013:1135)

RHEL 5 : nss and nspr (RHSA-2013:1791)

RHEL 5 : nss and nspr (RHSA-2014:1246)

RHEL 5 : nss and nspr (RHSA-2015:1980)

RHEL 5 : nss and nspr (RHSA-2016:0684)

RHEL 5 : nss\_db (RHSA-2010:0347)

RHEL 5 : nss\_ldap (RHSA-2008:0389)

RHEL 5 : ntp (RHSA-2009:1039)

RHEL 5 : ntp (RHSA-2014:2025)

RHEL 5 : opal (RHSA-2007:0957)

RHEL 5 : OpenIPMI (RHSA-2013:0123)

RHEL 5 : openldap (RHSA-2007:1037)

RHEL 5 : openldap (RHSA-2010:0198)

RHEL 5 : openldap (RHSA-2010:0542)

RHEL 5 : openldap (RHSA-2011:0346)

RHEL 5 : openldap (RHSA-2014:0206)

RHEL 5 : openoffice.org (RHSA-2007:0069)

RHEL 5 : openoffice.org (RHSA-2008:0835)

RHEL 5 : openoffice.org (RHSA-2011:0182)

RHEL 5 : openoffice.org (RHSA-2012:0411)

RHEL 5 : openoffice.org (RHSA-2012:1136)

RHEL 5 : openoffice.org, hsqldb (RHSA-2007:1048)

RHEL 5 : openssh (RHSA-2007:0540)

RHEL 5 : openssh (RHSA-2009:1287)

RHEL 5 : openssh (RHSA-2009:1470)

RHEL 5 : openssl (RHSA-2007:0964)

RHEL 5 : openssl (RHSA-2009:1335)

RHEL 5 : openssl (RHSA-2010:0054)

RHEL 5 : openssl (RHSA-2010:0162)

RHEL 5 : openssl (RHSA-2010:0978)

RHEL 5 : openssl (RHSA-2012:0060)

RHEL 5 : openssl (RHSA-2014:0624)

RHEL 5 : openssl (RHSA-2014:1053)

RHEL 5 : openssl (RHSA-2014:1653) (POODLE)

RHEL 5 : openssl (RHSA-2015:0800) (FREAK)

RHEL 5 : openssl (RHSA-2015:1197) (Logjam)

RHEL 5 : openssl (RHSA-2015:2616)

RHEL 5 : openssl (RHSA-2016:0302) (DROWN)

RHEL 5 : openssl (RHSA-2016:0304) (DROWN)

RHEL 5 : openssl (RHSA-2016:1137)

RHEL 5 : openssl097a (RHSA-2010:0164)

RHEL 5 : openswan (RHSA-2009:0402)

RHEL 5 : openswan (RHSA-2009:1138)

RHEL 5 : pam (RHSA-2007:0555)

RHEL 5 : pam (RHSA-2010:0819)

RHEL 5 : pam\_krb5 (RHSA-2008:0907)

RHEL 5 : pam\_krb5 (RHSA-2010:0258)

RHEL 5 : pango (RHSA-2011:1326)

RHEL 5 : pcre (RHSA-2007:0967)

RHEL 5 : pcre (RHSA-2007:1059)

RHEL 5 : pcsc-lite (RHSA-2010:0533)

RHEL 5 : perl (RHSA-2010:0458)

RHEL 5 : perl-DBD-Pg (RHSA-2009:0479)

RHEL 5 : php (RHSA-2007:0082)

RHEL 5 : php (RHSA-2007:0153)

RHEL 5 : php (RHSA-2007:0348)

RHEL 5 : php (RHSA-2009:0338)

RHEL 5 : php (RHSA-2012:0033)

RHEL 5 : php (RHSA-2012:1045)

RHEL 5 : php (RHSA-2013:1814)

RHEL 5 : php (RHSA-2014:0311)

RHEL 5 : php (RHSA-2014:0312)

RHEL 5 : php (RHSA-2014:1824)

RHEL 5 : php53 (RHSA-2011:0196)

RHEL 5 : php53 (RHSA-2012:0092)

RHEL 5 : php53 (RHSA-2012:0547)

RHEL 5 : php53 (RHSA-2012:0569)

RHEL 5 : php53 (RHSA-2012:1047)

RHEL 5 : php53 (RHSA-2013:1050)

RHEL 5 : php53 (RHSA-2013:1062)

RHEL 5 : php53 (RHSA-2013:1307)

RHEL 5 : php53 (RHSA-2013:1825)

RHEL 5 : php53 (RHSA-2014:1768)

RHEL 5 : piranha (RHSA-2014:0174)

RHEL 5 : pki (RHSA-2012:1103)

RHEL 5 : pki (RHSA-2012:1550)

RHEL 5 : pki-tps (RHSA-2013:0856)

RHEL 5 : poppler (RHSA-2007:0732)

RHEL 5 : poppler (RHSA-2007:1026)

RHEL 5 : poppler (RHSA-2008:0239)

RHEL 5 : poppler (RHSA-2009:0480)

RHEL 5 : poppler (RHSA-2009:1504)

RHEL 5 : poppler (RHSA-2010:0749)

RHEL 5 : postgresql (RHSA-2007:0068)

RHEL 5 : postgresql (RHSA-2010:0429)

RHEL 5 : postgresql (RHSA-2012:0677)

RHEL 5 : postgresql (RHSA-2012:1036)

RHEL 5 : postgresql (RHSA-2012:1264)

RHEL 5 : postgresql (RHSA-2014:0249)

RHEL 5 : postgresql84 (RHSA-2010:0430)

RHEL 5 : postgresql84 (RHSA-2011:0198)

RHEL 5 : postgresql84 (RHSA-2011:1378)

RHEL 5 : pwlib (RHSA-2007:0932)

RHEL 5 : python (RHSA-2009:1176)

RHEL 5 : python (RHSA-2011:0027)

RHEL 5 : python (RHSA-2011:0492)

RHEL 5 : python (RHSA-2012:0745)

RHEL 5 : qspice (RHSA-2010:0633)

RHEL 5 : qspice (RHSA-2013:1474)

RHEL 5 : qspice-client (RHSA-2010:0632)

RHEL 5 : qt4 (RHSA-2011:1324)

RHEL 5 : quagga (RHSA-2012:1258)

RHEL 5 : quota (RHSA-2013:0120)

RHEL 5 : rdesktop (RHSA-2008:0575)

RHEL 5 : Red Hat Directory Server (RHSA-2013:0549)

RHEL 5 : redhat-ds-base (RHSA-2012:1041)

RHEL 5 : redhat-ds-base (RHSA-2013:1116)

RHEL 5 : redhat-ds-base (RHSA-2013:1753)

RHEL 5 : redhat-ds-base (RHSA-2014:1032)

RHEL 5 : redhat-release (EOL Notice) (RHSA-2011:0143)

RHEL 5 : redhat-release (EOL Notice) (RHSA-2011:0144)

RHEL 5 : redhat-release (EOL Notice) (RHSA-2011:1111)

RHEL 5 : redhat-release (EOL Notice) (RHSA-2013:0578)

RHEL 5 : rgmanager (RHSA-2009:1339)

RHEL 5 : rgmanager (RHSA-2011:1000)

RHEL 5 : rh-postgresql95-postgresql (RHSA-2017:1838)

RHEL 5 : rhev-hypervisor (RHSA-2010:0476)

RHEL 5 : rhev-hypervisor (RHSA-2010:0622)

RHEL 5 : rhev-hypervisor (RHSA-2011:0439)

RHEL 5 : rhev-hypervisor (RHSA-2011:1090)

RHEL 5 : rhev-hypervisor (RHSA-2011:1408)

RHEL 5 : rhev-hypervisor5 (RHSA-2012:0168)

RHEL 5 : rhev-hypervisor5 (RHSA-2012:0488)

RHEL 5 : rhev-hypervisor5 (RHSA-2012:1185)

RHEL 5 : rhev-hypervisor5 (RHSA-2012:1262)

RHEL 5 : rhev-hypervisor5 (RHSA-2012:1324)

RHEL 5 : rhn-client-tools (RHSA-2010:0449)

RHEL 5 : rhn-java-sat in Satellite Server (RHSA-2013:1513)

RHEL 5 : rpm (RHSA-2010:0679)

RHEL 5 : rsync (RHSA-2011:0999)

RHEL 5 : ruby (RHSA-2007:0965)

RHEL 5 : ruby (RHSA-2011:0909)

RHEL 5 : ruby (RHSA-2013:0129)

RHEL 5 : ruby (RHSA-2013:0611)

RHEL 5 : samba (RHSA-2007:0061)

RHEL 5 : samba (RHSA-2007:1017)

RHEL 5 : samba (RHSA-2008:0290)

RHEL 5 : samba (RHSA-2012:0313)

RHEL 5 : samba (RHSA-2014:0305)

RHEL 5 : samba (RHSA-2016:0621) (Badlock)

RHEL 5 : samba (RHSA-2016:0623) (Badlock)

RHEL 5 : samba3x (RHSA-2009:1585)

RHEL 5 : samba3x (RHSA-2010:0698)

RHEL 5 : samba3x (RHSA-2011:0306)

RHEL 5 : samba3x (RHSA-2011:1220)

RHEL 5 : samba3x (RHSA-2012:0466)

RHEL 5 : samba3x (RHSA-2013:1310)

RHEL 5 : samba3x (RHSA-2015:0249)

RHEL 5 : samba3x (RHSA-2015:0253)

RHEL 5 : samba3x (RHSA-2016:0613) (Badlock)

RHEL 5 : samba3x (RHSA-2016:0624) (Badlock)

RHEL 5 : samba3x (RHSA-2017:1272) (SambaCry)

RHEL 5 : Satellite Server (RHSA-2011:0300)

RHEL 5 : scsi-target-utils (RHSA-2010:0362)

RHEL 5 : scsi-target-utils (RHSA-2010:0518)

RHEL 5 : sendmail (RHSA-2010:0237)

RHEL 5 : setroubleshoot (RHSA-2008:0061)

RHEL 5 : sos (RHSA-2012:0153)

RHEL 5 : sos (RHSA-2013:1121)

RHEL 5 : spacewalk in Satellite Server (RHSA-2014:0149)

RHEL 5 : spacewalk-java (RHSA-2011:0879)

RHEL 5 : spamassassin (RHSA-2007:0075)

RHEL 5 : spice-xpi (RHSA-2010:0651)

RHEL 5 : spice-xpi (RHSA-2011:0427)

RHEL 5 : squid (RHSA-2007:0131)

RHEL 5 : squid (RHSA-2010:0221)

RHEL 5 : squirrelmail (RHSA-2013:0126)

RHEL 5 : sssd (RHSA-2011:0975)

RHEL 5 : sssd (RHSA-2013:1319)

RHEL 5 : struts (RHSA-2014:0474)

RHEL 5 : subversion (RHSA-2011:0257)

RHEL 5 : subversion (RHSA-2011:0327)

RHEL 5 : sudo (RHSA-2009:0267)

RHEL 5 : sudo (RHSA-2010:0122)

RHEL 5 : sudo (RHSA-2010:0361)

RHEL 5 : sudo (RHSA-2010:0475)

RHEL 5 : sudo (RHSA-2010:0675)

RHEL 5 : sudo (RHSA-2012:0309)

RHEL 5 : sudo (RHSA-2012:1149)

RHEL 5 : sudo (RHSA-2013:1353)

RHEL 5 : sudo (RHSA-2014:0266)

RHEL 5 : sudo (RHSA-2017:1381)

RHEL 5 : sysstat (RHSA-2011:1005)

RHEL 5 : systemtap (RHSA-2010:0124)

RHEL 5 : systemtap (RHSA-2011:0841)

RHEL 5 : systemtap (RHSA-2011:1089)

RHEL 5 : tcl (RHSA-2013:0122)

RHEL 5 : tcpdump (RHSA-2007:0368)

RHEL 5 : tetex (RHSA-2010:0400)

RHEL 5 : tetex (RHSA-2012:1201)

RHEL 5 : thunderbird (RHSA-2007:0108)

RHEL 5 : thunderbird (RHSA-2009:1126)

RHEL 5 : thunderbird (RHSA-2010:0153)

RHEL 5 : thunderbird (RHSA-2010:0545)

RHEL 5 : tk (RHSA-2008:0136)

RHEL 5 : tog-pegasus (RHSA-2008:1001)

RHEL 5 : tomcat (RHSA-2007:0327)

RHEL 5 : tomcat (RHSA-2007:0569)

RHEL 5 : tomcat (RHSA-2007:0871)

RHEL 5 : tomcat (RHSA-2008:0042)

RHEL 5 : tomcat (RHSA-2008:0648)

RHEL 5 : tomcat (RHSA-2009:1164)

RHEL 5 : tomcat5 (RHSA-2010:0580)

RHEL 5 : tomcat5 (RHSA-2011:0336)

RHEL 5 : tomcat5 (RHSA-2011:1845)

RHEL 5 : tomcat5 (RHSA-2012:0474)

RHEL 5 : tomcat5 (RHSA-2013:0640)

RHEL 5 : tomcat5 (RHSA-2013:0870)

RHEL 5 : udev (RHSA-2009:0427)

RHEL 5 : util-linux (RHSA-2012:0307)

RHEL 5 : vdsm (RHSA-2010:0473)

RHEL 5 : vdsm22 (RHSA-2010:0628)

RHEL 5 : vim (RHSA-2007:0346)

RHEL 5 : vim (RHSA-2008:0580)

RHEL 5 : vixie-cron (RHSA-2012:0304)

RHEL 5 : vsftpd (RHSA-2008:0295)

RHEL 5 : w3m (RHSA-2010:0565)

RHEL 5 : wireshark (RHSA-2007:0710)

RHEL 5 : wireshark (RHSA-2013:0125)

RHEL 5 : wireshark (RHSA-2014:0341)

RHEL 5 : wireshark (RHSA-2014:1677)

RHEL 5 : xen (RHSA-2007:0114)

RHEL 5 : xen (RHSA-2007:0323)

RHEL 5 : xen (RHSA-2008:0194)

RHEL 5 : xen (RHSA-2008:0892)

RHEL 5 : xen (RHSA-2009:0003)

RHEL 5 : xen (RHSA-2009:1472)

RHEL 5 : xen (RHSA-2011:0496)

RHEL 5 : xen (RHSA-2011:1401)

RHEL 5 : xen (RHSA-2012:0370)

RHEL 5 : xen (RHSA-2012:1130)

RHEL 5 : xen (RHSA-2012:1236)

RHEL 5 : xen (RHSA-2013:0241)

RHEL 5 : xen (RHSA-2013:0599)

RHEL 5 : xen (RHSA-2015:1002) (Venom)

RHEL 5 : xen (RHSA-2015:2065)

RHEL 5 : xen (RHSA-2016:2963)

RHEL 5 : xerces-j2 (RHSA-2009:1615)

RHEL 5 : xinetd (RHSA-2013:1302)

RHEL 5 : xorg-x11-apps and libX11 (RHSA-2007:0157)

RHEL 5 : xorg-x11-server (RHSA-2007:0127)

RHEL 5 : xorg-x11-server (RHSA-2008:0031)

RHEL 5 : xorg-x11-server (RHSA-2008:0504)

RHEL 5 : xorg-x11-server (RHSA-2010:0382)

RHEL 5 : xorg-x11-server (RHSA-2012:0303)

RHEL 5 : xorg-x11-server (RHSA-2014:1982)

RHEL 5 : xorg-x11-xfs (RHSA-2007:0520)

RHEL 5 : xulrunner (RHSA-2010:0809)

RHEL 5 : yum-rhn-plugin (RHSA-2008:0815)

RHEL 5 : yum-updatesd (RHSA-2014:1004)

RHEL 6 / 7 / 8 : JBoss EAP (RHSA-2019:2973)

RHEL 6 / 7 / 8 : JBoss EAP (RHSA-2019:3082)

RHEL 6 / 7 / 8 : JBoss EAP (RHSA-2020:0605)

RHEL 6 / 7 / 8 : JBoss EAP (RHSA-2020:0813)

RHEL 6 / 7 / 8 : JBoss Web Server (RHSA-2019:3929)

RHEL 6 / 7 / 8 : Red Hat JBoss Enterprise Application Platform 7.3 (RHSA-2020:0962)

RHEL 6 / 7 / 8 : Red Hat Satellite Tools (RHSA-2019:1223)

RHEL 6 / 7 / 8 : RH-SSO 7.3.4 adapters for Enterprise Application Platform 7.2 (RHSA-2019:3049)

RHEL 6 / 7 / 8 : Satellite Server (RHSA-2019:2780)

RHEL 6 / 7 : 389-ds-base (RHSA-2014:1031)

RHEL 6 / 7 : apr (RHSA-2017:3270)

RHEL 6 / 7 : apr (RHSA-2018:1253)

RHEL 6 / 7 : bind (RHSA-2015:1513)

RHEL 6 / 7 : bind (RHSA-2015:1705)

RHEL 6 / 7 : bind (RHSA-2015:2655)

RHEL 6 / 7 : bluez (RHSA-2017:2685) (BlueBorne)

RHEL 6 / 7 : ceph-deploy (RHSA-2015:1092)

RHEL 6 / 7 : cups (RHSA-2015:1123)

RHEL 6 / 7 : dovecot (RHSA-2014:0790)

RHEL 6 / 7 : eap7-jboss-ec2-eap (RHSA-2016:1840)

RHEL 6 / 7 : eap7-jboss-ec2-eap (RHSA-2017:0173)

RHEL 6 / 7 : eap7-jboss-ec2-eap (RHSA-2017:1412)

RHEL 6 / 7 : eap7-jboss-ec2-eap (RHSA-2017:1837)

RHEL 6 / 7 : eap7-jboss-ec2-eap (RHSA-2017:2811)

RHEL 6 / 7 : eap7-jboss-ec2-eap (RHSA-2017:3458)

RHEL 6 / 7 : eap7-jboss-ec2-eap (RHSA-2018:0005)

RHEL 6 / 7 : expat (RHSA-2016:2824)

RHEL 6 / 7 : firefox (RHSA-2017:1440)

RHEL 6 / 7 : firefox (RHSA-2017:2456)

RHEL 6 / 7 : firefox (RHSA-2017:2831)

RHEL 6 / 7 : firefox (RHSA-2017:3247)

RHEL 6 / 7 : firefox (RHSA-2017:3382)

RHEL 6 / 7 : firefox (RHSA-2018:0122)

RHEL 6 / 7 : firefox (RHSA-2018:0549)

RHEL 6 / 7 : flac (RHSA-2015:0767)

RHEL 6 / 7 : gdk-pixbuf2 (RHSA-2015:1694)

RHEL 6 / 7 : ghostscript (RHSA-2017:1230)

RHEL 6 / 7 : git (RHSA-2016:0496)

RHEL 6 / 7 : glibc (RHSA-2015:0092) (GHOST)

RHEL 6 / 7 : glibc (RHSA-2016:0225)

RHEL 6 / 7 : glibc (RHSA-2017:1479) (Stack Clash)

RHEL 6 / 7 : gnutls (RHSA-2016:0012) (SLOTH)

RHEL 6 / 7 : haproxy 1.5 (RHSA-2015:1741)

RHEL 6 / 7 : httpd24-httpd and httpd24-mod\_auth\_mellon (RHSA-2019:0746)

RHEL 6 / 7 : ImageMagick (RHSA-2016:0726) (ImageTragick)

RHEL 6 / 7 : ImageMagick (RHSA-2016:1237)

RHEL 6 / 7 : ipa (RHSA-2016:1797)

RHEL 6 / 7 : ISC DHCP Concurrent TCP Sessions DoS

RHEL 6 / 7 : jakarta-taglibs-standard (RHSA-2015:1695)

RHEL 6 / 7 : jasper (RHSA-2014:2021)

RHEL 6 / 7 : jasper (RHSA-2015:0074)

RHEL 6 / 7 : jasper (RHSA-2017:1208)

RHEL 6 / 7 : java-1.6.0-sun (RHSA-2017:1119)

RHEL 6 / 7 : java-1.6.0-sun (RHSA-2017:1792)

RHEL 6 / 7 : java-1.6.0-sun (RHSA-2017:3047)

RHEL 6 / 7 : java-1.6.0-sun (RHSA-2018:0115)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2014:0889)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2014:1620)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2015:0067) (POODLE)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2015:0806)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2015:1229) (Bar Mitzvah) (Logjam)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2015:1920)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2017:1204)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2017:2424)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2017:3392)

RHEL 6 / 7 : java-1.7.0-openjdk (RHSA-2018:0349)

RHEL 6 / 7 : java-1.7.0-oracle (RHSA-2017:1118)

RHEL 6 / 7 : java-1.7.0-oracle (RHSA-2017:1791)

RHEL 6 / 7 : java-1.7.0-oracle (RHSA-2017:3046)

RHEL 6 / 7 : java-1.7.0-oracle (RHSA-2018:0100)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2014:1880) (POODLE)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2015:0133)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2015:1020) (Bar Mitzvah)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2015:1485) (Logjam)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2015:2506)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2016:0099) (SLOTH)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2016:0701)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2016:1588)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2016:2137)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2017:0336)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2017:1221)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2017:2481)

RHEL 6 / 7 : java-1.7.1-ibm (RHSA-2017:3268)

RHEL 6 / 7 : java-1.8.0-ibm (RHSA-2016:1587)

RHEL 6 / 7 : java-1.8.0-ibm (RHSA-2016:2136)

RHEL 6 / 7 : java-1.8.0-ibm (RHSA-2017:0263)

RHEL 6 / 7 : java-1.8.0-ibm (RHSA-2017:0462)

RHEL 6 / 7 : java-1.8.0-ibm (RHSA-2017:1220)

RHEL 6 / 7 : java-1.8.0-ibm (RHSA-2017:2469)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2015:0809)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2015:1228) (Bar Mitzvah) (Logjam)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2015:1919)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2016:1458)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2016:2079)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2017:0180)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2017:1789)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2017:2998)

RHEL 6 / 7 : java-1.8.0-openjdk (RHSA-2018:0095)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2015:0854)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2015:1241) (Bar Mitzvah) (Logjam)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2015:1926)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2016:0055) (SLOTH)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2016:0516)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2016:0677)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2016:1475)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2016:2088)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2017:0175)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2017:1117)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2017:1790)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2017:2999)

RHEL 6 / 7 : java-1.8.0-oracle (RHSA-2018:0099)

RHEL 6 / 7 : JBoss Core Services (RHSA-2016:1851) (httpoxy)

RHEL 6 / 7 : JBoss Core Services (RHSA-2020:0250)

RHEL 6 / 7 : JBoss EAP (RHSA-2016:1332)

RHEL 6 / 7 : JBoss EAP (RHSA-2016:2642)

RHEL 6 / 7 : JBoss EAP (RHSA-2017:0834)

RHEL 6 / 7 : JBoss EAP (RHSA-2017:1658)

RHEL 6 / 7 : JBoss EAP (RHSA-2017:3123)

RHEL 6 / 7 : JBoss EAP (RHSA-2017:3240) (Optionsbleed)

RHEL 6 / 7 : JBoss EAP (RHSA-2018:0481)

RHEL 6 / 7 : JBoss EAP (RHSA-2018:0627)

RHEL 6 / 7 : JBoss EAP (RHSA-2018:0628)

RHEL 6 / 7 : JBoss EAP (RHSA-2018:1249)

RHEL 6 / 7 : JBoss EAP (RHSA-2018:2276)

RHEL 6 / 7 : JBoss Web Server (RHSA-2016:2807)

RHEL 6 / 7 : JBoss Web Server (RHSA-2017:2493)

RHEL 6 / 7 : libgcrypt (RHSA-2016:2674)

RHEL 6 / 7 : libldb (RHSA-2016:0009)

RHEL 6 / 7 : libreoffice (RHSA-2015:2619)

RHEL 6 / 7 : libssh2 (RHSA-2016:0428)

RHEL 6 / 7 : libtiff (RHSA-2017:0225)

RHEL 6 / 7 : libvncserver (RHSA-2014:1826)

RHEL 6 / 7 : libwmf (RHSA-2015:1917)

RHEL 6 / 7 : libXfont (RHSA-2014:1870)

RHEL 6 / 7 : libXfont (RHSA-2015:1708)

RHEL 6 / 7 : libxml2 (RHSA-2014:1655)

RHEL 6 / 7 : libxml2 (RHSA-2016:1292)

RHEL 6 / 7 : libyaml (RHSA-2015:0100)

RHEL 6 / 7 : lzo (RHSA-2014:0861)

RHEL 6 / 7 : mailx (RHSA-2014:1999)

RHEL 6 / 7 : mercurial (RHSA-2017:1576)

RHEL 6 / 7 : microcode\_ctl (RHSA-2018:0093) (Spectre)

RHEL 6 / 7 : mutt (RHSA-2018:2526)

RHEL 6 / 7 : net-snmp (RHSA-2015:1636)

RHEL 6 / 7 : nss (RHSA-2015:1185) (Logjam)

RHEL 6 / 7 : nss (RHSA-2016:0007) (SLOTH)

RHEL 6 / 7 : nss (RHSA-2017:2832)

RHEL 6 / 7 : nss and nss-util (RHSA-2017:1100)

RHEL 6 / 7 : nss, nss-util, and nspr (RHSA-2015:1981)

RHEL 6 / 7 : nss-softokn (RHSA-2015:1699)

RHEL 6 / 7 : nss-util (RHSA-2016:0370)

RHEL 6 / 7 : nss-util (RHSA-2016:0495)

RHEL 6 / 7 : nss-util (RHSA-2017:1102)

RHEL 6 / 7 : ntp (RHSA-2014:2024)

RHEL 6 / 7 : ntp (RHSA-2015:1930)

RHEL 6 / 7 : ntp (RHSA-2016:0063)

RHEL 6 / 7 : ntp (RHSA-2016:1141)

RHEL 6 / 7 : ntp (RHSA-2017:0252)

RHEL 6 / 7 : openssl (RHSA-2014:1052)

RHEL 6 / 7 : openssl (RHSA-2014:1652) (POODLE)

RHEL 6 / 7 : openssl (RHSA-2015:0066) (FREAK)

RHEL 6 / 7 : openssl (RHSA-2015:1072) (Logjam)

RHEL 6 / 7 : openssl (RHSA-2015:1115)

RHEL 6 / 7 : openssl (RHSA-2015:2617)

RHEL 6 / 7 : openssl (RHSA-2016:0008) (SLOTH)

RHEL 6 / 7 : openssl (RHSA-2016:0301) (DROWN)

RHEL 6 / 7 : openssl (RHSA-2016:0305) (DROWN)

RHEL 6 / 7 : openssl (RHSA-2016:1940)

RHEL 6 / 7 : openssl (RHSA-2017:0286)

RHEL 6 / 7 : openssl098e (RHSA-2016:0372) (DROWN)

RHEL 6 / 7 : pam (RHSA-2015:1640)

RHEL 6 / 7 : pcs (RHSA-2015:1700)

RHEL 6 / 7 : php (RHSA-2014:1767)

RHEL 6 / 7 : policycoreutils (RHSA-2016:2702)

RHEL 6 / 7 : postgresql (RHSA-2015:0750)

RHEL 6 / 7 : postgresql (RHSA-2015:1194)

RHEL 6 / 7 : python (RHSA-2016:1626) (httpoxy)

RHEL 6 / 7 : python-twisted-web (RHSA-2016:1978)

RHEL 6 / 7 : Red Hat JBoss Core Services Apache HTTP Server 2.4.29 (RHSA-2019:0367)

RHEL 6 / 7 : Red Hat JBoss Core Services Apache HTTP Server 2.4.29 SP2 (RHSA-2019:1297)

RHEL 6 / 7 : Red Hat JBoss Core Services Apache HTTP Server 2.4.29 SP3 (RHSA-2019:2946) (0-Length Headers Leak) (Internal Data Buffering)

RHEL 6 / 7 : Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP2 (RHSA-2020:1337)

RHEL 6 / 7 : Red Hat JBoss Web Server (RHSA-2017:3113) (Optionsbleed)

RHEL 6 / 7 : Red Hat JBoss Web Server 3.1 Service Pack 6 (RHSA-2019:0131)

RHEL 6 / 7 : Red Hat JBoss Web Server 3.1 Service Pack 7 (RHSA-2019:1711)

RHEL 6 / 7 : Red Hat JBoss Web Server 3.1 Service Pack 8 (RHSA-2020:0861)

RHEL 6 / 7 : Red Hat JBoss Web Server 3.1.0 Service Pack 1 (RHSA-2017:1801)

RHEL 6 / 7 : Red Hat JBoss Web Server 3.1.0 Service Pack 2 (RHSA-2018:0466)

RHEL 6 / 7 : Red Hat JBoss Web Server 3.1.0 Service Pack 4 (RHSA-2018:2469)

RHEL 6 / 7 : Red Hat JBoss Web Server 3.1.0 Service Pack 5 (RHSA-2018:2701)

RHEL 6 / 7 : Red Hat JBoss Web Server 5.0 Service Pack 1 (RHSA-2018:2868)

RHEL 6 / 7 : Red Hat JBoss Web Server 5.0 Service Pack 2 (RHSA-2019:0451)

RHEL 6 / 7 : Red Hat Satellite 6 (RHSA-2018:0273)

RHEL 6 / 7 : RH-SSO 7.3.4 adapters for Enterprise Application Platform 6 (RHSA-2019:3048)

RHEL 6 / 7 : rhev-hypervisor (RHSA-2017:1209)

RHEL 6 / 7 : rhev-hypervisor7 (RHSA-2018:0046) (Meltdown) (Spectre)

RHEL 6 / 7 : rpcbind (RHSA-2016:0005)

RHEL 6 / 7 : ruby193-rubygem-katello (RHSA-2016:1083)

RHEL 6 / 7 : samba (RHSA-2016:0448)

RHEL 6 / 7 : samba (RHSA-2017:1270) (SambaCry)

RHEL 6 / 7 : samba (RHSA-2017:1390) (SambaCry)

RHEL 6 / 7 : samba and samba4 (RHSA-2016:0612) (Badlock)

RHEL 6 / 7 : Satellite 6.1.7 (RHSA-2016:0174)

RHEL 6 / 7 : Satellite Server (RHSA-2015:2622)

RHEL 6 / 7 : Satellite Server (RHSA-2019:0734)

RHEL 6 / 7 : Satellite Server (RHSA-2019:2781)

RHEL 6 / 7 : Satellite Server (RHSA-2019:2782)

RHEL 6 / 7 : Storage Server (RHSA-2016:0014)

RHEL 6 / 7 : Storage Server (RHSA-2016:0447)

RHEL 6 / 7 : Storage Server (RHSA-2016:0614) (Badlock)

RHEL 6 / 7 : Storage Server (RHSA-2016:1494)

RHEL 6 / 7 : Storage Server (RHSA-2017:1273) (SambaCry)

RHEL 6 / 7 : Storage Server (RHSA-2017:1395)

RHEL 6 / 7 : Storage Server (RHSA-2017:2858)

RHEL 6 / 7 : Storage Server (RHSA-2017:3261)

RHEL 6 / 7 : sudo (RHSA-2016:2872)

RHEL 6 / 7 : sudo (RHSA-2017:1382)

RHEL 6 / 7 : sudo (RHSA-2017:1574)

RHEL 6 / 7 : thunderbird (RHSA-2017:1201)

RHEL 6 / 7 : thunderbird (RHSA-2017:1561)

RHEL 6 / 7 : thunderbird (RHSA-2017:2534)

RHEL 6 / 7 : thunderbird (RHSA-2017:2885)

RHEL 6 / 7 : thunderbird (RHSA-2017:3372)

RHEL 6 / 7 : thunderbird (RHSA-2018:0061)

RHEL 6 / 7 : thunderbird (RHSA-2018:0262)

RHEL 6 / 7 : unzip (RHSA-2015:0700)

RHEL 6 / 7 : vim (RHSA-2016:2972)

RHEL 6 / 7 : Virtualization (RHSA-2018:1711) (Spectre)

RHEL 6 / 7 : Virtualization (RHSA-2018:2246) (Spectre)

RHEL 6 / 7 : Virtualization (RHSA-2018:2404) (Foreshadow)

RHEL 6 / 7 : wget (RHSA-2014:1764)

RHEL 6 / 7 : wireshark (RHSA-2014:1676)

RHEL 6 / 7 : xerces-j2 (RHSA-2014:1319)

RHEL 6 / 7 : xorg-x11-server (RHSA-2014:1983)

RHEL 6 / 7 : xorg-x11-server (RHSA-2015:0797)

RHEL 6 : 389-ds-base (RHSA-2012:0813)

RHEL 6 : 389-ds-base (RHSA-2012:0997)

RHEL 6 : 389-ds-base (RHSA-2013:0503)

RHEL 6 : 389-ds-base (RHSA-2013:0628)

RHEL 6 : 389-ds-base (RHSA-2013:0742)

RHEL 6 : 389-ds-base (RHSA-2013:1119)

RHEL 6 : 389-ds-base (RHSA-2013:1182)

RHEL 6 : 389-ds-base (RHSA-2013:1752)

RHEL 6 : 389-ds-base (RHSA-2014:0292)

RHEL 6 : 389-ds-base (RHSA-2015:0628)

RHEL 6 : 389-ds-base (RHSA-2016:2765)

RHEL 6 : 389-ds-base (RHSA-2017:0893)

RHEL 6 : 389-ds-base (RHSA-2018:0515)

RHEL 6 : 389-ds-base (RHSA-2018:1364)

RHEL 6 : abrt (RHSA-2015:1210)

RHEL 6 : abrt and libreport (RHSA-2013:0215)

RHEL 6 : abrt, libreport, btparser, and python-meh (RHSA-2012:0841)

RHEL 6 : activemq (RHSA-2014:0245)

RHEL 6 : activemq (RHSA-2014:0254)

RHEL 6 : augeas (RHSA-2013:1537)

RHEL 6 : augeas (RHSA-2014:0044)

RHEL 6 : autofs (RHSA-2015:1344)

RHEL 6 : automake (RHSA-2013:0526)

RHEL 6 : avahi (RHSA-2011:0779)

RHEL 6 : axis (RHSA-2013:0269)

RHEL 6 : bash (RHSA-2017:0725)

RHEL 6 : bind (RHSA-2010:0975)

RHEL 6 : bind (RHSA-2012:1268)

RHEL 6 : bind (RHSA-2012:1549)

RHEL 6 : bind (RHSA-2013:0550)

RHEL 6 : bind (RHSA-2013:0689)

RHEL 6 : bind (RHSA-2013:1114)

RHEL 6 : bind (RHSA-2014:0043)

RHEL 6 : bind (RHSA-2015:1471)

RHEL 6 : bind (RHSA-2016:0078)

RHEL 6 : bind (RHSA-2016:0079)

RHEL 6 : bind (RHSA-2016:0562)

RHEL 6 : bind (RHSA-2016:0601)

RHEL 6 : bind (RHSA-2016:2099)

RHEL 6 : bind (RHSA-2016:2871)

RHEL 6 : bind (RHSA-2017:1105)

RHEL 6 : bind (RHSA-2017:1202)

RHEL 6 : bind (RHSA-2017:1582)

RHEL 6 : bind (RHSA-2017:1679)

RHEL 6 : bind (RHSA-2018:0101)

RHEL 6 : bind (RHSA-2018:0487)

RHEL 6 : bind (RHSA-2018:2571)

RHEL 6 : bind (RHSA-2019:1492)

RHEL 6 : bind-dyndb-ldap (RHSA-2012:0683)

RHEL 6 : bind-dyndb-ldap (RHSA-2012:1139)

RHEL 6 : busybox (RHSA-2012:0810)

RHEL 6 : busybox (RHSA-2013:1732)

RHEL 6 : bzip2 (RHSA-2010:0858)

RHEL 6 : ca-certificates (RHSA-2011:1248)

RHEL 6 : ca-certificates (RHSA-2013:1866)

RHEL 6 : candlepin in Subscription Asset Manager (RHSA-2013:1863)

RHEL 6 : ccid (RHSA-2013:0523)

RHEL 6 : chromium-browser (RHSA-2014:1626)

RHEL 6 : chromium-browser (RHSA-2014:1894)

RHEL 6 : chromium-browser (RHSA-2015:0093)

RHEL 6 : chromium-browser (RHSA-2015:0163)

RHEL 6 : chromium-browser (RHSA-2015:0627)

RHEL 6 : chromium-browser (RHSA-2015:0778)

RHEL 6 : chromium-browser (RHSA-2015:0816)

RHEL 6 : chromium-browser (RHSA-2015:0921)

RHEL 6 : chromium-browser (RHSA-2015:1023)

RHEL 6 : chromium-browser (RHSA-2015:1188)

RHEL 6 : chromium-browser (RHSA-2015:1499)

RHEL 6 : chromium-browser (RHSA-2015:1712)

RHEL 6 : chromium-browser (RHSA-2015:1841)

RHEL 6 : chromium-browser (RHSA-2015:1912)

RHEL 6 : chromium-browser (RHSA-2015:2545)

RHEL 6 : chromium-browser (RHSA-2015:2618)

RHEL 6 : chromium-browser (RHSA-2015:2665)

RHEL 6 : chromium-browser (RHSA-2016:0072)

RHEL 6 : chromium-browser (RHSA-2016:0241)

RHEL 6 : chromium-browser (RHSA-2016:0286)

RHEL 6 : chromium-browser (RHSA-2016:0359)

RHEL 6 : chromium-browser (RHSA-2016:0429)

RHEL 6 : chromium-browser (RHSA-2016:0525)

RHEL 6 : chromium-browser (RHSA-2016:0638)

RHEL 6 : chromium-browser (RHSA-2016:0707)

RHEL 6 : chromium-browser (RHSA-2016:1080)

RHEL 6 : chromium-browser (RHSA-2016:1190)

RHEL 6 : chromium-browser (RHSA-2016:1201)

RHEL 6 : chromium-browser (RHSA-2016:1262)

RHEL 6 : chromium-browser (RHSA-2016:1485)

RHEL 6 : chromium-browser (RHSA-2016:1580)

RHEL 6 : chromium-browser (RHSA-2016:1854)

RHEL 6 : chromium-browser (RHSA-2016:1905)

RHEL 6 : chromium-browser (RHSA-2016:2007)

RHEL 6 : chromium-browser (RHSA-2016:2067)

RHEL 6 : chromium-browser (RHSA-2016:2672)

RHEL 6 : chromium-browser (RHSA-2016:2718)

RHEL 6 : chromium-browser (RHSA-2016:2919)

RHEL 6 : chromium-browser (RHSA-2017:0206)

RHEL 6 : chromium-browser (RHSA-2017:0499)

RHEL 6 : chromium-browser (RHSA-2017:0860)

RHEL 6 : chromium-browser (RHSA-2017:1124)

RHEL 6 : chromium-browser (RHSA-2017:1228)

RHEL 6 : chromium-browser (RHSA-2017:1399)

RHEL 6 : chromium-browser (RHSA-2017:1495)

RHEL 6 : chromium-browser (RHSA-2017:1833)

RHEL 6 : chromium-browser (RHSA-2017:2676)

RHEL 6 : chromium-browser (RHSA-2017:2792)

RHEL 6 : chromium-browser (RHSA-2017:2997)

RHEL 6 : chromium-browser (RHSA-2017:3082)

RHEL 6 : chromium-browser (RHSA-2017:3151)

RHEL 6 : chromium-browser (RHSA-2017:3401)

RHEL 6 : chromium-browser (RHSA-2017:3479)

RHEL 6 : chromium-browser (RHSA-2018:0265)

RHEL 6 : chromium-browser (RHSA-2018:0334)

RHEL 6 : chromium-browser (RHSA-2018:0484)

RHEL 6 : chromium-browser (RHSA-2018:1195)

RHEL 6 : chromium-browser (RHSA-2018:1321)

RHEL 6 : chromium-browser (RHSA-2018:1446)

RHEL 6 : chromium-browser (RHSA-2018:1815)

RHEL 6 : chromium-browser (RHSA-2018:1825)

RHEL 6 : chromium-browser (RHSA-2018:1933)

RHEL 6 : chromium-browser (RHSA-2018:2282)

RHEL 6 : chromium-browser (RHSA-2018:2666)

RHEL 6 : chromium-browser (RHSA-2018:2818)

RHEL 6 : chromium-browser (RHSA-2018:3004)

RHEL 6 : chromium-browser (RHSA-2018:3648)

RHEL 6 : chromium-browser (RHSA-2018:3803)

RHEL 6 : chromium-browser (RHSA-2019:0309)

RHEL 6 : chromium-browser (RHSA-2019:0396)

RHEL 6 : chromium-browser (RHSA-2019:0481)

RHEL 6 : chromium-browser (RHSA-2019:0708)

RHEL 6 : chromium-browser (RHSA-2019:1021)

RHEL 6 : chromium-browser (RHSA-2019:1243)

RHEL 6 : chromium-browser (RHSA-2019:1477)

RHEL 6 : chromium-browser (RHSA-2019:1553)

RHEL 6 : chromium-browser (RHSA-2019:1930)

RHEL 6 : chromium-browser (RHSA-2019:2427)

RHEL 6 : chromium-browser (RHSA-2019:2670)

RHEL 6 : chromium-browser (RHSA-2019:3211)

RHEL 6 : chromium-browser (RHSA-2019:3759)

RHEL 6 : chromium-browser (RHSA-2019:3775)

RHEL 6 : chromium-browser (RHSA-2019:3955)

RHEL 6 : chromium-browser (RHSA-2019:4238)

RHEL 6 : chromium-browser (RHSA-2020:0005)

RHEL 6 : chromium-browser (RHSA-2020:0084)

RHEL 6 : chromium-browser (RHSA-2020:0214)

RHEL 6 : chromium-browser (RHSA-2020:0514)

RHEL 6 : chromium-browser (RHSA-2020:0738)

RHEL 6 : chromium-browser (RHSA-2020:0779)

RHEL 6 : chromium-browser (RHSA-2020:1270)

RHEL 6 : chromium-browser (RHSA-2020:1350)

RHEL 6 : chromium-browser (RHSA-2020:1487)

RHEL 6 : cifs-utils (RHSA-2012:0902)

RHEL 6 : cloud-init (RHSA-2015:0042)

RHEL 6 : cobbler (RHSA-2018:2372)

RHEL 6 : condor (RHSA-2015:0035)

RHEL 6 : Core X11 clients (RHSA-2013:0502)

RHEL 6 : coreutils (RHSA-2013:1652)

RHEL 6 : coreutils (RHSA-2017:0654)

RHEL 6 : cups (RHSA-2010:0866)

RHEL 6 : cups (RHSA-2011:1635)

RHEL 6 : cups (RHSA-2014:1388)

RHEL 6 : curl (RHSA-2014:0561)

RHEL 6 : curl (RHSA-2015:1254)

RHEL 6 : curl (RHSA-2017:0847)

RHEL 6 : cvs (RHSA-2010:0918)

RHEL 6 : dbus (RHSA-2012:1261)

RHEL 6 : dbus (RHSA-2019:1726)

RHEL 6 : dbus (RHSA-2019:2868)

RHEL 6 : dbus (RHSA-2019:2870)

RHEL 6 : devtoolset-2-axis (RHSA-2014:1123)

RHEL 6 : devtoolset-2-httpcomponents-client (RHSA-2014:1098)

RHEL 6 : dhcp (RHSA-2010:0923)

RHEL 6 : dhcp (RHSA-2011:0256)

RHEL 6 : dhcp (RHSA-2011:1819)

RHEL 6 : dhcp (RHSA-2012:1141)

RHEL 6 : dhcp (RHSA-2013:0504)

RHEL 6 : dhcp (RHSA-2018:0469)

RHEL 6 : dhcp (RHSA-2018:1454)

RHEL 6 : dhcp (RHSA-2018:1458)

RHEL 6 : dhcp (RHSA-2018:1459)

RHEL 6 : dhcp (RHSA-2018:1460)

RHEL 6 : dhcp (RHSA-2018:1461)

RHEL 6 : dnsmasq (RHSA-2013:0277)

RHEL 6 : dnsmasq (RHSA-2017:2838)

RHEL 6 : dnsmasq (RHSA-2017:2839)

RHEL 6 : dovecot (RHSA-2011:0600)

RHEL 6 : dovecot (RHSA-2013:0520)

RHEL 6 : dovecot (RHSA-2019:2885)

RHEL 6 : dracut (RHSA-2013:1674)

RHEL 6 : eap6-jboss-ec2-eap (RHSA-2018:1451)

RHEL 6 : eclipse (RHSA-2011:0568)

RHEL 6 : evince (RHSA-2011:0009)

RHEL 6 : evolution (RHSA-2013:0516)

RHEL 6 : evolution (RHSA-2013:1540)

RHEL 6 : file (RHSA-2014:1606)

RHEL 6 : file (RHSA-2016:0760)

RHEL 6 : firefox (RHSA-2010:0861)

RHEL 6 : firefox (RHSA-2017:1104)

RHEL 6 : firefox (RHSA-2018:0526)

RHEL 6 : firefox (RHSA-2018:1098)

RHEL 6 : firefox (RHSA-2018:1414)

RHEL 6 : firefox (RHSA-2018:2112)

RHEL 6 : firefox (RHSA-2018:2693)

RHEL 6 : firefox (RHSA-2018:2834)

RHEL 6 : firefox (RHSA-2018:2881)

RHEL 6 : firefox (RHSA-2018:3006)

RHEL 6 : firefox (RHSA-2018:3831)

RHEL 6 : firefox (RHSA-2019:0218)

RHEL 6 : firefox (RHSA-2019:0373)

RHEL 6 : firefox (RHSA-2019:0623)

RHEL 6 : firefox (RHSA-2019:0672)

RHEL 6 : firefox (RHSA-2019:1267)

RHEL 6 : firefox (RHSA-2019:1604)

RHEL 6 : firefox (RHSA-2019:1765)

RHEL 6 : firefox (RHSA-2019:2694)

RHEL 6 : firefox (RHSA-2019:3281)

RHEL 6 : firefox (RHSA-2019:4108)

RHEL 6 : firefox (RHSA-2020:0086)

RHEL 6 : firefox (RHSA-2020:0521)

RHEL 6 : firefox (RHSA-2020:0816)

RHEL 6 : firefox (RHSA-2020:1339)

RHEL 6 : firefox (RHSA-2020:1429)

RHEL 6 : flash-plugin (RHSA-2010:0867)

RHEL 6 : flash-plugin (RHSA-2012:1173)

RHEL 6 : flash-plugin (RHSA-2015:1893)

RHEL 6 : flash-plugin (RHSA-2015:1913)

RHEL 6 : flash-plugin (RHSA-2015:2023)

RHEL 6 : flash-plugin (RHSA-2016:2947)

RHEL 6 : flash-plugin (RHSA-2017:0057)

RHEL 6 : flash-plugin (RHSA-2017:0275)

RHEL 6 : flash-plugin (RHSA-2017:0526)

RHEL 6 : flash-plugin (RHSA-2017:0934)

RHEL 6 : flash-plugin (RHSA-2017:1219)

RHEL 6 : flash-plugin (RHSA-2017:1439)

RHEL 6 : flash-plugin (RHSA-2017:1731)

RHEL 6 : flash-plugin (RHSA-2017:2457)

RHEL 6 : flash-plugin (RHSA-2017:2702)

RHEL 6 : flash-plugin (RHSA-2017:2899)

RHEL 6 : flash-plugin (RHSA-2017:3222)

RHEL 6 : flash-plugin (RHSA-2018:0081)

RHEL 6 : flash-plugin (RHSA-2018:0285) (Underminer)

RHEL 6 : flash-plugin (RHSA-2018:0520)

RHEL 6 : flash-plugin (RHSA-2018:1119)

RHEL 6 : flash-plugin (RHSA-2018:1367)

RHEL 6 : flash-plugin (RHSA-2018:1827)

RHEL 6 : flash-plugin (RHSA-2018:2175)

RHEL 6 : flash-plugin (RHSA-2018:2435)

RHEL 6 : flash-plugin (RHSA-2018:2707)

RHEL 6 : flash-plugin (RHSA-2018:3618)

RHEL 6 : flash-plugin (RHSA-2018:3644)

RHEL 6 : flash-plugin (RHSA-2018:3795)

RHEL 6 : flash-plugin (RHSA-2019:0348)

RHEL 6 : flash-plugin (RHSA-2019:0737)

RHEL 6 : flash-plugin (RHSA-2019:1234)

RHEL 6 : flash-plugin (RHSA-2019:1476)

RHEL 6 : flash-plugin (RHSA-2019:2756)

RHEL 6 : flash-plugin (RHSA-2020:0513)

RHEL 6 : foomatic (RHSA-2011:1110)

RHEL 6 : foomatic (RHSA-2016:0491)

RHEL 6 : freeradius (RHSA-2012:1326)

RHEL 6 : freeradius (RHSA-2015:1287)

RHEL 6 : freeradius (RHSA-2017:1759)

RHEL 6 : freetype (RHSA-2010:0864)

RHEL 6 : freetype (RHSA-2011:1085)

RHEL 6 : freetype (RHSA-2019:4254)

RHEL 6 : fuse (RHSA-2011:1083)

RHEL 6 : gc (RHSA-2013:1500)

RHEL 6 : gdb (RHSA-2013:0522)

RHEL 6 : gdm (RHSA-2011:0395)

RHEL 6 : gegl (RHSA-2012:1455)

RHEL 6 : ghostscript (RHSA-2017:0014)

RHEL 6 : ghostscript (RHSA-2018:3760)

RHEL 6 : gimp (RHSA-2011:0839)

RHEL 6 : gimp (RHSA-2012:1180)

RHEL 6 : git (RHSA-2010:1003)

RHEL 6 : git (RHSA-2013:0589)

RHEL 6 : git (RHSA-2017:2485)

RHEL 6 : git (RHSA-2020:0316)

RHEL 6 : glibc (RHSA-2010:0872)

RHEL 6 : glibc (RHSA-2011:0413)

RHEL 6 : glibc (RHSA-2011:1526)

RHEL 6 : glibc (RHSA-2012:0058)

RHEL 6 : glibc (RHSA-2012:0393)

RHEL 6 : glibc (RHSA-2012:1098)

RHEL 6 : glibc (RHSA-2012:1208)

RHEL 6 : glibc (RHSA-2013:1605)

RHEL 6 : glibc (RHSA-2014:1391)

RHEL 6 : glibc (RHSA-2015:0016)

RHEL 6 : glibc (RHSA-2015:0863)

RHEL 6 : glibc (RHSA-2016:0175)

RHEL 6 : glibc (RHSA-2016:1207)

RHEL 6 : glibc (RHSA-2017:0680)

RHEL 6 : glibc (RHSA-2017:1480) (Stack Clash)

RHEL 6 : glibc (RHSA-2018:1879)

RHEL 6 : Gluster Storage (RHSA-2017:0484)

RHEL 6 : Gluster Storage (RHSA-2017:0494)

RHEL 6 : Gluster Storage (RHSA-2018:2608) (deprecated)

RHEL 6 : glusterfs (RHSA-2018:1137)

RHEL 6 : glusterfs (RHSA-2018:1268)

RHEL 6 : glusterfs (RHSA-2018:1955)

RHEL 6 : glusterfs (RHSA-2018:2892)

RHEL 6 : glusterfs (RHSA-2018:3431)

RHEL 6 : gnupg2 (RHSA-2018:2180)

RHEL 6 : gnutls (RHSA-2012:0429)

RHEL 6 : gnutls (RHSA-2014:0246)

RHEL 6 : gnutls (RHSA-2014:0595)

RHEL 6 : gnutls (RHSA-2015:1457)

RHEL 6 : gnutls (RHSA-2017:0574)

RHEL 6 : grep (RHSA-2015:1447)

RHEL 6 : gstreamer-plugins-bad-free (RHSA-2016:2974)

RHEL 6 : gstreamer-plugins-good (RHSA-2016:2975)

RHEL 6 : haproxy (RHSA-2013:0729)

RHEL 6 : haproxy (RHSA-2013:0868)

RHEL 6 : haproxy (RHSA-2013:1120)

RHEL 6 : haproxy (RHSA-2013:1204)

RHEL 6 : hivex (RHSA-2015:1378)

RHEL 6 : hplip (RHSA-2013:0500)

RHEL 6 : hplip (RHSA-2013:1274)

RHEL 6 : httpd (RHSA-2011:1391)

RHEL 6 : httpd (RHSA-2012:0128)

RHEL 6 : httpd (RHSA-2013:0512)

RHEL 6 : httpd (RHSA-2014:0370)

RHEL 6 : httpd (RHSA-2015:1249)

RHEL 6 : httpd (RHSA-2015:1668)

RHEL 6 : httpd (RHSA-2017:1721)

RHEL 6 : httpd (RHSA-2017:2478)

RHEL 6 : httpd (RHSA-2017:2972) (Optionsbleed)

RHEL 6 : httpd (RHSA-2017:3195) (Optionsbleed)

RHEL 6 : icedtea-web (RHSA-2011:1100)

RHEL 6 : icedtea-web (RHSA-2011:1441)

RHEL 6 : icedtea-web (RHSA-2012:1132)

RHEL 6 : icedtea-web (RHSA-2012:1434)

RHEL 6 : icedtea-web (RHSA-2013:0753)

RHEL 6 : icedtea-web (RHSA-2016:0778)

RHEL 6 : icu (RHSA-2020:0896)

RHEL 6 : ImageMagick (RHSA-2012:0544)

RHEL 6 : ipa (RHSA-2011:1533)

RHEL 6 : ipa (RHSA-2013:0188)

RHEL 6 : ipa (RHSA-2013:0528)

RHEL 6 : ipa (RHSA-2015:1462)

RHEL 6 : ipmitool (RHSA-2011:1814)

RHEL 6 : ipmitool (RHSA-2020:1331)

RHEL 6 : jakarta-commons-collections (RHSA-2015:2521)

RHEL 6 : jasper (RHSA-2011:1807)

RHEL 6 : jasperreports-server-pro (RHSA-2014:0037)

RHEL 6 : jasperreports-server-pro (RHSA-2014:0389)

RHEL 6 : java-1.5.0-ibm (RHSA-2010:0873)

RHEL 6 : java-1.6.0-ibm (RHSA-2017:1222)

RHEL 6 : java-1.6.0-ibm (RHSA-2017:2530)

RHEL 6 : java-1.6.0-openjdk (RHSA-2010:0865)

RHEL 6 : java-1.6.0-openjdk (RHSA-2011:0856)

RHEL 6 : java-1.6.0-openjdk (RHSA-2012:0135)

RHEL 6 : java-1.6.0-openjdk (RHSA-2012:0729)

RHEL 6 : java-1.6.0-openjdk (RHSA-2012:1221)

RHEL 6 : java-1.6.0-openjdk (RHSA-2012:1384) (ROBOT)

RHEL 6 : java-1.6.0-openjdk (RHSA-2013:0245)

RHEL 6 : java-1.6.0-openjdk (RHSA-2013:0273)

RHEL 6 : java-1.6.0-openjdk (RHSA-2013:0605)

RHEL 6 : java-1.6.0-sun (RHSA-2018:1203)

RHEL 6 : java-1.6.0-sun (RHSA-2018:3008)

RHEL 6 : java-1.7.0-ibm (RHSA-2012:1289)

RHEL 6 : java-1.7.0-ibm (RHSA-2012:1467) (ROBOT)

RHEL 6 : java-1.7.0-ibm (RHSA-2014:1882) (POODLE)

RHEL 6 : java-1.7.0-openjdk (RHSA-2012:1009)

RHEL 6 : java-1.7.0-openjdk (RHSA-2012:1223)

RHEL 6 : java-1.7.0-openjdk (RHSA-2012:1386) (ROBOT)

RHEL 6 : java-1.7.0-openjdk (RHSA-2013:0602)

RHEL 6 : java-1.7.0-openjdk (RHSA-2013:0751)

RHEL 6 : java-1.7.0-openjdk (RHSA-2013:0957)

RHEL 6 : java-1.7.0-openjdk (RHSA-2013:1451)

RHEL 6 : java-1.7.0-openjdk (RHSA-2014:0026)

RHEL 6 : java-1.7.0-openjdk (RHSA-2014:0406)

RHEL 6 : java-1.7.0-openjdk (RHSA-2016:0053) (SLOTH)

RHEL 6 : java-1.7.0-openjdk (RHSA-2016:0511)

RHEL 6 : java-1.7.0-openjdk (RHSA-2016:0675)

RHEL 6 : java-1.7.0-openjdk (RHSA-2018:1270)

RHEL 6 : java-1.7.0-openjdk (RHSA-2018:1647) (Spectre)

RHEL 6 : java-1.7.0-openjdk (RHSA-2018:2283)

RHEL 6 : java-1.7.0-openjdk (RHSA-2018:3409)

RHEL 6 : java-1.7.0-openjdk (RHSA-2019:0462)

RHEL 6 : java-1.7.0-openjdk (RHSA-2019:0790)

RHEL 6 : java-1.7.0-openjdk (RHSA-2019:1840)

RHEL 6 : java-1.7.0-openjdk (RHSA-2019:3158)

RHEL 6 : java-1.7.0-openjdk (RHSA-2020:0632)

RHEL 6 : java-1.7.0-oracle (RHSA-2012:1019)

RHEL 6 : java-1.7.0-oracle (RHSA-2012:1225)

RHEL 6 : java-1.7.0-oracle (RHSA-2012:1391)

RHEL 6 : java-1.7.0-oracle (RHSA-2018:1206)

RHEL 6 : java-1.7.0-oracle (RHSA-2018:2255)

RHEL 6 : java-1.7.0-oracle (RHSA-2018:3000)

RHEL 6 : java-1.7.1-ibm (RHSA-2017:1216)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:0521)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:1724)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:1812)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:1974)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:2576)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:2712)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:3671)

RHEL 6 : java-1.7.1-ibm (RHSA-2018:3779)

RHEL 6 : java-1.7.1-ibm (RHSA-2019:0474)

RHEL 6 : java-1.7.1-ibm (RHSA-2019:1165)

RHEL 6 : java-1.7.1-ibm (RHSA-2019:2494)

RHEL 6 : java-1.7.1-ibm (RHSA-2019:4109)

RHEL 6 : java-1.7.1-ibm (RHSA-2020:0467)

RHEL 6 : java-1.8.0-ibm (RHSA-2016:1039)

RHEL 6 : java-1.8.0-ibm (RHSA-2017:3267)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:0352)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:1463)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:1722)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:1975)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:2575)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:2713)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:3533)

RHEL 6 : java-1.8.0-ibm (RHSA-2018:3852)

RHEL 6 : java-1.8.0-ibm (RHSA-2019:0469)

RHEL 6 : java-1.8.0-ibm (RHSA-2019:0640)

RHEL 6 : java-1.8.0-ibm (RHSA-2019:1163)

RHEL 6 : java-1.8.0-ibm (RHSA-2019:1325)

RHEL 6 : java-1.8.0-ibm (RHSA-2019:2592)

RHEL 6 : java-1.8.0-ibm (RHSA-2019:2737)

RHEL 6 : java-1.8.0-ibm (RHSA-2019:4113)

RHEL 6 : java-1.8.0-ibm (RHSA-2020:0006)

RHEL 6 : java-1.8.0-ibm (RHSA-2020:0469)

RHEL 6 : java-1.8.0-ibm (RHSA-2020:0856)

RHEL 6 : java-1.8.0-openjdk (RHSA-2014:1636)

RHEL 6 : java-1.8.0-openjdk (RHSA-2015:0069) (POODLE)

RHEL 6 : java-1.8.0-openjdk (RHSA-2016:0050) (SLOTH)

RHEL 6 : java-1.8.0-openjdk (RHSA-2016:0514)

RHEL 6 : java-1.8.0-openjdk (RHSA-2016:0651)

RHEL 6 : java-1.8.0-openjdk (RHSA-2017:1109)

RHEL 6 : java-1.8.0-openjdk (RHSA-2018:1188)

RHEL 6 : java-1.8.0-openjdk (RHSA-2018:1650) (Spectre)

RHEL 6 : java-1.8.0-openjdk (RHSA-2018:2241)

RHEL 6 : java-1.8.0-openjdk (RHSA-2018:2943)

RHEL 6 : java-1.8.0-openjdk (RHSA-2019:0416)

RHEL 6 : java-1.8.0-openjdk (RHSA-2019:0774)

RHEL 6 : java-1.8.0-openjdk (RHSA-2019:1811)

RHEL 6 : java-1.8.0-openjdk (RHSA-2019:3136)

RHEL 6 : java-1.8.0-openjdk (RHSA-2020:0157)

RHEL 6 : java-1.8.0-oracle (RHSA-2015:0080) (POODLE)

RHEL 6 : java-1.8.0-oracle (RHSA-2018:1202)

RHEL 6 : java-1.8.0-oracle (RHSA-2018:2256)

RHEL 6 : java-1.8.0-oracle (RHSA-2018:3003)

RHEL 6 : JBoss Core Services (RHSA-2017:0193)

RHEL 6 : JBoss Core Services (RHSA-2017:1414)

RHEL 6 : JBoss Core Services (RHSA-2017:2710)

RHEL 6 : JBoss Core Services (RHSA-2019:3932) (0-Length Headers Leak) (Data Dribble) (Internal Data Buffering) (Resource Loop)

RHEL 6 : JBoss EAP (RHSA-2011:0946)

RHEL 6 : JBoss EAP (RHSA-2011:1798)

RHEL 6 : JBoss EAP (RHSA-2012:1592)

RHEL 6 : JBoss EAP (RHSA-2013:0834)

RHEL 6 : JBoss EAP (RHSA-2013:1208)

RHEL 6 : JBoss EAP (RHSA-2013:1786)

RHEL 6 : JBoss EAP (RHSA-2014:0171)

RHEL 6 : JBoss EAP (RHSA-2014:0344)

RHEL 6 : JBoss EAP (RHSA-2014:0563)

RHEL 6 : JBoss EAP (RHSA-2014:0799)

RHEL 6 : JBoss EAP (RHSA-2014:1020)

RHEL 6 : JBoss EAP (RHSA-2014:1285)

RHEL 6 : JBoss EAP (RHSA-2014:1818)

RHEL 6 : JBoss EAP (RHSA-2015:0217)

RHEL 6 : JBoss EAP (RHSA-2015:0847)

RHEL 6 : JBoss EAP (RHSA-2015:1670)

RHEL 6 : JBoss EAP (RHSA-2015:1905)

RHEL 6 : JBoss EAP (RHSA-2015:1907)

RHEL 6 : JBoss EAP (RHSA-2015:2539)

RHEL 6 : JBoss EAP (RHSA-2015:2542)

RHEL 6 : JBoss EAP (RHSA-2016:0122)

RHEL 6 : JBoss EAP (RHSA-2016:0596)

RHEL 6 : JBoss EAP (RHSA-2016:1433)

RHEL 6 : JBoss EAP (RHSA-2016:1838)

RHEL 6 : JBoss EAP (RHSA-2016:2055)

RHEL 6 : JBoss EAP (RHSA-2016:2640)

RHEL 6 : JBoss EAP (RHSA-2017:0170)

RHEL 6 : JBoss EAP (RHSA-2017:0244)

RHEL 6 : JBoss EAP (RHSA-2017:0827)

RHEL 6 : JBoss EAP (RHSA-2017:0831)

RHEL 6 : JBoss EAP (RHSA-2017:1254)

RHEL 6 : JBoss EAP (RHSA-2017:1410)

RHEL 6 : JBoss EAP (RHSA-2017:1549)

RHEL 6 : JBoss EAP (RHSA-2017:1834)

RHEL 6 : JBoss EAP (RHSA-2017:2635)

RHEL 6 : JBoss EAP (RHSA-2017:2809)

RHEL 6 : JBoss EAP (RHSA-2017:3217)

RHEL 6 : JBoss EAP (RHSA-2017:3399)

RHEL 6 : JBoss EAP (RHSA-2017:3454)

RHEL 6 : JBoss EAP (RHSA-2018:0002)

RHEL 6 : JBoss EAP (RHSA-2018:0270)

RHEL 6 : JBoss EAP (RHSA-2018:0479)

RHEL 6 : JBoss EAP (RHSA-2018:1248)

RHEL 6 : JBoss EAP (RHSA-2018:1449)

RHEL 6 : JBoss EAP (RHSA-2018:1607)

RHEL 6 : JBoss EAP (RHSA-2018:1609)

RHEL 6 : JBoss EAP (RHSA-2018:2090)

RHEL 6 : JBoss EAP (RHSA-2018:2423)

RHEL 6 : JBoss EAP (RHSA-2018:2743)

RHEL 6 : JBoss EAP (RHSA-2018:3517)

RHEL 6 : JBoss EAP (RHSA-2018:3529)

RHEL 6 : JBoss EAP (RHSA-2019:0136)

RHEL 6 : JBoss EAP (RHSA-2019:0364)

RHEL 6 : JBoss EAP (RHSA-2019:1107)

RHEL 6 : JBoss EAP (RHSA-2019:1160)

RHEL 6 : JBoss EAP (RHSA-2019:1419)

RHEL 6 : JBoss EAP (RHSA-2019:2935)

RHEL 6 : JBoss EAP (RHSA-2019:4018) (Data Dribble) (Ping Flood) (Reset Flood) (Settings Flood)

RHEL 6 : JBoss EAP (RHSA-2020:0159)

RHEL 6 : JBoss EAP (RHSA-2020:0804)

RHEL 6 : JBoss EWP (RHSA-2013:0195)

RHEL 6 : JBoss Web Server (RHSA-2013:1012)

RHEL 6 : JBoss Web Server (RHSA-2014:1087)

RHEL 6 : JBoss Web Server (RHSA-2015:2659)

RHEL 6 : JBoss Web Server (RHSA-2016:1087)

RHEL 6 : JBoss Web Server (RHSA-2016:1649) (httpoxy)

RHEL 6 : jboss-ec2-eap (RHSA-2012:1376)

RHEL 6 : jboss-ec2-eap (RHSA-2016:0124)

RHEL 6 : jboss-ec2-eap (RHSA-2016:0598)

RHEL 6 : jboss-ec2-eap (RHSA-2016:1432)

RHEL 6 : jboss-ec2-eap (RHSA-2016:2072)

RHEL 6 : jboss-ec2-eap (RHSA-2017:0250)

RHEL 6 : jboss-ec2-eap (RHSA-2017:0829)

RHEL 6 : jboss-ec2-eap (RHSA-2017:1260)

RHEL 6 : jboss-ec2-eap (RHSA-2017:1552)

RHEL 6 : jboss-ec2-eap (RHSA-2017:2638)

RHEL 6 : jboss-ec2-eap (RHSA-2017:3219)

RHEL 6 : jboss-ec2-eap (RHSA-2018:0275)

RHEL 6 : jboss-ec2-eap bug fix (RHSA-2015:1673)

RHEL 6 : jenkins (RHSA-2013:0700)

RHEL 6 : katello in Subscription Asset Manager (RHSA-2012:1187)

RHEL 6 : katello-configure (RHSA-2014:1186)

RHEL 6 : kdelibs (RHSA-2011:0464)

RHEL 6 : kdelibs (RHSA-2011:1364)

RHEL 6 : kdelibs (RHSA-2012:1416)

RHEL 6 : kdelibs (RHSA-2012:1418)

RHEL 6 : kdenetwork (RHSA-2011:0465)

RHEL 6 : kernel (RHSA-2010:0842)

RHEL 6 : kernel (RHSA-2011:0007)

RHEL 6 : kernel (RHSA-2011:0283)

RHEL 6 : kernel (RHSA-2011:0329)

RHEL 6 : kernel (RHSA-2011:0421)

RHEL 6 : kernel (RHSA-2011:0498)

RHEL 6 : kernel (RHSA-2011:0542)

RHEL 6 : kernel (RHSA-2011:0836)

RHEL 6 : kernel (RHSA-2011:0883)

RHEL 6 : kernel (RHSA-2011:0928)

RHEL 6 : kernel (RHSA-2011:1106)

RHEL 6 : kernel (RHSA-2011:1189)

RHEL 6 : kernel (RHSA-2011:1350)

RHEL 6 : kernel (RHSA-2011:1465)

RHEL 6 : kernel (RHSA-2011:1530)

RHEL 6 : kernel (RHSA-2011:1849)

RHEL 6 : kernel (RHSA-2012:0052)

RHEL 6 : kernel (RHSA-2012:0116)

RHEL 6 : kernel (RHSA-2012:0350)

RHEL 6 : kernel (RHSA-2012:0481)

RHEL 6 : kernel (RHSA-2012:0571)

RHEL 6 : kernel (RHSA-2012:0743)

RHEL 6 : kernel (RHSA-2012:0862)

RHEL 6 : kernel (RHSA-2012:1042)

RHEL 6 : kernel (RHSA-2012:1064)

RHEL 6 : kernel (RHSA-2012:1114)

RHEL 6 : kernel (RHSA-2012:1129)

RHEL 6 : kernel (RHSA-2012:1148)

RHEL 6 : kernel (RHSA-2012:1156)

RHEL 6 : kernel (RHSA-2012:1304)

RHEL 6 : kernel (RHSA-2012:1366)

RHEL 6 : kernel (RHSA-2012:1401)

RHEL 6 : kernel (RHSA-2012:1426)

RHEL 6 : kernel (RHSA-2012:1430)

RHEL 6 : kernel (RHSA-2012:1541)

RHEL 6 : kernel (RHSA-2012:1580)

RHEL 6 : kernel (RHSA-2012:1589)

RHEL 6 : kernel (RHSA-2013:0223)

RHEL 6 : kernel (RHSA-2013:0496)

RHEL 6 : kernel (RHSA-2013:0567)

RHEL 6 : kernel (RHSA-2013:0630)

RHEL 6 : kernel (RHSA-2013:0661)

RHEL 6 : kernel (RHSA-2013:0662)

RHEL 6 : kernel (RHSA-2013:0741)

RHEL 6 : kernel (RHSA-2013:0744)

RHEL 6 : kernel (RHSA-2013:0830)

RHEL 6 : kernel (RHSA-2013:0832)

RHEL 6 : kernel (RHSA-2013:0840)

RHEL 6 : kernel (RHSA-2013:0841)

RHEL 6 : kernel (RHSA-2013:0882)

RHEL 6 : kernel (RHSA-2013:0911)

RHEL 6 : kernel (RHSA-2013:0928)

RHEL 6 : kernel (RHSA-2013:1026)

RHEL 6 : kernel (RHSA-2013:1051)

RHEL 6 : kernel (RHSA-2013:1173)

RHEL 6 : kernel (RHSA-2013:1436)

RHEL 6 : kernel (RHSA-2013:1450)

RHEL 6 : kernel (RHSA-2013:1519)

RHEL 6 : kernel (RHSA-2013:1645)

RHEL 6 : kernel (RHSA-2013:1783)

RHEL 6 : kernel (RHSA-2013:1801)

RHEL 6 : kernel (RHSA-2014:0159)

RHEL 6 : kernel (RHSA-2014:0284)

RHEL 6 : kernel (RHSA-2014:0328)

RHEL 6 : kernel (RHSA-2014:0419)

RHEL 6 : kernel (RHSA-2014:0432)

RHEL 6 : kernel (RHSA-2014:0475)

RHEL 6 : kernel (RHSA-2014:0512)

RHEL 6 : kernel (RHSA-2014:0520)

RHEL 6 : kernel (RHSA-2014:0593)

RHEL 6 : kernel (RHSA-2014:0634)

RHEL 6 : kernel (RHSA-2014:0771)

RHEL 6 : kernel (RHSA-2014:0800)

RHEL 6 : kernel (RHSA-2014:0900)

RHEL 6 : kernel (RHSA-2014:0924)

RHEL 6 : kernel (RHSA-2014:0925)

RHEL 6 : kernel (RHSA-2014:0949)

RHEL 6 : kernel (RHSA-2014:0981)

RHEL 6 : kernel (RHSA-2014:1025)

RHEL 6 : kernel (RHSA-2014:1101)

RHEL 6 : kernel (RHSA-2014:1167)

RHEL 6 : kernel (RHSA-2014:1365)

RHEL 6 : kernel (RHSA-2014:1392)

RHEL 6 : kernel (RHSA-2014:1668)

RHEL 6 : kernel (RHSA-2014:1763)

RHEL 6 : kernel (RHSA-2014:1843)

RHEL 6 : kernel (RHSA-2014:1872)

RHEL 6 : kernel (RHSA-2014:1997)

RHEL 6 : kernel (RHSA-2014:2009)

RHEL 6 : kernel (RHSA-2014:2028)

RHEL 6 : kernel (RHSA-2014:2030)

RHEL 6 : kernel (RHSA-2015:0043)

RHEL 6 : kernel (RHSA-2015:0062)

RHEL 6 : kernel (RHSA-2015:0087)

RHEL 6 : kernel (RHSA-2015:0115)

RHEL 6 : kernel (RHSA-2015:0284)

RHEL 6 : kernel (RHSA-2015:0285)

RHEL 6 : kernel (RHSA-2015:0674)

RHEL 6 : kernel (RHSA-2015:0695)

RHEL 6 : kernel (RHSA-2015:0782)

RHEL 6 : kernel (RHSA-2015:0803)

RHEL 6 : kernel (RHSA-2015:0864)

RHEL 6 : kernel (RHSA-2015:1030)

RHEL 6 : kernel (RHSA-2015:1081)

RHEL 6 : kernel (RHSA-2015:1082)

RHEL 6 : kernel (RHSA-2015:1199)

RHEL 6 : kernel (RHSA-2015:1211)

RHEL 6 : kernel (RHSA-2015:1221)

RHEL 6 : kernel (RHSA-2015:1272)

RHEL 6 : kernel (RHSA-2015:1583)

RHEL 6 : kernel (RHSA-2015:1623)

RHEL 6 : kernel (RHSA-2015:1643)

RHEL 6 : kernel (RHSA-2015:2636)

RHEL 6 : kernel (RHSA-2015:2645)

RHEL 6 : kernel (RHSA-2016:0004)

RHEL 6 : kernel (RHSA-2016:0024)

RHEL 6 : kernel (RHSA-2016:0046)

RHEL 6 : kernel (RHSA-2016:0494)

RHEL 6 : kernel (RHSA-2016:0617)

RHEL 6 : kernel (RHSA-2016:0715)

RHEL 6 : kernel (RHSA-2016:0855)

RHEL 6 : kernel (RHSA-2016:1096)

RHEL 6 : kernel (RHSA-2016:1100)

RHEL 6 : kernel (RHSA-2016:1225)

RHEL 6 : kernel (RHSA-2016:1406)

RHEL 6 : kernel (RHSA-2016:1489)

RHEL 6 : kernel (RHSA-2016:1581)

RHEL 6 : kernel (RHSA-2016:1617)

RHEL 6 : kernel (RHSA-2016:1640)

RHEL 6 : kernel (RHSA-2016:1664)

RHEL 6 : kernel (RHSA-2016:1814)

RHEL 6 : kernel (RHSA-2016:1815)

RHEL 6 : kernel (RHSA-2016:1939)

RHEL 6 : kernel (RHSA-2016:2006)

RHEL 6 : kernel (RHSA-2016:2074)

RHEL 6 : kernel (RHSA-2016:2076)

RHEL 6 : kernel (RHSA-2016:2105) (Dirty COW)

RHEL 6 : kernel (RHSA-2016:2106) (Dirty COW)

RHEL 6 : kernel (RHSA-2016:2120) (Dirty COW)

RHEL 6 : kernel (RHSA-2016:2128) (Dirty COW)

RHEL 6 : kernel (RHSA-2016:2132) (Dirty COW)

RHEL 6 : kernel (RHSA-2016:2133) (Dirty COW)

RHEL 6 : kernel (RHSA-2016:2766)

RHEL 6 : kernel (RHSA-2017:0031)

RHEL 6 : kernel (RHSA-2017:0036)

RHEL 6 : kernel (RHSA-2017:0065)

RHEL 6 : kernel (RHSA-2017:0196)

RHEL 6 : kernel (RHSA-2017:0215)

RHEL 6 : kernel (RHSA-2017:0216)

RHEL 6 : kernel (RHSA-2017:0293)

RHEL 6 : kernel (RHSA-2017:0307)

RHEL 6 : kernel (RHSA-2017:0316)

RHEL 6 : kernel (RHSA-2017:0324)

RHEL 6 : kernel (RHSA-2017:0345)

RHEL 6 : kernel (RHSA-2017:0365)

RHEL 6 : kernel (RHSA-2017:0366)

RHEL 6 : kernel (RHSA-2017:0817)

RHEL 6 : kernel (RHSA-2017:0869)

RHEL 6 : kernel (RHSA-2017:0892)

RHEL 6 : kernel (RHSA-2017:0986)

RHEL 6 : kernel (RHSA-2017:1126)

RHEL 6 : kernel (RHSA-2017:1232)

RHEL 6 : kernel (RHSA-2017:1233)

RHEL 6 : kernel (RHSA-2017:1372)

RHEL 6 : kernel (RHSA-2017:1486) (Stack Clash)

RHEL 6 : kernel (RHSA-2017:1487) (Stack Clash)

RHEL 6 : kernel (RHSA-2017:1488) (Stack Clash)

RHEL 6 : kernel (RHSA-2017:1489) (Stack Clash)

RHEL 6 : kernel (RHSA-2017:1490) (Stack Clash)

RHEL 6 : kernel (RHSA-2017:1491) (Stack Clash)

RHEL 6 : kernel (RHSA-2017:1715)

RHEL 6 : kernel (RHSA-2017:1723)

RHEL 6 : kernel (RHSA-2017:1798)

RHEL 6 : kernel (RHSA-2017:2428)

RHEL 6 : kernel (RHSA-2017:2429)

RHEL 6 : kernel (RHSA-2017:2681) (BlueBorne)

RHEL 6 : kernel (RHSA-2017:2682) (BlueBorne)

RHEL 6 : kernel (RHSA-2017:2683) (BlueBorne)

RHEL 6 : kernel (RHSA-2017:2707) (BlueBorne)

RHEL 6 : kernel (RHSA-2017:2731) (BlueBorne)

RHEL 6 : kernel (RHSA-2017:2732) (BlueBorne)

RHEL 6 : kernel (RHSA-2017:2760)

RHEL 6 : kernel (RHSA-2017:2795)

RHEL 6 : kernel (RHSA-2017:2796)

RHEL 6 : kernel (RHSA-2017:2797)

RHEL 6 : kernel (RHSA-2017:2798)

RHEL 6 : kernel (RHSA-2017:2799)

RHEL 6 : kernel (RHSA-2017:2800)

RHEL 6 : kernel (RHSA-2017:2863)

RHEL 6 : kernel (RHSA-2017:3200)

RHEL 6 : kernel (RHSA-2018:0008) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:0011) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:0017) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:0018) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:0020) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:0022) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:0169)

RHEL 6 : kernel (RHSA-2018:0496) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:0512) (Meltdown) (Spectre)

RHEL 6 : kernel (RHSA-2018:1319) (Meltdown)

RHEL 6 : kernel (RHSA-2018:1346) (Meltdown)

RHEL 6 : kernel (RHSA-2018:1349)

RHEL 6 : kernel (RHSA-2018:1350)

RHEL 6 : kernel (RHSA-2018:1351)

RHEL 6 : kernel (RHSA-2018:1638) (Spectre)

RHEL 6 : kernel (RHSA-2018:1639) (Spectre)

RHEL 6 : kernel (RHSA-2018:1640) (Spectre)

RHEL 6 : kernel (RHSA-2018:1641) (Spectre)

RHEL 6 : kernel (RHSA-2018:1651) (Spectre)

RHEL 6 : kernel (RHSA-2018:1826) (Spectre)

RHEL 6 : kernel (RHSA-2018:1854) (Spectre)

RHEL 6 : kernel (RHSA-2018:2164) (Spectre)

RHEL 6 : kernel (RHSA-2018:2250) (Spectre)

RHEL 6 : kernel (RHSA-2018:2309) (Spectre)

RHEL 6 : kernel (RHSA-2018:2390) (Foreshadow)

RHEL 6 : kernel (RHSA-2018:2391) (Foreshadow)

RHEL 6 : kernel (RHSA-2018:2392) (Foreshadow)

RHEL 6 : kernel (RHSA-2018:2393) (Foreshadow)

RHEL 6 : kernel (RHSA-2018:2394) (Foreshadow) (Spectre)

RHEL 6 : kernel (RHSA-2018:2645)

RHEL 6 : kernel (RHSA-2018:2791)

RHEL 6 : kernel (RHSA-2018:2846)

RHEL 6 : kernel (RHSA-2018:2924)

RHEL 6 : kernel (RHSA-2018:2925)

RHEL 6 : kernel (RHSA-2018:2933)

RHEL 6 : kernel (RHSA-2018:3643)

RHEL 6 : kernel (RHSA-2019:0415)

RHEL 6 : kernel (RHSA-2019:0717)

RHEL 6 : kernel (RHSA-2019:1169) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : kernel (RHSA-2019:1193) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : kernel (RHSA-2019:1196) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : kernel (RHSA-2019:1488) (SACK Panic) (SACK Slowness)

RHEL 6 : kernel (RHSA-2019:1489) (SACK Panic) (SACK Slowness)

RHEL 6 : kernel (RHSA-2019:1490) (SACK Panic) (SACK Slowness)

RHEL 6 : kernel (RHSA-2019:2473)

RHEL 6 : kernel (RHSA-2019:2476)

RHEL 6 : kernel (RHSA-2019:2695)

RHEL 6 : kernel (RHSA-2019:2736)

RHEL 6 : kernel (RHSA-2019:2863)

RHEL 6 : kernel (RHSA-2019:2869)

RHEL 6 : kernel (RHSA-2019:2901)

RHEL 6 : kernel (RHSA-2019:3836)

RHEL 6 : kernel (RHSA-2019:3842)

RHEL 6 : kernel (RHSA-2019:3843)

RHEL 6 : kernel (RHSA-2019:3878)

RHEL 6 : kernel (RHSA-2019:4056)

RHEL 6 : kernel (RHSA-2019:4255)

RHEL 6 : kernel (RHSA-2019:4256)

RHEL 6 : kernel (RHSA-2020:0790)

RHEL 6 : kernel-rt (RHSA-2014:0913)

RHEL 6 : kernel-rt (RHSA-2014:1943)

RHEL 6 : kernel-rt (RHSA-2014:1998)

RHEL 6 : kernel-rt (RHSA-2015:1787)

RHEL 6 : kernel-rt (RHSA-2018:0181)

RHEL 6 : kernel-rt (RHSA-2020:0100)

RHEL 6 : kernel-rt (RHSA-2020:1353)

RHEL 6 : kexec-tools (RHSA-2011:1532)

RHEL 6 : krb5 (RHSA-2010:0863)

RHEL 6 : krb5 (RHSA-2010:0925)

RHEL 6 : krb5 (RHSA-2011:0200)

RHEL 6 : krb5 (RHSA-2011:0356)

RHEL 6 : krb5 (RHSA-2011:0447)

RHEL 6 : krb5 (RHSA-2011:1379)

RHEL 6 : krb5 (RHSA-2011:1790)

RHEL 6 : krb5 (RHSA-2012:1131)

RHEL 6 : krb5 (RHSA-2013:0656)

RHEL 6 : krb5 (RHSA-2013:0748)

RHEL 6 : krb5 (RHSA-2014:1389)

RHEL 6 : krb5 (RHSA-2015:0794)

RHEL 6 : krb5 (RHSA-2016:0493)

RHEL 6 : krb5-appl (RHSA-2011:0920)

RHEL 6 : krb5-appl (RHSA-2011:1852)

RHEL 6 : krb5-appl (RHSA-2011:1854)

RHEL 6 : krb5-appl (RHSA-2020:1349)

RHEL 6 : ksh (RHSA-2020:0515)

RHEL 6 : libarchive (RHSA-2011:1507)

RHEL 6 : libarchive (RHSA-2016:1850)

RHEL 6 : libcap (RHSA-2011:1694)

RHEL 6 : libcgroup (RHSA-2011:0320)

RHEL 6 : libguestfs (RHSA-2011:0586)

RHEL 6 : libguestfs (RHSA-2012:0774)

RHEL 6 : libguestfs (RHSA-2013:1536)

RHEL 6 : libguestfs (RHSA-2017:0564)

RHEL 6 : libjpeg-turbo (RHSA-2013:1803)

RHEL 6 : libpng (RHSA-2011:1105)

RHEL 6 : libpng (RHSA-2015:2594)

RHEL 6 : libproxy (RHSA-2012:1461)

RHEL 6 : librelp (RHSA-2018:1225)

RHEL 6 : librelp (RHSA-2018:1701)

RHEL 6 : librelp (RHSA-2018:1702)

RHEL 6 : libreoffice (RHSA-2012:1135)

RHEL 6 : libreoffice (RHSA-2015:1458)

RHEL 6 : libreoffice (RHSA-2017:0979)

RHEL 6 : libreoffice (RHSA-2018:0517)

RHEL 6 : libreport (RHSA-2015:2504)

RHEL 6 : librsvg2 (RHSA-2011:1289)

RHEL 6 : librsvg2 (RHSA-2014:0127)

RHEL 6 : libsndfile (RHSA-2011:1084)

RHEL 6 : libsoup (RHSA-2011:1102)

RHEL 6 : libssh2 (RHSA-2019:1652)

RHEL 6 : libtar (RHSA-2013:1418)

RHEL 6 : libtasn1 (RHSA-2012:0427)

RHEL 6 : libtasn1 (RHSA-2014:0596)

RHEL 6 : libtiff (RHSA-2011:0452)

RHEL 6 : libtiff (RHSA-2014:0222)

RHEL 6 : libtiff (RHSA-2016:1547)

RHEL 6 : libtirpc (RHSA-2013:0884)

RHEL 6 : libtirpc (RHSA-2017:1268)

RHEL 6 : libuser (RHSA-2015:1482)

RHEL 6 : libvirt (RHSA-2011:0479)

RHEL 6 : libvirt (RHSA-2011:1197)

RHEL 6 : libvirt (RHSA-2012:0748)

RHEL 6 : libvirt (RHSA-2012:1202)

RHEL 6 : libvirt (RHSA-2012:1359)

RHEL 6 : libvirt (RHSA-2013:0199)

RHEL 6 : libvirt (RHSA-2013:0276)

RHEL 6 : libvirt (RHSA-2013:0831)

RHEL 6 : libvirt (RHSA-2013:1272)

RHEL 6 : libvirt (RHSA-2014:0103)

RHEL 6 : libvirt (RHSA-2014:0560)

RHEL 6 : libvirt (RHSA-2014:1873)

RHEL 6 : libvirt (RHSA-2018:0030) (Spectre)

RHEL 6 : libvirt (RHSA-2018:0108) (Spectre)

RHEL 6 : libvirt (RHSA-2018:0109) (Spectre)

RHEL 6 : libvirt (RHSA-2018:0110) (Spectre)

RHEL 6 : libvirt (RHSA-2018:0111) (Spectre)

RHEL 6 : libvirt (RHSA-2018:0112) (Spectre)

RHEL 6 : libvirt (RHSA-2018:1664) (Spectre)

RHEL 6 : libvirt (RHSA-2018:1665) (Spectre)

RHEL 6 : libvirt (RHSA-2018:1666) (Spectre)

RHEL 6 : libvirt (RHSA-2018:1667) (Spectre)

RHEL 6 : libvirt (RHSA-2018:1669) (Spectre)

RHEL 6 : libvirt (RHSA-2018:1929)

RHEL 6 : libvirt (RHSA-2018:3396) (Spectre)

RHEL 6 : libvirt (RHSA-2018:3399) (Spectre)

RHEL 6 : libvirt (RHSA-2018:3400) (Spectre)

RHEL 6 : libvirt (RHSA-2018:3402) (Spectre)

RHEL 6 : libvirt (RHSA-2019:1180) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : libvirt (RHSA-2019:1194) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : libvirt (RHSA-2019:1197) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : libvirt (RHSA-2019:1578)

RHEL 6 : libvncserver (RHSA-2015:0113)

RHEL 6 : libvorbis (RHSA-2018:0649)

RHEL 6 : libvpx (RHSA-2010:0999)

RHEL 6 : libxml2 (RHSA-2011:1749)

RHEL 6 : libxml2 (RHSA-2012:0018)

RHEL 6 : libxml2 (RHSA-2014:0513)

RHEL 6 : libxml2 (RHSA-2015:1419)

RHEL 6 : libxml2 (RHSA-2015:2549)

RHEL 6 : libyaml (RHSA-2014:0415)

RHEL 6 : logrotate (RHSA-2011:0407)

RHEL 6 : luci (RHSA-2013:1603)

RHEL 6 : luci (RHSA-2014:1390)

RHEL 6 : mailman (RHSA-2011:0308)

RHEL 6 : mailman (RHSA-2015:1417)

RHEL 6 : mailman (RHSA-2018:0504)

RHEL 6 : memcached (RHSA-2016:2820)

RHEL 6 : mesa (RHSA-2013:0897)

RHEL 6 : microcode\_ctl (RHSA-2018:0013) (Spectre)

RHEL 6 : microcode\_ctl (RHSA-2018:0036) (Spectre)

RHEL 6 : microcode\_ctl (RHSA-2018:0037) (Spectre)

RHEL 6 : microcode\_ctl (RHSA-2018:0038) (Spectre)

RHEL 6 : microcode\_ctl (RHSA-2018:0039) (Spectre)

RHEL 6 : microcode\_ctl (RHSA-2018:0040) (Spectre)

RHEL 6 : mingw32-libxml2 (RHSA-2013:0217)

RHEL 6 : mod\_auth\_mellon (RHSA-2014:1803)

RHEL 6 : mod\_auth\_mysql (RHSA-2010:1002)

RHEL 6 : mod\_perl (RHSA-2018:2737)

RHEL 6 : mod\_proxy\_fcgi (RHSA-2015:1855)

RHEL 6 : mod\_wsgi (RHSA-2014:0788)

RHEL 6 : mongodb and pymongo (RHSA-2013:1170)

RHEL 6 : MRG (RHSA-2011:1250)

RHEL 6 : MRG (RHSA-2011:1253)

RHEL 6 : MRG (RHSA-2012:0010)

RHEL 6 : MRG (RHSA-2012:0061)

RHEL 6 : MRG (RHSA-2012:0099)

RHEL 6 : MRG (RHSA-2012:0333)

RHEL 6 : MRG (RHSA-2012:0477)

RHEL 6 : MRG (RHSA-2012:0528)

RHEL 6 : MRG (RHSA-2012:0670)

RHEL 6 : MRG (RHSA-2012:1150)

RHEL 6 : MRG (RHSA-2012:1169)

RHEL 6 : MRG (RHSA-2012:1281)

RHEL 6 : MRG (RHSA-2012:1282)

RHEL 6 : MRG (RHSA-2012:1491)

RHEL 6 : MRG (RHSA-2013:0562)

RHEL 6 : MRG (RHSA-2013:0565)

RHEL 6 : MRG (RHSA-2013:0566)

RHEL 6 : MRG (RHSA-2013:0622)

RHEL 6 : MRG (RHSA-2013:0829)

RHEL 6 : MRG (RHSA-2013:1024)

RHEL 6 : MRG (RHSA-2013:1172)

RHEL 6 : MRG (RHSA-2013:1264)

RHEL 6 : MRG (RHSA-2013:1294)

RHEL 6 : MRG (RHSA-2013:1490)

RHEL 6 : MRG (RHSA-2013:1852)

RHEL 6 : MRG (RHSA-2014:0100)

RHEL 6 : MRG (RHSA-2014:0439)

RHEL 6 : MRG (RHSA-2014:0440)

RHEL 6 : MRG (RHSA-2014:0557)

RHEL 6 : MRG (RHSA-2014:0858)

RHEL 6 : MRG (RHSA-2014:1083)

RHEL 6 : MRG (RHSA-2014:1318)

RHEL 6 : MRG (RHSA-2015:0661)

RHEL 6 : MRG (RHSA-2015:0694)

RHEL 6 : MRG (RHSA-2015:0707)

RHEL 6 : MRG (RHSA-2015:0751)

RHEL 6 : MRG (RHSA-2015:0989)

RHEL 6 : MRG (RHSA-2015:1138)

RHEL 6 : MRG (RHSA-2015:1564)

RHEL 6 : MRG (RHSA-2015:1976)

RHEL 6 : MRG (RHSA-2016:0068)

RHEL 6 : MRG (RHSA-2016:0224)

RHEL 6 : MRG (RHSA-2016:1055)

RHEL 6 : MRG (RHSA-2016:1341)

RHEL 6 : MRG (RHSA-2016:1532)

RHEL 6 : MRG (RHSA-2016:1631)

RHEL 6 : MRG (RHSA-2016:1883)

RHEL 6 : MRG (RHSA-2016:2107) (Dirty COW)

RHEL 6 : MRG (RHSA-2017:0113)

RHEL 6 : MRG (RHSA-2017:0402)

RHEL 6 : MRG (RHSA-2017:0932)

RHEL 6 : MRG (RHSA-2017:1297)

RHEL 6 : MRG (RHSA-2017:1647) (Stack Clash)

RHEL 6 : MRG (RHSA-2017:2444)

RHEL 6 : MRG (RHSA-2017:2669)

RHEL 6 : MRG (RHSA-2017:2705) (BlueBorne)

RHEL 6 : MRG (RHSA-2017:2918)

RHEL 6 : MRG (RHSA-2017:3295)

RHEL 6 : MRG (RHSA-2017:3493)

RHEL 6 : MRG (RHSA-2018:0021) (Meltdown) (Spectre)

RHEL 6 : MRG (RHSA-2018:0470)

RHEL 6 : MRG (RHSA-2018:1170)

RHEL 6 : MRG (RHSA-2018:1354)

RHEL 6 : MRG (RHSA-2018:1642) (Spectre)

RHEL 6 : MRG (RHSA-2018:2165)

RHEL 6 : MRG (RHSA-2018:2396) (Foreshadow) (Spectre)

RHEL 6 : MRG (RHSA-2018:2789)

RHEL 6 : MRG (RHSA-2018:3586)

RHEL 6 : MRG (RHSA-2019:0641)

RHEL 6 : MRG (RHSA-2019:1190) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : MRG (RHSA-2019:1487) (SACK Panic) (SACK Slowness)

RHEL 6 : MRG (RHSA-2019:2730)

RHEL 6 : MRG (RHSA-2019:3165)

RHEL 6 : MRG (RHSA-2019:3844)

RHEL 6 : MRG (RHSA-2019:3908)

RHEL 6 : MRG (RHSA-2019:4057)

RHEL 6 : MRG (RHSA-2020:0609)

RHEL 6 : MRG Messaging (RHSA-2012:1279)

RHEL 6 : mutt (RHSA-2011:0959)

RHEL 6 : mutt (RHSA-2014:0304)

RHEL 6 : mysql (RHSA-2011:0164)

RHEL 6 : mysql (RHSA-2012:0105)

RHEL 6 : mysql (RHSA-2012:0874)

RHEL 6 : mysql (RHSA-2012:1462)

RHEL 6 : mysql (RHSA-2012:1551)

RHEL 6 : mysql (RHSA-2013:0219)

RHEL 6 : mysql (RHSA-2013:0772)

RHEL 6 : mysql (RHSA-2014:0164)

RHEL 6 : mysql (RHSA-2017:0184)

RHEL 6 : nagios (RHSA-2017:0259)

RHEL 6 : net-snmp (RHSA-2012:0876)

RHEL 6 : net-snmp (RHSA-2014:0321)

RHEL 6 : net-snmp (RHSA-2015:1385)

RHEL 6 : NetworkManager (RHSA-2011:0930)

RHEL 6 : NetworkManager (RHSA-2011:1338)

RHEL 6 : nfs-utils (RHSA-2011:1534)

RHEL 6 : node.js (RHSA-2015:1545) (POODLE)

RHEL 6 : node.js (RHSA-2015:1546) (POODLE)

RHEL 6 : nspluginwrapper (RHSA-2012:1459)

RHEL 6 : nss (RHSA-2010:0862)

RHEL 6 : nss (RHSA-2013:1840)

RHEL 6 : nss (RHSA-2017:1364)

RHEL 6 : nss (RHSA-2018:2898)

RHEL 6 : nss and nspr (RHSA-2014:0917)

RHEL 6 : nss, nspr, and nss-util (RHSA-2012:1091)

RHEL 6 : nss, nspr, and nss-util (RHSA-2013:1829)

RHEL 6 : nss, nss-util, and nspr (RHSA-2012:0973)

RHEL 6 : nss, nss-util, and nspr (RHSA-2013:0213)

RHEL 6 : nss, nss-util, and nspr (RHSA-2015:2068)

RHEL 6 : nss, nss-util, and nspr (RHSA-2016:0591)

RHEL 6 : nss, nss-util, nss-softokn, and nspr (RHSA-2013:1144)

RHEL 6 : nss-pam-ldapd (RHSA-2013:0590)

RHEL 6 : nss-softokn (RHSA-2019:4152)

RHEL 6 : nss-softokn (RHSA-2020:0466)

RHEL 6 : ntp (RHSA-2015:0104)

RHEL 6 : ntp (RHSA-2015:1459)

RHEL 6 : ntp (RHSA-2015:2520)

RHEL 6 : ntp (RHSA-2016:0780)

RHEL 6 : ntp (RHSA-2016:1552)

RHEL 6 : ntp (RHSA-2017:3071)

RHEL 6 : ntp (RHSA-2018:3853)

RHEL 6 : ntp (RHSA-2018:3854)

RHEL 6 : ocaml (RHSA-2017:0565)

RHEL 6 : openchange (RHSA-2013:0515)

RHEL 6 : openjpeg (RHSA-2012:1068)

RHEL 6 : openjpeg (RHSA-2012:1283)

RHEL 6 : openjpeg (RHSA-2013:1850)

RHEL 6 : openjpeg (RHSA-2017:0559)

RHEL 6 : openldap (RHSA-2011:0347)

RHEL 6 : openldap (RHSA-2012:0899)

RHEL 6 : openldap (RHSA-2012:1151)

RHEL 6 : openldap (RHSA-2014:0126)

RHEL 6 : openoffice.org (RHSA-2011:0183)

RHEL 6 : openshift (RHSA-2013:0220)

RHEL 6 : openshift (RHSA-2013:0582)

RHEL 6 : openshift (RHSA-2013:0638)

RHEL 6 : openshift (RHSA-2014:0487)

RHEL 6 : openshift (RHSA-2014:1796)

RHEL 6 : openshift-console (RHSA-2012:1555)

RHEL 6 : openshift-origin-broker (RHSA-2014:0422)

RHEL 6 : openshift-origin-broker (RHSA-2014:0423)

RHEL 6 : openshift-origin-broker-util (RHSA-2014:0460)

RHEL 6 : openshift-origin-broker-util (RHSA-2014:0461)

RHEL 6 : openshift-origin-node-util (RHSA-2013:0148)

RHEL 6 : openslp (RHSA-2018:2308)

RHEL 6 : openslp (RHSA-2020:0199)

RHEL 6 : openssh (RHSA-2012:0884)

RHEL 6 : openssh (RHSA-2013:0519)

RHEL 6 : openssh (RHSA-2013:1591)

RHEL 6 : openssh (RHSA-2014:1552)

RHEL 6 : openssh (RHSA-2016:0466)

RHEL 6 : openssh (RHSA-2016:0741)

RHEL 6 : openssh (RHSA-2017:0641)

RHEL 6 : openssh (RHSA-2017:2563)

RHEL 6 : openssh (RHSA-2019:0711)

RHEL 6 : openssl (RHSA-2010:0888)

RHEL 6 : openssl (RHSA-2010:0979)

RHEL 6 : openssl (RHSA-2011:0677)

RHEL 6 : openssl (RHSA-2011:1409)

RHEL 6 : openssl (RHSA-2012:0059)

RHEL 6 : openssl (RHSA-2014:0015)

RHEL 6 : openssl (RHSA-2014:0376)

RHEL 6 : openssl (RHSA-2014:0625)

RHEL 6 : openssl (RHSA-2015:0715)

RHEL 6 : openssl (RHSA-2016:0303) (DROWN)

RHEL 6 : openssl (RHSA-2016:0996)

RHEL 6 : openssl (RHSA-2016:2073)

RHEL 6 : openssl (RHSA-2016:2802)

RHEL 6 : openssl (RHSA-2019:2471)

RHEL 6 : openswan (RHSA-2010:0892)

RHEL 6 : openswan (RHSA-2011:1356)

RHEL 6 : pacemaker (RHSA-2013:1635)

RHEL 6 : pacemaker (RHSA-2015:1424)

RHEL 6 : pacemaker (RHSA-2016:2675)

RHEL 6 : pam (RHSA-2010:0891)

RHEL 6 : pam (RHSA-2013:0521)

RHEL 6 : pango (RHSA-2011:0309)

RHEL 6 : patch (RHSA-2018:1199)

RHEL 6 : patch (RHSA-2018:2094)

RHEL 6 : patch (RHSA-2018:2095)

RHEL 6 : patch (RHSA-2018:2096)

RHEL 6 : patch (RHSA-2018:2097)

RHEL 6 : pcs (RHSA-2015:0990)

RHEL 6 : pcs (RHSA-2018:1927)

RHEL 6 : pcsc-lite (RHSA-2013:0525)

RHEL 6 : perl (RHSA-2011:0558)

RHEL 6 : perl (RHSA-2011:1424)

RHEL 6 : php (RHSA-2011:0195)

RHEL 6 : php (RHSA-2012:1046)

RHEL 6 : php (RHSA-2013:0514)

RHEL 6 : php (RHSA-2013:1615)

RHEL 6 : php (RHSA-2015:0021)

RHEL 6 : php (RHSA-2015:1218)

RHEL 6 : php (RHSA-2016:1609) (httpoxy)

RHEL 6 : php (RHSA-2019:3287)

RHEL 6 : php-pear (RHSA-2011:1741)

RHEL 6 : php-pecl-apc (RHSA-2012:0811)

RHEL 6 : pidgin (RHSA-2010:0890)

RHEL 6 : pidgin (RHSA-2011:0616)

RHEL 6 : pidgin (RHSA-2011:1821)

RHEL 6 : piranha (RHSA-2014:0175)

RHEL 6 : pixman (RHSA-2013:0687)

RHEL 6 : pki-core (RHSA-2013:0511)

RHEL 6 : pki-core (RHSA-2015:1347)

RHEL 6 : policycoreutils (RHSA-2011:0414)

RHEL 6 : polkit (RHSA-2011:0455)

RHEL 6 : polkit (RHSA-2013:1270)

RHEL 6 : polkit (RHSA-2019:0420)

RHEL 6 : polkit (RHSA-2019:0832)

RHEL 6 : poppler (RHSA-2010:0859)

RHEL 6 : poppler (RHSA-2017:2550)

RHEL 6 : postfix (RHSA-2011:0423)

RHEL 6 : postgresql (RHSA-2010:0908)

RHEL 6 : postgresql (RHSA-2015:2081)

RHEL 6 : postgresql (RHSA-2016:0347)

RHEL 6 : postgresql (RHSA-2017:2860)

RHEL 6 : postgresql92 in Satellite Server (RHSA-2016:0590)

RHEL 6 : postgresql92 in Satellite Server (RHSA-2016:1060)

RHEL 6 : postgresql92-postgresql (RHSA-2015:0856)

RHEL 6 : ppp (RHSA-2020:0631)

RHEL 6 : procps (RHSA-2018:1777)

RHEL 6 : procps (RHSA-2018:2267)

RHEL 6 : procps (RHSA-2018:2268)

RHEL 6 : python (RHSA-2011:0554)

RHEL 6 : python (RHSA-2012:0744)

RHEL 6 : python (RHSA-2013:1582)

RHEL 6 : python (RHSA-2015:1330)

RHEL 6 : python (RHSA-2019:1467)

RHEL 6 : python-imaging (RHSA-2020:0898)

RHEL 6 : python-jinja2 (RHSA-2014:0747)

RHEL 6 : python-paramiko (RHSA-2018:1124)

RHEL 6 : python-paramiko (RHSA-2018:1125)

RHEL 6 : python-paramiko (RHSA-2018:3406)

RHEL 6 : python-paste-script (RHSA-2012:1206)

RHEL 6 : python-reportlab (RHSA-2020:0197)

RHEL 6 : python-sqlalchemy (RHSA-2012:0369)

RHEL 6 : qemu-kvm (RHSA-2011:0345)

RHEL 6 : qemu-kvm (RHSA-2011:0534)

RHEL 6 : qemu-kvm (RHSA-2011:0919)

RHEL 6 : qemu-kvm (RHSA-2011:1531)

RHEL 6 : qemu-kvm (RHSA-2011:1777)

RHEL 6 : qemu-kvm (RHSA-2011:1801)

RHEL 6 : qemu-kvm (RHSA-2012:0050)

RHEL 6 : qemu-kvm (RHSA-2012:1234)

RHEL 6 : qemu-kvm (RHSA-2013:0609)

RHEL 6 : qemu-kvm (RHSA-2013:0896)

RHEL 6 : qemu-kvm (RHSA-2013:1100)

RHEL 6 : qemu-kvm (RHSA-2013:1553)

RHEL 6 : qemu-kvm (RHSA-2014:0420)

RHEL 6 : qemu-kvm (RHSA-2014:0743)

RHEL 6 : qemu-kvm (RHSA-2014:1075)

RHEL 6 : qemu-kvm (RHSA-2015:0867)

RHEL 6 : qemu-kvm (RHSA-2015:0998) (Venom)

RHEL 6 : qemu-kvm (RHSA-2015:1031) (Venom)

RHEL 6 : qemu-kvm (RHSA-2015:1087)

RHEL 6 : qemu-kvm (RHSA-2015:1833)

RHEL 6 : qemu-kvm (RHSA-2015:1924)

RHEL 6 : qemu-kvm (RHSA-2015:2694)

RHEL 6 : qemu-kvm (RHSA-2016:0082)

RHEL 6 : qemu-kvm (RHSA-2016:0997)

RHEL 6 : qemu-kvm (RHSA-2016:1585)

RHEL 6 : qemu-kvm (RHSA-2017:0309)

RHEL 6 : qemu-kvm (RHSA-2017:0352)

RHEL 6 : qemu-kvm (RHSA-2017:0621)

RHEL 6 : qemu-kvm (RHSA-2017:1206)

RHEL 6 : qemu-kvm (RHSA-2018:0024) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:0103) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:0104) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:0105) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:0106) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:0107) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:0516)

RHEL 6 : qemu-kvm (RHSA-2018:1656) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:1657) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:1658) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:1659) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:1660) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:2162) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:3397) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:3401) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:3424) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2018:3425) (Spectre)

RHEL 6 : qemu-kvm (RHSA-2019:1181) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : qemu-kvm (RHSA-2019:1195) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : qemu-kvm (RHSA-2019:1198) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 6 : qemu-kvm (RHSA-2019:1650)

RHEL 6 : qemu-kvm (RHSA-2019:2892)

RHEL 6 : qemu-kvm (RHSA-2020:0775)

RHEL 6 : qemu-kvm-rhev (RHSA-2012:1233)

RHEL 6 : qemu-kvm-rhev (RHSA-2013:0610)

RHEL 6 : qemu-kvm-rhev (RHSA-2013:0791)

RHEL 6 : qemu-kvm-rhev (RHSA-2014:0421)

RHEL 6 : qemu-kvm-rhev (RHSA-2014:0744)

RHEL 6 : qemu-kvm-rhev (RHSA-2014:1076)

RHEL 6 : qemu-kvm-rhev (RHSA-2015:0868)

RHEL 6 : qemu-kvm-rhev (RHSA-2015:1001) (Venom)

RHEL 6 : qemu-kvm-rhev (RHSA-2015:1088)

RHEL 6 : qemu-kvm-rhev (RHSA-2015:1740)

RHEL 6 : qemu-kvm-rhev (RHSA-2015:1923)

RHEL 6 : qemu-kvm-rhev (RHSA-2015:2696)

RHEL 6 : qemu-kvm-rhev (RHSA-2016:0081)

RHEL 6 : qemu-kvm-rhev (RHSA-2016:1224)

RHEL 6 : qemu-kvm-rhev (RHSA-2016:1586)

RHEL 6 : qemu-kvm-rhev (RHSA-2017:0344)

RHEL 6 : qemu-kvm-rhev (RHSA-2017:0351)

RHEL 6 : qemu-kvm-rhev (RHSA-2017:1205)

RHEL 6 : qemu-kvm-rhev, qemu-kvm-rhev-tools, qemu-img-rhev (RHSA-2013:1754)

RHEL 6 : qpid (RHSA-2012:1269)

RHEL 6 : qt (RHSA-2011:1323)

RHEL 6 : qt (RHSA-2011:1328)

RHEL 6 : qt (RHSA-2012:0880)

RHEL 6 : qt (RHSA-2013:0669)

RHEL 6 : quagga (RHSA-2010:0945)

RHEL 6 : quagga (RHSA-2011:0406)

RHEL 6 : quagga (RHSA-2012:1259)

RHEL 6 : quagga (RHSA-2017:0794)

RHEL 6 : raptor (RHSA-2012:0410)

RHEL 6 : rdma (RHSA-2013:0509)

RHEL 6 : RDMA stack (RHSA-2013:1661)

RHEL 6 : Red Hat JBoss Core Services Apache HTTP Server 2.4.23 (RHSA-2017:3477) (Optionsbleed)

RHEL 6 : Red Hat JBoss Core Services Apache HTTP Server 2.4.29 RHEL 6 (RHSA-2018:2186)

RHEL 6 : Red Hat JBoss Web Server 3.0.3 Service Pack 1 (RHSA-2016:1636) (httpoxy)

RHEL 6 : Red Hat JBoss Web Server 3.1.0 (RHSA-2017:0455)

RHEL 6 : Red Hat OpenShift Enterprise 2.1.9 (RHSA-2014:1906)

RHEL 6 : Red Hat OpenShift Enterprise 2.2.10 (RHSA-2016:1773)

RHEL 6 : Red Hat OpenShift Enterprise 2.2.7 (RHSA-2015:1844)

RHEL 6 : Red Hat OpenShift Enterprise 2.2.8 (RHSA-2015:2666)

RHEL 6 : Red Hat OpenShift Enterprise 2.2.9 (RHSA-2016:0489)

RHEL 6 : Red Hat Satellite IBM Java Runtime (RHSA-2015:0263)

RHEL 6 : Red Hat Single Sign-On 7.2.5 on RHEL 6 (RHSA-2018:3592)

RHEL 6 : Red Hat Single Sign-On 7.2.7 (RHSA-2019:0857)

RHEL 6 : Red Hat Single Sign-On 7.3.4 (RHSA-2019:3044)

RHEL 6 : Red Hat Single Sign-On 7.3.5 (RHSA-2019:4040) (Ping Flood) (Reset Flood) (Settings Flood)

RHEL 6 : Red Hat Single Sign-On 7.3.7 security update on RHEL 6 (Important) (RHSA-2020:0945)

RHEL 6 : redhat-release (EOL Notice) (RHSA-2012:1015)

RHEL 6 : redhat-release (EOL Notice) (RHSA-2012:1417)

RHEL 6 : redhat-release (EOL Notice) (RHSA-2012:1511)

RHEL 6 : redhat-release (EOL Notice) (RHSA-2012:1514)

RHEL 6 : redhat-support-plugin-rhev (RHSA-2014:0224)

RHEL 6 : redhat-support-plugin-rhev (RHSA-2016:0426)

RHEL 6 : resource-agents (RHSA-2011:1580)

RHEL 6 : rh-sso7-keycloak (RHSA-2017:2904)

RHEL 6 : rhev 3.2 - vdsm (RHSA-2013:0886)

RHEL 6 : rhev 3.2.2 - vdsm (RHSA-2013:1155)

RHEL 6 : rhev-3.1.0 vdsm (RHSA-2012:1508)

RHEL 6 : rhev-guest-tools-iso (RHSA-2013:0925)

RHEL 6 : rhev-guest-tools-iso (RHSA-2013:1122)

RHEL 6 : rhev-hypervisor (RHSA-2015:1713)

RHEL 6 : rhev-hypervisor (RHSA-2016:0277)

RHEL 6 : rhev-hypervisor (RHSA-2016:0379) (DROWN)

RHEL 6 : rhev-hypervisor6 (RHSA-2011:1850)

RHEL 6 : rhev-hypervisor6 (RHSA-2012:0109)

RHEL 6 : rhev-hypervisor6 (RHSA-2012:0422)

RHEL 6 : rhev-hypervisor6 (RHSA-2012:0531)

RHEL 6 : rhev-hypervisor6 (RHSA-2012:1200)

RHEL 6 : rhev-hypervisor6 (RHSA-2012:1325)

RHEL 6 : rhev-hypervisor6 (RHSA-2012:1375)

RHEL 6 : rhev-hypervisor6 (RHSA-2012:1505)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:0579)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:0636)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:0746)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:0907)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:1076)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:1181)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:1260)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:1460)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:1527)

RHEL 6 : rhev-hypervisor6 (RHSA-2013:1802)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:0041)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:0339)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:0378) (Heartbleed)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:0396) (Heartbleed)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:0629)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:0815)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:0979)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:1168)

RHEL 6 : rhev-hypervisor6 (RHSA-2014:1354) (Shellshock)

RHEL 6 : rhev-hypervisor6 (RHSA-2015:0126) (GHOST)

RHEL 6 : rhev-hypervisor6 3.4.0 (RHSA-2014:0674)

RHEL 6 : rhevm (RHSA-2012:0421)

RHEL 6 : rhevm (RHSA-2013:1210)

RHEL 6 : rhevm (RHSA-2014:0506)

RHEL 6 : rhevm (RHSA-2014:0814)

RHEL 6 : rhevm (RHSA-2014:1002)

RHEL 6 : rhevm 3.1.2 (RHSA-2013:0211)

RHEL 6 : rhevm-dwh 3.3.3 (RHSA-2014:0559)

RHEL 6 : rhevm-log-collector (RHSA-2014:1947)

RHEL 6 : rhevm-reports 3.3.3 (RHSA-2014:0558)

RHEL 6 : rhevm-setup-plugins (RHSA-2018:0052) (Spectre)

RHEL 6 : rhevm-spice-client (RHSA-2014:0416)

RHEL 6 : rhevm-spice-client (RHSA-2015:0197)

RHEL 6 : rhevm-spice-client (RHSA-2015:0698) (POODLE)

RHEL 6 : rpcbind (RHSA-2017:1267)

RHEL 6 : rsync (RHSA-2011:0390)

RHEL 6 : rsyslog (RHSA-2011:1247)

RHEL 6 : rsyslog (RHSA-2012:0796)

RHEL 6 : rsyslog7 (RHSA-2014:1654)

RHEL 6 : rtkit (RHSA-2013:1282)

RHEL 6 : ruby (RHSA-2011:0910)

RHEL 6 : ruby (RHSA-2011:1581)

RHEL 6 : ruby (RHSA-2012:0069)

RHEL 6 : ruby (RHSA-2013:0612)

RHEL 6 : ruby (RHSA-2013:1764)

RHEL 6 : ruby (RHSA-2013:1767)

RHEL 6 : ruby (RHSA-2014:1911)

RHEL 6 : Ruby on Rails (RHSA-2013:0153)

RHEL 6 : Ruby on Rails in Subscription Asset Manager (RHSA-2013:0154)

RHEL 6 : ruby193-ruby (RHSA-2013:1137)

RHEL 6 : ruby193-ruby, rubygem-json and rubygem-rdoc (RHSA-2013:0701)

RHEL 6 : ruby193-rubygem-activerecord (RHSA-2013:0699)

RHEL 6 : rubygem packages (RHSA-2013:0728)

RHEL 6 : rubygem-actionpack and ruby193-rubygem-actionpack (RHSA-2013:0698)

RHEL 6 : rubygem-activesupport (RHSA-2013:0202)

RHEL 6 : rubygem-activesupport in Subscription Asset Manager (RHSA-2013:0201)

RHEL 6 : rubygem-openshift-origin-console (RHSA-2015:1808)

RHEL 6 : rubygem-openshift-origin-node (RHSA-2014:0529)

RHEL 6 : rubygem-openshift-origin-node (RHSA-2014:0530)

RHEL 6 : rubygem-openshift-origin-node (RHSA-2014:0762)

RHEL 6 : rubygem-openshift-origin-node (RHSA-2014:0763)

RHEL 6 : rubygem-openshift-origin-node (RHSA-2014:0764)

RHEL 6 : rubygem-passenger (RHSA-2013:1136)

RHEL 6 : rubygems (RHSA-2013:1203)

RHEL 6 : rubygems (RHSA-2013:1441)

RHEL 6 : rubygems (RHSA-2014:0207)

RHEL 6 : samba (RHSA-2010:0860)

RHEL 6 : samba (RHSA-2013:1542)

RHEL 6 : samba (RHSA-2015:0251)

RHEL 6 : samba (RHSA-2015:0254)

RHEL 6 : samba (RHSA-2016:0011)

RHEL 6 : samba (RHSA-2016:0611) (Badlock)

RHEL 6 : samba (RHSA-2016:0619) (Badlock)

RHEL 6 : samba (RHSA-2017:0662)

RHEL 6 : samba (RHSA-2017:2789)

RHEL 6 : samba (RHSA-2018:1860)

RHEL 6 : samba (RHSA-2019:4023)

RHEL 6 : samba and cifs-utils (RHSA-2011:1221)

RHEL 6 : samba4 (RHSA-2013:0506)

RHEL 6 : samba4 (RHSA-2013:1543)

RHEL 6 : samba4 (RHSA-2013:1805)

RHEL 6 : samba4 (RHSA-2014:0383)

RHEL 6 : samba4 (RHSA-2014:1009)

RHEL 6 : samba4 (RHSA-2015:0250)

RHEL 6 : samba4 (RHSA-2015:0255)

RHEL 6 : samba4 (RHSA-2016:0010)

RHEL 6 : samba4 (RHSA-2016:0449)

RHEL 6 : samba4 (RHSA-2016:0620) (Badlock)

RHEL 6 : samba4 (RHSA-2016:1487)

RHEL 6 : samba4 (RHSA-2017:0744)

RHEL 6 : samba4 (RHSA-2017:1271) (SambaCry)

RHEL 6 : samba4 (RHSA-2017:2791)

RHEL 6 : samba4 (RHSA-2017:3278)

RHEL 6 : samba4 (RHSA-2018:1883)

RHEL 6 : Satellite Server (RHSA-2015:0033)

RHEL 6 : Satellite Server (RHSA-2015:0957)

RHEL 6 : Satellite Server (RHSA-2015:1592)

RHEL 6 : Satellite Server (RHSA-2016:1484)

RHEL 6 : Satellite Server (RHSA-2017:1558)

RHEL 6 : Satellite Server (RHSA-2017:2645)

RHEL 6 : Satellite Server (RHSA-2017:3453)

RHEL 6 : sblim-cim-client2 (RHSA-2012:0987)

RHEL 6 : setroubleshoot and setroubleshoot-plugins (RHSA-2016:1267)

RHEL 6 : Single Sign-On (RHSA-2017:0872)

RHEL 6 : sos (RHSA-2011:1536)

RHEL 6 : sos (RHSA-2012:0958)

RHEL 6 : sos (RHSA-2016:0152)

RHEL 6 : spacewalk-backend (RHSA-2012:0436)

RHEL 6 : spacewalk-backend (RHSA-2019:1661)

RHEL 6 : spacewalk-backend and spacewalk-proxy (RHSA-2019:1663)

RHEL 6 : spice-gtk (RHSA-2012:1284)

RHEL 6 : spice-gtk (RHSA-2013:1273)

RHEL 6 : spice-gtk (RHSA-2020:0471)

RHEL 6 : spice-gtk and spice-server (RHSA-2018:2732)

RHEL 6 : spice-server (RHSA-2013:1192)

RHEL 6 : spice-server (RHSA-2013:1473)

RHEL 6 : spice-server (RHSA-2015:1715)

RHEL 6 : spice-server (RHSA-2015:1889)

RHEL 6 : spice-server (RHSA-2016:1204)

RHEL 6 : spice-server (RHSA-2017:0253)

RHEL 6 : spice-server (RHSA-2018:3522)

RHEL 6 : spice-server (RHSA-2019:0232)

RHEL 6 : spice-xpi (RHSA-2011:0426)

RHEL 6 : sqlite (RHSA-2015:1634)

RHEL 6 : squid (RHSA-2011:0545)

RHEL 6 : squid (RHSA-2011:1293)

RHEL 6 : squid (RHSA-2011:1791)

RHEL 6 : squid (RHSA-2013:0505)

RHEL 6 : squid (RHSA-2014:0597)

RHEL 6 : squid (RHSA-2016:1138)

RHEL 6 : squid (RHSA-2016:1573)

RHEL 6 : squid34 (RHSA-2016:1140)

RHEL 6 : squid34 (RHSA-2017:0183)

RHEL 6 : sssd (RHSA-2011:0560)

RHEL 6 : sssd (RHSA-2013:0508)

RHEL 6 : sssd (RHSA-2013:0663)

RHEL 6 : sssd (RHSA-2015:2019)

RHEL 6 : sssd and ding-libs (RHSA-2018:1877)

RHEL 6 : Storage Server (RHSA-2013:1205)

RHEL 6 : Storage Server (RHSA-2013:1263)

RHEL 6 : Storage Server (RHSA-2014:0009)

RHEL 6 : Storage Server (RHSA-2014:0377) (Heartbleed)

RHEL 6 : Storage Server (RHSA-2014:0409)

RHEL 6 : Storage Server (RHSA-2014:0628)

RHEL 6 : Storage Server (RHSA-2014:1054)

RHEL 6 : Storage Server (RHSA-2014:1692) (POODLE)

RHEL 6 : Storage Server (RHSA-2015:0256)

RHEL 6 : Storage Server (RHSA-2015:0752)

RHEL 6 : Storage Server (RHSA-2016:0015)

RHEL 6 : Storage Server (RHSA-2016:0329)

RHEL 6 : Storage Server (RHSA-2017:2778)

RHEL 6 : Storage Server (RHSA-2017:3110)

RHEL 6 : Storage Server (RHSA-2018:2612) (deprecated)

RHEL 6 : Storage Server (RHSA-2019:1967)

RHEL 6 : struts (RHSA-2014:0500)

RHEL 6 : stunnel (RHSA-2013:0714)

RHEL 6 : Subscription Asset Manager (RHSA-2013:0544)

RHEL 6 : Subscription Asset Manager (RHSA-2014:1863)

RHEL 6 : subscription-manager (RHSA-2017:0698)

RHEL 6 : subversion (RHSA-2011:0258)

RHEL 6 : subversion (RHSA-2011:0328)

RHEL 6 : subversion (RHSA-2015:0165)

RHEL 6 : subversion (RHSA-2015:1633)

RHEL 6 : sudo (RHSA-2011:0599)

RHEL 6 : sudo (RHSA-2013:1701)

RHEL 6 : sudo (RHSA-2015:1409)

RHEL 6 : sudo (RHSA-2019:3754)

RHEL 6 : sudo (RHSA-2019:3755)

RHEL 6 : sudo (RHSA-2019:3895)

RHEL 6 : sudo (RHSA-2020:0726)

RHEL 6 : swiftonfile (RHSA-2015:1845)

RHEL 6 : swiftonfile (RHSA-2015:1918)

RHEL 6 : system-config-firewall (RHSA-2011:0953)

RHEL 6 : systemtap (RHSA-2011:0842)

RHEL 6 : systemtap (RHSA-2011:1088)

RHEL 6 : t1lib (RHSA-2012:0062)

RHEL 6 : telnet (RHSA-2020:1335)

RHEL 6 : texlive (RHSA-2012:0137)

RHEL 6 : thunderbird (RHSA-2010:0896)

RHEL 6 : thunderbird (RHSA-2010:0969)

RHEL 6 : thunderbird (RHSA-2011:0311)

RHEL 6 : thunderbird (RHSA-2011:0475)

RHEL 6 : thunderbird (RHSA-2011:0886)

RHEL 6 : thunderbird (RHSA-2011:1166)

RHEL 6 : thunderbird (RHSA-2011:1342)

RHEL 6 : thunderbird (RHSA-2011:1439)

RHEL 6 : thunderbird (RHSA-2012:0080)

RHEL 6 : thunderbird (RHSA-2012:0140)

RHEL 6 : thunderbird (RHSA-2018:0647)

RHEL 6 : thunderbird (RHSA-2018:1726)

RHEL 6 : thunderbird (RHSA-2018:2251)

RHEL 6 : thunderbird (RHSA-2018:3403)

RHEL 6 : thunderbird (RHSA-2018:3531)

RHEL 6 : thunderbird (RHSA-2019:0159)

RHEL 6 : thunderbird (RHSA-2019:0269)

RHEL 6 : thunderbird (RHSA-2019:0680)

RHEL 6 : thunderbird (RHSA-2019:1310)

RHEL 6 : thunderbird (RHSA-2019:1624)

RHEL 6 : thunderbird (RHSA-2019:1777)

RHEL 6 : thunderbird (RHSA-2019:2807)

RHEL 6 : thunderbird (RHSA-2019:3756)

RHEL 6 : thunderbird (RHSA-2019:4205)

RHEL 6 : thunderbird (RHSA-2020:0123)

RHEL 6 : thunderbird (RHSA-2020:0574)

RHEL 6 : thunderbird (RHSA-2020:0914)

RHEL 6 : thunderbird (RHSA-2020:1488)

RHEL 6 : tigervnc (RHSA-2011:0871)

RHEL 6 : tigervnc (RHSA-2017:0630)

RHEL 6 : tomcat6 (RHSA-2011:0335)

RHEL 6 : tomcat6 (RHSA-2011:0791)

RHEL 6 : tomcat6 (RHSA-2011:1780)

RHEL 6 : tomcat6 (RHSA-2012:0475)

RHEL 6 : tomcat6 (RHSA-2013:0623)

RHEL 6 : tomcat6 (RHSA-2013:0869)

RHEL 6 : tomcat6 (RHSA-2013:0964)

RHEL 6 : tomcat6 (RHSA-2014:0429)

RHEL 6 : tomcat6 (RHSA-2014:0865)

RHEL 6 : tomcat6 (RHSA-2014:1038)

RHEL 6 : tomcat6 (RHSA-2015:0991)

RHEL 6 : tomcat6 (RHSA-2016:0492)

RHEL 6 : tomcat6 (RHSA-2016:2045) (httpoxy)

RHEL 6 : tomcat6 (RHSA-2017:0527)

RHEL 6 : tomcat6 (RHSA-2017:3080)

RHEL 6 : trousers (RHSA-2014:1507)

RHEL 6 : udisks (RHSA-2014:0293)

RHEL 6 : util-linux-ng (RHSA-2011:1691)

RHEL 6 : util-linux-ng (RHSA-2013:0517)

RHEL 6 : vim (RHSA-2019:1774)

RHEL 6 : vino (RHSA-2013:0169)

RHEL 6 : virt-v2v (RHSA-2011:1615)

RHEL 6 : virtio-win (RHSA-2013:1101)

RHEL 6 : virtio-win (RHSA-2015:1043)

RHEL 6 : Virtualization (RHSA-2018:1688) (Spectre)

RHEL 6 : Virtualization (RHSA-2018:1689) (Spectre)

RHEL 6 : Virtualization Manager (RHSA-2012:1506)

RHEL 6 : Virtualization Manager (RHSA-2012:1537)

RHEL 6 : Virtualization Manager (RHSA-2013:0888)

RHEL 6 : Virtualization Manager (RHSA-2014:0038)

RHEL 6 : Virtualization Manager (RHSA-2014:1161)

RHEL 6 : Virtualization Manager (RHSA-2015:0158)

RHEL 6 : Virtualization Manager (RHSA-2015:0888)

RHEL 6 : Virtualization Manager (RHSA-2016:1929)

RHEL 6 : webkitgtk (RHSA-2011:0177)

RHEL 6 : wget (RHSA-2014:0151)

RHEL 6 : wget (RHSA-2014:1955)

RHEL 6 : wireshark (RHSA-2010:0924)

RHEL 6 : wireshark (RHSA-2011:0369)

RHEL 6 : wireshark (RHSA-2012:0509)

RHEL 6 : wireshark (RHSA-2013:1569)

RHEL 6 : wireshark (RHSA-2014:0342)

RHEL 6 : wireshark (RHSA-2015:1460)

RHEL 6 : wireshark (RHSA-2017:0631)

RHEL 6 : wpa\_supplicant (RHSA-2015:1439)

RHEL 6 : wpa\_supplicant (RHSA-2017:2911) (KRACK)

RHEL 6 : X11 client libraries (RHSA-2014:1436)

RHEL 6 : xerces-c (RHSA-2020:0702)

RHEL 6 : xerces-j2 (RHSA-2011:0858)

RHEL 6 : xinetd (RHSA-2013:0499)

RHEL 6 : xmlrpc3 (RHSA-2018:1779)

RHEL 6 : xorg-x11-drv-qxl (RHSA-2013:0218)

RHEL 6 : xorg-x11-server (RHSA-2012:0939)

RHEL 6 : xorg-x11-server (RHSA-2013:1620)

RHEL 6 : yum-utils (RHSA-2018:2284)

RHEL 6 : zsh (RHSA-2018:1932)

RHEL 6 : zsh (RHSA-2020:0892)

RHEL 7 / 8 : ansible (RHSA-2019:1706)

RHEL 7 / 8 : ansible (RHSA-2019:1708)

RHEL 7 / 8 : Ansible (RHSA-2019:2542)

RHEL 7 / 8 : Ansible (RHSA-2019:3203)

RHEL 7 / 8 : ansible (RHSA-2019:3926)

RHEL 7 / 8 : ansible (RHSA-2019:3927)

RHEL 7 / 8 : ansible (RHSA-2019:3928)

RHEL 7 / 8 : Ansible (RHSA-2020:0215)

RHEL 7 / 8 : Ansible (RHSA-2020:0216)

RHEL 7 / 8 : Ansible (RHSA-2020:0218)

RHEL 7 / 8 : OpenShift Container Platform 4.1 openshift (RHSA-2019:3266)

RHEL 7 / 8 : OpenShift Container Platform 4.1 openshift (RHSA-2019:4087)

RHEL 7 / 8 : OpenShift Container Platform 4.1.11 openshift (RHSA-2019:2504)

RHEL 7 / 8 : OpenShift Container Platform 4.1.17 cri-o (RHSA-2019:2825)

RHEL 7 / 8 : OpenShift Container Platform 4.1.20 golang (RHSA-2019:3131) (Ping Flood) (Reset Flood)

RHEL 7 / 8 : OpenShift Container Platform 4.1.20 openshift (RHSA-2019:3132)

RHEL 7 / 8 : OpenShift Container Platform 4.1.24 openshift (RHSA-2019:3942)

RHEL 7 / 8 : OpenShift Container Platform 4.3.8 openshift-clients (RHSA-2020:0928)

RHEL 7 / 8 : Red Hat OpenShift Container Platform 4.1 openshift RPM (RHSA-2019:2661) (Ping Flood) (Reset Flood)

RHEL 7 / 8 : vim (RHSA-2019:1619)

RHEL 7 : .NET Core (RHSA-2017:3248)

RHEL 7 : .NET Core on Red Hat Enterprise Linux (RHSA-2018:0379)

RHEL 7 : .NET Core on Red Hat Enterprise Linux (RHSA-2018:0522)

RHEL 7 : .NET Core on Red Hat Enterprise Linux (RHSA-2018:2167)

RHEL 7 : 389-ds-base (RHSA-2015:0416)

RHEL 7 : 389-ds-base (RHSA-2015:0895)

RHEL 7 : 389-ds-base (RHSA-2016:0204)

RHEL 7 : 389-ds-base (RHSA-2016:2594)

RHEL 7 : 389-ds-base (RHSA-2017:0920)

RHEL 7 : 389-ds-base (RHSA-2017:2569)

RHEL 7 : 389-ds-base (RHSA-2018:0163)

RHEL 7 : 389-ds-base (RHSA-2018:0414)

RHEL 7 : 389-ds-base (RHSA-2018:1380)

RHEL 7 : 389-ds-base (RHSA-2018:2757)

RHEL 7 : 389-ds-base (RHSA-2018:3127)

RHEL 7 : 389-ds-base (RHSA-2018:3507)

RHEL 7 : 389-ds-base (RHSA-2019:1789)

RHEL 7 : 389-ds-base (RHSA-2019:1896)

RHEL 7 : 389-ds-base (RHSA-2019:3981)

RHEL 7 : abrt (RHSA-2015:1083)

RHEL 7 : abrt and libreport (RHSA-2015:2505)

RHEL 7 : advancecomp (RHSA-2019:2332)

RHEL 7 : advancecomp (RHSA-2020:1037)

RHEL 7 : ansible (RHSA-2017:0515)

RHEL 7 : ansible (RHSA-2017:1499)

RHEL 7 : ansible (RHSA-2017:1685)

RHEL 7 : ansible (RHSA-2017:2524)

RHEL 7 : ansible (RHSA-2017:2966)

RHEL 7 : ansible (RHSA-2018:1949)

RHEL 7 : ansible (RHSA-2018:2022)

RHEL 7 : ansible (RHSA-2018:2150)

RHEL 7 : ansible (RHSA-2018:2151)

RHEL 7 : ansible (RHSA-2018:2152)

RHEL 7 : ansible (RHSA-2018:2166)

RHEL 7 : ansible (RHSA-2018:3460)

RHEL 7 : ansible (RHSA-2018:3461)

RHEL 7 : ansible (RHSA-2018:3462)

RHEL 7 : ansible (RHSA-2018:3463)

RHEL 7 : ansible (RHSA-2018:3770)

RHEL 7 : ansible (RHSA-2018:3771)

RHEL 7 : ansible (RHSA-2018:3772)

RHEL 7 : ansible (RHSA-2018:3773)

RHEL 7 : ansible (RHSA-2018:3835)

RHEL 7 : ansible (RHSA-2018:3836)

RHEL 7 : ansible (RHSA-2018:3837)

RHEL 7 : ansible (RHSA-2018:3838)

RHEL 7 : ansible (RHSA-2019:0430)

RHEL 7 : ansible (RHSA-2019:0431)

RHEL 7 : ansible (RHSA-2019:0432)

RHEL 7 : ansible (RHSA-2019:0433)

RHEL 7 : ansible (RHSA-2019:1705)

RHEL 7 : ansible (RHSA-2019:1707)

RHEL 7 : Ansible (RHSA-2019:2544)

RHEL 7 : Ansible (RHSA-2019:2545)

RHEL 7 : Ansible (RHSA-2019:3201)

RHEL 7 : Ansible (RHSA-2019:3202)

RHEL 7 : ansible (RHSA-2019:3925)

RHEL 7 : Ansible (RHSA-2020:0217)

RHEL 7 : ansible and gdeploy (RHSA-2017:0260)

RHEL 7 : ansible and openshift-ansible (RHSA-2017:0448)

RHEL 7 : ansible and openshift-ansible (RHSA-2017:1244)

RHEL 7 : apache-commons-beanutils (RHSA-2020:0194)

RHEL 7 : apache-commons-collections (RHSA-2015:2522)

RHEL 7 : atomic-openshift (RHSA-2016:1427)

RHEL 7 : atomic-openshift (RHSA-2016:2064)

RHEL 7 : atomic-openshift (RHSA-2016:2696)

RHEL 7 : atomic-openshift (RHSA-2016:2915)

RHEL 7 : atomic-openshift-utils (RHSA-2016:2778)

RHEL 7 : augeas (RHSA-2017:2788)

RHEL 7 : augeas (RHSA-2019:2403)

RHEL 7 : authconfig (RHSA-2017:2285)

RHEL 7 : autofs (RHSA-2015:2417)

RHEL 7 : avahi (RHSA-2020:1176)

RHEL 7 : bash (RHSA-2017:1931)

RHEL 7 : bash (RHSA-2020:1113)

RHEL 7 : bind (RHSA-2015:0672)

RHEL 7 : bind (RHSA-2015:1443)

RHEL 7 : bind (RHSA-2016:2615)

RHEL 7 : bind (RHSA-2017:0062)

RHEL 7 : bind (RHSA-2017:0276)

RHEL 7 : bind (RHSA-2017:1095)

RHEL 7 : bind (RHSA-2017:1583)

RHEL 7 : bind (RHSA-2017:1680)

RHEL 7 : bind (RHSA-2017:2533)

RHEL 7 : bind (RHSA-2018:0102)

RHEL 7 : bind (RHSA-2018:0488)

RHEL 7 : bind (RHSA-2018:2570)

RHEL 7 : bind (RHSA-2019:0194)

RHEL 7 : bind (RHSA-2019:1294)

RHEL 7 : bind (RHSA-2019:2057)

RHEL 7 : bind (RHSA-2019:2698)

RHEL 7 : bind (RHSA-2019:2977)

RHEL 7 : bind (RHSA-2020:1061)

RHEL 7 : binutils (RHSA-2015:2079)

RHEL 7 : binutils (RHSA-2018:3032)

RHEL 7 : binutils (RHSA-2019:2075)

RHEL 7 : blktrace (RHSA-2019:2162)

RHEL 7 : bluez (RHSA-2020:1101)

RHEL 7 : buildah (RHSA-2020:1231)

RHEL 7 : ceph (RHSA-2016:1384)

RHEL 7 : ceph (RHSA-2018:0546)

RHEL 7 : ceph (RHSA-2019:2577)

RHEL 7 : ceph-iscsi-cli (RHSA-2018:2837)

RHEL 7 : ceph-iscsi-cli (RHSA-2018:2838)

RHEL 7 : chrony (RHSA-2015:2241)

RHEL 7 : cloud-init (RHSA-2019:0597)

RHEL 7 : CloudForms (RHSA-2019:0796)

RHEL 7 : clutter (RHSA-2015:1510)

RHEL 7 : cockpit (RHSA-2019:0482)

RHEL 7 : collectd (RHSA-2017:1285)

RHEL 7 : collectd (RHSA-2018:0560)

RHEL 7 : compat-libtiff3 (RHSA-2019:2051)

RHEL 7 : containernetworking-plugins (RHSA-2020:0406) (Ping Flood) (Reset Flood)

RHEL 7 : corosync (RHSA-2018:1169)

RHEL 7 : cpio (RHSA-2015:2108)

RHEL 7 : cups (RHSA-2020:1050)

RHEL 7 : cups-filters (RHSA-2014:1795)

RHEL 7 : cups-filters (RHSA-2015:2360)

RHEL 7 : curl (RHSA-2015:2159)

RHEL 7 : curl (RHSA-2016:2575)

RHEL 7 : curl (RHSA-2017:2016)

RHEL 7 : curl (RHSA-2017:3263)

RHEL 7 : curl (RHSA-2019:1880)

RHEL 7 : curl (RHSA-2019:2181)

RHEL 7 : curl (RHSA-2020:0544)

RHEL 7 : curl (RHSA-2020:0594)

RHEL 7 : curl (RHSA-2020:1020)

RHEL 7 : curl and nss-pem (RHSA-2018:3157)

RHEL 7 : dhcp (RHSA-2016:2590)

RHEL 7 : dhcp (RHSA-2018:0158)

RHEL 7 : dhcp (RHSA-2018:0483)

RHEL 7 : dhcp (RHSA-2018:1453)

RHEL 7 : dhcp (RHSA-2018:1455)

RHEL 7 : dhcp (RHSA-2018:1456)

RHEL 7 : dhcp (RHSA-2018:1457)

RHEL 7 : dhcp (RHSA-2019:2060)

RHEL 7 : dnsmasq (RHSA-2017:2836)

RHEL 7 : dnsmasq (RHSA-2017:2837)

RHEL 7 : docker (RHSA-2014:0820)

RHEL 7 : docker (RHSA-2015:0623)

RHEL 7 : docker (RHSA-2015:0776)

RHEL 7 : docker (RHSA-2016:1034)

RHEL 7 : docker (RHSA-2016:2634)

RHEL 7 : docker (RHSA-2017:0116)

RHEL 7 : docker (RHSA-2018:2482)

RHEL 7 : docker (RHSA-2019:0304)

RHEL 7 : docker (RHSA-2019:0487)

RHEL 7 : docker (RHSA-2019:1910)

RHEL 7 : docker (RHSA-2020:1234)

RHEL 7 : docker-distribution (RHSA-2017:2603)

RHEL 7 : docker-latest (RHSA-2017:0123)

RHEL 7 : dotNET (RHSA-2018:2684)

RHEL 7 : dotNET (RHSA-2018:2902)

RHEL 7 : dotNET (RHSA-2018:3676)

RHEL 7 : dotNET (RHSA-2019:0040)

RHEL 7 : dotNET (RHSA-2019:0349)

RHEL 7 : dotNET (RHSA-2019:0544)

RHEL 7 : dotNET (RHSA-2019:1236)

RHEL 7 : dotNET (RHSA-2019:2732)

RHEL 7 : dotNET (RHSA-2020:0134)

RHEL 7 : dovecot (RHSA-2019:2836)

RHEL 7 : dovecot (RHSA-2020:1062)

RHEL 7 : doxygen (RHSA-2020:1034)

RHEL 7 : dpdk (RHSA-2018:2038)

RHEL 7 : dpdk (RHSA-2020:1226)

RHEL 7 : elfutils (RHSA-2019:2197)

RHEL 7 : elfutils (RHSA-2020:1471)

RHEL 7 : emacs (RHSA-2017:2771)

RHEL 7 : etcd (RHSA-2019:0237) (deprecated)

RHEL 7 : etcd (RHSA-2019:1352)

RHEL 7 : evince (RHSA-2017:2388)

RHEL 7 : evolution (RHSA-2020:1080)

RHEL 7 : exempi (RHSA-2019:2048)

RHEL 7 : exiv2 (RHSA-2019:2101)

RHEL 7 : expat (RHSA-2020:1011)

RHEL 7 : fence-agents (RHSA-2019:2037)

RHEL 7 : file (RHSA-2015:2155)

RHEL 7 : file (RHSA-2020:1022)

RHEL 7 : firefox (RHSA-2017:0461)

RHEL 7 : firefox (RHSA-2017:0558)

RHEL 7 : firefox (RHSA-2017:1106)

RHEL 7 : firefox (RHSA-2018:0527)

RHEL 7 : firefox (RHSA-2018:1099)

RHEL 7 : firefox (RHSA-2018:1415)

RHEL 7 : firefox (RHSA-2018:2113)

RHEL 7 : firefox (RHSA-2018:2692)

RHEL 7 : firefox (RHSA-2018:2835)

RHEL 7 : firefox (RHSA-2018:2884)

RHEL 7 : firefox (RHSA-2018:3005)

RHEL 7 : firefox (RHSA-2018:3833)

RHEL 7 : firefox (RHSA-2019:0219)

RHEL 7 : firefox (RHSA-2019:0374)

RHEL 7 : firefox (RHSA-2019:0622)

RHEL 7 : firefox (RHSA-2019:0671)

RHEL 7 : firefox (RHSA-2019:1265)

RHEL 7 : firefox (RHSA-2019:1603)

RHEL 7 : firefox (RHSA-2019:1763)

RHEL 7 : firefox (RHSA-2019:2729)

RHEL 7 : firefox (RHSA-2019:3193)

RHEL 7 : firefox (RHSA-2019:4107)

RHEL 7 : firefox (RHSA-2020:0085)

RHEL 7 : firefox (RHSA-2020:0520)

RHEL 7 : firefox (RHSA-2020:0815)

RHEL 7 : firefox (RHSA-2020:1338)

RHEL 7 : firefox (RHSA-2020:1420)

RHEL 7 : firewalld (RHSA-2016:2597)

RHEL 7 : flatpak (RHSA-2018:2766)

RHEL 7 : flatpak (RHSA-2019:0375)

RHEL 7 : flatpak (RHSA-2019:1024)

RHEL 7 : fontconfig (RHSA-2016:2601)

RHEL 7 : freeradius (RHSA-2017:1581)

RHEL 7 : freeradius (RHSA-2017:2389)

RHEL 7 : freeradius (RHSA-2019:1131)

RHEL 7 : freerdp (RHSA-2019:0697)

RHEL 7 : freerdp and vinagre (RHSA-2019:2157)

RHEL 7 : freetype (RHSA-2015:0696)

RHEL 7 : fribidi (RHSA-2019:4326)

RHEL 7 : fuse (RHSA-2018:3324)

RHEL 7 : gcab (RHSA-2018:0350)

RHEL 7 : gcc (RHSA-2018:0849)

RHEL 7 : gdm and gnome-session (RHSA-2017:2128)

RHEL 7 : gettext (RHSA-2020:1138)

RHEL 7 : ghostscript (RHSA-2017:0013)

RHEL 7 : ghostscript (RHSA-2017:2180)

RHEL 7 : ghostscript (RHSA-2018:2918)

RHEL 7 : ghostscript (RHSA-2018:3650)

RHEL 7 : ghostscript (RHSA-2018:3761)

RHEL 7 : ghostscript (RHSA-2018:3834)

RHEL 7 : ghostscript (RHSA-2019:0229)

RHEL 7 : ghostscript (RHSA-2019:0633)

RHEL 7 : ghostscript (RHSA-2019:1017)

RHEL 7 : ghostscript (RHSA-2019:2281)

RHEL 7 : ghostscript (RHSA-2019:2462)

RHEL 7 : ghostscript (RHSA-2019:2586)

RHEL 7 : ghostscript (RHSA-2019:3888)

RHEL 7 : gimp (RHSA-2016:2589)

RHEL 7 : git (RHSA-2015:2561)

RHEL 7 : git (RHSA-2017:2004)

RHEL 7 : git (RHSA-2017:2484)

RHEL 7 : git (RHSA-2018:1957)

RHEL 7 : git (RHSA-2018:3408)

RHEL 7 : git (RHSA-2020:0124)

RHEL 7 : glibc (RHSA-2014:2023)

RHEL 7 : glibc (RHSA-2015:0327)

RHEL 7 : glibc (RHSA-2015:2172)

RHEL 7 : glibc (RHSA-2015:2199)

RHEL 7 : glibc (RHSA-2015:2589)

RHEL 7 : glibc (RHSA-2016:0176)

RHEL 7 : glibc (RHSA-2016:2573)

RHEL 7 : glibc (RHSA-2017:1481) (Stack Clash)

RHEL 7 : glibc (RHSA-2017:1916)

RHEL 7 : glibc (RHSA-2018:0805)

RHEL 7 : glibc (RHSA-2018:3092)

RHEL 7 : glibc (RHSA-2019:2118)

RHEL 7 : Gluster Storage (RHSA-2017:0486)

RHEL 7 : Gluster Storage (RHSA-2017:0495)

RHEL 7 : Gluster Storage (RHSA-2018:2607)

RHEL 7 : Gluster Storage Server (RHSA-2019:3253)

RHEL 7 : glusterfs (RHSA-2018:1269)

RHEL 7 : glusterfs (RHSA-2018:1954)

RHEL 7 : glusterfs (RHSA-2018:3242)

RHEL 7 : glusterfs (RHSA-2018:3432)

RHEL 7 : GNOME (RHSA-2018:3140)

RHEL 7 : GNOME (RHSA-2020:1021)

RHEL 7 : GNOME Shell (RHSA-2015:0535)

RHEL 7 : gnupg2 (RHSA-2018:2181)

RHEL 7 : gnutls (RHSA-2014:0684)

RHEL 7 : gnutls (RHSA-2014:1846)

RHEL 7 : gnutls (RHSA-2017:2292)

RHEL 7 : gnutls (RHSA-2018:3050)

RHEL 7 : go-toolset-1.11 and go-toolset-1.11-golang (RHSA-2019:2682) (Ping Flood) (Reset Flood)

RHEL 7 : go-toolset-1.11-golang (RHSA-2019:1300)

RHEL 7 : go-toolset-1.12-golang (RHSA-2020:0101)

RHEL 7 : go-toolset-7 and go-toolset-7-golang (RHSA-2017:3463)

RHEL 7 : go-toolset-7 and go-toolset-7-golang (RHSA-2018:1304)

RHEL 7 : golang (RHSA-2016:1538) (httpoxy)

RHEL 7 : golang (RHSA-2017:1859)

RHEL 7 : golang (RHSA-2018:0878)

RHEL 7 : grafana (RHSA-2019:0019)

RHEL 7 : graphite2 (RHSA-2016:0594)

RHEL 7 : graphite2 (RHSA-2017:1793)

RHEL 7 : grep (RHSA-2015:2111)

RHEL 7 : groovy (RHSA-2017:2486)

RHEL 7 : grub2 (RHSA-2015:2401)

RHEL 7 : grub2 (RHSA-2015:2623)

RHEL 7 : GStreamer (RHSA-2017:2060)

RHEL 7 : gstreamer-plugins-bad-free (RHSA-2017:0018)

RHEL 7 : gstreamer-plugins-good (RHSA-2017:0019)

RHEL 7 : gstreamer1-plugins-bad-free (RHSA-2017:0021)

RHEL 7 : gstreamer1-plugins-good (RHSA-2017:0020)

RHEL 7 : gtk-vnc (RHSA-2017:2258)

RHEL 7 : gvfs (RHSA-2019:2145)

RHEL 7 : haproxy (RHSA-2014:1292)

RHEL 7 : heketi (RHSA-2017:3481)

RHEL 7 : heketi (RHSA-2019:3255)

RHEL 7 : hivex (RHSA-2015:0301)

RHEL 7 : http-parser (RHSA-2019:2258)

RHEL 7 : http-parser (RHSA-2020:0703)

RHEL 7 : httpcomponents-client (RHSA-2014:1146)

RHEL 7 : httpd (RHSA-2014:0921)

RHEL 7 : httpd (RHSA-2015:0325)

RHEL 7 : httpd (RHSA-2015:1667)

RHEL 7 : httpd (RHSA-2016:1422) (httpoxy)

RHEL 7 : httpd (RHSA-2017:0906)

RHEL 7 : httpd (RHSA-2017:2479)

RHEL 7 : httpd (RHSA-2017:2882) (Optionsbleed)

RHEL 7 : httpd (RHSA-2017:3193) (Optionsbleed)

RHEL 7 : httpd (RHSA-2017:3194) (Optionsbleed)

RHEL 7 : httpd (RHSA-2019:1898)

RHEL 7 : httpd (RHSA-2019:2343)

RHEL 7 : httpd (RHSA-2020:1121)

RHEL 7 : icedtea-web (RHSA-2019:2003)

RHEL 7 : icoutils (RHSA-2017:0837)

RHEL 7 : icu (RHSA-2020:0897)

RHEL 7 : ImageMagick (RHSA-2020:1180)

RHEL 7 : ipa (RHSA-2015:0442)

RHEL 7 : ipa (RHSA-2017:0001)

RHEL 7 : ipa (RHSA-2017:0388)

RHEL 7 : ipa (RHSA-2020:0378)

RHEL 7 : ipa and slapi-nis (RHSA-2015:0728)

RHEL 7 : ipmitool (RHSA-2020:0984)

RHEL 7 : ipmitool (RHSA-2020:1486)

RHEL 7 : ipsilon (RHSA-2016:2809)

RHEL 7 : jasper (RHSA-2018:3253)

RHEL 7 : java-1.6.0-openjdk (RHSA-2014:0685)

RHEL 7 : java-1.6.0-sun (RHSA-2018:1205)

RHEL 7 : java-1.6.0-sun (RHSA-2018:3007)

RHEL 7 : java-1.7.0-openjdk (RHSA-2014:0675)

RHEL 7 : java-1.7.0-openjdk (RHSA-2018:1278)

RHEL 7 : java-1.7.0-openjdk (RHSA-2018:1648) (Spectre)

RHEL 7 : java-1.7.0-openjdk (RHSA-2018:2286)

RHEL 7 : java-1.7.0-openjdk (RHSA-2018:3350)

RHEL 7 : java-1.7.0-openjdk (RHSA-2019:0464)

RHEL 7 : java-1.7.0-openjdk (RHSA-2019:0791)

RHEL 7 : java-1.7.0-openjdk (RHSA-2019:1839)

RHEL 7 : java-1.7.0-openjdk (RHSA-2019:3157)

RHEL 7 : java-1.7.0-openjdk (RHSA-2020:0541)

RHEL 7 : java-1.7.0-oracle (RHSA-2018:1201)

RHEL 7 : java-1.7.0-oracle (RHSA-2018:2254)

RHEL 7 : java-1.7.0-oracle (RHSA-2018:3001)

RHEL 7 : java-1.7.1-ibm (RHSA-2014:0705)

RHEL 7 : java-1.7.1-ibm (RHSA-2014:1042)

RHEL 7 : java-1.7.1-ibm (RHSA-2018:0458)

RHEL 7 : java-1.7.1-ibm (RHSA-2018:1723)

RHEL 7 : java-1.7.1-ibm (RHSA-2018:2569)

RHEL 7 : java-1.7.1-ibm (RHSA-2018:3672)

RHEL 7 : java-1.7.1-ibm (RHSA-2019:0473)

RHEL 7 : java-1.7.1-ibm (RHSA-2019:1166)

RHEL 7 : java-1.7.1-ibm (RHSA-2019:2495)

RHEL 7 : java-1.7.1-ibm (RHSA-2019:4110)

RHEL 7 : java-1.7.1-ibm (RHSA-2020:0468)

RHEL 7 : java-1.8.0-ibm (RHSA-2015:2509)

RHEL 7 : java-1.8.0-ibm (RHSA-2016:0098) (SLOTH)

RHEL 7 : java-1.8.0-ibm (RHSA-2016:0716)

RHEL 7 : java-1.8.0-ibm (RHSA-2017:3264)

RHEL 7 : java-1.8.0-ibm (RHSA-2018:0351)

RHEL 7 : java-1.8.0-ibm (RHSA-2018:1721)

RHEL 7 : java-1.8.0-ibm (RHSA-2018:2568)

RHEL 7 : java-1.8.0-ibm (RHSA-2018:3534)

RHEL 7 : java-1.8.0-ibm (RHSA-2019:0472)

RHEL 7 : java-1.8.0-ibm (RHSA-2019:1164)

RHEL 7 : java-1.8.0-ibm (RHSA-2019:2585)

RHEL 7 : java-1.8.0-ibm (RHSA-2019:4115)

RHEL 7 : java-1.8.0-ibm (RHSA-2020:0470)

RHEL 7 : java-1.8.0-openjdk (RHSA-2016:0049) (SLOTH)

RHEL 7 : java-1.8.0-openjdk (RHSA-2016:0513)

RHEL 7 : java-1.8.0-openjdk (RHSA-2016:0650)

RHEL 7 : java-1.8.0-openjdk (RHSA-2017:1108)

RHEL 7 : java-1.8.0-openjdk (RHSA-2018:1191)

RHEL 7 : java-1.8.0-openjdk (RHSA-2018:1649) (Spectre)

RHEL 7 : java-1.8.0-openjdk (RHSA-2018:2242)

RHEL 7 : java-1.8.0-openjdk (RHSA-2018:2942)

RHEL 7 : java-1.8.0-openjdk (RHSA-2019:0435)

RHEL 7 : java-1.8.0-openjdk (RHSA-2019:0775)

RHEL 7 : java-1.8.0-openjdk (RHSA-2019:1815)

RHEL 7 : java-1.8.0-openjdk (RHSA-2019:3128)

RHEL 7 : java-1.8.0-openjdk (RHSA-2020:0196)

RHEL 7 : java-1.8.0-oracle (RHSA-2018:1204)

RHEL 7 : java-1.8.0-oracle (RHSA-2018:2253)

RHEL 7 : java-1.8.0-oracle (RHSA-2018:3002)

RHEL 7 : java-11-openjdk (RHSA-2018:3521)

RHEL 7 : java-11-openjdk (RHSA-2019:0436)

RHEL 7 : java-11-openjdk (RHSA-2019:0778)

RHEL 7 : java-11-openjdk (RHSA-2019:1810)

RHEL 7 : java-11-openjdk (RHSA-2019:3127)

RHEL 7 : java-11-openjdk (RHSA-2020:0122)

RHEL 7 : JBoss Core Services (RHSA-2017:0194)

RHEL 7 : JBoss Core Services (RHSA-2017:1413)

RHEL 7 : JBoss Core Services (RHSA-2017:2709)

RHEL 7 : JBoss Core Services (RHSA-2019:3933) (0-Length Headers Leak) (Data Dribble) (Internal Data Buffering) (Resource Loop)

RHEL 7 : JBoss EAP (RHSA-2014:1287)

RHEL 7 : JBoss EAP (RHSA-2014:1822)

RHEL 7 : JBoss EAP (RHSA-2015:0218)

RHEL 7 : JBoss EAP (RHSA-2015:0848)

RHEL 7 : JBoss EAP (RHSA-2015:1671)

RHEL 7 : JBoss EAP (RHSA-2015:1906)

RHEL 7 : JBoss EAP (RHSA-2015:2540)

RHEL 7 : JBoss EAP (RHSA-2016:0123)

RHEL 7 : JBoss EAP (RHSA-2016:0597)

RHEL 7 : JBoss EAP (RHSA-2016:1434)

RHEL 7 : JBoss EAP (RHSA-2016:1839)

RHEL 7 : JBoss EAP (RHSA-2016:2054)

RHEL 7 : JBoss EAP (RHSA-2016:2069)

RHEL 7 : JBoss EAP (RHSA-2016:2641)

RHEL 7 : JBoss EAP (RHSA-2017:0171)

RHEL 7 : JBoss EAP (RHSA-2017:0245)

RHEL 7 : JBoss EAP (RHSA-2017:0828)

RHEL 7 : JBoss EAP (RHSA-2017:0832)

RHEL 7 : JBoss EAP (RHSA-2017:1253)

RHEL 7 : JBoss EAP (RHSA-2017:1411)

RHEL 7 : JBoss EAP (RHSA-2017:1548)

RHEL 7 : JBoss EAP (RHSA-2017:1835)

RHEL 7 : JBoss EAP (RHSA-2017:2636)

RHEL 7 : JBoss EAP (RHSA-2017:2808)

RHEL 7 : JBoss EAP (RHSA-2017:3218)

RHEL 7 : JBoss EAP (RHSA-2017:3455)

RHEL 7 : JBoss EAP (RHSA-2018:0004)

RHEL 7 : JBoss EAP (RHSA-2018:0268)

RHEL 7 : JBoss EAP (RHSA-2018:0480)

RHEL 7 : JBoss EAP (RHSA-2018:1247)

RHEL 7 : JBoss EAP (RHSA-2018:1448)

RHEL 7 : JBoss EAP (RHSA-2018:2089)

RHEL 7 : JBoss EAP (RHSA-2018:2424)

RHEL 7 : JBoss EAP (RHSA-2018:2741)

RHEL 7 : JBoss EAP (RHSA-2018:3528)

RHEL 7 : JBoss EAP (RHSA-2019:0137)

RHEL 7 : JBoss EAP (RHSA-2019:0365)

RHEL 7 : JBoss EAP (RHSA-2019:1108)

RHEL 7 : JBoss EAP (RHSA-2019:1161)

RHEL 7 : JBoss EAP (RHSA-2019:1420)

RHEL 7 : JBoss EAP (RHSA-2019:2936)

RHEL 7 : JBoss EAP (RHSA-2019:4019) (Data Dribble) (Ping Flood) (Reset Flood) (Settings Flood)

RHEL 7 : JBoss EAP (RHSA-2020:0160)

RHEL 7 : JBoss EAP (RHSA-2020:0805)

RHEL 7 : JBoss Web Server (RHSA-2015:2660)

RHEL 7 : JBoss Web Server (RHSA-2016:1088)

RHEL 7 : JBoss Web Server (RHSA-2016:1648) (httpoxy)

RHEL 7 : jenkins (RHSA-2016:0711)

RHEL 7 : jenkins (RHSA-2016:1206)

RHEL 7 : json-c (RHSA-2014:0703)

RHEL 7 : jss (RHSA-2019:3067)

RHEL 7 : jss (RHSA-2019:3225)

RHEL 7 : kde-workspace (RHSA-2019:2141)

RHEL 7 : kdelibs (RHSA-2017:1264)

RHEL 7 : kdelibs and kde-settings (RHSA-2019:2606)

RHEL 7 : kdenetwork (RHSA-2014:1827)

RHEL 7 : keepalived (RHSA-2019:0022)

RHEL 7 : keepalived (RHSA-2019:1792)

RHEL 7 : keepalived (RHSA-2019:1945)

RHEL 7 : keepalived (RHSA-2019:2285)

RHEL 7 : kernel (RHSA-2014:0678)

RHEL 7 : kernel (RHSA-2014:0786)

RHEL 7 : kernel (RHSA-2014:0923)

RHEL 7 : kernel (RHSA-2014:1023)

RHEL 7 : kernel (RHSA-2014:1281)

RHEL 7 : kernel (RHSA-2014:1724)

RHEL 7 : kernel (RHSA-2014:1971)

RHEL 7 : kernel (RHSA-2014:2010)

RHEL 7 : kernel (RHSA-2015:0102)

RHEL 7 : kernel (RHSA-2015:0290)

RHEL 7 : kernel (RHSA-2015:0726)

RHEL 7 : kernel (RHSA-2015:0987)

RHEL 7 : kernel (RHSA-2015:1137)

RHEL 7 : kernel (RHSA-2015:1534)

RHEL 7 : kernel (RHSA-2015:1778)

RHEL 7 : kernel (RHSA-2015:1978)

RHEL 7 : kernel (RHSA-2015:2152)

RHEL 7 : kernel (RHSA-2015:2552)

RHEL 7 : kernel (RHSA-2015:2587)

RHEL 7 : kernel (RHSA-2016:0064)

RHEL 7 : kernel (RHSA-2016:0103)

RHEL 7 : kernel (RHSA-2016:0185)

RHEL 7 : kernel (RHSA-2016:1033)

RHEL 7 : kernel (RHSA-2016:1277)

RHEL 7 : kernel (RHSA-2016:1395)

RHEL 7 : kernel (RHSA-2016:1539)

RHEL 7 : kernel (RHSA-2016:1633)

RHEL 7 : kernel (RHSA-2016:1657)

RHEL 7 : kernel (RHSA-2016:1847)

RHEL 7 : kernel (RHSA-2016:2047)

RHEL 7 : kernel (RHSA-2016:2098) (Dirty COW)

RHEL 7 : kernel (RHSA-2016:2118) (Dirty COW)

RHEL 7 : kernel (RHSA-2016:2574)

RHEL 7 : kernel (RHSA-2016:2695)

RHEL 7 : kernel (RHSA-2017:0004)

RHEL 7 : kernel (RHSA-2017:0086)

RHEL 7 : kernel (RHSA-2017:0217)

RHEL 7 : kernel (RHSA-2017:0270)

RHEL 7 : kernel (RHSA-2017:0294)

RHEL 7 : kernel (RHSA-2017:0386)

RHEL 7 : kernel (RHSA-2017:0403)

RHEL 7 : kernel (RHSA-2017:0501)

RHEL 7 : kernel (RHSA-2017:0933)

RHEL 7 : kernel (RHSA-2017:1125)

RHEL 7 : kernel (RHSA-2017:1308)

RHEL 7 : kernel (RHSA-2017:1484) (Stack Clash)

RHEL 7 : kernel (RHSA-2017:1485) (Stack Clash)

RHEL 7 : kernel (RHSA-2017:1615)

RHEL 7 : kernel (RHSA-2017:1766)

RHEL 7 : kernel (RHSA-2017:1842) (Stack Clash)

RHEL 7 : kernel (RHSA-2017:2437)

RHEL 7 : kernel (RHSA-2017:2473)

RHEL 7 : kernel (RHSA-2017:2679) (BlueBorne)

RHEL 7 : kernel (RHSA-2017:2680) (BlueBorne)

RHEL 7 : kernel (RHSA-2017:2706) (BlueBorne)

RHEL 7 : kernel (RHSA-2017:2770)

RHEL 7 : kernel (RHSA-2017:2793)

RHEL 7 : kernel (RHSA-2017:2794)

RHEL 7 : kernel (RHSA-2017:2869)

RHEL 7 : kernel (RHSA-2017:2930)

RHEL 7 : kernel (RHSA-2017:3315)

RHEL 7 : kernel (RHSA-2018:0007) (Meltdown) (Spectre)

RHEL 7 : kernel (RHSA-2018:0009) (Meltdown) (Spectre)

RHEL 7 : kernel (RHSA-2018:0010) (Meltdown) (Spectre)

RHEL 7 : kernel (RHSA-2018:0151) (Meltdown) (Spectre)

RHEL 7 : kernel (RHSA-2018:0182) (Meltdown) (Spectre)

RHEL 7 : kernel (RHSA-2018:0395)

RHEL 7 : kernel (RHSA-2018:0399)

RHEL 7 : kernel (RHSA-2018:1062)

RHEL 7 : kernel (RHSA-2018:1129) (Meltdown) (Spectre)

RHEL 7 : kernel (RHSA-2018:1130)

RHEL 7 : kernel (RHSA-2018:1216)

RHEL 7 : kernel (RHSA-2018:1318)

RHEL 7 : kernel (RHSA-2018:1345)

RHEL 7 : kernel (RHSA-2018:1347)

RHEL 7 : kernel (RHSA-2018:1348)

RHEL 7 : kernel (RHSA-2018:1629) (Spectre)

RHEL 7 : kernel (RHSA-2018:1635) (Spectre)

RHEL 7 : kernel (RHSA-2018:1636) (Spectre)

RHEL 7 : kernel (RHSA-2018:1637) (Spectre)

RHEL 7 : kernel (RHSA-2018:1737) (Spectre)

RHEL 7 : kernel (RHSA-2018:1738) (Spectre)

RHEL 7 : kernel (RHSA-2018:1852)

RHEL 7 : kernel (RHSA-2018:1965) (Spectre)

RHEL 7 : kernel (RHSA-2018:2161) (Spectre)

RHEL 7 : kernel (RHSA-2018:2216) (Spectre)

RHEL 7 : kernel (RHSA-2018:2384) (Foreshadow)

RHEL 7 : kernel (RHSA-2018:2387) (Foreshadow) (Spectre)

RHEL 7 : kernel (RHSA-2018:2388) (Foreshadow)

RHEL 7 : kernel (RHSA-2018:2389) (Foreshadow)

RHEL 7 : kernel (RHSA-2018:2748)

RHEL 7 : kernel (RHSA-2018:2776)

RHEL 7 : kernel (RHSA-2018:2785)

RHEL 7 : kernel (RHSA-2018:2790)

RHEL 7 : kernel (RHSA-2018:3083)

RHEL 7 : kernel (RHSA-2018:3459)

RHEL 7 : kernel (RHSA-2018:3540)

RHEL 7 : kernel (RHSA-2018:3590)

RHEL 7 : kernel (RHSA-2018:3591)

RHEL 7 : kernel (RHSA-2018:3651)

RHEL 7 : kernel (RHSA-2018:3843)

RHEL 7 : kernel (RHSA-2019:0163)

RHEL 7 : kernel (RHSA-2019:0202)

RHEL 7 : kernel (RHSA-2019:0324)

RHEL 7 : kernel (RHSA-2019:0512)

RHEL 7 : kernel (RHSA-2019:0818)

RHEL 7 : kernel (RHSA-2019:1155) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : kernel (RHSA-2019:1168) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : kernel (RHSA-2019:1170) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : kernel (RHSA-2019:1171) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : kernel (RHSA-2019:1172) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : kernel (RHSA-2019:1481) (SACK Panic) (SACK Slowness)

RHEL 7 : kernel (RHSA-2019:1482) (SACK Panic) (SACK Slowness)

RHEL 7 : kernel (RHSA-2019:1483) (SACK Panic) (SACK Slowness)

RHEL 7 : kernel (RHSA-2019:1484) (SACK Panic) (SACK Slowness)

RHEL 7 : kernel (RHSA-2019:1485) (SACK Panic) (SACK Slowness)

RHEL 7 : kernel (RHSA-2019:1873)

RHEL 7 : kernel (RHSA-2019:1946)

RHEL 7 : kernel (RHSA-2019:2029)

RHEL 7 : kernel (RHSA-2019:2566)

RHEL 7 : kernel (RHSA-2019:2600)

RHEL 7 : kernel (RHSA-2019:2696)

RHEL 7 : kernel (RHSA-2019:2829)

RHEL 7 : kernel (RHSA-2019:2837)

RHEL 7 : kernel (RHSA-2019:2864)

RHEL 7 : kernel (RHSA-2019:2866)

RHEL 7 : kernel (RHSA-2019:2867)

RHEL 7 : kernel (RHSA-2019:2899)

RHEL 7 : kernel (RHSA-2019:2900)

RHEL 7 : kernel (RHSA-2019:2975)

RHEL 7 : kernel (RHSA-2019:3055)

RHEL 7 : kernel (RHSA-2019:3187)

RHEL 7 : kernel (RHSA-2019:3218)

RHEL 7 : kernel (RHSA-2019:3220)

RHEL 7 : kernel (RHSA-2019:3834)

RHEL 7 : kernel (RHSA-2019:3837)

RHEL 7 : kernel (RHSA-2019:3838)

RHEL 7 : kernel (RHSA-2019:3839)

RHEL 7 : kernel (RHSA-2019:3840)

RHEL 7 : kernel (RHSA-2019:3841)

RHEL 7 : kernel (RHSA-2019:3872)

RHEL 7 : kernel (RHSA-2019:3873)

RHEL 7 : kernel (RHSA-2019:3877)

RHEL 7 : kernel (RHSA-2019:3883)

RHEL 7 : kernel (RHSA-2019:3889)

RHEL 7 : kernel (RHSA-2019:3967)

RHEL 7 : kernel (RHSA-2019:3979)

RHEL 7 : kernel (RHSA-2019:4058)

RHEL 7 : kernel (RHSA-2019:4159)

RHEL 7 : kernel (RHSA-2019:4164)

RHEL 7 : kernel (RHSA-2019:4168)

RHEL 7 : kernel (RHSA-2020:0036)

RHEL 7 : kernel (RHSA-2020:0103)

RHEL 7 : kernel (RHSA-2020:0178)

RHEL 7 : kernel (RHSA-2020:0179)

RHEL 7 : kernel (RHSA-2020:0374)

RHEL 7 : kernel (RHSA-2020:0543)

RHEL 7 : kernel (RHSA-2020:0592)

RHEL 7 : kernel (RHSA-2020:0653)

RHEL 7 : kernel (RHSA-2020:0661)

RHEL 7 : kernel (RHSA-2020:0664)

RHEL 7 : kernel (RHSA-2020:0834)

RHEL 7 : kernel (RHSA-2020:1016)

RHEL 7 : kernel (RHSA-2020:1266)

RHEL 7 : kernel (RHSA-2020:1347)

RHEL 7 : kernel (RHSA-2020:1460)

RHEL 7 : kernel (RHSA-2020:1465)

RHEL 7 : kernel (RHSA-2020:1473)

RHEL 7 : kernel-alt (RHSA-2018:0654)

RHEL 7 : kernel-alt (RHSA-2018:1374)

RHEL 7 : kernel-alt (RHSA-2018:1967) (Spectre)

RHEL 7 : kernel-alt (RHSA-2018:2772)

RHEL 7 : kernel-alt (RHSA-2018:2948) (Spectre)

RHEL 7 : kernel-alt (RHSA-2018:3656)

RHEL 7 : kernel-alt (RHSA-2019:0162)

RHEL 7 : kernel-alt (RHSA-2019:0525)

RHEL 7 : kernel-alt (RHSA-2019:0831)

RHEL 7 : kernel-alt (RHSA-2019:1350)

RHEL 7 : kernel-alt (RHSA-2019:1602) (SACK Panic) (SACK Slowness)

RHEL 7 : kernel-alt (RHSA-2019:1973)

RHEL 7 : kernel-alt (RHSA-2019:2809)

RHEL 7 : kernel-alt (RHSA-2019:2862)

RHEL 7 : kernel-alt (RHSA-2019:3217)

RHEL 7 : kernel-alt (RHSA-2019:4154)

RHEL 7 : kernel-alt (RHSA-2020:0174)

RHEL 7 : kernel-alt (RHSA-2020:0740)

RHEL 7 : kernel-alt (RHSA-2020:1493)

RHEL 7 : kernel-rt (RHSA-2015:0727)

RHEL 7 : kernel-rt (RHSA-2015:0981)

RHEL 7 : kernel-rt (RHSA-2015:1139)

RHEL 7 : kernel-rt (RHSA-2015:1565)

RHEL 7 : kernel-rt (RHSA-2015:1788)

RHEL 7 : kernel-rt (RHSA-2015:1977)

RHEL 7 : kernel-rt (RHSA-2015:2411)

RHEL 7 : kernel-rt (RHSA-2016:0065)

RHEL 7 : kernel-rt (RHSA-2016:0212)

RHEL 7 : kernel-rt (RHSA-2016:1051)

RHEL 7 : kernel-rt (RHSA-2016:1301)

RHEL 7 : kernel-rt (RHSA-2016:1541)

RHEL 7 : kernel-rt (RHSA-2016:1632)

RHEL 7 : kernel-rt (RHSA-2016:1875)

RHEL 7 : kernel-rt (RHSA-2016:2110) (Dirty COW)

RHEL 7 : kernel-rt (RHSA-2016:2584)

RHEL 7 : kernel-rt (RHSA-2017:0091)

RHEL 7 : kernel-rt (RHSA-2017:0295)

RHEL 7 : kernel-rt (RHSA-2017:0387)

RHEL 7 : kernel-rt (RHSA-2017:0931)

RHEL 7 : kernel-rt (RHSA-2017:1298)

RHEL 7 : kernel-rt (RHSA-2017:1616) (Stack Clash)

RHEL 7 : kernel-rt (RHSA-2017:2077)

RHEL 7 : kernel-rt (RHSA-2017:2585)

RHEL 7 : kernel-rt (RHSA-2017:2704) (BlueBorne)

RHEL 7 : kernel-rt (RHSA-2017:2931)

RHEL 7 : kernel-rt (RHSA-2017:3322)

RHEL 7 : kernel-rt (RHSA-2018:0016) (Meltdown) (Spectre)

RHEL 7 : kernel-rt (RHSA-2018:0152)

RHEL 7 : kernel-rt (RHSA-2018:0412)

RHEL 7 : kernel-rt (RHSA-2018:0676)

RHEL 7 : kernel-rt (RHSA-2018:1355)

RHEL 7 : kernel-rt (RHSA-2018:1630) (Spectre)

RHEL 7 : kernel-rt (RHSA-2018:1944)

RHEL 7 : kernel-rt (RHSA-2018:2003) (Spectre)

RHEL 7 : kernel-rt (RHSA-2018:2395) (Foreshadow)

RHEL 7 : kernel-rt (RHSA-2018:2763)

RHEL 7 : kernel-rt (RHSA-2018:3096)

RHEL 7 : kernel-rt (RHSA-2018:3666)

RHEL 7 : kernel-rt (RHSA-2019:0188)

RHEL 7 : kernel-rt (RHSA-2019:0514)

RHEL 7 : kernel-rt (RHSA-2019:0833)

RHEL 7 : kernel-rt (RHSA-2019:1176) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : kernel-rt (RHSA-2019:1486) (SACK Panic) (SACK Slowness)

RHEL 7 : kernel-rt (RHSA-2019:1891)

RHEL 7 : kernel-rt (RHSA-2019:2043)

RHEL 7 : kernel-rt (RHSA-2019:2609)

RHEL 7 : kernel-rt (RHSA-2019:2830)

RHEL 7 : kernel-rt (RHSA-2019:3089)

RHEL 7 : kernel-rt (RHSA-2019:3835)

RHEL 7 : kernel-rt (RHSA-2019:3887)

RHEL 7 : kernel-rt (RHSA-2019:3978)

RHEL 7 : kernel-rt (RHSA-2020:0375)

RHEL 7 : kernel-rt (RHSA-2020:0839)

RHEL 7 : kernel-rt (RHSA-2020:1070)

RHEL 7 : kexec-tools (RHSA-2015:0986)

RHEL 7 : keycloak-httpd-client-install (RHSA-2019:2137)

RHEL 7 : kpatch-patch (RHSA-2019:2854)

RHEL 7 : kpatch-patch (RHSA-2019:2865)

RHEL 7 : kpatch-patch (RHSA-2019:2945)

RHEL 7 : kpatch-patch (RHSA-2019:3076)

RHEL 7 : kpatch-patch (RHSA-2019:3231)

RHEL 7 : kpatch-patch (RHSA-2019:4171)

RHEL 7 : kpatch-patch (RHSA-2020:0026)

RHEL 7 : kpatch-patch (RHSA-2020:0027)

RHEL 7 : kpatch-patch (RHSA-2020:0028)

RHEL 7 : kpatch-patch (RHSA-2020:0698)

RHEL 7 : krb5 (RHSA-2015:0439)

RHEL 7 : krb5 (RHSA-2015:2154)

RHEL 7 : krb5 (RHSA-2016:0532)

RHEL 7 : krb5 (RHSA-2016:2591)

RHEL 7 : krb5 (RHSA-2018:0666)

RHEL 7 : krb5 (RHSA-2018:3071)

RHEL 7 : ksh (RHSA-2020:0568)

RHEL 7 : ksh (RHSA-2020:1332)

RHEL 7 : ksh (RHSA-2020:1333)

RHEL 7 : kubernetes (RHSA-2015:1945)

RHEL 7 : kubernetes (RHSA-2016:0351)

RHEL 7 : lftp (RHSA-2020:1045)

RHEL 7 : libarchive (RHSA-2016:1844)

RHEL 7 : libarchive (RHSA-2019:2298)

RHEL 7 : libarchive (RHSA-2020:0203)

RHEL 7 : libcdio (RHSA-2018:3246)

RHEL 7 : libcgroup (RHSA-2019:2047)

RHEL 7 : libcomps (RHSA-2019:3898)

RHEL 7 : libguestfs and virt-p2v (RHSA-2016:2576)

RHEL 7 : libguestfs-winsupport (RHSA-2019:2308)

RHEL 7 : libjpeg-turbo (RHSA-2019:2052)

RHEL 7 : libkdcraw (RHSA-2018:3065)

RHEL 7 : liblouis (RHSA-2017:3111)

RHEL 7 : liblouis (RHSA-2017:3384)

RHEL 7 : libmspack (RHSA-2018:3327)

RHEL 7 : libmspack (RHSA-2019:2049)

RHEL 7 : libndp (RHSA-2016:1086)

RHEL 7 : libosinfo (RHSA-2020:1051)

RHEL 7 : libpng (RHSA-2015:2596)

RHEL 7 : libpng12 (RHSA-2015:2595)

RHEL 7 : libqb (RHSA-2020:1189)

RHEL 7 : librelp (RHSA-2018:1223)

RHEL 7 : librelp (RHSA-2018:1703)

RHEL 7 : librelp (RHSA-2018:1704)

RHEL 7 : librelp (RHSA-2018:1707)

RHEL 7 : libreoffice (RHSA-2015:0377)

RHEL 7 : libreoffice (RHSA-2016:2579)

RHEL 7 : libreoffice (RHSA-2017:0914)

RHEL 7 : libreoffice (RHSA-2017:1975)

RHEL 7 : libreoffice (RHSA-2018:0418)

RHEL 7 : libreoffice (RHSA-2018:3054)

RHEL 7 : libreoffice (RHSA-2019:2130)

RHEL 7 : libreoffice (RHSA-2020:1151)

RHEL 7 : libreswan (RHSA-2015:1154)

RHEL 7 : libreswan (RHSA-2015:1979)

RHEL 7 : libreswan (RHSA-2016:2603)

RHEL 7 : libsndfile (RHSA-2020:1185)

RHEL 7 : libsolv (RHSA-2019:2290)

RHEL 7 : libsoup (RHSA-2017:2459)

RHEL 7 : libssh (RHSA-2016:0566)

RHEL 7 : libssh2 (RHSA-2015:2140)

RHEL 7 : libssh2 (RHSA-2019:0679)

RHEL 7 : libssh2 (RHSA-2019:1791)

RHEL 7 : libssh2 (RHSA-2019:1884)

RHEL 7 : libssh2 (RHSA-2019:1943)

RHEL 7 : libssh2 (RHSA-2019:2136)

RHEL 7 : libssh2 (RHSA-2019:2399)

RHEL 7 : libtasn1 (RHSA-2014:0687)

RHEL 7 : libtasn1 (RHSA-2017:1860)

RHEL 7 : libtiff (RHSA-2016:1546)

RHEL 7 : libtiff (RHSA-2019:2053)

RHEL 7 : libtirpc (RHSA-2017:1263)

RHEL 7 : libuser (RHSA-2015:1483)

RHEL 7 : libvirt (RHSA-2014:0914)

RHEL 7 : libvirt (RHSA-2014:1352)

RHEL 7 : libvirt (RHSA-2015:0008)

RHEL 7 : libvirt (RHSA-2015:0323)

RHEL 7 : libvirt (RHSA-2016:2577)

RHEL 7 : libvirt (RHSA-2018:0029) (Spectre)

RHEL 7 : libvirt (RHSA-2018:0031) (Spectre)

RHEL 7 : libvirt (RHSA-2018:0032) (Spectre)

RHEL 7 : libvirt (RHSA-2018:1396)

RHEL 7 : libvirt (RHSA-2018:1632) (Spectre)

RHEL 7 : libvirt (RHSA-2018:1652) (Spectre)

RHEL 7 : libvirt (RHSA-2018:1653) (Spectre)

RHEL 7 : libvirt (RHSA-2018:1668) (Spectre)

RHEL 7 : libvirt (RHSA-2018:1997) (Spectre)

RHEL 7 : libvirt (RHSA-2018:2006) (Spectre)

RHEL 7 : libvirt (RHSA-2018:3113)

RHEL 7 : libvirt (RHSA-2018:3398) (Spectre)

RHEL 7 : libvirt (RHSA-2018:3407) (Spectre)

RHEL 7 : libvirt (RHSA-2019:1177) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : libvirt (RHSA-2019:1182) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : libvirt (RHSA-2019:1184) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : libvirt (RHSA-2019:1186) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : libvirt (RHSA-2019:1187) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : libvirt (RHSA-2019:1264)

RHEL 7 : libvirt (RHSA-2019:1579)

RHEL 7 : libvirt (RHSA-2019:2294)

RHEL 7 : libvncserver (RHSA-2018:1055)

RHEL 7 : libvncserver (RHSA-2019:0059)

RHEL 7 : libvncserver (RHSA-2020:0913)

RHEL 7 : libvorbis (RHSA-2018:1058)

RHEL 7 : libwpd (RHSA-2019:2126)

RHEL 7 : libxml2 (RHSA-2015:0749)

RHEL 7 : libxml2 (RHSA-2015:2550)

RHEL 7 : libxml2 (RHSA-2020:1190)

RHEL 7 : linux-firmware (RHSA-2018:0014) (Spectre)

RHEL 7 : linux-firmware (RHSA-2018:0015) (Spectre)

RHEL 7 : linux-firmware (RHSA-2018:0053) (Spectre)

RHEL 7 : linux-firmware (RHSA-2018:0094) (Spectre)

RHEL 7 : linux-firmware (RHSA-2019:2169)

RHEL 7 : log4j (RHSA-2017:2423)

RHEL 7 : mailman (RHSA-2015:1153)

RHEL 7 : mailman (RHSA-2018:0505)

RHEL 7 : mailman (RHSA-2020:1054)

RHEL 7 : mariadb (RHSA-2014:0702)

RHEL 7 : mariadb (RHSA-2014:1861)

RHEL 7 : mariadb (RHSA-2015:0118)

RHEL 7 : mariadb (RHSA-2015:1665) (BACKRONYM)

RHEL 7 : mariadb (RHSA-2016:0534)

RHEL 7 : mariadb (RHSA-2016:1602)

RHEL 7 : mariadb (RHSA-2016:2595)

RHEL 7 : mariadb (RHSA-2017:2192)

RHEL 7 : mariadb (RHSA-2018:2439)

RHEL 7 : mariadb (RHSA-2019:2327)

RHEL 7 : mariadb (RHSA-2020:1100)

RHEL 7 : memcached (RHSA-2016:2819)

RHEL 7 : mercurial (RHSA-2016:0706)

RHEL 7 : mercurial (RHSA-2017:2489)

RHEL 7 : mercurial (RHSA-2019:2276)

RHEL 7 : microcode\_ctl (RHSA-2018:0012) (Spectre)

RHEL 7 : microcode\_ctl (RHSA-2018:0034) (Spectre)

RHEL 7 : microcode\_ctl (RHSA-2018:0035) (Spectre)

RHEL 7 : Mobile Application Platform (RHSA-2017:2674)

RHEL 7 : mod\_auth\_mellon (RHSA-2019:0766)

RHEL 7 : mod\_auth\_mellon (RHSA-2020:1003)

RHEL 7 : mod\_auth\_openidc (RHSA-2019:2112)

RHEL 7 : mod\_nss (RHSA-2016:2602)

RHEL 7 : mod\_wsgi (RHSA-2014:1091)

RHEL 7 : MRG (RHSA-2015:0660)

RHEL 7 : MRG (RHSA-2015:0708)

RHEL 7 : mutt (RHSA-2020:1126)

RHEL 7 : nagios (RHSA-2017:0258)

RHEL 7 : nautilus (RHSA-2018:0223)

RHEL 7 : nbdkit (RHSA-2020:1167)

RHEL 7 : net-snmp (RHSA-2015:2345)

RHEL 7 : net-snmp (RHSA-2020:1081)

RHEL 7 : netcf (RHSA-2015:2248)

RHEL 7 : nettle (RHSA-2016:2582)

RHEL 7 : NetworkManager (RHSA-2015:2315)

RHEL 7 : NetworkManager (RHSA-2016:2581)

RHEL 7 : NetworkManager (RHSA-2018:3665)

RHEL 7 : NetworkManager and libnl3 (RHSA-2017:2299)

RHEL 7 : nodejs and nodejs-tough-cookie (RHSA-2016:2101)

RHEL 7 : nss (RHSA-2017:1365)

RHEL 7 : nss (RHSA-2018:2768)

RHEL 7 : nss, nspr, nss-softokn, and nss-util (RHSA-2016:0685)

RHEL 7 : nss, nss-softokn, nss-util (RHSA-2019:4190)

RHEL 7 : nss, nss-softokn, nss-util, and nspr (RHSA-2019:2237)

RHEL 7 : nss, nss-util, nss-softokn (RHSA-2014:1073)

RHEL 7 : nss-softokn (RHSA-2020:1267)

RHEL 7 : nss-softokn (RHSA-2020:1345)

RHEL 7 : nss-softokn (RHSA-2020:1461)

RHEL 7 : ntp (RHSA-2015:2231)

RHEL 7 : ntp (RHSA-2016:2583)

RHEL 7 : ntp (RHSA-2018:0855)

RHEL 7 : ntp (RHSA-2019:2077)

RHEL 7 : ocaml (RHSA-2016:1296)

RHEL 7 : okular (RHSA-2020:1173)

RHEL 7 : openhpi (RHSA-2015:2369)

RHEL 7 : openjpeg (RHSA-2017:0838)

RHEL 7 : openjpeg2 (RHSA-2020:0262)

RHEL 7 : openjpeg2 (RHSA-2020:0550)

RHEL 7 : openldap (RHSA-2015:2131)

RHEL 7 : openldap (RHSA-2017:1852)

RHEL 7 : opensc (RHSA-2019:2154)

RHEL 7 : openshift (RHSA-2015:1650)

RHEL 7 : openshift (RHSA-2015:1736)

RHEL 7 : openshift (RHSA-2015:2544)

RHEL 7 : openshift (RHSA-2016:0070)

RHEL 7 : openshift (RHSA-2016:1038)

RHEL 7 : openshift (RHSA-2019:0741)

RHEL 7 : OpenShift Container Platform 3.1 (RHSA-2018:1243)

RHEL 7 : OpenShift Container Platform 3.10 (RHSA-2018:3549)

RHEL 7 : OpenShift Container Platform 3.10 (RHSA-2019:2690) (Ping Flood) (Reset Flood)

RHEL 7 : OpenShift Container Platform 3.10 atomic-openshift (RHSA-2019:3239)

RHEL 7 : OpenShift Container Platform 3.10 atomic-openshift kube-apiserver (RHSA-2019:2989)

RHEL 7 : OpenShift Container Platform 3.10 atomic-openshift-web-console (RHSA-2019:2552)

RHEL 7 : OpenShift Container Platform 3.10 haproxy (RHSA-2019:0548)

RHEL 7 : OpenShift Container Platform 3.10 mediawiki (RHSA-2019:3238)

RHEL 7 : OpenShift Container Platform 3.11 (RHSA-2018:3537)

RHEL 7 : OpenShift Container Platform 3.11 (RHSA-2019:1851)

RHEL 7 : OpenShift Container Platform 3.11 (RHSA-2019:2817) (Ping Flood) (Reset Flood)

RHEL 7 : OpenShift Container Platform 3.11 (RHSA-2019:2818)

RHEL 7 : OpenShift Container Platform 3.11 (RHSA-2020:0795)

RHEL 7 : OpenShift Container Platform 3.11 atomic-openshift (RHSA-2019:3143)

RHEL 7 : OpenShift Container Platform 3.11 atomic-openshift (RHSA-2019:3905)

RHEL 7 : OpenShift Container Platform 3.11 atomic-openshift (RHSA-2019:4052)

RHEL 7 : OpenShift Container Platform 3.11 atomic-openshift (RHSA-2020:0020)

RHEL 7 : OpenShift Container Platform 3.11 atomic-openshift-web-console (RHSA-2019:1422)

RHEL 7 : OpenShift Container Platform 3.11 HTTP/2 (RHSA-2019:3906) (Ping Flood) (Reset Flood)

RHEL 7 : OpenShift Container Platform 3.11 jenkins (RHSA-2019:2503)

RHEL 7 : OpenShift Container Platform 3.11 jenkins (RHSA-2019:3144)

RHEL 7 : OpenShift Container Platform 3.11 jenkins-2-plugins (RHSA-2019:4055)

RHEL 7 : OpenShift Container Platform 3.11 jenkins-2-plugins (RHSA-2020:0964)

RHEL 7 : OpenShift Container Platform 3.11 mediawiki (RHSA-2019:3142)

RHEL 7 : OpenShift Container Platform 3.11 openshift-external-storage (RHSA-2019:4054)

RHEL 7 : OpenShift Container Platform 3.2 (RHSA-2018:1241)

RHEL 7 : OpenShift Container Platform 3.2 (RHSA-2018:3742)

RHEL 7 : OpenShift Container Platform 3.3 (RHSA-2018:1239)

RHEL 7 : OpenShift Container Platform 3.3 (RHSA-2018:3754)

RHEL 7 : OpenShift Container Platform 3.4 (RHSA-2018:1237)

RHEL 7 : OpenShift Container Platform 3.4 (RHSA-2018:3752)

RHEL 7 : OpenShift Container Platform 3.4, 3.5, 3.6, and 3.7 (RHSA-2019:0408)

RHEL 7 : OpenShift Container Platform 3.5 (RHSA-2018:1235)

RHEL 7 : OpenShift Container Platform 3.5 (RHSA-2018:3624)

RHEL 7 : OpenShift Container Platform 3.6 (RHSA-2018:1233)

RHEL 7 : OpenShift Container Platform 3.6 (RHSA-2018:2654)

RHEL 7 : OpenShift Container Platform 3.6 (RHSA-2018:3598)

RHEL 7 : OpenShift Container Platform 3.7 (RHSA-2018:1231)

RHEL 7 : OpenShift Container Platform 3.7 (RHSA-2018:2906)

RHEL 7 : OpenShift Container Platform 3.8 (RHSA-2018:1229)

RHEL 7 : OpenShift Container Platform 3.8 (RHSA-2018:3551)

RHEL 7 : OpenShift Container Platform 3.9 (RHSA-2018:1227)

RHEL 7 : OpenShift Container Platform 3.9 (RHSA-2018:2013)

RHEL 7 : OpenShift Container Platform 3.9 (RHSA-2018:2908)

RHEL 7 : OpenShift Container Platform 3.9 (RHSA-2019:2769) (Ping Flood) (Reset Flood)

RHEL 7 : OpenShift Container Platform 3.9 atomic-openshift (RHSA-2019:1852)

RHEL 7 : OpenShift Container Platform 3.9 atomic-openshift (RHSA-2019:3811)

RHEL 7 : OpenShift Container Platform 3.9 atomic-openshift-web-console (RHSA-2019:2551)

RHEL 7 : OpenShift Container Platform 3.9 cri-o (RHSA-2019:3812)

RHEL 7 : OpenShift Container Platform 3.9 haproxy (RHSA-2019:0547)

RHEL 7 : OpenShift Container Platform 3.9 mediawiki123 (RHSA-2019:3813)

RHEL 7 : OpenShift Container Platform 4.1 (RHSA-2019:3265) (Ping Flood) (Reset Flood)

RHEL 7 : OpenShift Container Platform 4.1 jenkins (RHSA-2019:2548)

RHEL 7 : OpenShift Container Platform 4.1 jenkins-2-plugins (RHSA-2019:1636)

RHEL 7 : OpenShift Container Platform 4.1 jenkins-2-plugins (RHSA-2019:4089)

RHEL 7 : OpenShift Container Platform 4.1 openshift-external-storage (RHSA-2019:4225)

RHEL 7 : OpenShift Container Platform 4.1.16 jenkins (RHSA-2019:2789)

RHEL 7 : OpenShift Container Platform 4.1.18 (RHSA-2019:2860)

RHEL 7 : OpenShift Container Platform 4.2 (RHSA-2019:3245) (Ping Flood) (Reset Flood)

RHEL 7 : OpenShift Container Platform 4.2 jenkins-2-plugins (RHSA-2019:4097)

RHEL 7 : OpenShift Container Platform 4.2 openshift-external-storage (RHSA-2019:4096)

RHEL 7 : openslp (RHSA-2018:2240)

RHEL 7 : openslp (RHSA-2019:4240)

RHEL 7 : openssh (RHSA-2015:0425)

RHEL 7 : openssh (RHSA-2015:2088)

RHEL 7 : openssh (RHSA-2016:0043)

RHEL 7 : openssh (RHSA-2016:0465)

RHEL 7 : openssh (RHSA-2016:2588)

RHEL 7 : openssh (RHSA-2017:2029)

RHEL 7 : openssh (RHSA-2018:0980)

RHEL 7 : openssh (RHSA-2019:2143)

RHEL 7 : openssl (RHSA-2014:0679)

RHEL 7 : openssl (RHSA-2015:0716)

RHEL 7 : openssl (RHSA-2016:0722)

RHEL 7 : openssl (RHSA-2018:0998)

RHEL 7 : openssl (RHSA-2018:3221)

RHEL 7 : openssl (RHSA-2019:0483)

RHEL 7 : openssl (RHSA-2019:2304)

RHEL 7 : openssl098e (RHSA-2014:0680)

RHEL 7 : openvswitch (RHSA-2016:0615)

RHEL 7 : openvswitch (RHSA-2017:2418)

RHEL 7 : openvswitch (RHSA-2018:1267)

RHEL 7 : openvswitch (RHSA-2018:3500)

RHEL 7 : openvswitch (RHSA-2020:0165)

RHEL 7 : openvswitch2.11 (RHSA-2020:0166)

RHEL 7 : openvswitch2.12 (RHSA-2020:0168)

RHEL 7 : openwsman (RHSA-2019:0638)

RHEL 7 : org.ovirt.engine-root (RHSA-2016:1967)

RHEL 7 : org.ovirt.engine-root (RHSA-2017:3427)

RHEL 7 : ovirt-engine-extension-aaa-jdbc (RHSA-2017:0257)

RHEL 7 : ovmf (RHSA-2018:3090)

RHEL 7 : ovmf (RHSA-2019:0809)

RHEL 7 : ovmf (RHSA-2019:2125)

RHEL 7 : pacemaker (RHSA-2015:2383)

RHEL 7 : pacemaker (RHSA-2016:2578)

RHEL 7 : pacemaker (RHSA-2016:2614)

RHEL 7 : pacemaker (RHSA-2019:1278)

RHEL 7 : PackageKit (RHSA-2018:1224)

RHEL 7 : pango (RHSA-2019:2571)

RHEL 7 : pango (RHSA-2019:3234)

RHEL 7 : patch (RHSA-2018:1200)

RHEL 7 : patch (RHSA-2018:2091)

RHEL 7 : patch (RHSA-2018:2092)

RHEL 7 : patch (RHSA-2018:2093)

RHEL 7 : patch (RHSA-2019:2033)

RHEL 7 : patch (RHSA-2019:2964)

RHEL 7 : patch (RHSA-2019:3757)

RHEL 7 : patch (RHSA-2019:3758)

RHEL 7 : patch (RHSA-2019:4061)

RHEL 7 : pcre (RHSA-2015:0330)

RHEL 7 : pcre (RHSA-2016:1025)

RHEL 7 : pcs (RHSA-2015:0980)

RHEL 7 : pcs (RHSA-2015:2290)

RHEL 7 : pcs (RHSA-2016:2596)

RHEL 7 : pcs (RHSA-2018:1060)

RHEL 7 : perl (RHSA-2019:0109)

RHEL 7 : perl (RHSA-2019:1790)

RHEL 7 : perl (RHSA-2019:1942)

RHEL 7 : perl (RHSA-2019:2400)

RHEL 7 : perl-Archive-Tar (RHSA-2019:2097)

RHEL 7 : php (RHSA-2014:1013)

RHEL 7 : php (RHSA-2014:1327)

RHEL 7 : php (RHSA-2015:1135)

RHEL 7 : php (RHSA-2016:1613) (httpoxy)

RHEL 7 : php (RHSA-2016:2598)

RHEL 7 : php (RHSA-2017:3221)

RHEL 7 : php (RHSA-2018:0406)

RHEL 7 : php (RHSA-2019:3286)

RHEL 7 : php (RHSA-2020:1112)

RHEL 7 : pidgin (RHSA-2017:1854)

RHEL 7 : pki-core (RHSA-2017:2335)

RHEL 7 : pki-core (RHSA-2018:1979)

RHEL 7 : plexus-archiver (RHSA-2018:1836)

RHEL 7 : podman (RHSA-2018:2037)

RHEL 7 : podman (RHSA-2019:1907)

RHEL 7 : podman (RHSA-2020:1227)

RHEL 7 : policycoreutils (RHSA-2017:0535)

RHEL 7 : policycoreutils (RHSA-2017:0536)

RHEL 7 : policycoreutils (RHSA-2018:0913)

RHEL 7 : polkit (RHSA-2016:0189)

RHEL 7 : polkit (RHSA-2019:0230)

RHEL 7 : polkit (RHSA-2019:2046)

RHEL 7 : polkit (RHSA-2019:2699)

RHEL 7 : polkit (RHSA-2019:2978)

RHEL 7 : polkit (RHSA-2019:3232)

RHEL 7 : polkit (RHSA-2020:1135)

RHEL 7 : polkit-qt (RHSA-2014:1359)

RHEL 7 : poppler (RHSA-2016:2580)

RHEL 7 : poppler (RHSA-2017:2551)

RHEL 7 : poppler (RHSA-2019:2022)

RHEL 7 : postgresql (RHSA-2015:2078)

RHEL 7 : postgresql (RHSA-2016:0346)

RHEL 7 : postgresql (RHSA-2016:2606)

RHEL 7 : postgresql (RHSA-2017:1983)

RHEL 7 : postgresql (RHSA-2017:2728)

RHEL 7 : postgresql (RHSA-2017:3402)

RHEL 7 : postgresql (RHSA-2018:2557)

RHEL 7 : ppp (RHSA-2020:0630)

RHEL 7 : procmail (RHSA-2017:3269)

RHEL 7 : procps-ng (RHSA-2018:1700)

RHEL 7 : procps-ng (RHSA-2019:1944)

RHEL 7 : procps-ng (RHSA-2019:2189)

RHEL 7 : procps-ng (RHSA-2019:2401)

RHEL 7 : procps-ng (RHSA-2020:0595)

RHEL 7 : procps-ng (RHSA-2020:1265)

RHEL 7 : python (RHSA-2015:2101)

RHEL 7 : python (RHSA-2016:2586)

RHEL 7 : python (RHSA-2017:1868)

RHEL 7 : python (RHSA-2018:2123)

RHEL 7 : python (RHSA-2018:3041)

RHEL 7 : python (RHSA-2019:0710)

RHEL 7 : python (RHSA-2019:1587)

RHEL 7 : python (RHSA-2019:2030)

RHEL 7 : python (RHSA-2019:2980)

RHEL 7 : python (RHSA-2019:3170)

RHEL 7 : python (RHSA-2020:1131)

RHEL 7 : python (RHSA-2020:1268)

RHEL 7 : python (RHSA-2020:1346)

RHEL 7 : python (RHSA-2020:1462)

RHEL 7 : python-flask (RHSA-2020:0870)

RHEL 7 : python-jinja2 (RHSA-2019:1022)

RHEL 7 : python-jinja2 (RHSA-2019:3964)

RHEL 7 : python-jinja2 (RHSA-2019:4062)

RHEL 7 : python-paramiko (RHSA-2018:0591)

RHEL 7 : python-paramiko (RHSA-2018:0646)

RHEL 7 : python-paramiko (RHSA-2018:1213)

RHEL 7 : python-paramiko (RHSA-2018:3347)

RHEL 7 : python-pillow (RHSA-2020:0578)

RHEL 7 : python-pip (RHSA-2020:0850)

RHEL 7 : python-reportlab (RHSA-2020:0195)

RHEL 7 : python-requests (RHSA-2019:2035)

RHEL 7 : python-twisted-web (RHSA-2020:1091)

RHEL 7 : python-urllib3 (RHSA-2019:2272)

RHEL 7 : python-virtualenv (RHSA-2020:0851)

RHEL 7 : python3 (RHSA-2020:1132)

RHEL 7 : qemu-kvm (RHSA-2014:0704)

RHEL 7 : qemu-kvm (RHSA-2014:0927)

RHEL 7 : qemu-kvm (RHSA-2014:1669)

RHEL 7 : qemu-kvm (RHSA-2015:0349)

RHEL 7 : qemu-kvm (RHSA-2015:0999) (Venom)

RHEL 7 : qemu-kvm (RHSA-2015:1507)

RHEL 7 : qemu-kvm (RHSA-2015:1793)

RHEL 7 : qemu-kvm (RHSA-2015:1943)

RHEL 7 : qemu-kvm (RHSA-2016:0083)

RHEL 7 : qemu-kvm (RHSA-2016:0724)

RHEL 7 : qemu-kvm (RHSA-2016:1606)

RHEL 7 : qemu-kvm (RHSA-2016:2585)

RHEL 7 : qemu-kvm (RHSA-2017:0083)

RHEL 7 : qemu-kvm (RHSA-2017:0396)

RHEL 7 : qemu-kvm (RHSA-2017:0987)

RHEL 7 : qemu-kvm (RHSA-2017:1430)

RHEL 7 : qemu-kvm (RHSA-2017:1681)

RHEL 7 : qemu-kvm (RHSA-2017:1856)

RHEL 7 : qemu-kvm (RHSA-2017:2445)

RHEL 7 : qemu-kvm (RHSA-2017:3368)

RHEL 7 : qemu-kvm (RHSA-2018:0023) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:0026) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:0027) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:0816)

RHEL 7 : qemu-kvm (RHSA-2018:1416)

RHEL 7 : qemu-kvm (RHSA-2018:1633) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:1661) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:1662) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:1663) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:2001) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2018:2462)

RHEL 7 : qemu-kvm (RHSA-2018:3423) (Spectre)

RHEL 7 : qemu-kvm (RHSA-2019:1178) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : qemu-kvm (RHSA-2019:1183) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : qemu-kvm (RHSA-2019:1185) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : qemu-kvm (RHSA-2019:1188) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : qemu-kvm (RHSA-2019:1189) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : qemu-kvm (RHSA-2019:1883)

RHEL 7 : qemu-kvm (RHSA-2019:2078)

RHEL 7 : qemu-kvm (RHSA-2019:2607)

RHEL 7 : qemu-kvm (RHSA-2020:0366)

RHEL 7 : qemu-kvm (RHSA-2020:0666)

RHEL 7 : qemu-kvm (RHSA-2020:1116)

RHEL 7 : qemu-kvm (RHSA-2020:1208)

RHEL 7 : qemu-kvm (RHSA-2020:1351)

RHEL 7 : qemu-kvm-ma (RHSA-2018:2762)

RHEL 7 : qemu-kvm-ma (RHSA-2018:3062)

RHEL 7 : qemu-kvm-ma (RHSA-2019:1881)

RHEL 7 : qemu-kvm-ma (RHSA-2019:2166)

RHEL 7 : qemu-kvm-ma (RHSA-2019:3968)

RHEL 7 : qemu-kvm-ma (RHSA-2020:0669)

RHEL 7 : qemu-kvm-ma (RHSA-2020:1150)

RHEL 7 : qemu-kvm-ma (RHSA-2020:1209)

RHEL 7 : qemu-kvm-ma (RHSA-2020:1352)

RHEL 7 : qemu-kvm-rhev (RHSA-2014:1670)

RHEL 7 : qemu-kvm-rhev (RHSA-2015:0624)

RHEL 7 : qemu-kvm-rhev (RHSA-2015:1000) (Venom)

RHEL 7 : qemu-kvm-rhev (RHSA-2015:1508)

RHEL 7 : qemu-kvm-rhev (RHSA-2015:1739)

RHEL 7 : qemu-kvm-rhev (RHSA-2015:1837)

RHEL 7 : qemu-kvm-rhev (RHSA-2015:1931)

RHEL 7 : qemu-kvm-rhev (RHSA-2016:0084)

RHEL 7 : qemu-kvm-rhev (RHSA-2016:0725)

RHEL 7 : qemu-kvm-rhev (RHSA-2016:1607)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:0350)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:0985)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:1431)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:1682)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:2390)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:2392)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:2628)

RHEL 7 : qemu-kvm-rhev (RHSA-2017:3369)

RHEL 7 : qemu-kvm-rhev (RHSA-2018:1369)

RHEL 7 : qemu-kvm-rhev (RHSA-2018:2060) (Spectre)

RHEL 7 : qemu-kvm-rhev (RHSA-2020:1216)

RHEL 7 : qemu-kvm-rhev (RHSA-2020:1292)

RHEL 7 : qemu-kvm-rhev (RHSA-2020:1296)

RHEL 7 : qemu-kvm-rhev (RHSA-2020:1300)

RHEL 7 : qt (RHSA-2020:1172)

RHEL 7 : qt5 (RHSA-2019:2135)

RHEL 7 : quagga (RHSA-2018:0377)

RHEL 7 : realmd (RHSA-2015:2184)

RHEL 7 : Red Hat Ceph Storage (RHSA-2016:2815)

RHEL 7 : Red Hat Ceph Storage (RHSA-2019:4353)

RHEL 7 : Red Hat Ceph Storage 1.3 (RHSA-2016:2847)

RHEL 7 : Red Hat Ceph Storage 1.3 (RHSA-2016:2994)

RHEL 7 : Red Hat Ceph Storage 1.3.1 (RHSA-2015:2066)

RHEL 7 : Red Hat Ceph Storage 1.3.3 (RHSA-2016:1972)

RHEL 7 : Red Hat Ceph Storage 2.1 (RHSA-2016:2954)

RHEL 7 : Red Hat Ceph Storage 2.5 (RHSA-2018:2261)

RHEL 7 : Red Hat Ceph Storage 2.5 (RHSA-2019:0747)

RHEL 7 : Red Hat Ceph Storage 3.0 (RHSA-2018:2177)

RHEL 7 : Red Hat Ceph Storage 3.2 (RHSA-2019:0911)

RHEL 7 : Red Hat Ceph Storage 3.3 (RHSA-2019:2538)

RHEL 7 : Red Hat Gluster Storage (RHSA-2017:2338)

RHEL 7 : Red Hat JBoss Core Services Apache HTTP Server 2.4.23 (RHSA-2017:3476) (Optionsbleed)

RHEL 7 : Red Hat JBoss Core Services Apache HTTP Server 2.4.29 RHEL 7 (RHSA-2018:2185)

RHEL 7 : Red Hat JBoss Web Server 3.0.3 Service Pack 1 (RHSA-2016:1635) (httpoxy)

RHEL 7 : Red Hat JBoss Web Server 3.1.0 (RHSA-2017:0456)

RHEL 7 : Red Hat Mobile Application Platform 4.6.0 (RHSA-2018:1263)

RHEL 7 : Red Hat OpenShift Application Runtimes Node.js 10.9.0 (RHSA-2018:2553)

RHEL 7 : Red Hat OpenShift Application Runtimes Node.js 8.11.4 (RHSA-2018:2552)

RHEL 7 : Red Hat OpenShift Container Platform (RHSA-2018:0475)

RHEL 7 : Red Hat OpenShift Container Platform 3.10 (RHSA-2018:2709)

RHEL 7 : Red Hat OpenShift Container Platform 3.10 atomic-openshift (RHSA-2019:1632)

RHEL 7 : Red Hat OpenShift Container Platform 3.11 atomic-openshift (RHSA-2019:1633)

RHEL 7 : Red Hat OpenShift Container Platform 3.11 jenkins-2-plugins (RHSA-2019:0739)

RHEL 7 : Red Hat OpenShift Container Platform 3.11 jenkins-2-plugins (RHSA-2019:1423)

RHEL 7 : Red Hat OpenShift Container Platform 3.11 jenkins-2-plugins (RHSA-2019:2651)

RHEL 7 : Red Hat OpenShift Container Platform 3.7 (RHSA-2017:3188)

RHEL 7 : Red Hat OpenShift Container Platform 4.1 jenkins-2-plugins (RHSA-2019:2662)

RHEL 7 : Red Hat OpenShift Enterprise (RHSA-2016:1605)

RHEL 7 : Red Hat OpenShift Enterprise (RHSA-2017:3389)

RHEL 7 : Red Hat OpenShift Enterprise 3.1 (RHSA-2016:1095)

RHEL 7 : Red Hat OpenShift Enterprise 3.1 (RHSA-2016:1852)

RHEL 7 : Red Hat OpenShift Enterprise 3.2 (RHSA-2016:1064)

RHEL 7 : Red Hat OpenShift Enterprise 3.2 (RHSA-2016:1094)

RHEL 7 : Red Hat OpenShift Enterprise 3.2 (RHSA-2016:1853)

RHEL 7 : Red Hat OpenShift Enterprise Kibana (RHSA-2016:1836)

RHEL 7 : Red Hat Single Sign-On 7.2.5 on RHEL 7 (RHSA-2018:3593)

RHEL 7 : Red Hat Single Sign-On 7.2.7 (RHSA-2019:0856)

RHEL 7 : Red Hat Single Sign-On 7.3.4 (RHSA-2019:3045)

RHEL 7 : Red Hat Single Sign-On 7.3.5 (RHSA-2019:4041) (Ping Flood) (Reset Flood) (Settings Flood)

RHEL 7 : Red Hat Single Sign-On 7.3.7 security update on RHEL 7 (Important) (RHSA-2020:0946)

RHEL 7 : Red Hat Virtualization Engine security, bug fix 4.3.9 (Low) (RHSA-2020:1308)

RHEL 7 : redhat-certification (RHSA-2018:2373)

RHEL 7 : redhat-virtualization-host (RHSA-2017:0549)

RHEL 7 : redhat-virtualization-host (RHSA-2018:0044) (Meltdown) (Spectre)

RHEL 7 : redhat-virtualization-host (RHSA-2018:0047) (Meltdown) (Spectre)

RHEL 7 : rest (RHSA-2015:2237)

RHEL 7 : resteasy-base (RHSA-2014:1011)

RHEL 7 : resteasy-base (RHSA-2016:2604)

RHEL 7 : rh-eclipse46-jackson-databind (RHSA-2018:0116)

RHEL 7 : rh-eclipse47-jackson-databind (RHSA-2017:3189)

RHEL 7 : rh-maven35-jackson-databind (RHSA-2018:0342)

RHEL 7 : rh-sso7-keycloak (RHSA-2017:2905)

RHEL 7 : rhev-hypervisor (RHSA-2015:1011) (Venom)

RHEL 7 : rhevm-appliance (RHSA-2017:0552)

RHEL 7 : rhevm-setup-plugins (RHSA-2018:0051) (Spectre)

RHEL 7 : RHGS WA (RHSA-2018:3829)

RHEL 7 : rhvm-appliance (RHSA-2017:3141)

RHEL 7 : rhvm-appliance (RHSA-2018:0045) (Meltdown) (Spectre)

RHEL 7 : rpcbind (RHSA-2017:1262)

RHEL 7 : rpm (RHSA-2014:1976)

RHEL 7 : rpm-ostree and rpm-ostree-client (RHSA-2017:0444)

RHEL 7 : rsyslog (RHSA-2014:1397)

RHEL 7 : rsyslog (RHSA-2019:2110)

RHEL 7 : rsyslog (RHSA-2020:1000)

RHEL 7 : ruby (RHSA-2014:1912)

RHEL 7 : ruby (RHSA-2018:0378)

RHEL 7 : ruby (RHSA-2018:3738)

RHEL 7 : ruby (RHSA-2019:1235)

RHEL 7 : ruby (RHSA-2019:1948)

RHEL 7 : ruby (RHSA-2019:2028)

RHEL 7 : ruby (RHSA-2019:2565)

RHEL 7 : ruby (RHSA-2019:2806)

RHEL 7 : ruby (RHSA-2020:0542)

RHEL 7 : ruby (RHSA-2020:0591)

RHEL 7 : ruby (RHSA-2020:0663)

RHEL 7 : rubygem-bundler and rubygem-thor (RHSA-2015:2180)

RHEL 7 : runc (RHSA-2017:0127)

RHEL 7 : runc (RHSA-2019:0303)

RHEL 7 : runc (RHSA-2020:0942)

RHEL 7 : samba (RHSA-2014:0867)

RHEL 7 : samba (RHSA-2014:1008)

RHEL 7 : samba (RHSA-2015:0252)

RHEL 7 : samba (RHSA-2016:0006)

RHEL 7 : samba (RHSA-2016:0618) (Badlock)

RHEL 7 : samba (RHSA-2016:1486)

RHEL 7 : samba (RHSA-2017:1265)

RHEL 7 : samba (RHSA-2017:1950)

RHEL 7 : samba (RHSA-2017:2790)

RHEL 7 : samba (RHSA-2017:3260)

RHEL 7 : samba (RHSA-2018:3056)

RHEL 7 : samba (RHSA-2019:2099)

RHEL 7 : samba (RHSA-2020:0943)

RHEL 7 : samba (RHSA-2020:1084)

RHEL 7 : Satellite Server (RHSA-2015:1591)

RHEL 7 : Satellite Server (RHSA-2018:0336)

RHEL 7 : Satellite Server (RHSA-2018:2733)

RHEL 7 : Satellite Server (RHSA-2018:2927)

RHEL 7 : Satellite Server (RHSA-2019:0733)

RHEL 7 : Satellite Server (RHSA-2019:0735)

RHEL 7 : Satellite Server (RHSA-2019:1222)

RHEL 7 : Satellite Server (RHSA-2019:2777)

RHEL 7 : Satellite Server (RHSA-2019:2778)

RHEL 7 : Satellite Server (RHSA-2019:2779)

RHEL 7 : Satellite Server (RHSA-2019:3172)

RHEL 7 : SDL (RHSA-2019:3950)

RHEL 7 : SDL (RHSA-2019:4024)

RHEL 7 : setroubleshoot and setroubleshoot-plugins (RHSA-2016:1293)

RHEL 7 : setup (RHSA-2018:3249)

RHEL 7 : shim (RHSA-2014:1801)

RHEL 7 : Single Sign-On (RHSA-2017:0873)

RHEL 7 : skopeo (RHSA-2020:1230)

RHEL 7 : slf4j (RHSA-2018:0592)

RHEL 7 : sos (RHSA-2016:0188)

RHEL 7 : sos-collector (RHSA-2018:3663)

RHEL 7 : sox (RHSA-2019:2283)

RHEL 7 : spamassassin (RHSA-2018:2916)

RHEL 7 : spice (RHSA-2015:1714)

RHEL 7 : spice (RHSA-2015:1890)

RHEL 7 : spice (RHSA-2016:1205)

RHEL 7 : spice (RHSA-2017:0254)

RHEL 7 : spice (RHSA-2017:2471)

RHEL 7 : spice (RHSA-2019:0231)

RHEL 7 : spice and spice-gtk (RHSA-2018:2731)

RHEL 7 : spice-gtk (RHSA-2019:2229)

RHEL 7 : sqlite (RHSA-2015:1635)

RHEL 7 : sqlite (RHSA-2020:0227)

RHEL 7 : squid (RHSA-2014:1147)

RHEL 7 : squid (RHSA-2015:2378)

RHEL 7 : squid (RHSA-2016:1139)

RHEL 7 : squid (RHSA-2016:2600)

RHEL 7 : squid (RHSA-2017:0182)

RHEL 7 : squid (RHSA-2020:1068)

RHEL 7 : sssd (RHSA-2015:2355)

RHEL 7 : sssd (RHSA-2017:3379)

RHEL 7 : sssd (RHSA-2018:3158)

RHEL 7 : sssd (RHSA-2019:2177)

RHEL 7 : Storage Server (RHSA-2016:0016)

RHEL 7 : Storage Server (RHSA-2016:0328)

RHEL 7 : Storage Server (RHSA-2017:1334)

RHEL 7 : Storage Server (RHSA-2017:3277)

RHEL 7 : Storage Server (RHSA-2018:2613)

RHEL 7 : Storage Server (RHSA-2018:2615)

RHEL 7 : Storage Server (RHSA-2018:2616)

RHEL 7 : Storage Server (RHSA-2019:0265)

RHEL 7 : Storage Server (RHSA-2019:1966)

RHEL 7 : subscription-manager (RHSA-2016:2592)

RHEL 7 : subversion (RHSA-2015:0166)

RHEL 7 : subversion (RHSA-2015:1742)

RHEL 7 : subversion (RHSA-2017:2480)

RHEL 7 : sudo (RHSA-2016:2593)

RHEL 7 : sudo (RHSA-2019:3197)

RHEL 7 : sudo (RHSA-2019:3204)

RHEL 7 : sudo (RHSA-2019:3205)

RHEL 7 : sudo (RHSA-2019:3209)

RHEL 7 : sudo (RHSA-2019:3219)

RHEL 7 : sudo (RHSA-2019:3278)

RHEL 7 : sudo (RHSA-2020:0540)

RHEL 7 : swiftonfile (RHSA-2015:1846)

RHEL 7 : systemd (RHSA-2016:2610)

RHEL 7 : systemd (RHSA-2016:2694)

RHEL 7 : systemd (RHSA-2017:0003)

RHEL 7 : systemd (RHSA-2018:0260)

RHEL 7 : systemd (RHSA-2019:0049)

RHEL 7 : systemd (RHSA-2019:0201)

RHEL 7 : systemd (RHSA-2019:0204)

RHEL 7 : systemd (RHSA-2019:0271)

RHEL 7 : systemd (RHSA-2019:0368)

RHEL 7 : systemd (RHSA-2019:1322)

RHEL 7 : systemd (RHSA-2019:1502)

RHEL 7 : systemd (RHSA-2019:2091)

RHEL 7 : systemd (RHSA-2019:2402)

RHEL 7 : systemd (RHSA-2019:2805)

RHEL 7 : systemd (RHSA-2019:3222)

RHEL 7 : systemd (RHSA-2020:0593)

RHEL 7 : systemd (RHSA-2020:1264)

RHEL 7 : taglib (RHSA-2020:1175)

RHEL 7 : tcpdump (RHSA-2017:1871)

RHEL 7 : tcpdump (RHSA-2019:3976)

RHEL 7 : telnet (RHSA-2020:1334)

RHEL 7 : thunderbird (RHSA-2015:0642)

RHEL 7 : thunderbird (RHSA-2018:0648)

RHEL 7 : thunderbird (RHSA-2018:1725)

RHEL 7 : thunderbird (RHSA-2018:2252)

RHEL 7 : thunderbird (RHSA-2018:3458)

RHEL 7 : thunderbird (RHSA-2018:3532)

RHEL 7 : thunderbird (RHSA-2019:0160)

RHEL 7 : thunderbird (RHSA-2019:0270)

RHEL 7 : thunderbird (RHSA-2019:0681)

RHEL 7 : thunderbird (RHSA-2019:1309)

RHEL 7 : thunderbird (RHSA-2019:1626)

RHEL 7 : thunderbird (RHSA-2019:1775)

RHEL 7 : thunderbird (RHSA-2019:2773)

RHEL 7 : thunderbird (RHSA-2019:3210)

RHEL 7 : thunderbird (RHSA-2019:4148)

RHEL 7 : thunderbird (RHSA-2020:0120)

RHEL 7 : thunderbird (RHSA-2020:0576)

RHEL 7 : thunderbird (RHSA-2020:0905)

RHEL 7 : thunderbird (RHSA-2020:1489)

RHEL 7 : tigervnc (RHSA-2015:2233)

RHEL 7 : tigervnc and fltk (RHSA-2017:2000)

RHEL 7 : tomcat (RHSA-2014:0686)

RHEL 7 : tomcat (RHSA-2014:0827)

RHEL 7 : tomcat (RHSA-2014:1034)

RHEL 7 : tomcat (RHSA-2015:0983)

RHEL 7 : tomcat (RHSA-2016:2046) (httpoxy)

RHEL 7 : tomcat (RHSA-2016:2599)

RHEL 7 : tomcat (RHSA-2017:0935)

RHEL 7 : tomcat (RHSA-2017:1809)

RHEL 7 : tomcat (RHSA-2017:2247)

RHEL 7 : tomcat (RHSA-2017:3081)

RHEL 7 : tomcat (RHSA-2018:2921)

RHEL 7 : tomcat (RHSA-2019:0485)

RHEL 7 : tomcat (RHSA-2019:2205)

RHEL 7 : tomcat (RHSA-2020:0855)

RHEL 7 : udisks2 (RHSA-2019:2178)

RHEL 7 : unbound (RHSA-2015:2455)

RHEL 7 : unixODBC (RHSA-2019:2336)

RHEL 7 : unzip (RHSA-2019:2159)

RHEL 7 : unzip (RHSA-2020:1181)

RHEL 7 : uriparser (RHSA-2019:2280)

RHEL 7 : util-linux (RHSA-2016:2605)

RHEL 7 : util-linux (RHSA-2017:0907)

RHEL 7 : vim (RHSA-2019:1793)

RHEL 7 : vim (RHSA-2019:1947)

RHEL 7 : virt-who (RHSA-2015:0430)

RHEL 7 : virtio-win (RHSA-2015:1044)

RHEL 7 : Virtualization (RHSA-2018:0025) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:0028) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:0048) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:0050) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:1104)

RHEL 7 : Virtualization (RHSA-2018:1274)

RHEL 7 : Virtualization (RHSA-2018:1275)

RHEL 7 : Virtualization (RHSA-2018:1452)

RHEL 7 : Virtualization (RHSA-2018:1524)

RHEL 7 : Virtualization (RHSA-2018:1525)

RHEL 7 : Virtualization (RHSA-2018:1654) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:1655) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:1675) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:1690) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:1696) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:1710) (Spectre)

RHEL 7 : Virtualization (RHSA-2018:1713)

RHEL 7 : Virtualization (RHSA-2018:1820)

RHEL 7 : Virtualization (RHSA-2018:2317)

RHEL 7 : Virtualization (RHSA-2018:2321)

RHEL 7 : Virtualization (RHSA-2018:2402) (Foreshadow)

RHEL 7 : Virtualization (RHSA-2018:2403) (Foreshadow)

RHEL 7 : Virtualization (RHSA-2018:2626)

RHEL 7 : Virtualization (RHSA-2018:2643)

RHEL 7 : Virtualization Manager (RHSA-2018:1674) (Spectre)

RHEL 7 : Virtualization Manager (RHSA-2018:1676) (Spectre)

RHEL 7 : Virtualization Manager (RHSA-2018:2071)

RHEL 7 : Virtualization Manager (RHSA-2018:2079)

RHEL 7 : Virtualization Manager (RHSA-2018:2328) (Spectre)

RHEL 7 : Virtualization Manager (RHSA-2018:2887)

RHEL 7 : Virtualization Manager (RHSA-2018:3470)

RHEL 7 : Virtualization Manager (RHSA-2019:0342)

RHEL 7 : Virtualization Manager (RHSA-2019:0361)

RHEL 7 : Virtualization Manager (RHSA-2019:0457)

RHEL 7 : Virtualization Manager (RHSA-2019:0458)

RHEL 7 : Virtualization Manager (RHSA-2019:0461)

RHEL 7 : Virtualization Manager (RHSA-2019:1046) (Spectre)

RHEL 7 : Virtualization Manager (RHSA-2019:1116)

RHEL 7 : Virtualization Manager (RHSA-2019:1179) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1203) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1204) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1205) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1206) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1207) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1208) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1209) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:1569)

RHEL 7 : Virtualization Manager (RHSA-2019:1571)

RHEL 7 : Virtualization Manager (RHSA-2019:1594) (SACK Panic) (SACK Slowness)

RHEL 7 : Virtualization Manager (RHSA-2019:1699) (SACK Panic) (SACK Slowness)

RHEL 7 : Virtualization Manager (RHSA-2019:1968)

RHEL 7 : Virtualization Manager (RHSA-2019:2433)

RHEL 7 : Virtualization Manager (RHSA-2019:2437)

RHEL 7 : Virtualization Manager (RHSA-2019:2439)

RHEL 7 : Virtualization Manager (RHSA-2019:2499)

RHEL 7 : Virtualization Manager (RHSA-2019:2553) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 7 : Virtualization Manager (RHSA-2019:2889)

RHEL 7 : Virtualization Manager (RHSA-2019:2924)

RHEL 7 : Virtualization Manager (RHSA-2019:3011)

RHEL 7 : Virtualization Manager (RHSA-2019:3023)

RHEL 7 : Virtualization Manager (RHSA-2019:3024)

RHEL 7 : Virtualization Manager (RHSA-2019:3179)

RHEL 7 : Virtualization Manager (RHSA-2019:3860)

RHEL 7 : Virtualization Manager (RHSA-2020:0498)

RHEL 7 : Virtualization Manager (RHSA-2020:0730)

RHEL 7 : wget (RHSA-2016:2587)

RHEL 7 : wget (RHSA-2017:3075)

RHEL 7 : wget (RHSA-2018:3052)

RHEL 7 : wget (RHSA-2019:1228)

RHEL 7 : wget (RHSA-2019:2979)

RHEL 7 : wget (RHSA-2019:3168)

RHEL 7 : wireshark (RHSA-2015:2393)

RHEL 7 : wireshark (RHSA-2020:1047)

RHEL 7 : wpa\_supplicant (RHSA-2014:1956)

RHEL 7 : wpa\_supplicant (RHSA-2015:1090)

RHEL 7 : wpa\_supplicant (RHSA-2017:2907) (KRACK)

RHEL 7 : wpa\_supplicant (RHSA-2018:3107)

RHEL 7 : X.org X11 (RHSA-2018:3059)

RHEL 7 : X.org X11 libraries (RHSA-2017:1865)

RHEL 7 : xdg-user-dirs (RHSA-2018:0842)

RHEL 7 : xerces-c (RHSA-2015:1193)

RHEL 7 : xerces-c (RHSA-2016:0430)

RHEL 7 : xerces-c (RHSA-2018:3335)

RHEL 7 : xerces-c (RHSA-2018:3506)

RHEL 7 : xerces-c (RHSA-2018:3514)

RHEL 7 : xerces-c (RHSA-2020:0704)

RHEL 7 : xfsprogs (RHSA-2015:2151)

RHEL 7 : xmlrpc (RHSA-2018:1780)

RHEL 7 : xmlsec1 (RHSA-2017:2492)

RHEL 7 : Xorg (RHSA-2019:2079)

RHEL 7 : xorg-x11-server (RHSA-2018:3410)

RHEL 7 : yum-utils (RHSA-2018:2285)

RHEL 7 : zsh (RHSA-2018:3073)

RHEL 7 : zsh (RHSA-2019:2017)

RHEL 7 : zsh (RHSA-2020:0853)

RHEL 7 : zziplib (RHSA-2018:3229)

RHEL 7 : zziplib (RHSA-2019:2196)

RHEL 7 : zziplib (RHSA-2020:1178)

RHEL 8 : .NET Core on Red Hat Enterprise Linux (RHSA-2019:2731)

RHEL 8 : .NET Core on Red Hat Enterprise Linux (RHSA-2020:0130)

RHEL 8 : 389-ds:1.4 (RHSA-2019:3401)

RHEL 8 : 389-ds:1.4 (RHSA-2020:0464)

RHEL 8 : bind (RHSA-2019:1145)

RHEL 8 : bind (RHSA-2019:1714)

RHEL 8 : bind (RHSA-2019:3552)

RHEL 8 : container-tools:1.0 (RHSA-2019:3494)

RHEL 8 : container-tools:1.0 (RHSA-2019:4273) (Ping Flood) (Reset Flood)

RHEL 8 : container-tools:rhel8 (RHSA-2019:0975)

RHEL 8 : container-tools:rhel8 (RHSA-2019:3403)

RHEL 8 : container-tools:rhel8 (RHSA-2019:4269) (Ping Flood) (Reset Flood)

RHEL 8 : container-tools:rhel8 (RHSA-2020:0348)

RHEL 8 : container-tools:rhel8 (RHSA-2020:1379)

RHEL 8 : curl (RHSA-2019:3701)

RHEL 8 : cyrus-imapd (RHSA-2019:1771)

RHEL 8 : dbus (RHSA-2019:3707)

RHEL 8 : dhcp (RHSA-2019:3525)

RHEL 8 : dotnet (RHSA-2019:1259)

RHEL 8 : dovecot (RHSA-2019:2822)

RHEL 8 : dovecot (RHSA-2019:3467)

RHEL 8 : edk2 (RHSA-2019:0968)

RHEL 8 : edk2 (RHSA-2019:3338)

RHEL 8 : elfutils (RHSA-2019:3575)

RHEL 8 : evolution (RHSA-2019:3699)

RHEL 8 : firefox (RHSA-2019:0966)

RHEL 8 : firefox (RHSA-2019:1269)

RHEL 8 : firefox (RHSA-2019:1696)

RHEL 8 : firefox (RHSA-2019:1764)

RHEL 8 : firefox (RHSA-2019:2663)

RHEL 8 : firefox (RHSA-2019:3196)

RHEL 8 : firefox (RHSA-2019:4111)

RHEL 8 : firefox (RHSA-2020:0111)

RHEL 8 : firefox (RHSA-2020:0295)

RHEL 8 : firefox (RHSA-2020:0512)

RHEL 8 : firefox (RHSA-2020:0519)

RHEL 8 : firefox (RHSA-2020:0819)

RHEL 8 : firefox (RHSA-2020:0820)

RHEL 8 : firefox (RHSA-2020:1340)

RHEL 8 : firefox (RHSA-2020:1341)

RHEL 8 : flatpak (RHSA-2019:1143)

RHEL 8 : freeradius:3.0 (RHSA-2019:1142)

RHEL 8 : freeradius:3.0 (RHSA-2019:3353)

RHEL 8 : fribidi (RHSA-2019:4361)

RHEL 8 : fribidi (RHSA-2020:0291)

RHEL 8 : gdb (RHSA-2019:3352)

RHEL 8 : gettext (RHSA-2019:3643)

RHEL 8 : ghostscript (RHSA-2019:0971)

RHEL 8 : ghostscript (RHSA-2019:2465)

RHEL 8 : ghostscript (RHSA-2019:2591)

RHEL 8 : ghostscript (RHSA-2019:3890)

RHEL 8 : ghostscript (RHSA-2020:0222)

RHEL 8 : git (RHSA-2019:4356)

RHEL 8 : git (RHSA-2020:0228)

RHEL 8 : glib2 (RHSA-2019:3530)

RHEL 8 : glibc (RHSA-2019:3513)

RHEL 8 : GNOME (RHSA-2019:3553)

RHEL 8 : gnutls (RHSA-2019:3600)

RHEL 8 : go-toolset:rhel8 (RHSA-2019:1519)

RHEL 8 : go-toolset:rhel8 (RHSA-2019:2726) (Ping Flood) (Reset Flood)

RHEL 8 : go-toolset:rhel8 (RHSA-2019:3433)

RHEL 8 : go-toolset:rhel8 (RHSA-2020:0329)

RHEL 8 : grub2 (RHSA-2020:0335)

RHEL 8 : gvfs (RHSA-2019:1517)

RHEL 8 : haproxy (RHSA-2020:1288)

RHEL 8 : haproxy (RHSA-2020:1289)

RHEL 8 : http-parser (RHSA-2019:3497)

RHEL 8 : http-parser (RHSA-2020:0707)

RHEL 8 : http-parser (RHSA-2020:0708)

RHEL 8 : httpd:2.4 (RHSA-2019:0980)

RHEL 8 : httpd:2.4 (RHSA-2019:2893) (Internal Data Buffering)

RHEL 8 : httpd:2.4 (RHSA-2019:3436)

RHEL 8 : icedtea-web (RHSA-2019:2004)

RHEL 8 : icu (RHSA-2020:0901)

RHEL 8 : icu (RHSA-2020:0902)

RHEL 8 : idm:DL1 (RHSA-2020:1269)

RHEL 8 : ipmitool (RHSA-2020:0979)

RHEL 8 : ipmitool (RHSA-2020:0981)

RHEL 8 : java-1.8.0-ibm (RHSA-2019:1238)

RHEL 8 : java-1.8.0-ibm (RHSA-2019:2590)

RHEL 8 : java-1.8.0-ibm (RHSA-2020:0046)

RHEL 8 : java-1.8.0-ibm (RHSA-2020:0465)

RHEL 8 : java-1.8.0-openjdk (RHSA-2019:1146)

RHEL 8 : java-1.8.0-openjdk (RHSA-2019:1816)

RHEL 8 : java-1.8.0-openjdk (RHSA-2019:3134)

RHEL 8 : java-1.8.0-openjdk (RHSA-2020:0202)

RHEL 8 : java-1.8.0-openjdk (RHSA-2020:0231)

RHEL 8 : java-11-openjdk (RHSA-2019:1518)

RHEL 8 : java-11-openjdk (RHSA-2019:1817)

RHEL 8 : java-11-openjdk (RHSA-2019:3135)

RHEL 8 : java-11-openjdk (RHSA-2020:0128)

RHEL 8 : java-11-openjdk (RHSA-2020:0232)

RHEL 8 : JBoss EAP (RHSA-2019:1421)

RHEL 8 : JBoss EAP (RHSA-2019:2937)

RHEL 8 : JBoss EAP (RHSA-2019:4020) (Data Dribble) (Ping Flood) (Reset Flood) (Settings Flood)

RHEL 8 : JBoss EAP (RHSA-2020:0161)

RHEL 8 : JBoss EAP (RHSA-2020:0806)

RHEL 8 : kernel (RHSA-2019:1167) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 8 : kernel (RHSA-2019:1479) (SACK Panic) (SACK Slowness)

RHEL 8 : kernel (RHSA-2019:1959)

RHEL 8 : kernel (RHSA-2019:2411)

RHEL 8 : kernel (RHSA-2019:2703)

RHEL 8 : kernel (RHSA-2019:2827)

RHEL 8 : kernel (RHSA-2019:3517)

RHEL 8 : kernel (RHSA-2019:3832)

RHEL 8 : kernel (RHSA-2019:3871)

RHEL 8 : kernel (RHSA-2020:0204)

RHEL 8 : kernel (RHSA-2020:0339)

RHEL 8 : kernel (RHSA-2020:0831)

RHEL 8 : kernel-rt (RHSA-2019:1174) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 8 : kernel-rt (RHSA-2019:1480) (SACK Panic) (SACK Slowness)

RHEL 8 : kernel-rt (RHSA-2019:1971)

RHEL 8 : kernel-rt (RHSA-2019:2405)

RHEL 8 : kernel-rt (RHSA-2019:2741)

RHEL 8 : kernel-rt (RHSA-2019:2828)

RHEL 8 : kernel-rt (RHSA-2019:3309)

RHEL 8 : kernel-rt (RHSA-2019:3833)

RHEL 8 : kernel-rt (RHSA-2019:3870)

RHEL 8 : kernel-rt (RHSA-2020:0328)

RHEL 8 : kernel-rt (RHSA-2020:1378)

RHEL 8 : kpatch-patch (RHSA-2019:3936)

RHEL 8 : kpatch-patch (RHSA-2019:4245)

RHEL 8 : ksh (RHSA-2020:0431)

RHEL 8 : ksh (RHSA-2020:0559)

RHEL 8 : libarchive (RHSA-2019:3698)

RHEL 8 : libarchive (RHSA-2020:0246)

RHEL 8 : libarchive (RHSA-2020:0271)

RHEL 8 : libjpeg-turbo (RHSA-2019:3705)

RHEL 8 : libqb (RHSA-2019:3610)

RHEL 8 : libreswan (RHSA-2019:3391)

RHEL 8 : libseccomp (RHSA-2019:3624)

RHEL 8 : libtiff (RHSA-2019:3419)

RHEL 8 : libvncserver (RHSA-2020:0921)

RHEL 8 : libvorbis (RHSA-2019:3703)

RHEL 8 : libwmf (RHSA-2019:2722)

RHEL 8 : libyang (RHSA-2019:4360)

RHEL 8 : lldpad (RHSA-2019:3673)

RHEL 8 : lua (RHSA-2019:3706)

RHEL 8 : mariadb:10.3 (RHSA-2019:3708)

RHEL 8 : mod\_auth\_mellon (RHSA-2019:0985)

RHEL 8 : mod\_auth\_mellon (RHSA-2019:3421)

RHEL 8 : mysql:8.0 (RHSA-2019:2511)

RHEL 8 : nghttp2 (RHSA-2019:2692) (Data Dribble) (Resource Loop)

RHEL 8 : nginx:1.14 (RHSA-2019:2799) (0-Length Headers Leak) (Data Dribble) (Resource Loop)

RHEL 8 : nodejs:10 (RHSA-2019:2925) (0-Length Headers Leak) (Data Dribble) (Empty Frames Flood) (Internal Data Buffering) (Ping Flood) (Reset Flood) (Resource Loop) (Settings Flood)

RHEL 8 : nodejs:10 (RHSA-2020:0573)

RHEL 8 : nodejs:10 (RHSA-2020:0579)

RHEL 8 : nodejs:10 (RHSA-2020:1317)

RHEL 8 : nodejs:10 (RHSA-2020:1343)

RHEL 8 : nodejs:12 (RHSA-2020:0598)

RHEL 8 : nodejs:12 (RHSA-2020:1293)

RHEL 8 : nss (RHSA-2019:4114)

RHEL 8 : nss (RHSA-2020:0243)

RHEL 8 : nss and nspr (RHSA-2019:1951)

RHEL 8 : numpy (RHSA-2019:3704)

RHEL 8 : openjpeg2 (RHSA-2020:0274)

RHEL 8 : openjpeg2 (RHSA-2020:0296)

RHEL 8 : openjpeg2 (RHSA-2020:0569)

RHEL 8 : openjpeg2 (RHSA-2020:0570)

RHEL 8 : openshift (RHSA-2019:3041) (Data Dribble) (Resource Loop)

RHEL 8 : openshift (RHSA-2020:0477)

RHEL 8 : openshift (RHSA-2020:0734)

RHEL 8 : OpenShift Container Platform 4.1.24 runc (RHSA-2019:3940)

RHEL 8 : OpenShift Container Platform 4.1.38 (RHSA-2020:0695)

RHEL 8 : OpenShift Container Platform 4.1.38 skopeo (RHSA-2020:0697)

RHEL 8 : OpenShift Container Platform 4.2 runc (RHSA-2019:4074)

RHEL 8 : OpenShift Container Platform 4.2.22 runc (RHSA-2020:0688)

RHEL 8 : OpenShift Container Platform 4.2.22 skopeo (RHSA-2020:0689)

RHEL 8 : OpenShift Container Platform 4.2.28 (RHSA-2020:1401)

RHEL 8 : OpenShift Container Platform 4.3.5 podman (RHSA-2020:0680)

RHEL 8 : OpenShift Container Platform 4.3.5 skopeo (RHSA-2020:0679)

RHEL 8 : openssh (RHSA-2019:3702)

RHEL 8 : openssl (RHSA-2019:3700)

RHEL 8 : openstack-manila (RHSA-2020:1326)

RHEL 8 : openvswitch2.11 (RHSA-2020:0171)

RHEL 8 : openvswitch2.12 (RHSA-2020:0172)

RHEL 8 : openwsman (RHSA-2019:0972)

RHEL 8 : osinfo-db and libosinfo (RHSA-2019:3387)

RHEL 8 : pacemaker (RHSA-2019:1279)

RHEL 8 : pango (RHSA-2019:2582)

RHEL 8 : patch (RHSA-2019:2798)

RHEL 8 : php:7.2 (RHSA-2019:3735)

RHEL 8 : php:7.2 (RHSA-2020:0322)

RHEL 8 : php:7.3 (RHSA-2019:3736)

RHEL 8 : pki-deps:10.6 (RHSA-2019:1529)

RHEL 8 : pki-deps:10.6 (RHSA-2019:2720)

RHEL 8 : poppler (RHSA-2019:2713)

RHEL 8 : ppp (RHSA-2020:0633)

RHEL 8 : ppp (RHSA-2020:0634)

RHEL 8 : python-jinja2 (RHSA-2019:1152)

RHEL 8 : python-pillow (RHSA-2020:0566)

RHEL 8 : python-pillow (RHSA-2020:0580)

RHEL 8 : python-reportlab (RHSA-2020:0201)

RHEL 8 : python-reportlab (RHSA-2020:0230)

RHEL 8 : python-urllib3 (RHSA-2019:3590)

RHEL 8 : python-XStatic-jQuery (RHSA-2020:1325)

RHEL 8 : python27:2.7 (RHSA-2019:0981)

RHEL 8 : python27:2.7 (RHSA-2019:3335)

RHEL 8 : python3 (RHSA-2019:0997)

RHEL 8 : python3 (RHSA-2019:3520)

RHEL 8 : python36:3.6 (RHSA-2019:0984)

RHEL 8 : qt5-qtbase (RHSA-2019:3390)

RHEL 8 : Red Hat OpenShift Service Mesh 1.0.3 RPMs (RHSA-2019:4222)

RHEL 8 : Red Hat Single Sign-On 7.3.4 (RHSA-2019:3046)

RHEL 8 : Red Hat Single Sign-On 7.3.5 (RHSA-2019:4042) (Ping Flood) (Reset Flood) (Settings Flood)

RHEL 8 : Red Hat Single Sign-On 7.3.7 security update on RHEL 8 (Important) (RHSA-2020:0947)

RHEL 8 : redis:5 (RHSA-2019:2002)

RHEL 8 : ruby:2.5 (RHSA-2019:1972)

RHEL 8 : samba (RHSA-2019:3582)

RHEL 8 : SDL (RHSA-2019:3951)

RHEL 8 : SDL (RHSA-2020:0293)

RHEL 8 : sqlite (RHSA-2020:0229)

RHEL 8 : sqlite (RHSA-2020:0273)

RHEL 8 : squid:4 (RHSA-2019:2593)

RHEL 8 : squid:4 (RHSA-2019:3476)

RHEL 8 : sssd (RHSA-2019:3651)

RHEL 8 : subversion:1.10 (RHSA-2019:2512)

RHEL 8 : sudo (RHSA-2019:3694)

RHEL 8 : sudo (RHSA-2020:0388)

RHEL 8 : sudo (RHSA-2020:0487)

RHEL 8 : sudo (RHSA-2020:0509)

RHEL 8 : systemd (RHSA-2019:0990)

RHEL 8 : systemd (RHSA-2019:3592)

RHEL 8 : systemd (RHSA-2020:0564)

RHEL 8 : systemd (RHSA-2020:0575)

RHEL 8 : telnet (RHSA-2020:1318)

RHEL 8 : telnet (RHSA-2020:1342)

RHEL 8 : thunderbird (RHSA-2019:1144)

RHEL 8 : thunderbird (RHSA-2019:1308)

RHEL 8 : thunderbird (RHSA-2019:1623)

RHEL 8 : thunderbird (RHSA-2019:1799)

RHEL 8 : thunderbird (RHSA-2019:2774)

RHEL 8 : thunderbird (RHSA-2019:3237)

RHEL 8 : thunderbird (RHSA-2019:4195)

RHEL 8 : thunderbird (RHSA-2020:0127)

RHEL 8 : thunderbird (RHSA-2020:0292)

RHEL 8 : thunderbird (RHSA-2020:0565)

RHEL 8 : thunderbird (RHSA-2020:0577)

RHEL 8 : thunderbird (RHSA-2020:0918)

RHEL 8 : thunderbird (RHSA-2020:0919)

RHEL 8 : thunderbird (RHSA-2020:1495)

RHEL 8 : thunderbird (RHSA-2020:1496)

RHEL 8 : virt-manager (RHSA-2019:3464)

RHEL 8 : virt:rhel (RHSA-2019:1175) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 8 : virt:rhel (RHSA-2019:1268)

RHEL 8 : virt:rhel (RHSA-2019:1580)

RHEL 8 : virt:rhel (RHSA-2019:3345)

RHEL 8 : virt:rhel (RHSA-2020:0279)

RHEL 8 : virt:rhel (RHSA-2020:1344)

RHEL 8 : Virtualization Manager (RHSA-2019:1455) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

RHEL 8 : Virtualization Manager (RHSA-2019:1762)

RHEL 8 : Virtualization Manager (RHSA-2020:0555)

RHEL 8 : Virtualization Manager (RHSA-2020:0731)

RHEL 8 : WALinuxAgent (RHSA-2019:1527)

RHEL 8 : wget (RHSA-2019:0983)

RHEL 8 : yum (RHSA-2019:3583)

RHEL 8 : zsh (RHSA-2020:0903)

RHEL 8 : zsh (RHSA-2020:0978)

RHSA-2003-145: kernel

# PhotonOS Local Security Checks

Photon OS 1.0 : freetype2 / binutils (PhotonOS-PHSA-2018-1.0-0148) (deprecated)

Photon OS 1.0 : gcc / nghttp2 (PhotonOS-PHSA-2018-1.0-0150 (deprecated)

Photon OS 1.0 : libmspack (PhotonOS-PHSA-2018-1.0-0140) (deprecated)

Photon OS 1.0 : linux / linux-esx (PhotonOS-PHSA-2018-1.0-0151) (Spectre) (deprecated)

Photon OS 1.0 : openssl / libsoup (PhotonOS-PHSA-2018-1.0-0149) (deprecated)

Photon OS 1.0 : patch (PhotonOS-PHSA-2018-1.0-0142) (deprecated)

Photon OS 1.0 : unzip (PhotonOS-PHSA-2018-1.0-0144) (deprecated)

Photon OS 1.0: Apache / Binutils PHSA-2018-1.0-0154 (deprecated)

Photon OS 1.0: Apache / Mercurial PHSA-2016-0011 (deprecated)

Photon OS 1.0: Apache PHSA-2017-0012 (deprecated)

Photon OS 1.0: Apache PHSA-2019-1.0-0227

Photon OS 1.0: Apache PHSA-2019-1.0-0244

Photon OS 1.0: Apache PHSA-2020-1.0-0264

Photon OS 1.0: Apr / Krb5 / Linux / Ncurses / Subversion PHSA-2017-1.0-0093 (deprecated)

Photon OS 1.0: Apr PHSA-2017-1.0-0093

Photon OS 1.0: Bash / Curl / Mariadb / Openvswitch / Systemd PHSA-2017-0044 (deprecated)

Photon OS 1.0: Bash / Glibc / Libgcrypt / Libtar / Openjdk / Openjre / Strongswan / Unzip PHSA-2017-0040 (deprecated)

Photon OS 1.0: Bash PHSA-2017-0009

Photon OS 1.0: Bash PHSA-2017-0009 (deprecated)

Photon OS 1.0: Bash PHSA-2017-0040

Photon OS 1.0: Bash PHSA-2017-0044

Photon OS 1.0: Bash PHSA-2019-1.0-0229

Photon OS 1.0: Bash PHSA-2019-1.0-0252

Photon OS 1.0: Bash PHSA-2019-1.0-0255

Photon OS 1.0: Bash PHSA-2020-1.0-0277

Photon OS 1.0: Bindutils / Krb5 / Ruby / Sudo / Zlib PHSA-2017-0021 (deprecated)

Photon OS 1.0: Bindutils PHSA-2017-0021

Photon OS 1.0: Bindutils PHSA-2020-1.0-0287

Photon OS 1.0: Binutils / C / Dnsmasq / Git / Gnutls / Krb5 / Linux / Mercurial / Mesos / Nginx PHSA-2017-0038 (deprecated)

Photon OS 1.0: Binutils / Curl / Docker / Linux / Rpm PHSA-2017-1.0-0095 (deprecated)

Photon OS 1.0: Binutils / File / Linux / Pcre / Shadow PHSA-2018-1.0-0171 (deprecated)

Photon OS 1.0: Binutils / Glibc / Linux / Mongodb / Openssh / Procmail / Python2 / Rsync PHSA-2017-0052 (deprecated)

Photon OS 1.0: Binutils / Httpd / Mercurial / Mysql / Net / Paramiko / Patch / Pycrypto / Python3 / Sqlite / Strongswan / Xerces PHSA-2018-1.0-0126 (deprecated)

Photon OS 1.0: Binutils / Libarchive / Ntp PHSA-2017-0010 (deprecated)

Photon OS 1.0: Binutils PHSA-2017-0010

Photon OS 1.0: Binutils PHSA-2017-1.0-0095

Photon OS 1.0: Binutils PHSA-2018-1.0-0104

Photon OS 1.0: Binutils PHSA-2018-1.0-0104 (deprecated)

Photon OS 1.0: Binutils PHSA-2018-1.0-0112

Photon OS 1.0: Binutils PHSA-2018-1.0-0112 (deprecated)

Photon OS 1.0: Binutils PHSA-2018-1.0-0126

Photon OS 1.0: Binutils PHSA-2018-1.0-0148

Photon OS 1.0: Binutils PHSA-2018-1.0-0154

Photon OS 1.0: Binutils PHSA-2018-1.0-0171

Photon OS 1.0: Binutils PHSA-2019-1.0-0203

Photon OS 1.0: Binutils PHSA-2019-1.0-0218

Photon OS 1.0: Binutils PHSA-2019-1.0-0237

Photon OS 1.0: Binutils PHSA-2019-1.0-0239

Photon OS 1.0: Binutils PHSA-2019-1.0-0242

Photon OS 1.0: Binutils PHSA-2019-1.0-0257

Photon OS 1.0: Blktrace / Libmspack / Ntp / Openjdk / Perl / Systemd / Vim PHSA-2018-1.0-0167 (deprecated)

Photon OS 1.0: Blktrace PHSA-2018-1.0-0167

Photon OS 1.0: Bzip2 PHSA-2019-1.0-0242

Photon OS 1.0: Cairo / Go / Libxml2 / Openvswitch PHSA-2017-0039 (deprecated)

Photon OS 1.0: Cairo PHSA-2017-0039

Photon OS 1.0: Cairo PHSA-2019-1.0-0220

Photon OS 1.0: Cassandra / Libxml2 / Linux / Ruby PHSA-2017-0029 (deprecated)

Photon OS 1.0: Cpio PHSA-2020-1.0-0267

Photon OS 1.0: Cracklib / Glibc / Httpd / Libevent / Libgcrypt PHSA-2017-0013 (deprecated)

Photon OS 1.0: Cracklib PHSA-2017-0013

Photon OS 1.0: Curl / Freetype2 / Glibc / Systemd PHSA-2017-0041 (deprecated)

Photon OS 1.0: Curl / Glibc PHSA-2017-0048 (deprecated)

Photon OS 1.0: Curl / Postgresql PHSA-2018-1.0-0108 (deprecated)

Photon OS 1.0: Curl PHSA-2017-0041

Photon OS 1.0: Curl PHSA-2017-0044

Photon OS 1.0: Curl PHSA-2017-1.0-0095

Photon OS 1.0: Curl PHSA-2018-1.0-0108

Photon OS 1.0: Curl PHSA-2018-1.0-0124

Photon OS 1.0: Curl PHSA-2018-1.0-0124 (deprecated)

Photon OS 1.0: Curl PHSA-2018-1.0-0158

Photon OS 1.0: Curl PHSA-2018-1.0-0158 (deprecated)

Photon OS 1.0: Curl PHSA-2018-1.0-0186

Photon OS 1.0: Curl PHSA-2018-1.0-0186 (deprecated)

Photon OS 1.0: Curl PHSA-2019-1.0-0203

Photon OS 1.0: Curl PHSA-2019-1.0-0205

Photon OS 1.0: Curl PHSA-2019-1.0-0209

Photon OS 1.0: Curl PHSA-2019-1.0-0237

Photon OS 1.0: Cyrus PHSA-2020-1.0-0283

Photon OS 1.0: Dbus PHSA-2019-1.0-0249

Photon OS 1.0: Dbus PHSA-2020-1.0-0264

Photon OS 1.0: Dhcp / Libtasn1 / Subversion / Unzip PHSA-2016-0013 (deprecated)

Photon OS 1.0: Dhcp PHSA-2016-0013

Photon OS 1.0: Dhcp PHSA-2019-1.0-0259

Photon OS 1.0: Dnsmasq / Grub2 / Haproxy / Linux / Nginx / Vim / Wget / Zookeeper PHSA-2016-0012 (deprecated)

Photon OS 1.0: Dnsmasq / Libtasn1 PHSA-2018-1.0-0109 (deprecated)

Photon OS 1.0: Dnsmasq PHSA-2016-0012

Photon OS 1.0: Dnsmasq PHSA-2017-0035

Photon OS 1.0: Dnsmasq PHSA-2017-0035 (deprecated)

Photon OS 1.0: Dnsmasq PHSA-2018-1.0-0109

Photon OS 1.0: Dnsmasq PHSA-2020-1.0-0265

Photon OS 1.0: Docker PHSA-2017-1.0-0095

Photon OS 1.0: Docker PHSA-2019-1.0-0238

Photon OS 1.0: E2Fsprogs PHSA-2020-1.0-0268

Photon OS 1.0: Elasticsearch PHSA-2019-1.0-0205

Photon OS 1.0: Elasticsearch PHSA-2019-1.0-0209

Photon OS 1.0: Elfutils PHSA-2018-1.0-0194

Photon OS 1.0: Elfutils PHSA-2019-1.0-0204

Photon OS 1.0: Elfutils PHSA-2019-1.0-0226

Photon OS 1.0: Elfutils PHSA-2019-1.0-0239

Photon OS 1.0: Envoy PHSA-2019-1.0-0241

Photon OS 1.0: Envoy PHSA-2020-1.0-0268

Photon OS 1.0: Envoy PHSA-2020-1.0-0281

Photon OS 1.0: Envoy PHSA-2020-1.0-0286

Photon OS 1.0: Expat PHSA-2019-1.0-0247

Photon OS 1.0: File PHSA-2018-1.0-0171

Photon OS 1.0: Freetype2 / Gnutls / Linux / Tar PHSA-2017-0015 (deprecated)

Photon OS 1.0: Freetype2 / Libtirpc / Rpcbind PHSA-2017-0017 (deprecated)

Photon OS 1.0: Freetype2 PHSA-2017-0015

Photon OS 1.0: Freetype2 PHSA-2017-0017

Photon OS 1.0: Freetype2 PHSA-2017-0041

Photon OS 1.0: Freetype2 PHSA-2018-1.0-0148

Photon OS 1.0: Fuse PHSA-2019-1.0-0204

Photon OS 1.0: Gc PHSA-2019-1.0-0260

Photon OS 1.0: Gcc PHSA-2018-1.0-0150

Photon OS 1.0: Gdb PHSA-2020-1.0-0287

Photon OS 1.0: Git PHSA-2018-1.0-0145

Photon OS 1.0: Git PHSA-2019-1.0-0263

Photon OS 1.0: Glib PHSA-2018-1.0-0194

Photon OS 1.0: Glib PHSA-2019-1.0-0237

Photon OS 1.0: Glib PHSA-2019-1.0-0245

Photon OS 1.0: Glibc / Linux PHSA-2017-0022 (deprecated)

Photon OS 1.0: Glibc / Ruby PHSA-2018-1.0-0098-(a) (deprecated)

Photon OS 1.0: Glibc / Shadow / Systemd / Wget PHSA-2017-0023 (deprecated)

Photon OS 1.0: Glibc PHSA-2017-0013

Photon OS 1.0: Glibc PHSA-2017-0022

Photon OS 1.0: Glibc PHSA-2017-0023

Photon OS 1.0: Glibc PHSA-2017-0040

Photon OS 1.0: Glibc PHSA-2017-0041

Photon OS 1.0: Glibc PHSA-2018-1.0-0098-(a)

Photon OS 1.0: Glibc PHSA-2018-1.0-0111

Photon OS 1.0: Glibc PHSA-2018-1.0-0111 (deprecated)

Photon OS 1.0: Glibc PHSA-2018-1.0-0155

Photon OS 1.0: Glibc PHSA-2018-1.0-0155 (deprecated)

Photon OS 1.0: Glibc PHSA-2018-1.0-0159

Photon OS 1.0: Glibc PHSA-2018-1.0-0159 (deprecated)

Photon OS 1.0: Glibc PHSA-2019-1.0-0209

Photon OS 1.0: Gnupg PHSA-2019-1.0-0237

Photon OS 1.0: Gnupg PHSA-2019-1.0-0246

Photon OS 1.0: Gnupg PHSA-2020-1.0-0288

Photon OS 1.0: Gnutls / Linux / Openjdk / Openjre PHSA-2017-0016 (deprecated)

Photon OS 1.0: Gnutls PHSA-2017-0015

Photon OS 1.0: Gnutls PHSA-2017-0016

Photon OS 1.0: Gnutls PHSA-2019-1.0-0224

Photon OS 1.0: Go PHSA-2017-0039

Photon OS 1.0: Go PHSA-2018-1.0-0117

Photon OS 1.0: Go PHSA-2018-1.0-0117 (deprecated)

Photon OS 1.0: Go PHSA-2018-1.0-0123

Photon OS 1.0: Go PHSA-2018-1.0-0123 (deprecated)

Photon OS 1.0: Go PHSA-2019-1.0-0250

Photon OS 1.0: Go PHSA-2020-1.0-0264

Photon OS 1.0: Grub2 PHSA-2016-0012

Photon OS 1.0: Guile / Ntp / Ntpstat PHSA-2017-0003 (deprecated)

Photon OS 1.0: Guile PHSA-2017-0003

Photon OS 1.0: Haproxy PHSA-2016-0012

Photon OS 1.0: Haproxy PHSA-2019-1.0-0220

Photon OS 1.0: Haproxy PHSA-2019-1.0-0226

Photon OS 1.0: Haproxy PHSA-2019-1.0-0249

Photon OS 1.0: Haproxy PHSA-2019-1.0-0263

Photon OS 1.0: Httpd PHSA-2017-0013

Photon OS 1.0: Httpd PHSA-2017-0027

Photon OS 1.0: Httpd PHSA-2017-0027 (deprecated)

Photon OS 1.0: Httpd PHSA-2018-1.0-0126

Photon OS 1.0: Httpd PHSA-2018-1.0-0181

Photon OS 1.0: Httpd PHSA-2018-1.0-0181 (deprecated)

Photon OS 1.0: Httpd PHSA-2019-1.0-0203

Photon OS 1.0: Httpd PHSA-2019-1.0-0230

Photon OS 1.0: Httpd PHSA-2019-1.0-0253

Photon OS 1.0: Ipmitool PHSA-2020-1.0-0278

Photon OS 1.0: Keepalived PHSA-2019-1.0-0212

Photon OS 1.0: Keepalived PHSA-2019-1.0-0235

Photon OS 1.0: Kibana PHSA-2019-1.0-0205

Photon OS 1.0: Kibana PHSA-2019-1.0-0209

Photon OS 1.0: Krb5 / Linux PHSA-2017-0011 (deprecated)

Photon OS 1.0: Krb5 PHSA-2017-0011

Photon OS 1.0: Krb5 PHSA-2017-0021

Photon OS 1.0: Krb5 PHSA-2017-1.0-0093

Photon OS 1.0: Krb5 PHSA-2018-1.0-0177

Photon OS 1.0: Krb5 PHSA-2018-1.0-0177 (deprecated)

Photon OS 1.0: Krb5 PHSA-2019-1.0-0239

Photon OS 1.0: Kubernetes PHSA-2019-1.0-0202

Photon OS 1.0: Kubernetes PHSA-2019-1.0-0242

Photon OS 1.0: Kubernetes PHSA-2019-1.0-0252

Photon OS 1.0: Kubernetes PHSA-2019-1.0-0255

Photon OS 1.0: Kubernetes PHSA-2020-1.0-0264

Photon OS 1.0: Kubernetes PHSA-2020-1.0-0288

Photon OS 1.0: Libarchive PHSA-2017-0010

Photon OS 1.0: Libarchive PHSA-2019-1.0-0227

Photon OS 1.0: Libarchive PHSA-2019-1.0-0257

Photon OS 1.0: Libevent PHSA-2017-0013

Photon OS 1.0: Libgcrypt / Libsoup PHSA-2018-1.0-0182 (deprecated)

Photon OS 1.0: Libgcrypt PHSA-2017-0013

Photon OS 1.0: Libgcrypt PHSA-2017-0040

Photon OS 1.0: Libgcrypt PHSA-2018-1.0-0182

Photon OS 1.0: Libgcrypt PHSA-2020-1.0-0288

Photon OS 1.0: Libmspack PHSA-2018-1.0-0140

Photon OS 1.0: Libmspack PHSA-2018-1.0-0167

Photon OS 1.0: Libmspack PHSA-2019-1.0-0247

Photon OS 1.0: Libpng PHSA-2019-1.0-0246

Photon OS 1.0: Librelp / Libvirt PHSA-2018-1.0-0129 (deprecated)

Photon OS 1.0: Librelp PHSA-2018-1.0-0129

Photon OS 1.0: Libseccomp PHSA-2019-1.0-0228

Photon OS 1.0: Libsolv PHSA-2019-1.0-0212

Photon OS 1.0: Libsoup PHSA-2018-1.0-0149

Photon OS 1.0: Libsoup PHSA-2018-1.0-0182

Photon OS 1.0: Libsoup PHSA-2019-1.0-0236

Photon OS 1.0: Libsoup PHSA-2019-1.0-0257

Photon OS 1.0: Libssh2 PHSA-2019-1.0-0220

Photon OS 1.0: Libssh2 PHSA-2019-1.0-0222

Photon OS 1.0: Libssh2 PHSA-2019-1.0-0263

Photon OS 1.0: Libtar PHSA-2017-0040

Photon OS 1.0: Libtasn1 PHSA-2016-0013

Photon OS 1.0: Libtasn1 PHSA-2018-1.0-0109

Photon OS 1.0: Libtirpc PHSA-2017-0017

Photon OS 1.0: Libtirpc PHSA-2018-1.0-0198

Photon OS 1.0: Libtirpc PHSA-2018-1.0-0198 (deprecated)

Photon OS 1.0: Libvirt PHSA-2018-1.0-0129

Photon OS 1.0: Libvirt PHSA-2019-1.0-0237

Photon OS 1.0: Libvirt PHSA-2020-1.0-0276

Photon OS 1.0: Libxml2 / Linux / Openssh PHSA-2017-0001 (deprecated)

Photon OS 1.0: Libxml2 / Ncurses / Openldap / Ruby PHSA-2017-0024 (deprecated)

Photon OS 1.0: Libxml2 PHSA-2017-0001

Photon OS 1.0: Libxml2 PHSA-2017-0024

Photon OS 1.0: Libxml2 PHSA-2017-0029

Photon OS 1.0: Libxml2 PHSA-2017-0039

Photon OS 1.0: Libxml2 PHSA-2018-1.0-0193

Photon OS 1.0: Libxml2 PHSA-2020-1.0-0271

Photon OS 1.0: Libxslt / Linux / Sqlite PHSA-2017-0025 (deprecated)

Photon OS 1.0: Libxslt PHSA-2017-0025

Photon OS 1.0: Libxslt PHSA-2019-1.0-0224

Photon OS 1.0: Libxslt PHSA-2019-1.0-0246

Photon OS 1.0: Libxslt PHSA-2019-1.0-0257

Photon OS 1.0: Libxslt PHSA-2019-1.0-0263

Photon OS 1.0: Linux / Openssh PHSA-2016-0014 (deprecated)

Photon OS 1.0: Linux / Openssl PHSA-2017-0042 (deprecated)

Photon OS 1.0: Linux / Rsync PHSA-2018-1.0-0096 (deprecated)

Photon OS 1.0: Linux / Rsync PHSA-2018-1.0-0132 (deprecated)

Photon OS 1.0: Linux / Vim PHSA-2017-0006 (deprecated)

Photon OS 1.0: Linux PHSA-2016-0012

Photon OS 1.0: Linux PHSA-2016-0014

Photon OS 1.0: Linux PHSA-2017-0001

Photon OS 1.0: Linux PHSA-2017-0006

Photon OS 1.0: Linux PHSA-2017-0008 (deprecated)

Photon OS 1.0: Linux PHSA-2017-0011

Photon OS 1.0: Linux PHSA-2017-0014

Photon OS 1.0: Linux PHSA-2017-0014 (deprecated)

Photon OS 1.0: Linux PHSA-2017-0015

Photon OS 1.0: Linux PHSA-2017-0016

Photon OS 1.0: Linux PHSA-2017-0018 (deprecated)

Photon OS 1.0: Linux PHSA-2017-0019

Photon OS 1.0: Linux PHSA-2017-0019 (deprecated)

Photon OS 1.0: Linux PHSA-2017-0022

Photon OS 1.0: Linux PHSA-2017-0025

Photon OS 1.0: Linux PHSA-2017-0028

Photon OS 1.0: Linux PHSA-2017-0028 (deprecated)

Photon OS 1.0: Linux PHSA-2017-0029

Photon OS 1.0: Linux PHSA-2017-0032

Photon OS 1.0: Linux PHSA-2017-0032 (deprecated)

Photon OS 1.0: Linux PHSA-2017-0036

Photon OS 1.0: Linux PHSA-2017-0036 (deprecated)

Photon OS 1.0: Linux PHSA-2017-0042

Photon OS 1.0: Linux PHSA-2017-0049

Photon OS 1.0: Linux PHSA-2017-0049 (deprecated)

Photon OS 1.0: Linux PHSA-2017-1.0-0093

Photon OS 1.0: Linux PHSA-2017-1.0-0095

Photon OS 1.0: Linux PHSA-2018-1.0-0096

Photon OS 1.0: Linux PHSA-2018-1.0-0097

Photon OS 1.0: Linux PHSA-2018-1.0-0097 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0098

Photon OS 1.0: Linux PHSA-2018-1.0-0098 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0102

Photon OS 1.0: Linux PHSA-2018-1.0-0102 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0107

Photon OS 1.0: Linux PHSA-2018-1.0-0107 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0132

Photon OS 1.0: Linux PHSA-2018-1.0-0132-(a)

Photon OS 1.0: Linux PHSA-2018-1.0-0132-(a) (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0133

Photon OS 1.0: Linux PHSA-2018-1.0-0133 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0134

Photon OS 1.0: Linux PHSA-2018-1.0-0134 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0135

Photon OS 1.0: Linux PHSA-2018-1.0-0135 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0151

Photon OS 1.0: Linux PHSA-2018-1.0-0161

Photon OS 1.0: Linux PHSA-2018-1.0-0161 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0165

Photon OS 1.0: Linux PHSA-2018-1.0-0165 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0169

Photon OS 1.0: Linux PHSA-2018-1.0-0169 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0174

Photon OS 1.0: Linux PHSA-2018-1.0-0174 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0180

Photon OS 1.0: Linux PHSA-2018-1.0-0184

Photon OS 1.0: Linux PHSA-2018-1.0-0184 (deprecated)

Photon OS 1.0: Linux PHSA-2018-1.0-0188

Photon OS 1.0: Linux PHSA-2018-1.0-0188 (deprecated)

Photon OS 1.0: Linux PHSA-2019-1.0-0205

Photon OS 1.0: Linux PHSA-2019-1.0-0211

Photon OS 1.0: Linux PHSA-2019-1.0-0235

Photon OS 1.0: Linux PHSA-2019-1.0-0236

Photon OS 1.0: Linux PHSA-2019-1.0-0240

Photon OS 1.0: Linux PHSA-2019-1.0-0251

Photon OS 1.0: Linux PHSA-2019-1.0-0252

Photon OS 1.0: Linux PHSA-2019-1.0-0255

Photon OS 1.0: Linux PHSA-2019-1.0-0259

Photon OS 1.0: Linux PHSA-2019-1.0-0262

Photon OS 1.0: Linux PHSA-2020-1.0-0279

Photon OS 1.0: Linux PHSA-2020-1.0-0287

Photon OS 1.0: Logstash PHSA-2019-1.0-0260

Photon OS 1.0: Mariadb PHSA-2017-0044

Photon OS 1.0: Mercurial PHSA-2016-0011

Photon OS 1.0: Mercurial PHSA-2018-1.0-0126

Photon OS 1.0: Mercurial PHSA-2019-1.0-0235

Photon OS 1.0: Mesos PHSA-2019-1.0-0239

Photon OS 1.0: Mysql / Openjdk PHSA-2018-1.0-0130 (deprecated)

Photon OS 1.0: Mysql PHSA-2018-1.0-0103

Photon OS 1.0: Mysql PHSA-2018-1.0-0103 (deprecated)

Photon OS 1.0: Mysql PHSA-2018-1.0-0126

Photon OS 1.0: Mysql PHSA-2018-1.0-0130

Photon OS 1.0: Mysql PHSA-2018-1.0-0170

Photon OS 1.0: Mysql PHSA-2018-1.0-0170 (deprecated)

Photon OS 1.0: Mysql PHSA-2019-1.0-0212

Photon OS 1.0: Mysql PHSA-2020-1.0-0284

Photon OS 1.0: Ncurses / Strongswan PHSA-2018-1.0-0164 (deprecated)

Photon OS 1.0: Ncurses PHSA-2017-0024

Photon OS 1.0: Ncurses PHSA-2017-1.0-0093

Photon OS 1.0: Ncurses PHSA-2018-1.0-0164

Photon OS 1.0: Ncurses PHSA-2020-1.0-0281

Photon OS 1.0: Net PHSA-2018-1.0-0126

Photon OS 1.0: Net PHSA-2019-1.0-0203

Photon OS 1.0: Nettle PHSA-2018-1.0-0119

Photon OS 1.0: Nettle PHSA-2018-1.0-0119 (deprecated)

Photon OS 1.0: Nghttp2 PHSA-2018-1.0-0150

Photon OS 1.0: Nginx PHSA-2016-0012

Photon OS 1.0: Nginx PHSA-2018-1.0-0201

Photon OS 1.0: Nginx PHSA-2019-1.0-0211

Photon OS 1.0: Nginx PHSA-2020-1.0-0276

Photon OS 1.0: Nodejs PHSA-2019-1.0-0257

Photon OS 1.0: Nss PHSA-2019-1.0-0239

Photon OS 1.0: Ntp / Linux PHSA-2018-1.0-0180 (deprecated)

Photon OS 1.0: Ntp PHSA-2017-0003

Photon OS 1.0: Ntp PHSA-2017-0010

Photon OS 1.0: Ntp PHSA-2018-1.0-0167

Photon OS 1.0: Ntp PHSA-2018-1.0-0180

Photon OS 1.0: Ntpstat PHSA-2017-0003

Photon OS 1.0: Openjdk / Openjre / Postgresql PHSA-2016-0015 (deprecated)

Photon OS 1.0: Openjdk / Openjre / Pycrypto / Python3 PHSA-2017-0026 (deprecated)

Photon OS 1.0: Openjdk PHSA-2016-0015

Photon OS 1.0: Openjdk PHSA-2017-0016

Photon OS 1.0: Openjdk PHSA-2017-0026

Photon OS 1.0: Openjdk PHSA-2017-0040

Photon OS 1.0: Openjdk PHSA-2018-1.0-0101

Photon OS 1.0: Openjdk PHSA-2018-1.0-0101 (deprecated)

Photon OS 1.0: Openjdk PHSA-2018-1.0-0130

Photon OS 1.0: Openjdk PHSA-2018-1.0-0167

Photon OS 1.0: Openjdk PHSA-2018-1.0-0192

Photon OS 1.0: Openjdk PHSA-2018-1.0-0192 (deprecated)

Photon OS 1.0: Openjdk PHSA-2019-1.0-0250

Photon OS 1.0: Openjre PHSA-2016-0015

Photon OS 1.0: Openjre PHSA-2017-0016

Photon OS 1.0: Openjre PHSA-2017-0026

Photon OS 1.0: Openjre PHSA-2017-0040

Photon OS 1.0: Openldap PHSA-2017-0024

Photon OS 1.0: Openssh PHSA-2016-0014

Photon OS 1.0: Openssh PHSA-2017-0001

Photon OS 1.0: Openssh PHSA-2019-1.0-0237

Photon OS 1.0: Openssl PHSA-2017-0042

Photon OS 1.0: Openssl PHSA-2018-1.0-0097-(a)

Photon OS 1.0: Openssl PHSA-2018-1.0-0097-(a) (deprecated)

Photon OS 1.0: Openssl PHSA-2018-1.0-0149

Photon OS 1.0: Openssl PHSA-2018-1.0-0175

Photon OS 1.0: Openssl PHSA-2018-1.0-0199

Photon OS 1.0: Openssl PHSA-2019-1.0-0252

Photon OS 1.0: Openssl PHSA-2019-1.0-0255

Photon OS 1.0: Openssl PHSA-2020-1.0-0264

Photon OS 1.0: Openvswitch PHSA-2017-0020

Photon OS 1.0: Openvswitch PHSA-2017-0020 (deprecated)

Photon OS 1.0: Openvswitch PHSA-2017-0039

Photon OS 1.0: Openvswitch PHSA-2017-0044

Photon OS 1.0: Openvswitch PHSA-2020-1.0-0288

Photon OS 1.0: Paramiko PHSA-2019-1.0-0205

Photon OS 1.0: Patch PHSA-2018-1.0-0126

Photon OS 1.0: Patch PHSA-2018-1.0-0142

Photon OS 1.0: Patch PHSA-2018-1.0-0189

Photon OS 1.0: Patch PHSA-2018-1.0-0189 (deprecated)

Photon OS 1.0: Pcre PHSA-2018-1.0-0171

Photon OS 1.0: Perl / Ruby PHSA-2017-0037 (deprecated)

Photon OS 1.0: Perl PHSA-2017-0037

Photon OS 1.0: Perl PHSA-2018-1.0-0167

Photon OS 1.0: Perl PHSA-2018-1.0-0175

Photon OS 1.0: Perl PHSA-2019-1.0-0212

Photon OS 1.0: Polkit PHSA-2019-1.0-0227

Photon OS 1.0: Polkit PHSA-2019-1.0-0236

Photon OS 1.0: Postgresql / Python2 / Python3 / Strongswan PHSA-2018-1.0-0178 (deprecated)

Photon OS 1.0: Postgresql PHSA-2016-0015

Photon OS 1.0: Postgresql PHSA-2018-1.0-0108

Photon OS 1.0: Postgresql PHSA-2018-1.0-0122

Photon OS 1.0: Postgresql PHSA-2018-1.0-0122 (deprecated)

Photon OS 1.0: Postgresql PHSA-2018-1.0-0178

Photon OS 1.0: Postgresql PHSA-2019-1.0-0243

Photon OS 1.0: Postgresql PHSA-2019-1.0-0257

Photon OS 1.0: Postgresql PHSA-2019-1.0-0261

Photon OS 1.0: Postgresql PHSA-2020-1.0-0287

Photon OS 1.0: Procps PHSA-2018-1.0-0175

Photon OS 1.0: Pycrypto PHSA-2017-0026

Photon OS 1.0: Pycrypto PHSA-2018-1.0-0126

Photon OS 1.0: Python2 PHSA-2018-1.0-0125

Photon OS 1.0: Python2 PHSA-2018-1.0-0125 (deprecated)

Photon OS 1.0: Python2 PHSA-2018-1.0-0178

Photon OS 1.0: Python2 PHSA-2019-1.0-0203

Photon OS 1.0: Python2 PHSA-2019-1.0-0220

Photon OS 1.0: Python2 PHSA-2019-1.0-0236

Photon OS 1.0: Python2 PHSA-2019-1.0-0237

Photon OS 1.0: Python2 PHSA-2019-1.0-0240

Photon OS 1.0: Python2 PHSA-2019-1.0-0246

Photon OS 1.0: Python2 PHSA-2019-1.0-0252

Photon OS 1.0: Python2 PHSA-2019-1.0-0255

Photon OS 1.0: Python2 PHSA-2019-1.0-0257

Photon OS 1.0: Python2 PHSA-2020-1.0-0280

Photon OS 1.0: Python2 PHSA-2020-1.0-0287

Photon OS 1.0: Python2 PHSA-2020-1.0-0288

Photon OS 1.0: Python3 PHSA-2018-1.0-0126

Photon OS 1.0: Python3 PHSA-2018-1.0-0178

Photon OS 1.0: Python3 PHSA-2019-1.0-0212

Photon OS 1.0: Python3 PHSA-2019-1.0-0237

Photon OS 1.0: Python3 PHSA-2019-1.0-0240

Photon OS 1.0: Python3 PHSA-2019-1.0-0246

Photon OS 1.0: Python3 PHSA-2019-1.0-0251

Photon OS 1.0: Python3 PHSA-2020-1.0-0276

Photon OS 1.0: Pyyaml PHSA-2019-1.0-0224

Photon OS 1.0: Pyyaml PHSA-2020-1.0-0283

Photon OS 1.0: Redis PHSA-2018-1.0-0156

Photon OS 1.0: Redis PHSA-2018-1.0-0156 (deprecated)

Photon OS 1.0: Redis PHSA-2019-1.0-0247

Photon OS 1.0: Redis PHSA-2019-1.0-0249

Photon OS 1.0: Rpcbind PHSA-2017-0017

Photon OS 1.0: Rpm PHSA-2017-1.0-0095

Photon OS 1.0: Rpm PHSA-2018-1.0-0194

Photon OS 1.0: Rsync PHSA-2018-1.0-0096

Photon OS 1.0: Rsync PHSA-2018-1.0-0132

Photon OS 1.0: Rsyslog / Shadow PHSA-2017-0030 (deprecated)

Photon OS 1.0: Rsyslog PHSA-2017-0030

Photon OS 1.0: Rsyslog PHSA-2019-1.0-0212

Photon OS 1.0: Ruby / Tcpdump PHSA-2017-0034 (deprecated)

Photon OS 1.0: Ruby PHSA-2017-0002

Photon OS 1.0: Ruby PHSA-2017-0002 (deprecated)

Photon OS 1.0: Ruby PHSA-2017-0021

Photon OS 1.0: Ruby PHSA-2017-0024

Photon OS 1.0: Ruby PHSA-2017-0029

Photon OS 1.0: Ruby PHSA-2017-0034

Photon OS 1.0: Ruby PHSA-2017-0037

Photon OS 1.0: Ruby PHSA-2018-1.0-0098-(a)

Photon OS 1.0: Ruby PHSA-2018-1.0-0100

Photon OS 1.0: Ruby PHSA-2018-1.0-0100 (deprecated)

Photon OS 1.0: Ruby PHSA-2019-1.0-0205

Photon OS 1.0: Ruby PHSA-2019-1.0-0263

Photon OS 1.0: Rubygem PHSA-2019-1.0-0205

Photon OS 1.0: Salt PHSA-2018-1.0-0106

Photon OS 1.0: Salt PHSA-2018-1.0-0106 (deprecated)

Photon OS 1.0: Shadow PHSA-2017-0023

Photon OS 1.0: Shadow PHSA-2017-0030

Photon OS 1.0: Shadow PHSA-2018-1.0-0171

Photon OS 1.0: Snappy PHSA-2019-1.0-0235

Photon OS 1.0: Sqlite PHSA-2017-0025

Photon OS 1.0: Sqlite PHSA-2018-1.0-0126

Photon OS 1.0: Sqlite PHSA-2019-1.0-0209

Photon OS 1.0: Sqlite PHSA-2019-1.0-0228

Photon OS 1.0: Sqlite PHSA-2019-1.0-0231

Photon OS 1.0: Sqlite PHSA-2019-1.0-0237

Photon OS 1.0: Sqlite PHSA-2020-1.0-0264

Photon OS 1.0: Sqlite PHSA-2020-1.0-0270

Photon OS 1.0: Strongswan PHSA-2017-0040

Photon OS 1.0: Strongswan PHSA-2018-1.0-0126

Photon OS 1.0: Strongswan PHSA-2018-1.0-0164

Photon OS 1.0: Strongswan PHSA-2018-1.0-0178

Photon OS 1.0: Strongswan PHSA-2019-1.0-0203

Photon OS 1.0: Subversion PHSA-2016-0013

Photon OS 1.0: Subversion PHSA-2017-0031

Photon OS 1.0: Subversion PHSA-2017-0031 (deprecated)

Photon OS 1.0: Subversion PHSA-2017-1.0-0093

Photon OS 1.0: Sudo PHSA-2017-0021

Photon OS 1.0: Sudo PHSA-2019-1.0-0254

Photon OS 1.0: Sudo PHSA-2020-1.0-0264

Photon OS 1.0: Sysstat PHSA-2019-1.0-0263

Photon OS 1.0: Systemd PHSA-2017-0005

Photon OS 1.0: Systemd PHSA-2017-0005 (deprecated)

Photon OS 1.0: Systemd PHSA-2017-0023

Photon OS 1.0: Systemd PHSA-2017-0041

Photon OS 1.0: Systemd PHSA-2017-0044

Photon OS 1.0: Systemd PHSA-2018-1.0-0116

Photon OS 1.0: Systemd PHSA-2018-1.0-0116 (deprecated)

Photon OS 1.0: Systemd PHSA-2018-1.0-0167

Photon OS 1.0: Systemd PHSA-2018-1.0-0193

Photon OS 1.0: Systemd PHSA-2019-1.0-0203

Photon OS 1.0: Systemd PHSA-2019-1.0-0205

Photon OS 1.0: Systemd PHSA-2019-1.0-0220

Photon OS 1.0: Systemd PHSA-2019-1.0-0228

Photon OS 1.0: Tar PHSA-2017-0015

Photon OS 1.0: Tar PHSA-2019-1.0-0228

Photon OS 1.0: Tar PHSA-2019-1.0-0236

Photon OS 1.0: Tar PHSA-2019-1.0-0252

Photon OS 1.0: Tar PHSA-2019-1.0-0255

Photon OS 1.0: Tcpdump PHSA-2017-0004

Photon OS 1.0: Tcpdump PHSA-2017-0004 (deprecated)

Photon OS 1.0: Tcpdump PHSA-2017-0033

Photon OS 1.0: Tcpdump PHSA-2017-0033 (deprecated)

Photon OS 1.0: Tcpdump PHSA-2017-0034

Photon OS 1.0: Tcpdump PHSA-2019-1.0-0218

Photon OS 1.0: Tcpdump PHSA-2019-1.0-0249

Photon OS 1.0: Unzip PHSA-2016-0013

Photon OS 1.0: Unzip PHSA-2019-1.0-0246

Photon OS 1.0: Unzip PHSA-2020-1.0-0281

Photon OS 1.0: Util PHSA-2019-1.0-0212

Photon OS 1.0: Vim PHSA-2016-0012

Photon OS 1.0: Vim PHSA-2017-0006

Photon OS 1.0: Vim PHSA-2017-0007

Photon OS 1.0: Vim PHSA-2017-0007 (deprecated)

Photon OS 1.0: Vim PHSA-2018-1.0-0167

Photon OS 1.0: Vim PHSA-2019-1.0-0237

Photon OS 1.0: Wget PHSA-2016-0012

Photon OS 1.0: Wget PHSA-2017-0023

Photon OS 1.0: Wget PHSA-2017-0047

Photon OS 1.0: Wget PHSA-2017-0047 (deprecated)

Photon OS 1.0: Wget PHSA-2019-1.0-0237

Photon OS 1.0: Xerces PHSA-2018-1.0-0126

Photon OS 1.0: Xerces PHSA-2020-1.0-0271

Photon OS 1.0: Yarn PHSA-2019-1.0-0252

Photon OS 1.0: Yarn PHSA-2019-1.0-0255

Photon OS 1.0: Yarn PHSA-2020-1.0-0264

Photon OS 1.0: Yarn PHSA-2020-1.0-0283

Photon OS 1.0: Yarn PHSA-2020-1.0-0288

Photon OS 1.0: Yum PHSA-2019-1.0-0257

Photon OS 1.0: Zeromq PHSA-2019-1.0-0245

Photon OS 1.0: Zlib PHSA-2017-0021

Photon OS 1.0: Zookeeper PHSA-2019-1.0-0237

Photon OS 2.0 : binutils (PhotonOS-PHSA-2018-2.0-0021) (deprecated)

Photon OS 2.0 : ceph / linux-esx / rsync / linux / linux-secure / linux-aws (PhotonOS-PHSA-2018-2.0-0041) (deprecated)

Photon OS 2.0 : freetype2 / binutils (PhotonOS-PHSA-2018-2.0-0058) (deprecated)

Photon OS 2.0 : git (PhotonOS-PHSA-2018-2.0-0053) (deprecated)

Photon OS 2.0 : glibc (PhotonOS-PHSA-2018-2.0-0018) (deprecated)

Photon OS 2.0 : glibc (PhotonOS-PHSA-2018-2.0-0020) (deprecated)

Photon OS 2.0 : glibc / linux / rsync / curl (PhotonOS-PHSA-2018-2.0-0009) (deprecated)

Photon OS 2.0 : go (PhotonOS-PHSA-2018-2.0-0034) (deprecated)

Photon OS 2.0 : libtasn1 / libtiff / dnsmasq (PhotonOS-PHSA-2018-2.0-0017) (deprecated)

Photon OS 2.0 : libtiff (PhotonOS-PHSA-2018-2.0-0048) (deprecated)

Photon OS 2.0 : libtiff / glibc / libsoup (PhotonOS-PHSA-2018-2.0-0060) (deprecated)

Photon OS 2.0 : libtiff / openjdk8 / ruby (PhotonOS-PHSA-2018-2.0-0013) (deprecated)

Photon OS 2.0 : linux (PhotonOS-PHSA-2018-2.0-0010) (Meltdown) (deprecated)

Photon OS 2.0 : linux (PhotonOS-PHSA-2018-2.0-0011) (Spectre) (deprecated)

Photon OS 2.0 : linux (PhotonOS-PHSA-2018-2.0-0015) (deprecated)

Photon OS 2.0 : linux / linux-esx / linux-aws / linux-secure (PhotonOS-PHSA-2018-2.0-0042) (deprecated)

Photon OS 2.0 : Linux / Postgresql / Binutils / Curl / Libtiff (PhotonOS-PHSA-2018-2.0-0016) (deprecated)

Photon OS 2.0 : linux-aws / linux-esx / linux / linux-secure (PhotonOS-PHSA-2018-2.0-0062) (deprecated)

Photon OS 2.0 : linux-aws / linux-esx / linux-secure / linux (PhotonOS-PHSA-2018-2.0-0037-(a)) (deprecated)

Photon OS 2.0 : linux-esx / linux / linux-secure / linux-aws (PhotonOS-PHSA-2018-2.0-0043) (deprecated)

Photon OS 2.0 : linux-esx / linux / patch / linux-aws / linux-secure (PhotonOS-PHSA-2018-2.0-0049) (deprecated)

Photon OS 2.0 : mysql (PhotonOS-PHSA-2018-2.0-0014) (deprecated)

Photon OS 2.0 : mysql (PhotonOS-PHSA-2018-2.0-0040) (deprecated)

Photon OS 2.0 : openjdk8 / httpd / librelp / zsh / libvirt (PhotonOS-PHSA-2018-2.0-0039) (deprecated)

Photon OS 2.0 : openssl (PhotonOS-PHSA-2018-2.0-0010-(a)) (deprecated)

Photon OS 2.0 : perl / libmspack / zsh (PhotonOS-PHSA-2018-2.0-0050) (deprecated)

Photon OS 2.0 : postgresql (PhotonOS-PHSA-2018-2.0-0031) (deprecated)

Photon OS 2.0 : ruby / glibc (PhotonOS-PHSA-2018-2.0-0011-(a)) (deprecated)

Photon OS 2.0 : systemd / go (PhotonOS-PHSA-2018-2.0-0026) (deprecated)

Photon OS 2.0 : unzip (PhotonOS-PHSA-2018-2.0-0052) (deprecated)

Photon OS 2.0 : unzip / libtar (PhotonOS-PHSA-2018-2.0-0029) (deprecated)

Photon OS 2.0 : zsh (PhotonOS-PHSA-2018-2.0-0028) (deprecated)

Photon OS 2.0 : Zsh / Python3 / Xerces / Mercurial / Pmd / Pycrypto / Net / Python2 / Util / Mysql / Paramiko / Binutils / Patch / Sqlite (PhotonOS-PHSA-2018-2.0-0037) (deprecated)

Photon OS 2.0: Ansible PHSA-2019-2.0-0152

Photon OS 2.0: Ansible PHSA-2019-2.0-0172

Photon OS 2.0: Ansible PHSA-2020-2.0-0207

Photon OS 2.0: Ansible PHSA-2020-2.0-0226

Photon OS 2.0: Apache PHSA-2018-2.0-0065 (deprecated)

Photon OS 2.0: Apache PHSA-2020-2.0-0200

Photon OS 2.0: Apr / Ncurses PHSA-2017-0053 (deprecated)

Photon OS 2.0: Apr PHSA-2017-0053

Photon OS 2.0: Bash / Curl / Go / Libtiff / Systemd PHSA-2017-0045 (deprecated)

Photon OS 2.0: Bash PHSA-2017-0045

Photon OS 2.0: Bash PHSA-2020-2.0-0208

Photon OS 2.0: Bindutils PHSA-2020-2.0-0199

Photon OS 2.0: Bindutils PHSA-2020-2.0-0223

Photon OS 2.0: Binutils / File / Linux / Shadow PHSA-2018-2.0-0080 (deprecated)

Photon OS 2.0: Binutils / Glibc PHSA-2018-2.0-0064 (deprecated)

Photon OS 2.0: Binutils / Linux / Wget PHSA-2017-2.0-0008 (deprecated)

Photon OS 2.0: Binutils PHSA-2017-2.0-0008

Photon OS 2.0: Binutils PHSA-2018-2.0-0016

Photon OS 2.0: Binutils PHSA-2018-2.0-0021

Photon OS 2.0: Binutils PHSA-2018-2.0-0058

Photon OS 2.0: Binutils PHSA-2018-2.0-0064

Photon OS 2.0: Binutils PHSA-2018-2.0-0080

Photon OS 2.0: Binutils PHSA-2019-2.0-0119

Photon OS 2.0: Binutils PHSA-2019-2.0-0134

Photon OS 2.0: Binutils PHSA-2019-2.0-0164

Photon OS 2.0: Binutils PHSA-2019-2.0-0173

Photon OS 2.0: Binutils PHSA-2019-2.0-0190

Photon OS 2.0: Blktrace / Systemd / Vim PHSA-2018-2.0-0076 (deprecated)

Photon OS 2.0: Blktrace PHSA-2018-2.0-0076

Photon OS 2.0: Bzip2 PHSA-2019-2.0-0168

Photon OS 2.0: Ceph PHSA-2018-2.0-0041

Photon OS 2.0: Ceph PHSA-2018-2.0-0104

Photon OS 2.0: Ceph PHSA-2019-2.0-0154

Photon OS 2.0: Cpio PHSA-2020-2.0-0202

Photon OS 2.0: Curl / Libtiff / Linux PHSA-2017-0050 (deprecated)

Photon OS 2.0: Curl PHSA-2017-0045

Photon OS 2.0: Curl PHSA-2017-0050

Photon OS 2.0: Curl PHSA-2018-2.0-0009

Photon OS 2.0: Curl PHSA-2018-2.0-0016

Photon OS 2.0: Curl PHSA-2018-2.0-0068

Photon OS 2.0: Curl PHSA-2018-2.0-0068 (deprecated)

Photon OS 2.0: Curl PHSA-2018-2.0-0096

Photon OS 2.0: Curl PHSA-2018-2.0-0096 (deprecated)

Photon OS 2.0: Curl PHSA-2019-2.0-0131

Photon OS 2.0: Curl PHSA-2019-2.0-0171

Photon OS 2.0: Curl PHSA-2019-2.0-0177

Photon OS 2.0: Dhcp PHSA-2019-2.0-0152

Photon OS 2.0: Dhcp PHSA-2019-2.0-0192

Photon OS 2.0: Dnsmasq PHSA-2018-2.0-0017

Photon OS 2.0: Docker / Python2 / Strongswan PHSA-2018-2.0-0086 (deprecated)

Photon OS 2.0: Docker PHSA-2018-2.0-0086

Photon OS 2.0: Docker PHSA-2019-2.0-0162

Photon OS 2.0: Docker PHSA-2019-2.0-0193

Photon OS 2.0: E2Fsprogs PHSA-2019-2.0-0184

Photon OS 2.0: Elasticsearch PHSA-2019-2.0-0132

Photon OS 2.0: Elasticsearch PHSA-2019-2.0-0155

Photon OS 2.0: Elfutils PHSA-2018-2.0-0108

Photon OS 2.0: Elfutils PHSA-2019-2.0-0164

Photon OS 2.0: Envoy PHSA-2020-2.0-0202

Photon OS 2.0: Envoy PHSA-2020-2.0-0207

Photon OS 2.0: Envoy PHSA-2020-2.0-0222

Photon OS 2.0: Etcd PHSA-2019-2.0-0187

Photon OS 2.0: Expat PHSA-2019-2.0-0171

Photon OS 2.0: File PHSA-2018-2.0-0080

Photon OS 2.0: File PHSA-2019-2.0-0187

Photon OS 2.0: Freetype2 PHSA-2018-2.0-0058

Photon OS 2.0: Fuse PHSA-2019-2.0-0177

Photon OS 2.0: Gdb PHSA-2020-2.0-0225

Photon OS 2.0: Gettext PHSA-2018-2.0-0116

Photon OS 2.0: Git PHSA-2018-2.0-0053

Photon OS 2.0: Git PHSA-2019-2.0-0185

Photon OS 2.0: Git PHSA-2019-2.0-0196

Photon OS 2.0: Glib PHSA-2018-2.0-0108

Photon OS 2.0: Glib PHSA-2019-2.0-0171

Photon OS 2.0: Glibc PHSA-2018-2.0-0009

Photon OS 2.0: Glibc PHSA-2018-2.0-0011-(a)

Photon OS 2.0: Glibc PHSA-2018-2.0-0018

Photon OS 2.0: Glibc PHSA-2018-2.0-0020

Photon OS 2.0: Glibc PHSA-2018-2.0-0060

Photon OS 2.0: Glibc PHSA-2018-2.0-0064

Photon OS 2.0: Glibc PHSA-2018-2.0-0066

Photon OS 2.0: Glibc PHSA-2018-2.0-0066 (deprecated)

Photon OS 2.0: Glibc PHSA-2019-2.0-0134

Photon OS 2.0: Glibc PHSA-2019-2.0-0160

Photon OS 2.0: Gnupg PHSA-2019-2.0-0171

Photon OS 2.0: Gnutls PHSA-2019-2.0-0152

Photon OS 2.0: Go PHSA-2017-0045

Photon OS 2.0: Go PHSA-2018-2.0-0026

Photon OS 2.0: Go PHSA-2018-2.0-0034

Photon OS 2.0: Go PHSA-2019-2.0-0168

Photon OS 2.0: Go PHSA-2019-2.0-0173

Photon OS 2.0: Go PHSA-209-2.0-0175

Photon OS 2.0: Haproxy PHSA-2019-2.0-0150

Photon OS 2.0: Haproxy PHSA-2019-2.0-0187

Photon OS 2.0: Httpd PHSA-2018-2.0-0039

Photon OS 2.0: Httpd PHSA-2018-2.0-0089

Photon OS 2.0: Httpd PHSA-2018-2.0-0089 (deprecated)

Photon OS 2.0: Httpd PHSA-2019-2.0-0157

Photon OS 2.0: Httpd PHSA-2019-2.0-0178

Photon OS 2.0: Ipmitool PHSA-2020-2.0-0209

Photon OS 2.0: Keepalived PHSA-2019-2.0-0134

Photon OS 2.0: Keepalived PHSA-2019-2.0-0160

Photon OS 2.0: Kibana PHSA-2019-2.0-0132

Photon OS 2.0: Kibana PHSA-2019-2.0-0155

Photon OS 2.0: Krb5 / Libjpeg / Libtiff PHSA-2017-2.0-0007 (deprecated)

Photon OS 2.0: Krb5 / Postgresql PHSA-2018-2.0-0087 (deprecated)

Photon OS 2.0: Krb5 PHSA-2017-2.0-0007

Photon OS 2.0: Krb5 PHSA-2018-2.0-0087

Photon OS 2.0: Krb5 PHSA-2019-2.0-0164

Photon OS 2.0: Kubernetes PHSA-2018-2.0-0112

Photon OS 2.0: Kubernetes PHSA-2018-2.0-0112 (deprecated)

Photon OS 2.0: Kubernetes PHSA-2019-2.0-0148

Photon OS 2.0: Kubernetes PHSA-2019-2.0-0177

Photon OS 2.0: Libarchive PHSA-2019-2.0-0189

Photon OS 2.0: Libarchive PHSA-2020-2.0-0207

Photon OS 2.0: Libgcrypt / Libsoup PHSA-2018-2.0-0091 (deprecated)

Photon OS 2.0: Libgcrypt PHSA-2018-2.0-0091

Photon OS 2.0: Libgd PHSA-2018-2.0-0108

Photon OS 2.0: Libgd PHSA-2019-2.0-0153

Photon OS 2.0: Libgd PHSA-2020-2.0-0213

Photon OS 2.0: Libgd PHSA-2020-2.0-0223

Photon OS 2.0: Libjpeg PHSA-2017-2.0-0007

Photon OS 2.0: Libjpeg PHSA-2019-2.0-0126

Photon OS 2.0: Libmspack / Strongswan PHSA-2018-2.0-0075 (deprecated)

Photon OS 2.0: Libmspack PHSA-2018-2.0-0050

Photon OS 2.0: Libmspack PHSA-2018-2.0-0075

Photon OS 2.0: Libmspack PHSA-2018-2.0-0110

Photon OS 2.0: Libmspack PHSA-2019-2.0-0196

Photon OS 2.0: Libpcap PHSA-2019-2.0-0187

Photon OS 2.0: Libpng PHSA-2019-2.0-0160

Photon OS 2.0: Libpng PHSA-2019-2.0-0171

Photon OS 2.0: Librelp PHSA-2018-2.0-0039

Photon OS 2.0: Libsolv PHSA-2019-2.0-0136

Photon OS 2.0: Libsoup PHSA-2018-2.0-0060

Photon OS 2.0: Libsoup PHSA-2018-2.0-0091

Photon OS 2.0: Libsoup PHSA-2019-2.0-0190

Photon OS 2.0: Libssh2 PHSA-2019-2.0-0196

Photon OS 2.0: Libtar PHSA-2018-2.0-0029

Photon OS 2.0: Libtasn1 PHSA-2018-2.0-0017

Photon OS 2.0: Libtiff PHSA-2017-0045

Photon OS 2.0: Libtiff PHSA-2017-0050

Photon OS 2.0: Libtiff PHSA-2017-2.0-0007

Photon OS 2.0: Libtiff PHSA-2018-2.0-0013

Photon OS 2.0: Libtiff PHSA-2018-2.0-0016

Photon OS 2.0: Libtiff PHSA-2018-2.0-0017

Photon OS 2.0: Libtiff PHSA-2018-2.0-0039

Photon OS 2.0: Libtiff PHSA-2018-2.0-0048

Photon OS 2.0: Libtiff PHSA-2018-2.0-0060

Photon OS 2.0: Libtiff PHSA-2018-2.0-0110

Photon OS 2.0: Libtiff PHSA-2019-2.0-0118

Photon OS 2.0: Libtiff PHSA-2019-2.0-0131

Photon OS 2.0: Libtiff PHSA-2020-2.0-0202

Photon OS 2.0: Libtirpc PHSA-2018-2.0-0113

Photon OS 2.0: Libtirpc PHSA-2018-2.0-0113 (deprecated)

Photon OS 2.0: Libvirt / Linux / Openssh / Procmail / Python2 / Rsync PHSA-2017-0051 (deprecated)

Photon OS 2.0: Libvirt PHSA-2018-2.0-0039

Photon OS 2.0: Libvirt PHSA-2020-2.0-0214

Photon OS 2.0: Libxml2 PHSA-2018-2.0-0106

Photon OS 2.0: Libxml2 PHSA-2020-2.0-0203

Photon OS 2.0: Libxml2 PHSA-2020-2.0-0225

Photon OS 2.0: Libxslt PHSA-2019-2.0-0152

Photon OS 2.0: Libxslt PHSA-2019-2.0-0171

Photon OS 2.0: Libxslt PHSA-2019-2.0-0189

Photon OS 2.0: Libxslt PHSA-2019-2.0-0196

Photon OS 2.0: Linux PHSA-2017-0043

Photon OS 2.0: Linux PHSA-2017-0043 (deprecated)

Photon OS 2.0: Linux PHSA-2017-0050

Photon OS 2.0: Linux PHSA-2017-0051

Photon OS 2.0: Linux PHSA-2017-2.0-0008

Photon OS 2.0: Linux PHSA-2018-2.0-0009

Photon OS 2.0: Linux PHSA-2018-2.0-0010

Photon OS 2.0: Linux PHSA-2018-2.0-0011

Photon OS 2.0: Linux PHSA-2018-2.0-0015

Photon OS 2.0: Linux PHSA-2018-2.0-0016

Photon OS 2.0: Linux PHSA-2018-2.0-0037-(a)

Photon OS 2.0: Linux PHSA-2018-2.0-0041

Photon OS 2.0: Linux PHSA-2018-2.0-0042

Photon OS 2.0: Linux PHSA-2018-2.0-0043

Photon OS 2.0: Linux PHSA-2018-2.0-0049

Photon OS 2.0: Linux PHSA-2018-2.0-0062

Photon OS 2.0: Linux PHSA-2018-2.0-0072

Photon OS 2.0: Linux PHSA-2018-2.0-0072 (deprecated)

Photon OS 2.0: Linux PHSA-2018-2.0-0073

Photon OS 2.0: Linux PHSA-2018-2.0-0073 (deprecated)

Photon OS 2.0: Linux PHSA-2018-2.0-0083

Photon OS 2.0: Linux PHSA-2018-2.0-0083 (deprecated)

Photon OS 2.0: Linux PHSA-2018-2.0-0088

Photon OS 2.0: Linux PHSA-2018-2.0-0100

Photon OS 2.0: Linux PHSA-2018-2.0-0100 (deprecated)

Photon OS 2.0: Linux PHSA-2018-2.0-0101

Photon OS 2.0: Linux PHSA-2018-2.0-0101 (deprecated)

Photon OS 2.0: Linux PHSA-2018-2.0-0109

Photon OS 2.0: Linux PHSA-2019-2.0-0134

Photon OS 2.0: Linux PHSA-2019-2.0-0138

Photon OS 2.0: Linux PHSA-2019-2.0-0160

Photon OS 2.0: Linux PHSA-2019-2.0-0165

Photon OS 2.0: Linux PHSA-2019-2.0-0189

Photon OS 2.0: Linux PHSA-2019-2.0-0191

Photon OS 2.0: Linux PHSA-2020-2.0-0212

Photon OS 2.0: Linux PHSA-2020-2.0-0219

Photon OS 2.0: Linux PHSA-2020-2.0-0225

Photon OS 2.0: Linux PHSA-209-2.0-0175

Photon OS 2.0: Logstash PHSA-2019-2.0-0194

Photon OS 2.0: Mercurial PHSA-2019-2.0-0160

Photon OS 2.0: Mysql PHSA-2018-2.0-0014

Photon OS 2.0: Mysql PHSA-2018-2.0-0040

Photon OS 2.0: Mysql PHSA-2018-2.0-0079

Photon OS 2.0: Mysql PHSA-2018-2.0-0079 (deprecated)

Photon OS 2.0: Mysql PHSA-2019-2.0-0152

Photon OS 2.0: Mysql PHSA-2019-2.0-0160

Photon OS 2.0: Ncurses PHSA-2017-0053

Photon OS 2.0: Ncurses PHSA-2018-2.0-0074

Photon OS 2.0: Ncurses PHSA-2018-2.0-0074 (deprecated)

Photon OS 2.0: Net PHSA-2019-2.0-0118

Photon OS 2.0: Nginx PHSA-2019-2.0-0117

Photon OS 2.0: Nginx PHSA-2019-2.0-0132

Photon OS 2.0: Nginx PHSA-2020-2.0-0207

Photon OS 2.0: Nodejs PHSA-2018-2.0-0093

Photon OS 2.0: Nodejs PHSA-2018-2.0-0093 (deprecated)

Photon OS 2.0: Nodejs PHSA-2020-2.0-0210

Photon OS 2.0: Nss PHSA-2019-2.0-0164

Photon OS 2.0: Ntp / Linux PHSA-2018-2.0-0088 (deprecated)

Photon OS 2.0: Ntp PHSA-2018-2.0-0088

Photon OS 2.0: Nxtgn PHSA-2020-2.0-0204

Photon OS 2.0: Oniguruma PHSA-2019-2.0-0196

Photon OS 2.0: Openjdk8 PHSA-2018-2.0-0013

Photon OS 2.0: Openjdk8 PHSA-2018-2.0-0039

Photon OS 2.0: Openjdk8 PHSA-2018-2.0-0077

Photon OS 2.0: Openjdk8 PHSA-2018-2.0-0077 (deprecated)

Photon OS 2.0: Openjdk8 PHSA-2018-2.0-0106

Photon OS 2.0: Openjdk8 PHSA-2019-2.0-0173

Photon OS 2.0: Openssh PHSA-2017-0051

Photon OS 2.0: Openssh PHSA-2019-2.0-0126

Photon OS 2.0: Openssh PHSA-2019-2.0-0165

Photon OS 2.0: Openssl / Procps-ng / Perl PHSA-2018-2.0-0084 (deprecated)

Photon OS 2.0: Openssl PHSA-2018-2.0-0010-(a)

Photon OS 2.0: Openssl PHSA-2018-2.0-0078

Photon OS 2.0: Openssl PHSA-2018-2.0-0078 (deprecated)

Photon OS 2.0: Openssl PHSA-2018-2.0-0084

Photon OS 2.0: Openssl PHSA-2019-2.0-0177

Photon OS 2.0: Patch PHSA-2018-2.0-0049

Photon OS 2.0: Patch PHSA-2018-2.0-0102

Photon OS 2.0: Patch PHSA-2018-2.0-0102 (deprecated)

Photon OS 2.0: Patch PHSA-2019-2.0-0172

Photon OS 2.0: Perl PHSA-2018-2.0-0050

Photon OS 2.0: Perl PHSA-2018-2.0-0084

Photon OS 2.0: Perl PHSA-2019-2.0-0135

Photon OS 2.0: Polkit PHSA-2019-2.0-0153

Photon OS 2.0: Postgresql PHSA-2018-2.0-0016

Photon OS 2.0: Postgresql PHSA-2018-2.0-0031

Photon OS 2.0: Postgresql PHSA-2018-2.0-0087

Photon OS 2.0: Postgresql PHSA-2019-2.0-0190

Photon OS 2.0: Procmail PHSA-2017-0051

Photon OS 2.0: Procps PHSA-2018-2.0-0084

Photon OS 2.0: Python PHSA-2019-2.0-0198

Photon OS 2.0: Python2 PHSA-2017-0051

Photon OS 2.0: Python2 PHSA-2018-2.0-0086

Photon OS 2.0: Python2 PHSA-2019-2.0-0118

Photon OS 2.0: Python2 PHSA-2019-2.0-0165

Photon OS 2.0: Python2 PHSA-2019-2.0-0171

Photon OS 2.0: Python2 PHSA-2019-2.0-0177

Photon OS 2.0: Python2 PHSA-2019-2.0-0182

Photon OS 2.0: Python2 PHSA-2019-2.0-0187

Photon OS 2.0: Python2 PHSA-2019-2.0-0190

Photon OS 2.0: Python2 PHSA-2020-2.0-0211

Photon OS 2.0: Python2 PHSA-2020-2.0-0223

Photon OS 2.0: Python3 PHSA-2019-2.0-0132

Photon OS 2.0: Python3 PHSA-2019-2.0-0165

Photon OS 2.0: Python3 PHSA-2019-2.0-0171

Photon OS 2.0: Python3 PHSA-2019-2.0-0176

Photon OS 2.0: Python3 PHSA-2019-2.0-0182

Photon OS 2.0: Python3 PHSA-2019-2.0-0187

Photon OS 2.0: Python3 PHSA-2020-2.0-0223

Photon OS 2.0: Python3 PHSA-2020-2.0-0224

Photon OS 2.0: Python3 PHSA-2020-2.0-0226

Photon OS 2.0: Redis / Vim PHSA-2018-2.0-0070 (deprecated)

Photon OS 2.0: Redis PHSA-2018-2.0-0070

Photon OS 2.0: Redis PHSA-2019-2.0-0172

Photon OS 2.0: Redis PHSA-2019-2.0-0173

Photon OS 2.0: Rpm PHSA-2018-2.0-0108

Photon OS 2.0: Rsync PHSA-2017-0051

Photon OS 2.0: Rsync PHSA-2018-2.0-0009

Photon OS 2.0: Rsync PHSA-2018-2.0-0041

Photon OS 2.0: Rsyslog PHSA-2019-2.0-0134

Photon OS 2.0: Rsyslog PHSA-2019-2.0-0182

Photon OS 2.0: Rsyslog PHSA-2019-2.0-0184

Photon OS 2.0: Ruby PHSA-2018-2.0-0011-(a)

Photon OS 2.0: Ruby PHSA-2018-2.0-0013

Photon OS 2.0: Ruby PHSA-2019-2.0-0130

Photon OS 2.0: Ruby PHSA-2019-2.0-0196

Photon OS 2.0: Rubygem PHSA-2019-2.0-0130

Photon OS 2.0: Shadow PHSA-2018-2.0-0080

Photon OS 2.0: Snappy PHSA-2019-2.0-0160

Photon OS 2.0: Sqlite PHSA-2019-2.0-0154

Photon OS 2.0: Sqlite PHSA-2019-2.0-0157

Photon OS 2.0: Sqlite PHSA-2019-2.0-0162

Photon OS 2.0: Sqlite PHSA-2019-2.0-0184

Photon OS 2.0: Sqlite PHSA-2019-2.0-0198

Photon OS 2.0: Sqlite PHSA-2020-2.0-0200

Photon OS 2.0: Sqlite PHSA-2020-2.0-0204

Photon OS 2.0: Strongswan PHSA-2018-2.0-0075

Photon OS 2.0: Strongswan PHSA-2018-2.0-0086

Photon OS 2.0: Strongswan PHSA-2019-2.0-0125

Photon OS 2.0: Subversion PHSA-2019-2.0-0182

Photon OS 2.0: Sudo PHSA-2019-2.0-0183

Photon OS 2.0: Sysstat PHSA-2019-2.0-0184

Photon OS 2.0: Systemd PHSA-2017-0045

Photon OS 2.0: Systemd PHSA-2018-2.0-0026

Photon OS 2.0: Systemd PHSA-2018-2.0-0076

Photon OS 2.0: Systemd PHSA-2018-2.0-0107

Photon OS 2.0: Systemd PHSA-2019-2.0-0153

Photon OS 2.0: Systemd PHSA-2019-2.0-0166

Photon OS 2.0: Tar PHSA-2019-2.0-0154

Photon OS 2.0: Tar PHSA-2019-2.0-0187

Photon OS 2.0: Tcpdump PHSA-2019-2.0-0173

Photon OS 2.0: Tcpdump PHSA-2019-2.0-0182

Photon OS 2.0: Unzip PHSA-2018-2.0-0029

Photon OS 2.0: Unzip PHSA-2018-2.0-0052

Photon OS 2.0: Unzip PHSA-2019-2.0-0126

Photon OS 2.0: Unzip PHSA-2019-2.0-0171

Photon OS 2.0: Unzip PHSA-2020-2.0-0213

Photon OS 2.0: Vim PHSA-2018-2.0-0070

Photon OS 2.0: Vim PHSA-2018-2.0-0076

Photon OS 2.0: Vim PHSA-2019-2.0-0162

Photon OS 2.0: Wget PHSA-2017-0046

Photon OS 2.0: Wget PHSA-2017-0046 (deprecated)

Photon OS 2.0: Wget PHSA-2017-2.0-0008

Photon OS 2.0: Yarn PHSA-2019-2.0-0176

Photon OS 2.0: Yarn PHSA-2020-2.0-0200

Photon OS 2.0: Yum PHSA-2019-2.0-0190

Photon OS 2.0: Zeromq PHSA-2019-2.0-0171

Photon OS 2.0: Zsh PHSA-2018-2.0-0028

Photon OS 2.0: Zsh PHSA-2018-2.0-0039

Photon OS 2.0: Zsh PHSA-2018-2.0-0050

Photon OS 2.0: Zsh PHSA-2019-2.0-0165

Photon OS 2.0: Zsh PHSA-2020-2.0-0222

Photon OS 3.0: Ansible PHSA-2019-3.0-0027

Photon OS 3.0: Ansible PHSA-2020-3.0-0058

Photon OS 3.0: Apache PHSA-2019-3.0-0024

Photon OS 3.0: Apache PHSA-2020-3.0-0051

Photon OS 3.0: Apache PHSA-2020-3.0-0069

Photon OS 3.0: Bash PHSA-2020-3.0-0057

Photon OS 3.0: Bindutils PHSA-2020-3.0-0063

Photon OS 3.0: Binutils PHSA-2019-3.0-0022

Photon OS 3.0: Binutils PHSA-2019-3.0-0026

Photon OS 3.0: Binutils PHSA-2019-3.0-0031

Photon OS 3.0: Bluez PHSA-2020-3.0-0073

Photon OS 3.0: Bubblewrap PHSA-2019-3.0-0019

Photon OS 3.0: Cloud PHSA-2020-3.0-0058

Photon OS 3.0: Consul PHSA-2020-3.0-0069

Photon OS 3.0: Cpio PHSA-2020-3.0-0053

Photon OS 3.0: Curl PHSA-2019-3.0-0032

Photon OS 3.0: Cyrus PHSA-2020-3.0-0077

Photon OS 3.0: Dhcp PHSA-2019-3.0-0044

Photon OS 3.0: Docker PHSA-2019-3.0-0019

Photon OS 3.0: E2Fsprogs PHSA-2020-3.0-0053

Photon OS 3.0: Elfutils PHSA-2019-3.0-0015

Photon OS 3.0: Expat PHSA-2019-3.0-0026

Photon OS 3.0: Git PHSA-2020-3.0-0047

Photon OS 3.0: Glib PHSA-2019-3.0-0018

Photon OS 3.0: Glib PHSA-2019-3.0-0024

Photon OS 3.0: Gnupg PHSA-2019-3.0-0024

Photon OS 3.0: Go PHSA-2019-3.0-0018

Photon OS 3.0: Go PHSA-2019-3.0-0019

Photon OS 3.0: Go PHSA-2019-3.0-0028

Photon OS 3.0: Haproxy PHSA-2019-3.0-0026

Photon OS 3.0: Haproxy PHSA-2019-3.0-0038

Photon OS 3.0: Haproxy PHSA-2020-3.0-0047

Photon OS 3.0: Httpd PHSA-2019-3.0-0035

Photon OS 3.0: Ipmitool PHSA-2020-3.0-0059

Photon OS 3.0: Keepalived PHSA-2019-3.0-0015

Photon OS 3.0: Krb5 PHSA-2019-3.0-0020

Photon OS 3.0: Kubernetes PHSA-2019-3.0-0015

Photon OS 3.0: Kubernetes PHSA-2019-3.0-0031

Photon OS 3.0: Libarchive PHSA-2019-3.0-0015

Photon OS 3.0: Libarchive PHSA-2019-3.0-0041

Photon OS 3.0: Libarchive PHSA-2020-3.0-0055

Photon OS 3.0: Libgd PHSA-2020-3.0-0063

Photon OS 3.0: Libjpeg PHSA-2020-3.0-0063

Photon OS 3.0: Libpcap PHSA-2019-3.0-0034

Photon OS 3.0: Libseccomp PHSA-2019-3.0-0009

Photon OS 3.0: Libsolv PHSA-2020-3.0-0057

Photon OS 3.0: Libssh2 PHSA-2019-3.0-0009

Photon OS 3.0: Libssh2 PHSA-2019-3.0-0026

Photon OS 3.0: Libssh2 PHSA-2020-3.0-0047

Photon OS 3.0: Libvirt PHSA-2019-3.0-0032

Photon OS 3.0: Libxml2 PHSA-2019-3.0-0024

Photon OS 3.0: Libxml2 PHSA-2020-3.0-0055

Photon OS 3.0: Libxslt PHSA-2019-3.0-0024

Photon OS 3.0: Libxslt PHSA-2020-3.0-0047

Photon OS 3.0: Linux PHSA-2019-3.0-0009

Photon OS 3.0: Linux PHSA-2019-3.0-0015

Photon OS 3.0: Linux PHSA-2019-3.0-0026

Photon OS 3.0: Linux PHSA-2019-3.0-0028

Photon OS 3.0: Linux PHSA-2019-3.0-0030

Photon OS 3.0: Linux PHSA-2019-3.0-0034

Photon OS 3.0: Linux PHSA-2019-3.0-0041

Photon OS 3.0: Linux PHSA-2019-3.0-0046

Photon OS 3.0: Linux PHSA-2020-3.0-0052

Photon OS 3.0: Linux PHSA-2020-3.0-0069

Photon OS 3.0: Linux PHSA-2020-3.0-0073

Photon OS 3.0: Logstash PHSA-2019-3.0-0046

Photon OS 3.0: Mercurial PHSA-2019-3.0-0015

Photon OS 3.0: Mysql PHSA-2019-3.0-0015

Photon OS 3.0: Mysql PHSA-2019-3.0-0026

Photon OS 3.0: Nginx PHSA-2020-3.0-0057

Photon OS 3.0: Nodejs PHSA-2020-3.0-0060

Photon OS 3.0: Nss PHSA-2019-3.0-0020

Photon OS 3.0: Ntp PHSA-2019-3.0-0024

Photon OS 3.0: Nxtgn PHSA-2019-3.0-0033

Photon OS 3.0: Nxtgn PHSA-2020-3.0-0054

Photon OS 3.0: Oniguruma PHSA-2019-3.0-0024

Photon OS 3.0: Oniguruma PHSA-2020-3.0-0047

Photon OS 3.0: Openjdk8 PHSA-2019-3.0-0035

Photon OS 3.0: Openssh PHSA-2019-3.0-0045

Photon OS 3.0: Openssl PHSA-2019-3.0-0032

Photon OS 3.0: Openssl PHSA-2020-3.0-0048

Photon OS 3.0: Patch PHSA-2019-3.0-0025

Photon OS 3.0: Python PHSA-2019-3.0-0009

Photon OS 3.0: Python2 PHSA-2019-3.0-0009

Photon OS 3.0: Python2 PHSA-2019-3.0-0024

Photon OS 3.0: Python2 PHSA-2019-3.0-0031

Photon OS 3.0: Python2 PHSA-2019-3.0-0035

Photon OS 3.0: Python2 PHSA-2020-3.0-0057

Photon OS 3.0: Python2 PHSA-2020-3.0-0073

Photon OS 3.0: Python3 PHSA-2019-3.0-0030

Photon OS 3.0: Python3 PHSA-2020-3.0-0073

Photon OS 3.0: Redis PHSA-2019-3.0-0024

Photon OS 3.0: Rsyslog PHSA-2019-3.0-0034

Photon OS 3.0: Ruby PHSA-2020-3.0-0047

Photon OS 3.0: Sqlite PHSA-2019-3.0-0018

Photon OS 3.0: Sqlite PHSA-2019-3.0-0030

Photon OS 3.0: Sqlite PHSA-2020-3.0-0055

Photon OS 3.0: Subversion PHSA-2019-3.0-0035

Photon OS 3.0: Sudo PHSA-2019-3.0-0035

Photon OS 3.0: Systemd PHSA-2019-3.0-0024

Photon OS 3.0: Tcpdump PHSA-2019-3.0-0028

Photon OS 3.0: Tcpdump PHSA-2019-3.0-0034

Photon OS 3.0: Unbound PHSA-2019-3.0-0035

Photon OS 3.0: Unbound PHSA-2020-3.0-0047

Photon OS 3.0: Unzip PHSA-2019-3.0-0024

Photon OS 3.0: Unzip PHSA-2020-3.0-0063

Photon OS 3.0: Yarn PHSA-2019-3.0-0034

Photon OS 3.0: Yarn PHSA-2020-3.0-0057

Photon OS 3.0: Zeromq PHSA-2019-3.0-0024

Photon OS 3.0: Zeromq PHSA-2019-3.0-0026

Photon OS 3.0: Zsh PHSA-2020-3.0-0073

Photon OS update (deprecated)

# Peer-To-Peer File Sharing

Apple iTunes < 10.0 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 10.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 10.2.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 10.5 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 10.5.1 Update Authenticity Verification Weakness (uncredentialed check)

Apple iTunes < 10.6 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 10.6.3 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 10.7 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 11.0.3 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 11.1 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 11.1.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 11.1.4 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 11.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 11.2.1 User Directory Insecure Permissions Vulnerability (uncredentialed check)

Apple iTunes < 12.0.1 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.10.3 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.10.4 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.10.5 Multiple Vulnerabilities (uncredentialed check) (HT211105)

Apple iTunes < 12.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.3 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.3.1 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.3.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.4 DLL Injection Arbitrary Code Execution (uncredentialed check)

Apple iTunes < 12.4.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.5.1 Multiple Vulnerabilities (uncredentialed Check)

Apple iTunes < 12.5.2 Multiple Vulnerabilities (Uncredentialed Check)

Apple iTunes < 12.5.4 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.5.5 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.6 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.6.1 WebKit Memory Corruption RCE (uncredentialed check)

Apple iTunes < 12.6.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.7 WebKit Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.7.1 WebKit Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.7.2 WebKit Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.7.3 WebKit Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.7.3 WebKit Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.7.5 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.8 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.9 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.9.1 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 12.9.6 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 7.4 Malformed Music File Heap Overflow (uncredentialed check)

Apple iTunes < 8.0 Integer Buffer Overflow (uncredentialed check)

Apple iTunes < 8.1 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 8.2 itms: URI Handling Overflow (uncredentialed check)

Apple iTunes < 9.0.1 PLS File Buffer Overflow (uncredentialed check)

Apple iTunes < 9.1 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 9.2 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes < 9.2.1 'itpc:' Buffer Overflow (uncredentialed check)

Apple iTunes AAC File Parsing Integer Overflow (uncredentialed check)

Apple iTunes for Windows < 12.9.5 Multiple Vulnerabilities (uncredentialed check)

Apple iTunes For Windows iTunesHelper.exe Path Subversion Local Privilege Escalation (uncredentialed check)

Apple iTunes Music Sharing Enabled

Ares Fileshare Detection

BitComet Client .torrent URI Handling Overflow

BitComet Detection

BitLord Detection

BitTornado Detection

BitTorrent / uTorrent Detection

BitTorrent Installed

BitTorrent Mainline DHT Detection

DC++ Detection

DC++ Download Drive Arbitrary File Appending

Direct Connect Hub Detection

eDonkey Detection

eMule IRC Module / Web Server DecodeBase16 Function Remote Overflow

eMule Malformed Data Handling Remote DoS

FastTrack (FT) Crafted Packet Handling Remote Overflow

GigaTribe Detection

Gnapster Absolute Path Name Request Arbitrary File Access

Gnutella Root Directory Misconfiguration

Gnutella Servent Detection

iMesh P2P Client Detection

Kazaa on Windows Detection

LimeWire Installed

Mercora IMRadio Detection

mldonkey Detection (telnet check)

mldonkey Detection (WWW)

Open DC Hub RedirectAll Value Remote Overflow

Orb Detection

Overnet Detection

Owner Free File System Client Detection

PeerCast Detection

PeerCast procConnectArgs() Function URL Handling Remote Overflow

PeerCast servhs.cpp handshakeHTTP Function SOURCE Request Remote Overflow

PeerCast URL Error Message Format String

Shareaza Detection

SoMud Detection

Soulseek Detection

uTorrent Installed

Vuze Detection

Vuze Installed

WinMX Detection

WinMX Detection (uncredentialed check)

Xedus Detection

Xedus Web Server Traversal Arbitrary File Access

Xedus Webserver Connection Saturation DoS

Xedus Webserver Multiple XSS

XoloX Detection

# Palo Alto Local Security Checks

Palo Alto Networks < 7.1.23 / 8.0.x < 8.0.16 / 8.1.x < 8.1.7 Denial of Service vulnerability (PAN-SA-2019-0007)

Palo Alto Networks 7.1.x < 7.1.22 / 8.0.x < 8.0.15 / 8.1.x < 8.1.6 Cross-Site Scripting Vulnerability (PAN-SA-2019-0001)

Palo Alto Networks 7.1.x < 7.1.22 / 8.0.x < 8.0.15 / 8.1.x < 8.1.6 Multiple Vulnerabilities (PAN-SA-2019-0002)

Palo Alto Networks 9.0.0 < 9.0.1 Authentication Bypass vulnerability (PAN-SA-2019-0005)

Palo Alto Networks < 7.1.23 / 8.0.x < 8.0.16 / 8.1.x < 8.1.7 Integer Overflow Vulnerability (PAN-SA-2019-0006)

Palo Alto Networks PAN-OS 8.1.x < 8.1.12 / 9.0.x < 9.0.6 Privilege Escalation Vulnerability

Palo Alto Networks PAN-OS 8.1.x < 8.1.13 / 9.0.x < 9.0.7 RCE

Palo Alto Networks PAN-OS 1.0 < 7.1.24-h1 / 8.0.x < 8.1.9-h4 / 9.0 < 9.0.3-h3 Vulnerability

Palo Alto Networks PAN-OS 3.1.10 / 4.x < 4.0.5 Multiple Command Injections

Palo Alto Networks PAN-OS 4.1.x < 4.1.16 / 5.0.x < 5.0.10 / 5.1.x < 5.1.5 API Key Bypass Flaw

Palo Alto Networks PAN-OS 5.0.9 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 5.0.x < 5.0.19 / 5.1.x < 5.1.12 / 6.0.x < 6.0.14 / 6.1.x < 6.1.12 / 7.0.x < 7.0.8 Privilege Escalation (PAN-SA-2016-0012)

Palo Alto Networks PAN-OS 5.0.x < 5.0.20 / 5.1.x < 5.1.13 / 6.0.x < 6.0.15 / 6.1.x < 6.1.15 / 7.0.x < 7.0.11 / 7.1.x < 7.1.6 Multiple Vulnerabilities (PAN-SA-2016-0033 / PAN-SA-2016-0034 / PAN-SA-2016-0035 / PAN-SA-2016-0037)

Palo Alto Networks PAN-OS 5.x < 5.0.9 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 6.0.x < 6.0.14 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 6.1.21 and earlier / 7.1.x < 7.1.19 / 8.0.x < 8.0.12 / 8.1.x < 8.1.3 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 6.1.x / 7.0.x < 7.0.18 / 7.1.x < 7.1.12 / 8.0.x < 8.0.4 Network Time Protocol Vulnerability

Palo Alto Networks PAN-OS 6.1.x < 6.1.11 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 6.1.x < 6.1.17 / 7.0.x < 7.0.15 / 7.1.x < 7.1.10 / 8.0.x < 8.0.2 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 6.1.x < 6.1.18 / 7.0.x < 7.0.17 / 7.1.x < 7.1.12 / 8.0.x < 8.0.3 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 6.1.x < 6.1.19 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 6.1.x < 6.1.22 / 7.1.x < 7.1.20 / 8.0.x < 8.0.13 / 8.1.x < 8.1.5 Multiple Vulnerabilities (PAN-SA-2018-0012)

Palo Alto Networks PAN-OS 6.1.x <= 6.1.20 / 7.1.x < 7.1.21 / 8.0.x < 8.0.14 / 8.1.x < 8.1.4 Multiple Vulnerabilities (PAN-SA-2018-0015)

Palo Alto Networks PAN-OS 6.x.x < 6.1.21 / 7.1.x < 7.1.18 / 8.0.x < 8.0.11-h1 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 7.0.0 LDAP Authentication Bypass (PAN-SA-2015-0005)

Palo Alto Networks PAN-OS 7.0.7 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 7.0.x < 7.0.12 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 7.0.x < 7.0.14 / 7.1.x < 7.1.9 Multiple Vulnerabilities (PAN-SA-2017-0008 - PAN-SA-2017-0010)

Palo Alto Networks PAN-OS 7.0.x < 7.0.19 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 7.0.x < 7.0.5 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 7.0.x < 7.0.6 DHCP Packet Handling Dataplane DoS

Palo Alto Networks PAN-OS 7.0.x < 7.0.8 Multiple Vulnerabilities (PAN-SA-2016-0008 / PAN-SA-2016-0009)

Palo Alto Networks PAN-OS 7.1 < 7.1.25 / 8.0 < 8.0.20 / 8.1 < 8.1.8 / 9.0 < 9.0.2 OpenSSL Vulnerability

Palo Alto Networks PAN-OS 7.1.1 Out-of-Sequence Packet Firewall Bypass

Palo Alto Networks PAN-OS 7.1.x < 7.1.13 Management Interface Unspecified Remote DoS

Palo Alto Networks PAN-OS 7.1.x < 7.1.14 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 7.1.x < 7.1.15 / 8.0.x < 8.0.7 Multiple Vulnerabilities (ROBOT)

Palo Alto Networks PAN-OS 7.1.x < 7.1.19 / 8.0.x < 8.0.12 / 8.1.x < 8.1.3 Vulnerability

Palo Alto Networks PAN-OS 7.1.x < 7.1.24 / 8.0.x < 8.0.18 / 8.1.x < 8.1.9 / 9.0.x < 9.0.3 Vulnerability

Palo Alto Networks PAN-OS 7.1.x < 7.1.24 / 8.0.x < 8.0.19 / 8.1.x < 8.1.8-h5 / 9.0.x < 9.0.2-h4 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 7.1.x < 7.1.24 / 8.0.x < 8.0.19 / 8.1.x < 8.1.8-h5 / 9.0.x < 9.0.2-h4 Vulnerability

Palo Alto Networks PAN-OS 7.1.x < 7.1.24-h1 / 8.0.x < 8.0.19-h1 / 8.1.x < 8.1.9-h4 / 9.0.x < 9.0.3-h3 Vulnerability

Palo Alto Networks PAN-OS 7.1.x < 7.1.24-h1 / 8.0.x < 8.0.19-h1 / 8.1.x < 8.1.9-h4 / 9.0.x < 9.0.3-h3 Vulnerability

Palo Alto Networks PAN-OS 8.0.x < 8.0.6 Multiple Vulnerabilities

Palo Alto Networks PAN-OS 8.0.x < 8.0.6-h3 Web Interface Packet Capture Management Unspecified Remote Command Injection

Palo Alto Networks PAN-OS 8.1.x < 8.1.13 Privilege Escalation (PAN-97584)

Palo Alto Networks PAN-OS 8.1.x < 8.1.13 Vulnerability

Palo Alto Networks PAN-OS 8.1.x < 8.1.13 Vulnerability

Palo Alto Networks PAN-OS 8.1.x < 8.1.9-h4 / 9.0.x < 9.0.3-h3 Vulnerability

Palo Alto Networks PAN-OS 9.0.x < 9.0.3 Vulnerability

Palo Alto Networks PAN-OS < 3.1.10 / 4.x < 4.0.4 Multiple Command Injections

Palo Alto Networks PAN-OS < 3.1.11 / 4.0.x < 4.0.8 / 4.1.x < 4.1.1 Command Injection

Palo Alto Networks PAN-OS < 3.1.11 / 4.0.x < 4.0.9 Multiple Vulnerabilities

Palo Alto Networks PAN-OS < 3.1.12 / 4.0.x < 4.0.10 / 4.1.x < 4.1.4 Multiple Vulnerabilities

Palo Alto Networks PAN-OS < 4.0.14 / 4.1.x < 4.1.11 / 5.0.x < 5.0.2 Security Bypass

Palo Alto Networks PAN-OS < 4.0.8 / 4.1.x < 4.1.1 Command Injection

Palo Alto Networks PAN-OS < 4.0.8 Multiple Vulnerabilities

Palo Alto Networks PAN-OS < 4.0.9 / 4.1.x < 4.1.2 Multiple Command Injections

Palo Alto Networks PAN-OS < 4.0.9 / 4.1.x < 4.1.3 Information Disclosure

Palo Alto Networks PAN-OS < 4.1.13 / 5.0.x < 5.0.6 XSS

Palo Alto Networks PAN-OS < 5.0.10 / 5.1.x < 5.1.5 XSS

Palo Alto Networks PAN-OS < 5.0.14 / 5.1.x < 5.1.9 / 6.0.x < 6.0.4 OpenSSL MitM

Palo Alto Networks PAN-OS < 5.0.15 / 5.1.x < 5.1.10 / 6.0.x < 6.0.6 / 6.1.x < 6.1.1 Bash Shell Remote Code Execution (Shellshock)

Palo Alto Networks PAN-OS < 5.0.15 / 5.1.x < 5.1.10 / 6.0.x < 6.0.6 XSS

Palo Alto Networks PAN-OS < 5.0.16 / 6.0.x < 6.0.9 / 6.1.x < 6.1.3 XSS

Palo Alto Networks PAN-OS < 6.1 / 7.x < 7.1 / 8.1.x < 8.1.4 Cross-Site Scripting Vulnerability (PAN-SA-2018-0014)

Palo Alto Networks PAN-OS < 7.1.7 Unified Log View Information Disclosure

Palo Alto Networks PAN-OS <= 5.0.15 / 6.0.x <= 6.0.8 / 6.1.x <= 6.1.2 GNU C Library (glibc) Buffer Overflow (GHOST)

Palo Alto Networks PAN-OS API Key Persistence Security Bypass (PAN-SA-2015-0006)

Palo Alto Networks PAN-OS HTTP Header Handling URL Filter Bypass (PAN-SA-2016-0006)

Palo Alto Networks PAN-OS Multiple Vulnerabilities (PAN-SA-2016-0002, PAN-SA-2016-0004)

Palo Alto Networks PAN-OS Multiple Vulnerabilities (PAN-SA-2016-0003, PAN-SA-2016-0005)

Palo Alto Networks PAN-OS Series PA-7000 9.0 < 9.0.5-h5 Remote Code Execution Vulnerability (PAN-SA-2019-0040)

Palo Alto Networks Panorama PAN-OS < 6.0.1 Firmware Signature Verification Bypass Arbitrary Code Execution

Unsupported PAN-OS Operating System

# OracleVM Local Security Checks

OracleVM 2.1 : acpid (OVMSA-2009-0008)

OracleVM 2.1 : curl (OVMSA-2009-0019)

OracleVM 2.1 : dnsmasq (OVMSA-2009-0022)

OracleVM 2.1 : elinks (OVMSA-2009-0030)

OracleVM 2.1 : freetype (OVMSA-2009-0012)

OracleVM 2.1 : ipsec-tools (OVMSA-2009-0010)

OracleVM 2.1 : kernel (OVMSA-2008-2002)

OracleVM 2.1 : kernel (OVMSA-2008-2005)

OracleVM 2.1 : kernel (OVMSA-2008-2006)

OracleVM 2.1 : kernel (OVMSA-2008-2009)

OracleVM 2.1 : kernel (OVMSA-2009-0004)

OracleVM 2.1 : kernel (OVMSA-2009-0009)

OracleVM 2.1 : kernel (OVMSA-2009-0014)

OracleVM 2.1 : kernel (OVMSA-2009-0017)

OracleVM 2.1 : kernel (OVMSA-2009-0023)

OracleVM 2.1 : krb5 (OVMSA-2009-0003)

OracleVM 2.1 : libtiff (OVMSA-2009-0027)

OracleVM 2.1 : libxml2 (OVMSA-2009-0018)

OracleVM 2.1 : newt (OVMSA-2009-0026)

OracleVM 2.1 : ntp (OVMSA-2009-0011)

OracleVM 2.1 : udev (OVMSA-2009-0006)

OracleVM 2.1 : xen (OVMSA-2008-2003)

OracleVM 2.1 : xen (OVMSA-2008-2007)

OracleVM 2.1 : xen (OVMSA-2009-0001)

OracleVM 2.1 : xen (OVMSA-2009-0031)

OracleVM 2.2 : acpid (OVMSA-2009-0037)

OracleVM 2.2 : bash (OVMSA-2014-0020)

OracleVM 2.2 : bash (OVMSA-2014-0024)

OracleVM 2.2 : glibc (OVMSA-2015-0024) (GHOST)

OracleVM 2.2 : kernel (OVMSA-2009-0033)

OracleVM 2.2 : kernel (OVMSA-2013-0039)

OracleVM 2.2 : krb5 (OVMSA-2011-0015)

OracleVM 2.2 : ntp (OVMSA-2009-0036)

OracleVM 2.2 : ntp (OVMSA-2015-0002)

OracleVM 2.2 : openssh (OVMSA-2016-0033)

OracleVM 2.2 : openssl (OVMSA-2014-0007)

OracleVM 2.2 : openssl (OVMSA-2014-0040) (POODLE)

OracleVM 2.2 : openssl (OVMSA-2015-0030) (FREAK)

OracleVM 2.2 : ovs-agent (OVMSA-2010-0015)

OracleVM 2.2 : ovs-agent (OVMSA-2014-0029)

OracleVM 2.2 : xen (OVMSA-2011-0007)

OracleVM 2.2 : xen (OVMSA-2011-0008)

OracleVM 2.2 : xen (OVMSA-2012-0022)

OracleVM 2.2 : xen (OVMSA-2012-0036)

OracleVM 2.2 : xen (OVMSA-2012-0048)

OracleVM 2.2 : xen (OVMSA-2012-0049)

OracleVM 2.2 : xen (OVMSA-2012-0058)

OracleVM 2.2 : xen (OVMSA-2013-0033)

OracleVM 2.2 : xen (OVMSA-2013-0074)

OracleVM 2.2 : xen (OVMSA-2013-0075)

OracleVM 2.2 : xen (OVMSA-2013-0088)

OracleVM 2.2 : xen (OVMSA-2013-0092)

OracleVM 2.2 : xen (OVMSA-2014-0011)

OracleVM 2.2 : xen (OVMSA-2014-0028)

OracleVM 2.2 : xen (OVMSA-2015-0027)

OracleVM 2.2 : xen (OVMSA-2015-0035)

OracleVM 2.2 : xen (OVMSA-2015-0059) (Venom)

OracleVM 2.2 : xen (OVMSA-2015-0151)

OracleVM 2.2 : xen (OVMSA-2016-0012)

OracleVM 3.0 : xen (OVMSA-2012-0020)

OracleVM 3.0 : xen (OVMSA-2012-0035)

OracleVM 3.0 : xen (OVMSA-2012-0040)

OracleVM 3.0 : xen (OVMSA-2012-0050)

OracleVM 3.0 : xen (OVMSA-2012-0056)

OracleVM 3.0 : xen (OVMSA-2013-0002)

OracleVM 3.1 : kernel-uek (OVMSA-2012-0042)

OracleVM 3.1 : kernel-uek (OVMSA-2013-0010)

OracleVM 3.1 : xen (OVMSA-2012-0021)

OracleVM 3.1 : xen (OVMSA-2012-0034)

OracleVM 3.1 : xen (OVMSA-2012-0039)

OracleVM 3.1 : xen (OVMSA-2012-0046)

OracleVM 3.1 : xen (OVMSA-2012-0051)

OracleVM 3.1 : xen (OVMSA-2012-0057)

OracleVM 3.1 : xen (OVMSA-2013-0001)

OracleVM 3.1 : xen (OVMSA-2013-0009)

OracleVM 3.1 : xen (OVMSA-2013-0032)

OracleVM 3.1 : xen (OVMSA-2013-0037)

OracleVM 3.1 : xen (OVMSA-2013-0041)

OracleVM 3.1 : xen (OVMSA-2013-0043)

OracleVM 3.1 : xen (OVMSA-2013-0057)

OracleVM 3.1 : xen (OVMSA-2013-0068)

OracleVM 3.1 : xen (OVMSA-2013-0071)

OracleVM 3.1 : xen (OVMSA-2013-0073)

OracleVM 3.1 : xen (OVMSA-2013-0087)

OracleVM 3.1 : xen (OVMSA-2013-0091)

OracleVM 3.1 : xen (OVMSA-2014-0002)

OracleVM 3.1 : xen (OVMSA-2014-0010)

OracleVM 3.2 / 3.3 / 3.4 : xen (OVMSA-2017-0162)

OracleVM 3.2 : bash (OVMSA-2014-0019)

OracleVM 3.2 : bash (OVMSA-2014-0022)

OracleVM 3.2 : bind (OVMSA-2016-0055)

OracleVM 3.2 : bind (OVMSA-2016-0137)

OracleVM 3.2 : bind (OVMSA-2016-0146)

OracleVM 3.2 : bind (OVMSA-2016-0153)

OracleVM 3.2 : bind (OVMSA-2017-0034)

OracleVM 3.2 : curl (OVMSA-2016-0056)

OracleVM 3.2 : dbus-glib (OVMSA-2016-0057)

OracleVM 3.2 : dhcp (OVMSA-2016-0058)

OracleVM 3.2 : glibc (OVMSA-2015-0023) (GHOST)

OracleVM 3.2 : glibc (OVMSA-2017-0124) (Stack Clash)

OracleVM 3.2 : kernel-uek (OVMSA-2013-0003)

OracleVM 3.2 : kernel-uek (OVMSA-2013-0008)

OracleVM 3.2 : kernel-uek (OVMSA-2013-0015)

OracleVM 3.2 : kernel-uek (OVMSA-2016-0037)

OracleVM 3.2 : kernel-uek (OVMSA-2016-0060)

OracleVM 3.2 : libgcrypt (OVMSA-2016-0062)

OracleVM 3.2 : libxml2 (OVMSA-2016-0063)

OracleVM 3.2 : nspr (OVMSA-2016-0065)

OracleVM 3.2 : nss (OVMSA-2016-0066)

OracleVM 3.2 : nss (OVMSA-2016-0160)

OracleVM 3.2 : ntp (OVMSA-2015-0001)

OracleVM 3.2 : onpenssl (OVMSA-2014-0008)

OracleVM 3.2 : OpenIPMI (OVMSA-2016-0068)

OracleVM 3.2 : openldap (OVMSA-2016-0069)

OracleVM 3.2 : openssh (OVMSA-2016-0030)

OracleVM 3.2 : openssh (OVMSA-2016-0070)

OracleVM 3.2 : openssl (OVMSA-2014-0039) (POODLE)

OracleVM 3.2 : openssl (OVMSA-2015-0029) (FREAK)

OracleVM 3.2 : openssl (OVMSA-2016-0071)

OracleVM 3.2 : openssl (OVMSA-2016-0086)

OracleVM 3.2 : openssl (OVMSA-2016-0141)

OracleVM 3.2 : ovs-agent (OVMSA-2014-0037) (POODLE)

OracleVM 3.2 : perl (OVMSA-2016-0076)

OracleVM 3.2 : rpm (OVMSA-2016-0077)

OracleVM 3.2 : sos (OVMSA-2016-0078)

OracleVM 3.2 : sudo (OVMSA-2016-0079)

OracleVM 3.2 : sudo (OVMSA-2017-0125)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2016-0158) (Dirty COW)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2016-0167)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2016-0181)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2017-0006)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2017-0041)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2017-0046)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2017-0058)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2017-0061)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2017-0106)

OracleVM 3.2 : Unbreakable / etc (OVMSA-2017-0121)

OracleVM 3.2 : xen (OVMSA-2013-0004)

OracleVM 3.2 : xen (OVMSA-2013-0011)

OracleVM 3.2 : xen (OVMSA-2013-0031)

OracleVM 3.2 : xen (OVMSA-2013-0036)

OracleVM 3.2 : xen (OVMSA-2013-0040)

OracleVM 3.2 : xen (OVMSA-2013-0042)

OracleVM 3.2 : xen (OVMSA-2013-0056)

OracleVM 3.2 : xen (OVMSA-2013-0059)

OracleVM 3.2 : xen (OVMSA-2013-0069)

OracleVM 3.2 : xen (OVMSA-2013-0070)

OracleVM 3.2 : xen (OVMSA-2013-0072)

OracleVM 3.2 : xen (OVMSA-2013-0085)

OracleVM 3.2 : xen (OVMSA-2013-0090)

OracleVM 3.2 : xen (OVMSA-2014-0001)

OracleVM 3.2 : xen (OVMSA-2014-0009)

OracleVM 3.2 : xen (OVMSA-2014-0026)

OracleVM 3.2 : xen (OVMSA-2014-0041) (POODLE)

OracleVM 3.2 : xen (OVMSA-2015-0028)

OracleVM 3.2 : xen (OVMSA-2015-0032)

OracleVM 3.2 : xen (OVMSA-2015-0058) (Venom)

OracleVM 3.2 : xen (OVMSA-2015-0063)

OracleVM 3.2 : xen (OVMSA-2015-0068) (POODLE) (Venom)

OracleVM 3.2 : xen (OVMSA-2015-0096)

OracleVM 3.2 : xen (OVMSA-2015-0112)

OracleVM 3.2 : xen (OVMSA-2015-0142)

OracleVM 3.2 : xen (OVMSA-2015-0143)

OracleVM 3.2 : xen (OVMSA-2016-0008)

OracleVM 3.2 : xen (OVMSA-2016-0081)

OracleVM 3.2 : xen (OVMSA-2016-0090)

OracleVM 3.2 : xen (OVMSA-2016-0104)

OracleVM 3.2 : xen (OVMSA-2016-0166)

OracleVM 3.2 : xen (OVMSA-2016-0172)

OracleVM 3.2 : xen (OVMSA-2016-0178)

OracleVM 3.2 : xen (OVMSA-2017-0009)

OracleVM 3.2 : xen (OVMSA-2017-0096)

OracleVM 3.2 : xen (OVMSA-2017-0118)

OracleVM 3.2 : xen (OVMSA-2017-0149)

OracleVM 3.2 : xen (OVMSA-2017-0159)

OracleVM 3.2 : xen (OVMSA-2017-0178)

OracleVM 3.2 : xen (OVMSA-2018-0029) (Meltdown) (Spectre)

OracleVM 3.2 : xen (OVMSA-2018-0225)

OracleVM 3.2 : xen (OVMSA-2018-0272) (Foreshadow) (Spectre)

OracleVM 3.3 / 3.4 : bash (OVMSA-2017-0050)

OracleVM 3.3 / 3.4 : bind (OVMSA-2016-0036)

OracleVM 3.3 / 3.4 : bind (OVMSA-2016-0136)

OracleVM 3.3 / 3.4 : bind (OVMSA-2016-0145)

OracleVM 3.3 / 3.4 : bind (OVMSA-2016-0152)

OracleVM 3.3 / 3.4 : bind (OVMSA-2017-0033)

OracleVM 3.3 / 3.4 : bind (OVMSA-2017-0066)

OracleVM 3.3 / 3.4 : bind (OVMSA-2017-0100)

OracleVM 3.3 / 3.4 : bind (OVMSA-2017-0122)

OracleVM 3.3 / 3.4 : bind (OVMSA-2018-0014)

OracleVM 3.3 / 3.4 : bind (OVMSA-2018-0252)

OracleVM 3.3 / 3.4 : bind (OVMSA-2019-0027)

OracleVM 3.3 / 3.4 : coreutils (OVMSA-2017-0052)

OracleVM 3.3 / 3.4 : curl (OVMSA-2017-0059)

OracleVM 3.3 / 3.4 : dbus (OVMSA-2019-0034)

OracleVM 3.3 / 3.4 : dhcp (OVMSA-2018-0042)

OracleVM 3.3 / 3.4 : expat (OVMSA-2016-0168)

OracleVM 3.3 / 3.4 : file (OVMSA-2016-0050)

OracleVM 3.3 / 3.4 : foomatic (OVMSA-2016-0040)

OracleVM 3.3 / 3.4 : ghostscript (OVMSA-2017-0002)

OracleVM 3.3 / 3.4 : ghostscript (OVMSA-2017-0103)

OracleVM 3.3 / 3.4 : ghostscript (OVMSA-2018-0285)

OracleVM 3.3 / 3.4 : glibc (OVMSA-2017-0051)

OracleVM 3.3 / 3.4 : glibc (OVMSA-2017-0113)

OracleVM 3.3 / 3.4 : glibc (OVMSA-2018-0235)

OracleVM 3.3 / 3.4 : gnupg2 (OVMSA-2018-0239)

OracleVM 3.3 / 3.4 : gnutls (OVMSA-2017-0054)

OracleVM 3.3 / 3.4 : jasper (OVMSA-2017-0102)

OracleVM 3.3 / 3.4 : krb5 (OVMSA-2016-0039)

OracleVM 3.3 / 3.4 : libgcrypt (OVMSA-2016-0156)

OracleVM 3.3 / 3.4 : libssh2 (OVMSA-2016-0035)

OracleVM 3.3 / 3.4 : libtiff (OVMSA-2016-0093)

OracleVM 3.3 / 3.4 : libtirpc (OVMSA-2017-0108)

OracleVM 3.3 / 3.4 : libxml2 (OVMSA-2016-0087)

OracleVM 3.3 / 3.4 : mysql (OVMSA-2017-0035)

OracleVM 3.3 / 3.4 : nss (OVMSA-2017-0109)

OracleVM 3.3 / 3.4 : nss (OVMSA-2018-0264)

OracleVM 3.3 / 3.4 : nss / nss-util (OVMSA-2017-0065)

OracleVM 3.3 / 3.4 : nss / nss-util / etc (OVMSA-2016-0042)

OracleVM 3.3 / 3.4 : nss-util (OVMSA-2016-0034)

OracleVM 3.3 / 3.4 : nssnss-util (OVMSA-2016-0159)

OracleVM 3.3 / 3.4 : ntp (OVMSA-2016-0082)

OracleVM 3.3 / 3.4 : ntp (OVMSA-2017-0038)

OracleVM 3.3 / 3.4 : ntp (OVMSA-2017-0165)

OracleVM 3.3 / 3.4 : ntp (OVMSA-2018-0290)

OracleVM 3.3 / 3.4 : ocaml (OVMSA-2017-0049)

OracleVM 3.3 / 3.4 : openjpeg (OVMSA-2017-0048)

OracleVM 3.3 / 3.4 : openssh (OVMSA-2016-0038)

OracleVM 3.3 / 3.4 : openssh (OVMSA-2016-0048)

OracleVM 3.3 / 3.4 : openssh (OVMSA-2017-0053)

OracleVM 3.3 / 3.4 : openssh (OVMSA-2017-0150)

OracleVM 3.3 / 3.4 : openssh (OVMSA-2019-0013)

OracleVM 3.3 / 3.4 : openssl (OVMSA-2016-0049) (SLOTH)

OracleVM 3.3 / 3.4 : openssl (OVMSA-2016-0135)

OracleVM 3.3 / 3.4 : openssl (OVMSA-2017-0042)

OracleVM 3.3 / 3.4 : ovm-consoled (OVMSA-2016-0151)

OracleVM 3.3 / 3.4 : patch (OVMSA-2018-0036)

OracleVM 3.3 / 3.4 : policycoreutils (OVMSA-2016-0157)

OracleVM 3.3 / 3.4 : polkit (OVMSA-2019-0008)

OracleVM 3.3 / 3.4 : poppler (OVMSA-2017-0147)

OracleVM 3.3 / 3.4 : procps (OVMSA-2018-0226)

OracleVM 3.3 / 3.4 : python (OVMSA-2016-0099) (httpoxy)

OracleVM 3.3 / 3.4 : python-paramiko (OVMSA-2018-0034)

OracleVM 3.3 / 3.4 : python-paramiko (OVMSA-2018-0270)

OracleVM 3.3 / 3.4 : rpcbind (OVMSA-2017-0107)

OracleVM 3.3 / 3.4 : sudo (OVMSA-2016-0170)

OracleVM 3.3 / 3.4 : sudo (OVMSA-2017-0110)

OracleVM 3.3 / 3.4 : sudo (OVMSA-2017-0114)

OracleVM 3.3 / 3.4 : sudo (OVMSA-2019-0050)

OracleVM 3.3 / 3.4 : vim (OVMSA-2016-0182)

OracleVM 3.3 : bash (OVMSA-2014-0018)

OracleVM 3.3 : bash (OVMSA-2014-0021)

OracleVM 3.3 : bind (OVMSA-2014-0084)

OracleVM 3.3 : bind (OVMSA-2015-0033)

OracleVM 3.3 : bind (OVMSA-2015-0105)

OracleVM 3.3 : bind (OVMSA-2015-0119)

OracleVM 3.3 : bind (OVMSA-2015-0156)

OracleVM 3.3 : bind (OVMSA-2016-0009)

OracleVM 3.3 : cups (OVMSA-2014-0035)

OracleVM 3.3 : cups (OVMSA-2015-0071)

OracleVM 3.3 : curl (OVMSA-2015-0107)

OracleVM 3.3 : dhcp (OVMSA-2018-0024)

OracleVM 3.3 : freetype (OVMSA-2015-0036)

OracleVM 3.3 : glibc (OVMSA-2014-0017)

OracleVM 3.3 : glibc (OVMSA-2014-0033)

OracleVM 3.3 : glibc (OVMSA-2015-0003)

OracleVM 3.3 : glibc (OVMSA-2015-0022) (GHOST)

OracleVM 3.3 : glibc (OVMSA-2015-0055)

OracleVM 3.3 : glibc (OVMSA-2016-0013) (GHOST)

OracleVM 3.3 : gnutls (OVMSA-2015-0101)

OracleVM 3.3 : gnutls (OVMSA-2016-0004)

OracleVM 3.3 : grep (OVMSA-2015-0100)

OracleVM 3.3 : ipmitool (OVMSA-2020-0012)

OracleVM 3.3 : jasper (OVMSA-2014-0087)

OracleVM 3.3 : jasper (OVMSA-2015-0006)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0034)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0040)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0056)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0060)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0069)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0072)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0094)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0104)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0109)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0113)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0114)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0122)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0144)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0147)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0150)

OracleVM 3.3 : kernel-uek (OVMSA-2015-0154)

OracleVM 3.3 : kernel-uek (OVMSA-2016-0005)

OracleVM 3.3 : kernel-uek (OVMSA-2016-0046)

OracleVM 3.3 : kernel-uek (OVMSA-2016-0053)

OracleVM 3.3 : kernel-uek (OVMSA-2016-0084)

OracleVM 3.3 : kernel-uek (OVMSA-2016-0092)

OracleVM 3.3 : krb5 (OVMSA-2014-0034)

OracleVM 3.3 : krb5 (OVMSA-2015-0054)

OracleVM 3.3 : libpng (OVMSA-2015-0153)

OracleVM 3.3 : libtiff (OVMSA-2017-0037)

OracleVM 3.3 : libuser (OVMSA-2015-0106)

OracleVM 3.3 : libvorbis (OVMSA-2018-0031)

OracleVM 3.3 : libXfont (OVMSA-2014-0080)

OracleVM 3.3 : libXfont (OVMSA-2015-0120)

OracleVM 3.3 : libxml2 (OVMSA-2014-0031)

OracleVM 3.3 : libxml2 (OVMSA-2015-0097)

OracleVM 3.3 : libxml2 (OVMSA-2015-0152)

OracleVM 3.3 : mailx (OVMSA-2014-0086)

OracleVM 3.3 : net-snmp (OVMSA-2015-0099)

OracleVM 3.3 : net-snmp (OVMSA-2015-0116)

OracleVM 3.3 : nss (OVMSA-2014-0014)

OracleVM 3.3 : nss (OVMSA-2014-0023)

OracleVM 3.3 : nss (OVMSA-2014-0082)

OracleVM 3.3 : nss (OVMSA-2015-0073)

OracleVM 3.3 : nss (OVMSA-2016-0003)

OracleVM 3.3 : nss (OVMSA-2017-0156)

OracleVM 3.3 : nss / nss-util,nspr (OVMSA-2015-0145)

OracleVM 3.3 : nss-softokn (OVMSA-2015-0118)

OracleVM 3.3 : nss-util (OVMSA-2014-0015)

OracleVM 3.3 : ntp (OVMSA-2014-0085)

OracleVM 3.3 : ntp (OVMSA-2015-0102)

OracleVM 3.3 : ntp (OVMSA-2015-0140)

OracleVM 3.3 : ntp (OVMSA-2016-0006)

OracleVM 3.3 : openldap (OVMSA-2015-0123)

OracleVM 3.3 : openssl (OVMSA-2014-0012)

OracleVM 3.3 : openssl (OVMSA-2014-0032) (Heartbleed) (POODLE)

OracleVM 3.3 : openssl (OVMSA-2015-0005) (FREAK)

OracleVM 3.3 : openssl (OVMSA-2015-0039)

OracleVM 3.3 : openssl (OVMSA-2015-0065) (Logjam)

OracleVM 3.3 : openssl (OVMSA-2015-0070)

OracleVM 3.3 : openssl (OVMSA-2015-0155)

OracleVM 3.3 : openssl (OVMSA-2016-0001) (SLOTH)

OracleVM 3.3 : openssl (OVMSA-2016-0031)

OracleVM 3.3 : pam (OVMSA-2015-0117)

OracleVM 3.3 : python (OVMSA-2015-0098)

OracleVM 3.3 : rpcbind (OVMSA-2016-0002)

OracleVM 3.3 : rpm (OVMSA-2014-0083)

OracleVM 3.3 : rsyslog (OVMSA-2014-0030)

OracleVM 3.3 : sos (OVMSA-2016-0011)

OracleVM 3.3 : sqlite (OVMSA-2015-0115)

OracleVM 3.3 : sudo (OVMSA-2015-0103)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0014)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0095)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0098)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0133)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0139)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0150) (Dirty COW)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0155)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0163)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0175)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2016-0180)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0005)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0040)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0045)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0057) (Dirty COW)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0060)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0105)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0112)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0120)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0127)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0144)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0152) (BlueBorne) (Stack Clash)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0164)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0168)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2017-0173) (BlueBorne) (Stack Clash)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2018-0016) (Meltdown) (Spectre)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2018-0041) (Spectre)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2018-0231)

OracleVM 3.3 : Unbreakable / etc (OVMSA-2018-0237)

OracleVM 3.3 : unzip (OVMSA-2015-0037)

OracleVM 3.3 : wget (OVMSA-2014-0036)

OracleVM 3.3 : xen (OVMSA-2014-0025)

OracleVM 3.3 : xen (OVMSA-2014-0038) (POODLE)

OracleVM 3.3 : xen (OVMSA-2015-0004)

OracleVM 3.3 : xen (OVMSA-2015-0026)

OracleVM 3.3 : xen (OVMSA-2015-0031)

OracleVM 3.3 : xen (OVMSA-2015-0057) (Venom)

OracleVM 3.3 : xen (OVMSA-2015-0064)

OracleVM 3.3 : xen (OVMSA-2015-0067)

OracleVM 3.3 : xen (OVMSA-2015-0095)

OracleVM 3.3 : xen (OVMSA-2015-0111)

OracleVM 3.3 : xen (OVMSA-2015-0141)

OracleVM 3.3 : xen (OVMSA-2016-0007)

OracleVM 3.3 : xen (OVMSA-2016-0089)

OracleVM 3.3 : xen (OVMSA-2016-0103)

OracleVM 3.3 : xen (OVMSA-2016-0165)

OracleVM 3.3 : xen (OVMSA-2016-0171)

OracleVM 3.3 : xen (OVMSA-2016-0177)

OracleVM 3.3 : xen (OVMSA-2017-0008)

OracleVM 3.3 : xen (OVMSA-2017-0095)

OracleVM 3.3 : xen (OVMSA-2017-0117)

OracleVM 3.3 : xen (OVMSA-2017-0148)

OracleVM 3.3 : xen (OVMSA-2017-0158)

OracleVM 3.3 : xen (OVMSA-2017-0177)

OracleVM 3.3 : xen (OVMSA-2018-0224) (Meltdown) (Spectre)

OracleVM 3.3 : xen (OVMSA-2018-0271) (Foreshadow) (Spectre)

OracleVM 3.4 : dhcp (OVMSA-2018-0023)

OracleVM 3.4 : dnsmasq (OVMSA-2017-0160)

OracleVM 3.4 : freetype (OVMSA-2020-0001)

OracleVM 3.4 : glusterfs (OVMSA-2018-0263)

OracleVM 3.4 : kernel-uek (OVMSA-2016-0041)

OracleVM 3.4 : kernel-uek (OVMSA-2016-0047)

OracleVM 3.4 : kernel-uek (OVMSA-2016-0052)

OracleVM 3.4 : kernel-uek (OVMSA-2016-0083)

OracleVM 3.4 : kernel-uek (OVMSA-2016-0091)

OracleVM 3.4 : libssh2 (OVMSA-2019-0028)

OracleVM 3.4 : libtiff (OVMSA-2017-0036)

OracleVM 3.4 : libvorbis (OVMSA-2018-0030)

OracleVM 3.4 : microcode\_ctl (OVMSA-2018-0003)

OracleVM 3.4 : microcode\_ctl (OVMSA-2018-0011) (Spectre)

OracleVM 3.4 : microcode\_ctl (OVMSA-2018-0013) (Spectre)

OracleVM 3.4 : nss (OVMSA-2017-0154)

OracleVM 3.4 : openssl (OVMSA-2019-0040)

OracleVM 3.4 : qemu-kvm (OVMSA-2016-0051)

OracleVM 3.4 : qemu-kvm (OVMSA-2016-0096)

OracleVM 3.4 : qemu-kvm (OVMSA-2017-0043)

OracleVM 3.4 : qemu-kvm (OVMSA-2017-0047)

OracleVM 3.4 : qemu-kvm (OVMSA-2017-0055)

OracleVM 3.4 : qemu-kvm (OVMSA-2017-0101)

OracleVM 3.4 : qemu-kvm (OVMSA-2018-0004) (Spectre)

OracleVM 3.4 : qemu-kvm (OVMSA-2018-0025)

OracleVM 3.4 : qemu-kvm (OVMSA-2018-0219) (Spectre)

OracleVM 3.4 : qemu-kvm (OVMSA-2018-0238) (Spectre)

OracleVM 3.4 : qemu-kvm (OVMSA-2019-0045)

OracleVM 3.4 : qemu-kvm (OVMSA-2020-0010)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0094)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0097)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0100)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0134)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0138)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0140)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0149) (Dirty COW)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0154)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0162)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0174)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2016-0179)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0004)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0039)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0044)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0056)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0062)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0104)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0111)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0115) (Stack Clash)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0119)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0126) (Stack Clash)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0143)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0145) (Stack Clash)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0151) (BlueBorne)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0163)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0167)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0169)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0172) (Dirty COW)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2017-0174) (BlueBorne) (Dirty COW) (Stack Clash)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0002)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0007) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0008) (Meltdown) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0010) (Meltdown) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0012) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0015) (BlueBorne) (Meltdown) (Spectre) (Stack Clash)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0017) (Meltdown)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0033)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0035) (Dirty COW) (Meltdown) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0037)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0038)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0040)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0223) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0228) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0230)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0236)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0247) (Foreshadow)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0253)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0254) (Foreshadow)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0256)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0258)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0261)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0266)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0273)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0284)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2018-0286)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0002)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0007) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0009)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0011)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0014)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0015)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0018) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0022)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0023) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0024)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0026) (SACK Panic) (SACK Slowness)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0035) (Spectre)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0038)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0039)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0044)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0046)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0047)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0052)

OracleVM 3.4 : Unbreakable / etc (OVMSA-2019-0056)

OracleVM 3.4 : xen (OVMSA-2016-0088) (Bunker Buster)

OracleVM 3.4 : xen (OVMSA-2016-0102)

OracleVM 3.4 : xen (OVMSA-2016-0164)

OracleVM 3.4 : xen (OVMSA-2016-0173)

OracleVM 3.4 : xen (OVMSA-2016-0176)

OracleVM 3.4 : xen (OVMSA-2017-0007)

OracleVM 3.4 : xen (OVMSA-2017-0094)

OracleVM 3.4 : xen (OVMSA-2017-0116)

OracleVM 3.4 : xen (OVMSA-2017-0142)

OracleVM 3.4 : xen (OVMSA-2017-0153)

OracleVM 3.4 : xen (OVMSA-2017-0157)

OracleVM 3.4 : xen (OVMSA-2017-0166)

OracleVM 3.4 : xen (OVMSA-2017-0176)

OracleVM 3.4 : xen (OVMSA-2018-0005) (Meltdown) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0006) (Meltdown) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0020) (Meltdown) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0021) (Meltdown) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0028) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0039)

OracleVM 3.4 : xen (OVMSA-2018-0218) (Meltdown) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0221)

OracleVM 3.4 : xen (OVMSA-2018-0232) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0233) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0246) (Foreshadow)

OracleVM 3.4 : xen (OVMSA-2018-0248) (Bunker Buster) (Foreshadow) (Meltdown) (POODLE) (Spectre)

OracleVM 3.4 : xen (OVMSA-2018-0251) (Foreshadow)

OracleVM 3.4 : xen (OVMSA-2018-0282) (Foreshadow) (Spectre)

OracleVM 3.4 : xen (OVMSA-2019-0016) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

OracleVM 3.4 : xen (OVMSA-2019-0054)

# Oracle Linux Local Security Checks

Oracle Linux 3 / 4 / 5 : acpid (ELSA-2009-0474)

Oracle Linux 3 / 4 / 5 : bind (ELSA-2007-0740)

Oracle Linux 3 / 4 / 5 : bind (ELSA-2008-0533)

Oracle Linux 3 / 4 / 5 : bind (ELSA-2009-0020)

Oracle Linux 3 / 4 / 5 : bzip2 (ELSA-2008-0893)

Oracle Linux 3 / 4 / 5 : bzip2 (ELSA-2010-0703)

Oracle Linux 3 / 4 / 5 : cups (ELSA-2007-0123)

Oracle Linux 3 / 4 / 5 : cups (ELSA-2007-0720)

Oracle Linux 3 / 4 / 5 : cups (ELSA-2008-0498)

Oracle Linux 3 / 4 / 5 : cups (ELSA-2008-0937)

Oracle Linux 3 / 4 / 5 : cups (ELSA-2010-0490)

Oracle Linux 3 / 4 / 5 : curl (ELSA-2009-0341)

Oracle Linux 3 / 4 / 5 : curl (ELSA-2009-1209)

Oracle Linux 3 / 4 / 5 : e2fsprogs (ELSA-2008-0003)

Oracle Linux 3 / 4 / 5 : ed (ELSA-2008-0946)

Oracle Linux 3 / 4 / 5 : expat (ELSA-2009-1625)

Oracle Linux 3 / 4 / 5 : fetchmail (ELSA-2007-0385)

Oracle Linux 3 / 4 / 5 : fetchmail (ELSA-2009-1427)

Oracle Linux 3 / 4 / 5 : freeradius (ELSA-2007-0338)

Oracle Linux 3 / 4 / 5 : freetype (ELSA-2007-0403)

Oracle Linux 3 / 4 / 5 : freetype (ELSA-2008-0556)

Oracle Linux 3 / 4 / 5 : freetype (ELSA-2010-0607)

Oracle Linux 3 / 4 / 5 : gcc / gcc4 (ELSA-2010-0039)

Oracle Linux 3 / 4 / 5 : ghostscript (ELSA-2008-0155)

Oracle Linux 3 / 4 / 5 : ghostscript (ELSA-2009-0345)

Oracle Linux 3 / 4 / 5 : gimp (ELSA-2007-0343)

Oracle Linux 3 / 4 / 5 : gimp (ELSA-2007-0513)

Oracle Linux 3 / 4 / 5 : gzip (ELSA-2010-0061)

Oracle Linux 3 / 4 / 5 : httpd (ELSA-2008-0967)

Oracle Linux 3 / 4 / 5 : ImageMagick (ELSA-2008-0145)

Oracle Linux 3 / 4 / 5 : ipsec-tools (ELSA-2008-0849)

Oracle Linux 3 / 4 / 5 : kdebase (ELSA-2007-0494)

Oracle Linux 3 / 4 / 5 : krb5 (ELSA-2007-0095)

Oracle Linux 3 / 4 / 5 : krb5 (ELSA-2010-0029)

Oracle Linux 3 / 4 / 5 : krb5 (ELSA-2010-0423)

Oracle Linux 3 / 4 / 5 : libpng (ELSA-2007-0356)

Oracle Linux 3 / 4 / 5 : libpng (ELSA-2007-0992)

Oracle Linux 3 / 4 / 5 : libpng (ELSA-2010-0534)

Oracle Linux 3 / 4 / 5 : libtiff (ELSA-2009-1159)

Oracle Linux 3 / 4 / 5 : libtool (ELSA-2009-1646)

Oracle Linux 3 / 4 / 5 : libvorbis (ELSA-2007-0845)

Oracle Linux 3 / 4 / 5 : libvorbis (ELSA-2008-0270)

Oracle Linux 3 / 4 / 5 : libvorbis (ELSA-2009-1219)

Oracle Linux 3 / 4 / 5 : libvorbis (ELSA-2009-1561)

Oracle Linux 3 / 4 / 5 : libxml / libxml2 (ELSA-2009-1206)

Oracle Linux 3 / 4 / 5 : libxml2 (ELSA-2008-0032)

Oracle Linux 3 / 4 / 5 : libxml2 (ELSA-2008-0836)

Oracle Linux 3 / 4 / 5 : libxml2 (ELSA-2008-0884)

Oracle Linux 3 / 4 / 5 : libxml2 (ELSA-2008-0988)

Oracle Linux 3 / 4 / 5 : libxslt (ELSA-2008-0287)

Oracle Linux 3 / 4 / 5 : lynx (ELSA-2008-0965)

Oracle Linux 3 / 4 / 5 : mikmod (ELSA-2010-0720)

Oracle Linux 3 / 4 / 5 : mod\_perl (ELSA-2007-0395)

Oracle Linux 3 / 4 / 5 : mutt (ELSA-2007-0386)

Oracle Linux 3 / 4 / 5 : net-snmp (ELSA-2008-0529)

Oracle Linux 3 / 4 / 5 : net-snmp (ELSA-2008-0971)

Oracle Linux 3 / 4 / 5 : newt (ELSA-2009-1463)

Oracle Linux 3 / 4 / 5 : openssl (ELSA-2009-0004)

Oracle Linux 3 / 4 / 5 : pango (ELSA-2009-0476)

Oracle Linux 3 / 4 / 5 : pango (ELSA-2010-0140)

Oracle Linux 3 / 4 / 5 : perl (ELSA-2007-0966)

Oracle Linux 3 / 4 / 5 : perl (ELSA-2008-0522)

Oracle Linux 3 / 4 / 5 : php (ELSA-2010-0040)

Oracle Linux 3 / 4 / 5 : postfix (ELSA-2008-0839)

Oracle Linux 3 / 4 / 5 : postgresql (ELSA-2007-0336)

Oracle Linux 3 / 4 / 5 : qt (ELSA-2007-0721)

Oracle Linux 3 / 4 / 5 : qt (ELSA-2007-0883)

Oracle Linux 3 / 4 / 5 : quagga (ELSA-2007-0389)

Oracle Linux 3 / 4 / 5 : samba (ELSA-2007-0354)

Oracle Linux 3 / 4 / 5 : samba (ELSA-2007-1114)

Oracle Linux 3 / 4 / 5 : samba (ELSA-2010-0697)

Oracle Linux 3 / 4 / 5 : samba / samba3x (ELSA-2010-0488)

Oracle Linux 3 / 4 / 5 : squid (ELSA-2007-1130)

Oracle Linux 3 / 4 / 5 : squid (ELSA-2008-0214)

Oracle Linux 3 / 4 / 5 : squirrelmail (ELSA-2007-0358)

Oracle Linux 3 / 4 / 5 : squirrelmail (ELSA-2009-0010)

Oracle Linux 3 / 4 / 5 : squirrelmail (ELSA-2009-0057)

Oracle Linux 3 / 4 / 5 : squirrelmail (ELSA-2009-1066)

Oracle Linux 3 / 4 / 5 : squirrelmail (ELSA-2009-1490)

Oracle Linux 3 / 4 / 5 : star (ELSA-2007-0873)

Oracle Linux 3 / 4 / 5 : tetex (ELSA-2007-0731)

Oracle Linux 3 / 4 / 5 : vixie-cron (ELSA-2007-0345)

Oracle Linux 3 / 4 / 5 : vnc (ELSA-2009-0261)

Oracle Linux 3 / 4 / 5 : wget (ELSA-2009-1549)

Oracle Linux 3 / 4 / 5 : wireshark (ELSA-2007-0066)

Oracle Linux 3 / 4 / 5 : wireshark (ELSA-2008-0890)

Oracle Linux 3 / 4 / 5 : wireshark (ELSA-2009-0313)

Oracle Linux 3 / 4 / 5 : wireshark (ELSA-2009-1100)

Oracle Linux 3 / 4 / 5 : wireshark (ELSA-2010-0360)

Oracle Linux 3 / 4 / 5 : wireshark (ELSA-2010-0625)

Oracle Linux 3 / 4 / 5 : xterm (ELSA-2009-0018)

Oracle Linux 3 / 4 : 4Suite (ELSA-2009-1572)

Oracle Linux 3 / 4 : bind (ELSA-2007-0044)

Oracle Linux 3 / 4 : cscope (ELSA-2009-1101)

Oracle Linux 3 / 4 : cups (ELSA-2008-0206)

Oracle Linux 3 / 4 : cups (ELSA-2009-1083)

Oracle Linux 3 / 4 : curl (ELSA-2010-0329)

Oracle Linux 3 / 4 : enscript (ELSA-2008-1021)

Oracle Linux 3 / 4 : evolution (ELSA-2007-0353)

Oracle Linux 3 / 4 : evolution (ELSA-2007-0509)

Oracle Linux 3 / 4 : evolution (ELSA-2008-0516)

Oracle Linux 3 / 4 : fetchmail (ELSA-2007-0018)

Oracle Linux 3 / 4 : freetype (ELSA-2007-0150)

Oracle Linux 3 / 4 : freetype (ELSA-2009-0329)

Oracle Linux 3 / 4 : ghostscript (ELSA-2009-0420)

Oracle Linux 3 / 4 : gnome-vfs / gnome-vfs2 (ELSA-2009-0005)

Oracle Linux 3 / 4 : gnomemeeting (ELSA-2007-0086)

Oracle Linux 3 / 4 : gnupg (ELSA-2007-0106)

Oracle Linux 3 / 4 : gzip (ELSA-2006-0667)

Oracle Linux 3 / 4 : httpd (ELSA-2006-0619)

Oracle Linux 3 / 4 : httpd (ELSA-2007-0662)

Oracle Linux 3 / 4 : ImageMagick (ELSA-2007-0015)

Oracle Linux 3 / 4 : kdelibs (ELSA-2006-0720)

Oracle Linux 3 / 4 : libgsf (ELSA-2007-0011)

Oracle Linux 3 / 4 : mailman (ELSA-2006-0600)

Oracle Linux 3 / 4 : ncompress (ELSA-2006-0663)

Oracle Linux 3 / 4 : net-snmp (ELSA-2007-1045)

Oracle Linux 3 / 4 : netpbm (ELSA-2008-0131)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2007-0033)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2007-0406)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2007-0848)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2008-0176)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2008-0538)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2008-0939)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2009-1426)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2010-0101)

Oracle Linux 3 / 4 : openoffice.org (ELSA-2010-0643)

Oracle Linux 3 / 4 : openssh (ELSA-2006-0738)

Oracle Linux 3 / 4 : openssl (ELSA-2010-0163)

Oracle Linux 3 / 4 : openssl096b (ELSA-2010-0173)

Oracle Linux 3 / 4 : perl (ELSA-2010-0457)

Oracle Linux 3 / 4 : php (ELSA-2007-0076)

Oracle Linux 3 / 4 : php (ELSA-2007-0155)

Oracle Linux 3 / 4 : php (ELSA-2009-0337)

Oracle Linux 3 / 4 : pidgin (ELSA-2008-0584)

Oracle Linux 3 / 4 : pidgin (ELSA-2009-1218)

Oracle Linux 3 / 4 : postgresql (ELSA-2007-0064)

Oracle Linux 3 / 4 : python (ELSA-2006-0713)

Oracle Linux 3 / 4 : python (ELSA-2007-1076)

Oracle Linux 3 / 4 : qt (ELSA-2006-0725)

Oracle Linux 3 / 4 : ruby (ELSA-2006-0604 / ELSA-2006-0729)

Oracle Linux 3 / 4 : samba (ELSA-2007-0060)

Oracle Linux 3 / 4 : samba (ELSA-2008-0288)

Oracle Linux 3 / 4 : seamonkey (ELSA-2007-0077)

Oracle Linux 3 / 4 : seamonkey (ELSA-2007-0402)

Oracle Linux 3 / 4 : seamonkey (ELSA-2007-0722)

Oracle Linux 3 / 4 : seamonkey (ELSA-2007-0980)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-0104)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-0208)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-0223)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-0547)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-0599)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-0882)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-0977)

Oracle Linux 3 / 4 : seamonkey (ELSA-2008-1037)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-0257)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-0325)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-0398)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-0437)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-1096)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-1134)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-1163)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-1531)

Oracle Linux 3 / 4 : seamonkey (ELSA-2009-1673)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0113)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0333)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0499)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0546)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0557)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0680)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0781)

Oracle Linux 3 / 4 : seamonkey (ELSA-2010-0810)

Oracle Linux 3 / 4 : squirrelmail (ELSA-2007-0022)

Oracle Linux 3 / 4 : tar (ELSA-2006-0749)

Oracle Linux 3 / 4 : texinfo (ELSA-2006-0727)

Oracle Linux 3 / 4 : util-linux (ELSA-2007-0969)

Oracle Linux 3 / 4 : vim (ELSA-2008-0617)

Oracle Linux 3 / 4 : xpdf (ELSA-2007-0735)

Oracle Linux 3 / 4 : xpdf (ELSA-2009-0430)

Oracle Linux 3 / 4 : xscreensaver (ELSA-2007-0322)

Oracle Linux 3 / 5 : httpd (ELSA-2009-1579)

Oracle Linux 3 / 5 : php (ELSA-2008-0544)

Oracle Linux 3 : bash (ELSA-2008-2005)

Oracle Linux 3 : bind (ELSA-2009-1181)

Oracle Linux 3 : cpio (ELSA-2010-0145)

Oracle Linux 3 : cups (ELSA-2007-1023)

Oracle Linux 3 : cups (ELSA-2008-0153)

Oracle Linux 3 : cups (ELSA-2008-1028)

Oracle Linux 3 : cups (ELSA-2009-0308)

Oracle Linux 3 : cups (ELSA-2009-0428)

Oracle Linux 3 : cups (ELSA-2010-0754)

Oracle Linux 3 : cyrus-sasl (ELSA-2007-0878)

Oracle Linux 3 : dhcp (ELSA-2009-1154)

Oracle Linux 3 : evolution (ELSA-2009-0358)

Oracle Linux 3 : freetype (ELSA-2010-0577)

Oracle Linux 3 : freetype (ELSA-2010-0736)

Oracle Linux 3 : gcc (ELSA-2007-0473)

Oracle Linux 3 : gdb (ELSA-2007-0469)

Oracle Linux 3 : gstreamer-plugins (ELSA-2009-0269)

Oracle Linux 3 : httpd (ELSA-2007-0533)

Oracle Linux 3 : httpd (ELSA-2008-0005)

Oracle Linux 3 : httpd (ELSA-2009-1108)

Oracle Linux 3 : httpd (ELSA-2009-1205)

Oracle Linux 3 : imap (ELSA-2009-0275)

Oracle Linux 3 : kdebase (ELSA-2006-0576)

Oracle Linux 3 : kdegraphics (ELSA-2006-0648)

Oracle Linux 3 : kdelibs (ELSA-2009-1128)

Oracle Linux 3 : kernel (ELSA-2006-0710)

Oracle Linux 3 : kernel (ELSA-2007-0436)

Oracle Linux 3 : kernel (ELSA-2007-0671)

Oracle Linux 3 : kernel (ELSA-2007-0938)

Oracle Linux 3 : kernel (ELSA-2007-1049)

Oracle Linux 3 : kernel (ELSA-2008-0211)

Oracle Linux 3 : kernel (ELSA-2008-0973)

Oracle Linux 3 : kernel (ELSA-2009-1233)

Oracle Linux 3 : kernel (ELSA-2009-1550)

Oracle Linux 3 : krb5 (ELSA-2007-0384)

Oracle Linux 3 : krb5 (ELSA-2008-0181)

Oracle Linux 3 : krb5 (ELSA-2009-0410)

Oracle Linux 3 : libpng (ELSA-2009-0340)

Oracle Linux 3 : libtiff (ELSA-2006-0603)

Oracle Linux 3 : libtiff (ELSA-2008-0863)

Oracle Linux 3 : libtiff (ELSA-2010-0520)

Oracle Linux 3 : net-snmp (ELSA-2009-0295)

Oracle Linux 3 : net-snmp (ELSA-2009-1124)

Oracle Linux 3 : ntp (ELSA-2009-1651)

Oracle Linux 3 : openldap (ELSA-2007-0430)

Oracle Linux 3 : openssl (ELSA-2006-0695)

Oracle Linux 3 : openssl (ELSA-2007-0813)

Oracle Linux 3 : pam (ELSA-2007-0465)

Oracle Linux 3 : pcre (ELSA-2007-1063)

Oracle Linux 3 : php (ELSA-2007-0889)

Oracle Linux 3 : pidgin (ELSA-2009-1059)

Oracle Linux 3 : pidgin (ELSA-2009-1535)

Oracle Linux 3 : postgresql (ELSA-2008-0039)

Oracle Linux 3 : postgresql (ELSA-2009-1485)

Oracle Linux 3 : postgresql (ELSA-2010-0427)

Oracle Linux 3 : python (ELSA-2009-1178)

Oracle Linux 3 : rdesktop (ELSA-2008-0576)

Oracle Linux 3 : ruby (ELSA-2006-0729)

Oracle Linux 3 : ruby (ELSA-2008-0562)

Oracle Linux 3 : ruby (ELSA-2008-0896)

Oracle Linux 3 : samba (ELSA-2007-1013)

Oracle Linux 3 : samba (ELSA-2009-1528)

Oracle Linux 3 : seamonkey (ELSA-2007-1084)

Oracle Linux 3 : seamonkey (ELSA-2009-1185)

Oracle Linux 3 : seamonkey (ELSA-2009-1432)

Oracle Linux 3 : shadow-utils (ELSA-2007-0431)

Oracle Linux 3 : tar (ELSA-2010-0142)

Oracle Linux 3 : tcltk (ELSA-2008-0134)

Oracle Linux 3 : tetex (ELSA-2007-1028)

Oracle Linux 3 : tetex (ELSA-2010-0401)

Oracle Linux 3 : unzip (ELSA-2008-0196)

Oracle Linux 3 : vsftpd (ELSA-2008-0579)

Oracle Linux 3 : wireshark (ELSA-2008-0059)

Oracle Linux 3 : XFree86 (ELSA-2007-0002)

Oracle Linux 3 : XFree86 (ELSA-2007-0125)

Oracle Linux 3 : XFree86 (ELSA-2008-0029)

Oracle Linux 3 : XFree86 (ELSA-2008-0502)

Oracle Linux 3 : xpdf (ELSA-2007-1030)

Oracle Linux 3 : xpdf (ELSA-2009-1500)

Oracle Linux 3 : xpdf (ELSA-2010-0750)

Oracle Linux 4 / 5 / 6 : apr (ELSA-2011-0507)

Oracle Linux 4 / 5 / 6 : apr (ELSA-2011-0844)

Oracle Linux 4 / 5 / 6 : apr-util (ELSA-2010-0950)

Oracle Linux 4 / 5 / 6 : curl (ELSA-2011-0918)

Oracle Linux 4 / 5 / 6 : cyrus-imapd (ELSA-2011-0859)

Oracle Linux 4 / 5 / 6 : cyrus-imapd (ELSA-2011-1317)

Oracle Linux 4 / 5 / 6 : cyrus-imapd (ELSA-2011-1508)

Oracle Linux 4 / 5 / 6 : dhcp (ELSA-2011-0428)

Oracle Linux 4 / 5 / 6 : dhcp (ELSA-2011-1160)

Oracle Linux 4 / 5 / 6 : dovecot (ELSA-2011-1187)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2010-0966)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-0310)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-0373)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-0471)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-0885)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-1164)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-1242)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-1268)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-1341)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2011-1437)

Oracle Linux 4 / 5 / 6 : firefox (ELSA-2012-0079)

Oracle Linux 4 / 5 / 6 : freetype (ELSA-2010-0889)

Oracle Linux 4 / 5 / 6 : freetype (ELSA-2011-1402)

Oracle Linux 4 / 5 / 6 : freetype (ELSA-2011-1455)

Oracle Linux 4 / 5 / 6 : httpd (ELSA-2011-1245)

Oracle Linux 4 / 5 / 6 : kdelibs / kdelibs3 (ELSA-2011-1385)

Oracle Linux 4 / 5 / 6 : libpng (ELSA-2012-0317)

Oracle Linux 4 / 5 / 6 : libtiff (ELSA-2011-0318)

Oracle Linux 4 / 5 / 6 : libtiff (ELSA-2011-0392)

Oracle Linux 4 / 5 / 6 : libuser (ELSA-2011-0170)

Oracle Linux 4 / 5 / 6 : libvorbis (ELSA-2012-0136)

Oracle Linux 4 / 5 / 6 : nspr / nss (ELSA-2011-1282)

Oracle Linux 4 / 5 / 6 : nss (ELSA-2011-0472)

Oracle Linux 4 / 5 / 6 : nss (ELSA-2011-1444)

Oracle Linux 4 / 5 / 6 : pango (ELSA-2011-0180)

Oracle Linux 4 / 5 / 6 : php (ELSA-2012-0093)

Oracle Linux 4 / 5 / 6 : postfix (ELSA-2011-0843)

Oracle Linux 4 / 5 / 6 : postgresql (ELSA-2011-0197)

Oracle Linux 4 / 5 / 6 : postgresql (ELSA-2011-1377)

Oracle Linux 4 / 5 / 6 : rpm (ELSA-2011-1349)

Oracle Linux 4 / 5 / 6 : rpm (ELSA-2012-0451)

Oracle Linux 4 / 5 / 6 : samba (ELSA-2011-0305)

Oracle Linux 4 / 5 / 6 : vsftpd (ELSA-2011-0337)

Oracle Linux 4 / 5 / 6 : wireshark (ELSA-2011-0013)

Oracle Linux 4 / 5 : apr / apr-util (ELSA-2009-1204)

Oracle Linux 4 / 5 : apr-util (ELSA-2009-1107)

Oracle Linux 4 / 5 : bluez-libs / bluez-utils (ELSA-2008-0581)

Oracle Linux 4 / 5 : cups (ELSA-2009-0429)

Oracle Linux 4 / 5 : cyrus-imapd (ELSA-2009-1116)

Oracle Linux 4 / 5 : cyrus-imapd (ELSA-2009-1459)

Oracle Linux 4 / 5 : device-mapper-multipath (ELSA-2009-0411)

Oracle Linux 4 / 5 : elinks (ELSA-2007-0933)

Oracle Linux 4 / 5 : elinks (ELSA-2009-1471)

Oracle Linux 4 / 5 : evolution-data-server (ELSA-2009-0354)

Oracle Linux 4 / 5 : exim (ELSA-2010-0970)

Oracle Linux 4 / 5 : exim (ELSA-2011-0153)

Oracle Linux 4 / 5 : file (ELSA-2007-0391)

Oracle Linux 4 / 5 : firefox (ELSA-2007-0400)

Oracle Linux 4 / 5 : firefox (ELSA-2007-0724)

Oracle Linux 4 / 5 : firefox (ELSA-2007-0979)

Oracle Linux 4 / 5 : firefox (ELSA-2007-1082)

Oracle Linux 4 / 5 : firefox (ELSA-2008-0103)

Oracle Linux 4 / 5 : firefox (ELSA-2008-0207)

Oracle Linux 4 / 5 : firefox (ELSA-2008-0222)

Oracle Linux 4 / 5 : firefox (ELSA-2008-1036)

Oracle Linux 4 / 5 : firefox (ELSA-2009-0256)

Oracle Linux 4 / 5 : firefox (ELSA-2009-0315)

Oracle Linux 4 / 5 : firefox (ELSA-2009-0397)

Oracle Linux 4 / 5 : firefox (ELSA-2009-0436)

Oracle Linux 4 / 5 : firefox (ELSA-2009-0449)

Oracle Linux 4 / 5 : firefox (ELSA-2009-1095)

Oracle Linux 4 / 5 : firefox (ELSA-2009-1162)

Oracle Linux 4 / 5 : firefox (ELSA-2009-1430)

Oracle Linux 4 / 5 : firefox (ELSA-2009-1530)

Oracle Linux 4 / 5 : firefox (ELSA-2009-1674)

Oracle Linux 4 / 5 : firefox (ELSA-2010-0112)

Oracle Linux 4 / 5 : firefox (ELSA-2010-0332)

Oracle Linux 4 / 5 : firefox (ELSA-2010-0547)

Oracle Linux 4 / 5 : firefox (ELSA-2010-0681)

Oracle Linux 4 / 5 : firefox (ELSA-2010-0782)

Oracle Linux 4 / 5 : flac (ELSA-2007-0975)

Oracle Linux 4 / 5 : foomatic (ELSA-2011-1109)

Oracle Linux 4 / 5 : freetype (ELSA-2010-0578)

Oracle Linux 4 / 5 : freetype (ELSA-2010-0737)

Oracle Linux 4 / 5 : gd (ELSA-2008-0146)

Oracle Linux 4 / 5 : gd (ELSA-2010-0003)

Oracle Linux 4 / 5 : gnutls (ELSA-2009-1232)

Oracle Linux 4 / 5 : htdig (ELSA-2007-1095)

Oracle Linux 4 / 5 : httpd (ELSA-2011-1392)

Oracle Linux 4 / 5 : kdebase (ELSA-2007-0905)

Oracle Linux 4 / 5 : kdebase (ELSA-2010-0348)

Oracle Linux 4 / 5 : kdelibs (ELSA-2007-0909)

Oracle Linux 4 / 5 : kdelibs (ELSA-2009-1127)

Oracle Linux 4 / 5 : kdelibs (ELSA-2009-1601)

Oracle Linux 4 / 5 : krb5 (ELSA-2007-0562)

Oracle Linux 4 / 5 : krb5 (ELSA-2010-0926)

Oracle Linux 4 / 5 : krb5 (ELSA-2011-1851)

Oracle Linux 4 / 5 : libexif (ELSA-2007-0501)

Oracle Linux 4 / 5 : libpng (ELSA-2009-0333)

Oracle Linux 4 / 5 : libsoup (ELSA-2009-0344)

Oracle Linux 4 / 5 : libtiff (ELSA-2010-0519)

Oracle Linux 4 / 5 : libwmf (ELSA-2009-0457)

Oracle Linux 4 / 5 : libxslt (ELSA-2008-0649)

Oracle Linux 4 / 5 : mailman (ELSA-2011-0307)

Oracle Linux 4 / 5 : mysql (ELSA-2007-0875)

Oracle Linux 4 / 5 : mysql (ELSA-2007-1155)

Oracle Linux 4 / 5 : neon (ELSA-2009-1452)

Oracle Linux 4 / 5 : netpbm (ELSA-2009-0012)

Oracle Linux 4 / 5 : netpbm (ELSA-2011-1811)

Oracle Linux 4 / 5 : nspr / nss (ELSA-2009-1184)

Oracle Linux 4 / 5 : nss (ELSA-2010-0165)

Oracle Linux 4 / 5 : ntp (ELSA-2009-0046)

Oracle Linux 4 / 5 : ntp (ELSA-2009-1648)

Oracle Linux 4 / 5 : openldap (ELSA-2008-0110)

Oracle Linux 4 / 5 : openldap (ELSA-2008-0583)

Oracle Linux 4 / 5 : openssh (ELSA-2008-0855)

Oracle Linux 4 / 5 : oracle-validated (ELSA-2011-2031)

Oracle Linux 4 / 5 : perl (ELSA-2011-1797)

Oracle Linux 4 / 5 : perl-Archive-Tar (ELSA-2010-0505)

Oracle Linux 4 / 5 : php (ELSA-2007-0890)

Oracle Linux 4 / 5 : php (ELSA-2010-0919)

Oracle Linux 4 / 5 : postfix (ELSA-2011-0422)

Oracle Linux 4 / 5 : postgresql (ELSA-2008-0038)

Oracle Linux 4 / 5 : postgresql (ELSA-2009-1484)

Oracle Linux 4 / 5 : postgresql / postgresql84 (ELSA-2010-0742)

Oracle Linux 4 / 5 : PyXML (ELSA-2010-0002)

Oracle Linux 4 / 5 : quagga (ELSA-2010-0785)

Oracle Linux 4 / 5 : ruby (ELSA-2008-0561)

Oracle Linux 4 / 5 : ruby (ELSA-2008-0897)

Oracle Linux 4 / 5 : ruby (ELSA-2008-0981)

Oracle Linux 4 / 5 : ruby (ELSA-2009-1140)

Oracle Linux 4 / 5 : ruby (ELSA-2012-0070)

Oracle Linux 4 / 5 : samba (ELSA-2009-1529)

Oracle Linux 4 / 5 : samba (ELSA-2011-1219)

Oracle Linux 4 / 5 : samba (ELSA-2012-0332)

Oracle Linux 4 / 5 : sblim (ELSA-2008-0497)

Oracle Linux 4 / 5 : spamassassin (ELSA-2007-0492)

Oracle Linux 4 / 5 : speex (ELSA-2008-0235)

Oracle Linux 4 / 5 : squirrelmail (ELSA-2012-0103)

Oracle Linux 4 / 5 : subversion (ELSA-2009-1203)

Oracle Linux 4 / 5 : system-config-printer (ELSA-2011-1196)

Oracle Linux 4 / 5 : systemtap (ELSA-2009-0373)

Oracle Linux 4 / 5 : tar (ELSA-2007-0860)

Oracle Linux 4 / 5 : tar (ELSA-2010-0141)

Oracle Linux 4 / 5 : tog-pegasus (ELSA-2008-0002)

Oracle Linux 4 / 5 : wireshark (ELSA-2008-0058)

Oracle Linux 4 / 5 : wireshark (ELSA-2011-0370)

Oracle Linux 4 / 5 : xmlsec1 (ELSA-2009-1428)

Oracle Linux 4 / 5 : xmlsec1 (ELSA-2011-0486)

Oracle Linux 4 / 6 : thunderbird (ELSA-2011-0374)

Oracle Linux 4 / 6 : thunderbird (ELSA-2011-1243)

Oracle Linux 4 / 6 : thunderbird (ELSA-2011-1267)

Oracle Linux 4 : autofs5 (ELSA-2007-1129)

Oracle Linux 4 : autofs5 (ELSA-2007-1177)

Oracle Linux 4 : bash (ELSA-2011-0261)

Oracle Linux 4 : bash (ELSA-2014-1294) (Shellshock)

Oracle Linux 4 : bash (ELSA-2014-3078)

Oracle Linux 4 : bash (ELSA-2014-3079)

Oracle Linux 4 : bind (ELSA-2009-1180)

Oracle Linux 4 : bind (ELSA-2010-1000)

Oracle Linux 4 : bind (ELSA-2011-1496)

Oracle Linux 4 : bind (ELSA-2012-1365)

Oracle Linux 4 : bind (ELSA-2012-2028)

Oracle Linux 4 : bluez-utils (ELSA-2007-0065)

Oracle Linux 4 : busybox (ELSA-2007-0244)

Oracle Linux 4 : cpio (ELSA-2007-0245)

Oracle Linux 4 : cpio (ELSA-2010-0143)

Oracle Linux 4 : cups (ELSA-2007-1022)

Oracle Linux 4 : cups (ELSA-2008-0161)

Oracle Linux 4 : cups (ELSA-2010-0755)

Oracle Linux 4 : cyrus-sasl (ELSA-2007-0795)

Oracle Linux 4 : dbus (ELSA-2007-0008)

Oracle Linux 4 : dhcp (ELSA-2009-1136)

Oracle Linux 4 : elinks (ELSA-2006-0742)

Oracle Linux 4 : evolution (ELSA-2008-0177)

Oracle Linux 4 : evolution / evolution-data-server (ELSA-2009-0355)

Oracle Linux 4 : evolution28 (ELSA-2008-0515)

Oracle Linux 4 : evolution28-pango (ELSA-2011-1325)

Oracle Linux 4 : file (ELSA-2007-0124)

Oracle Linux 4 : firefox (ELSA-2006-0733 / ELSA-2006-0675 / ELSA-2006-0610)

Oracle Linux 4 : firefox (ELSA-2006-0758)

Oracle Linux 4 : Firefox (ELSA-2007-0079)

Oracle Linux 4 : firefox (ELSA-2008-0549)

Oracle Linux 4 : firefox (ELSA-2008-0598)

Oracle Linux 4 : firefox (ELSA-2010-0500)

Oracle Linux 4 : firefox (ELSA-2010-0558)

Oracle Linux 4 : firefox (ELSA-2010-0808)

Oracle Linux 4 : firefox (ELSA-2012-0142)

Oracle Linux 4 : freetype (ELSA-2011-1161)

Oracle Linux 4 : frysk (ELSA-2011-1327)

Oracle Linux 4 : gcc (ELSA-2007-0220)

Oracle Linux 4 : gdb (ELSA-2007-0229)

Oracle Linux 4 : gdm (ELSA-2007-0286)

Oracle Linux 4 : gdm (ELSA-2010-0657)

Oracle Linux 4 : ghostscript (ELSA-2012-0096)

Oracle Linux 4 : gimp (ELSA-2011-0837)

Oracle Linux 4 : glibc (ELSA-2012-0125)

Oracle Linux 4 : glibc (ELSA-2015-0101) (GHOST)

Oracle Linux 4 : gnupg (ELSA-2006-0615)

Oracle Linux 4 : gnupg (ELSA-2006-0754)

Oracle Linux 4 : gnutls (ELSA-2006-0680)

Oracle Linux 4 : gnutls (ELSA-2008-0492)

Oracle Linux 4 : gnutls (ELSA-2010-0167)

Oracle Linux 4 : gpdf (ELSA-2007-0730)

Oracle Linux 4 : gpdf (ELSA-2007-1025)

Oracle Linux 4 : gpdf (ELSA-2008-0262)

Oracle Linux 4 : gpdf (ELSA-2009-0458)

Oracle Linux 4 : gpdf (ELSA-2009-1503)

Oracle Linux 4 : gpdf (ELSA-2009-1681)

Oracle Linux 4 : gpdf (ELSA-2010-0752)

Oracle Linux 4 : gstreamer-plugins (ELSA-2009-0270)

Oracle Linux 4 : gstreamer-plugins (ELSA-2011-0477)

Oracle Linux 4 : gstreamer-plugins (ELSA-2011-1264)

Oracle Linux 4 : gtk2 (ELSA-2007-0019)

Oracle Linux 4 : HelixPlayer (ELSA-2007-0605)

Oracle Linux 4 : HelixPlayer (ELSA-2010-0094)

Oracle Linux 4 : HelixPlayer removal (ELSA-2010-0981)

Oracle Linux 4 : httpd (ELSA-2007-0534)

Oracle Linux 4 : httpd (ELSA-2008-0006)

Oracle Linux 4 : httpd (ELSA-2009-1580)

Oracle Linux 4 : httpd (ELSA-2010-0175)

Oracle Linux 4 : ImageMagick (ELSA-2006-0633)

Oracle Linux 4 : ImageMagick (ELSA-2010-0653)

Oracle Linux 4 : kdegraphics (ELSA-2007-0729)

Oracle Linux 4 : kdegraphics (ELSA-2007-1024)

Oracle Linux 4 : kdegraphics (ELSA-2008-0238)

Oracle Linux 4 : kdegraphics (ELSA-2009-0431)

Oracle Linux 4 : kdegraphics (ELSA-2009-1512)

Oracle Linux 4 : kdegraphics (ELSA-2009-1682)

Oracle Linux 4 : kdegraphics (ELSA-2010-0753)

Oracle Linux 4 : kernel (ELSA-2006-0617 / ELSA-2006-0689)

Oracle Linux 4 : kernel (ELSA-2007-0014)

Oracle Linux 4 : kernel (ELSA-2007-0085)

Oracle Linux 4 : kernel (ELSA-2007-0488)

Oracle Linux 4 : kernel (ELSA-2007-0774)

Oracle Linux 4 : kernel (ELSA-2007-0937)

Oracle Linux 4 : kernel (ELSA-2007-0939)

Oracle Linux 4 : kernel (ELSA-2007-1104)

Oracle Linux 4 : kernel (ELSA-2008-0055)

Oracle Linux 4 : kernel (ELSA-2008-0167)

Oracle Linux 4 : kernel (ELSA-2008-0237)

Oracle Linux 4 : kernel (ELSA-2008-0508)

Oracle Linux 4 : kernel (ELSA-2008-0607)

Oracle Linux 4 : kernel (ELSA-2008-0972)

Oracle Linux 4 : kernel (ELSA-2009-0014)

Oracle Linux 4 : kernel (ELSA-2009-0331)

Oracle Linux 4 : kernel (ELSA-2009-0459)

Oracle Linux 4 : kernel (ELSA-2009-1132)

Oracle Linux 4 : kernel (ELSA-2009-1211)

Oracle Linux 4 : kernel (ELSA-2009-1223)

Oracle Linux 4 : kernel (ELSA-2009-1438)

Oracle Linux 4 : kernel (ELSA-2009-1522)

Oracle Linux 4 : kernel (ELSA-2009-1541)

Oracle Linux 4 : kernel (ELSA-2009-1671)

Oracle Linux 4 : kernel (ELSA-2010-0020)

Oracle Linux 4 : kernel (ELSA-2010-0076)

Oracle Linux 4 : kernel (ELSA-2010-0146)

Oracle Linux 4 : kernel (ELSA-2010-0394)

Oracle Linux 4 : kernel (ELSA-2010-0474)

Oracle Linux 4 : kernel (ELSA-2010-0606)

Oracle Linux 4 : kernel (ELSA-2010-0676)

Oracle Linux 4 : kernel (ELSA-2010-0718)

Oracle Linux 4 : kernel (ELSA-2010-0779)

Oracle Linux 4 : kernel (ELSA-2010-0936)

Oracle Linux 4 : kernel (ELSA-2011-0162)

Oracle Linux 4 : kernel (ELSA-2011-0263)

Oracle Linux 4 : krb5 (ELSA-2008-0180)

Oracle Linux 4 : krb5 (ELSA-2009-0409)

Oracle Linux 4 : libexif (ELSA-2007-1166)

Oracle Linux 4 : libgtop2 (ELSA-2007-0765)

Oracle Linux 4 : libpng (ELSA-2011-1103)

Oracle Linux 4 : libtiff (ELSA-2008-0848)

Oracle Linux 4 : libxml2 (ELSA-2012-0016)

Oracle Linux 4 : mod\_auth\_kerb (ELSA-2006-0746)

Oracle Linux 4 : mysql (ELSA-2007-0152)

Oracle Linux 4 : mysql (ELSA-2010-0110)

Oracle Linux 4 : mysql (ELSA-2010-0824)

Oracle Linux 4 : NetworkManager (ELSA-2009-0362)

Oracle Linux 4 : nfs-utils-lib (ELSA-2007-0913)

Oracle Linux 4 : nss (ELSA-2008-2011)

Oracle Linux 4 : nss\_ldap (ELSA-2006-0719)

Oracle Linux 4 : ntp (ELSA-2009-1040)

Oracle Linux 4 : openldap (ELSA-2007-0310)

Oracle Linux 4 : openldap (ELSA-2010-0543)

Oracle Linux 4 : openoffice.org (ELSA-2007-0001)

Oracle Linux 4 : openoffice.org (ELSA-2011-0181)

Oracle Linux 4 : openssh (ELSA-2006-0697)

Oracle Linux 4 : openssh (ELSA-2007-0257)

Oracle Linux 4 : openssl (ELSA-2006-0695 / ELSA-2006-0661)

Oracle Linux 4 : openssl (ELSA-2010-0977)

Oracle Linux 4 : openssl (ELSA-2012-0086)

Oracle Linux 4 : openssl (ELSA-2012-2011)

Oracle Linux 4 : openssl (ELSA-2014-3040)

Oracle Linux 4 : pcre (ELSA-2007-0968)

Oracle Linux 4 : pcre (ELSA-2007-1052)

Oracle Linux 4 : pcre (ELSA-2007-1068)

Oracle Linux 4 : perl-Net-DNS (ELSA-2007-0675)

Oracle Linux 4 : php (ELSA-2006-0730 / ELSA-2006-0669)

Oracle Linux 4 : php (ELSA-2007-0349)

Oracle Linux 4 : php (ELSA-2008-0545)

Oracle Linux 4 : php (ELSA-2012-0071)

Oracle Linux 4 : php (ELSA-2013-1063)

Oracle Linux 4 : pidgin (ELSA-2008-1023)

Oracle Linux 4 : pidgin (ELSA-2009-1060)

Oracle Linux 4 : pidgin (ELSA-2009-1139)

Oracle Linux 4 : pidgin (ELSA-2009-1453)

Oracle Linux 4 : pidgin (ELSA-2009-1536)

Oracle Linux 4 : pidgin (ELSA-2010-0044)

Oracle Linux 4 : pidgin (ELSA-2010-0115)

Oracle Linux 4 : pidgin (ELSA-2010-0788)

Oracle Linux 4 : pidgin (ELSA-2011-1371)

Oracle Linux 4 : pidgin (ELSA-2011-1820)

Oracle Linux 4 : postgresql (ELSA-2010-0428)

Oracle Linux 4 : python (ELSA-2009-1177)

Oracle Linux 4 : python (ELSA-2011-0260)

Oracle Linux 4 : python (ELSA-2011-0491)

Oracle Linux 4 : rpm (ELSA-2010-0678)

Oracle Linux 4 : ruby (ELSA-2007-0961)

Oracle Linux 4 : ruby (ELSA-2011-0908)

Oracle Linux 4 : samba (ELSA-2007-1016)

Oracle Linux 4 : samba (ELSA-2012-0478)

Oracle Linux 4 : seamonkey (ELSA-2006-0734 / ELSA-2006-0676)

Oracle Linux 4 : seamonkey (ELSA-2006-0759)

Oracle Linux 4 : seamonkey (ELSA-2007-0077-2)

Oracle Linux 4 : seamonkey (ELSA-2009-1431)

Oracle Linux 4 : seamonkey (ELSA-2010-0967)

Oracle Linux 4 : seamonkey (ELSA-2011-0313)

Oracle Linux 4 : seamonkey (ELSA-2011-0375)

Oracle Linux 4 : seamonkey (ELSA-2011-0473)

Oracle Linux 4 : seamonkey (ELSA-2011-0888)

Oracle Linux 4 : seamonkey (ELSA-2011-1167)

Oracle Linux 4 : seamonkey (ELSA-2011-1244)

Oracle Linux 4 : seamonkey (ELSA-2011-1266)

Oracle Linux 4 : seamonkey (ELSA-2011-1344)

Oracle Linux 4 : seamonkey (ELSA-2011-1440)

Oracle Linux 4 : seamonkey (ELSA-2012-0084)

Oracle Linux 4 : seamonkey (ELSA-2012-0141)

Oracle Linux 4 : sendmail (ELSA-2007-0252)

Oracle Linux 4 : sendmail (ELSA-2011-0262)

Oracle Linux 4 : shadow-utils (ELSA-2007-0276)

Oracle Linux 4 : spamassassin (ELSA-2007-0074)

Oracle Linux 4 : squirrelmail (ELSA-2006-0668)

Oracle Linux 4 : subversion (ELSA-2011-0861)

Oracle Linux 4 : systemtap (ELSA-2010-0125)

Oracle Linux 4 : systemtap (ELSA-2010-0895)

Oracle Linux 4 : tetex (ELSA-2007-1027)

Oracle Linux 4 : tetex (ELSA-2010-0399)

Oracle Linux 4 : thunderbird (ELSA-2006-0735 / ELSA-2006-0677 / ELBA-2006-0624 / ELSA-2006-0611)

Oracle Linux 4 : thunderbird (ELSA-2006-0760)

Oracle Linux 4 : thunderbird (ELSA-2007-0078)

Oracle Linux 4 : thunderbird (ELSA-2007-0401)

Oracle Linux 4 : thunderbird (ELSA-2007-0723)

Oracle Linux 4 : thunderbird (ELSA-2007-0981)

Oracle Linux 4 : thunderbird (ELSA-2007-1083)

Oracle Linux 4 : thunderbird (ELSA-2008-0105)

Oracle Linux 4 : thunderbird (ELSA-2008-0209)

Oracle Linux 4 : thunderbird (ELSA-2008-0224)

Oracle Linux 4 : thunderbird (ELSA-2008-0616)

Oracle Linux 4 : thunderbird (ELSA-2008-0908)

Oracle Linux 4 : thunderbird (ELSA-2008-0976)

Oracle Linux 4 : thunderbird (ELSA-2009-0002)

Oracle Linux 4 : thunderbird (ELSA-2009-0258)

Oracle Linux 4 : thunderbird (ELSA-2009-1125)

Oracle Linux 4 : thunderbird (ELSA-2010-0154)

Oracle Linux 4 : thunderbird (ELSA-2010-0544)

Oracle Linux 4 : thunderbird (ELSA-2010-0682)

Oracle Linux 4 : thunderbird (ELSA-2010-0780)

Oracle Linux 4 : thunderbird (ELSA-2010-0812)

Oracle Linux 4 : thunderbird (ELSA-2010-0968)

Oracle Linux 4 : thunderbird (ELSA-2011-0312)

Oracle Linux 4 : thunderbird (ELSA-2011-0474)

Oracle Linux 4 : thunderbird (ELSA-2011-0887)

Oracle Linux 4 : thunderbird (ELSA-2011-1165)

Oracle Linux 4 : thunderbird (ELSA-2011-1343)

Oracle Linux 4 : thunderbird (ELSA-2011-1438)

Oracle Linux 4 : thunderbird (ELSA-2012-0085)

Oracle Linux 4 : tk (ELSA-2008-0135)

Oracle Linux 4 : unzip (ELSA-2007-0203)

Oracle Linux 4 : util-linux (ELSA-2007-0235)

Oracle Linux 4 : w3c-libwww (ELSA-2007-0208)

Oracle Linux 4 : wireshark (ELSA-2006-0726 / ELSA-2006-0658 / ELSA-2006-0602)

Oracle Linux 4 : xorg-x11 (ELSA-2006-0665)

Oracle Linux 4 : xorg-x11 (ELSA-2007-0003)

Oracle Linux 4 : xorg-x11 (ELSA-2007-0126)

Oracle Linux 4 : xorg-x11 (ELSA-2007-0519)

Oracle Linux 4 : xorg-x11 (ELSA-2007-0898)

Oracle Linux 4 : xorg-x11 (ELSA-2008-0030)

Oracle Linux 4 : xorg-x11 (ELSA-2008-0503)

Oracle Linux 4 : xorg-x11 (ELSA-2011-0432)

Oracle Linux 4 : xorg-x11 (ELSA-2011-1155)

Oracle Linux 4 : xorg-x11 (ELSA-2011-1360)

Oracle Linux 4 : xpdf (ELSA-2007-1029)

Oracle Linux 4 : xpdf (ELSA-2008-0240)

Oracle Linux 4 : xpdf (ELSA-2009-1501)

Oracle Linux 4 : xpdf (ELSA-2009-1680)

Oracle Linux 4 : xpdf (ELSA-2010-0751)

Oracle Linux 5 / 6 / 7 : bash (ELSA-2014-1293) (Shellshock)

Oracle Linux 5 / 6 / 7 : bash (ELSA-2014-1306)

Oracle Linux 5 / 6 / 7 : bind (ELSA-2014-1984)

Oracle Linux 5 / 6 / 7 : bind (ELSA-2016-0073)

Oracle Linux 5 / 6 / 7 : bind (ELSA-2016-0459)

Oracle Linux 5 / 6 / 7 : bind (ELSA-2016-1944)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2014-0741)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2014-0919)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2014-1144)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2014-1635)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2014-1919)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-0046)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-0265)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-0718)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-0766)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-0988)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-1207)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-1581)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-1586)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-1693)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-1834)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-1982)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2015-2657)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-0071)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-0197)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-0373)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-0695)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-1217)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-1551)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-1912)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-2780)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-2843)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2016-2946)

Oracle Linux 5 / 6 / 7 : firefox (ELSA-2017-0190)

Oracle Linux 5 / 6 / 7 : glibc (ELSA-2014-1110)

Oracle Linux 5 / 6 / 7 : jakarta-commons-httpclient (ELSA-2014-1166)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2014-0907)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2014-1634)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2015-0085) (POODLE)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2015-0808)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2015-1526) (Bar Mitzvah) (Logjam)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2015-2086)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2016-0067)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2016-0723)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2016-1776)

Oracle Linux 5 / 6 / 7 : java-1.6.0-openjdk (ELSA-2017-0061)

Oracle Linux 5 / 6 / 7 : java-1.7.0-openjdk (ELSA-2016-1504)

Oracle Linux 5 / 6 / 7 : java-1.7.0-openjdk (ELSA-2016-2658)

Oracle Linux 5 / 6 / 7 : java-1.7.0-openjdk (ELSA-2017-0269)

Oracle Linux 5 / 6 / 7 : nss (ELSA-2014-1307)

Oracle Linux 5 / 6 / 7 : nss / nss-softokn / nss-util (ELSA-2014-1948) (POODLE)

Oracle Linux 5 / 6 / 7 : nss / nss-util (ELSA-2016-2779)

Oracle Linux 5 / 6 / 7 : openldap (ELSA-2015-1840)

Oracle Linux 5 / 6 / 7 : procmail (ELSA-2014-1172)

Oracle Linux 5 / 6 / 7 : setroubleshoot (ELSA-2015-0729)

Oracle Linux 5 / 6 : axis (ELSA-2014-1193)

Oracle Linux 5 / 6 : bind (ELSA-2011-0845)

Oracle Linux 5 / 6 : bind (ELSA-2011-0926)

Oracle Linux 5 / 6 : bind (ELSA-2011-1458)

Oracle Linux 5 / 6 : bind (ELSA-2012-0716)

Oracle Linux 5 / 6 : bind (ELSA-2012-1123)

Oracle Linux 5 / 6 : bind (ELSA-2012-1363)

Oracle Linux 5 / 6 : bind (ELSA-2016-2093)

Oracle Linux 5 / 6 : bind (ELSA-2016-2141)

Oracle Linux 5 / 6 : bind (ELSA-2017-0063)

Oracle Linux 5 / 6 : boost (ELSA-2013-0668)

Oracle Linux 5 / 6 : cups (ELSA-2013-0580)

Oracle Linux 5 / 6 : curl (ELSA-2013-0771)

Oracle Linux 5 / 6 : curl (ELSA-2013-0983)

Oracle Linux 5 / 6 : cvs (ELSA-2012-0321)

Oracle Linux 5 / 6 : dbus (ELSA-2011-0376)

Oracle Linux 5 / 6 : dbus (ELSA-2011-1132)

Oracle Linux 5 / 6 : dbus-glib (ELSA-2013-0568)

Oracle Linux 5 / 6 : ecryptfs-utils (ELSA-2011-1241)

Oracle Linux 5 / 6 : elinks (ELSA-2013-0250)

Oracle Linux 5 / 6 : expat (ELSA-2012-0731)

Oracle Linux 5 / 6 : firefox (ELSA-2012-0387)

Oracle Linux 5 / 6 : firefox (ELSA-2012-0515)

Oracle Linux 5 / 6 : firefox (ELSA-2012-0710)

Oracle Linux 5 / 6 : firefox (ELSA-2012-1088)

Oracle Linux 5 / 6 : firefox (ELSA-2012-1210)

Oracle Linux 5 / 6 : firefox (ELSA-2012-1350)

Oracle Linux 5 / 6 : firefox (ELSA-2012-1407)

Oracle Linux 5 / 6 : firefox (ELSA-2012-1482)

Oracle Linux 5 / 6 : firefox (ELSA-2013-0144)

Oracle Linux 5 / 6 : firefox (ELSA-2013-0271)

Oracle Linux 5 / 6 : firefox (ELSA-2013-0696)

Oracle Linux 5 / 6 : firefox (ELSA-2013-0820)

Oracle Linux 5 / 6 : firefox (ELSA-2013-0981)

Oracle Linux 5 / 6 : firefox (ELSA-2013-1140)

Oracle Linux 5 / 6 : firefox (ELSA-2013-1268)

Oracle Linux 5 / 6 : firefox (ELSA-2013-1476)

Oracle Linux 5 / 6 : firefox (ELSA-2013-1812)

Oracle Linux 5 / 6 : firefox (ELSA-2014-0132)

Oracle Linux 5 / 6 : firefox (ELSA-2014-0310)

Oracle Linux 5 / 6 : firefox (ELSA-2014-0448)

Oracle Linux 5 / 6 : firefox (ELSA-2017-0459)

Oracle Linux 5 / 6 : freetype (ELSA-2012-0467)

Oracle Linux 5 / 6 : freetype (ELSA-2013-0216)

Oracle Linux 5 / 6 : ghostscript (ELSA-2012-0095)

Oracle Linux 5 / 6 : ghostscript (ELSA-2012-1256)

Oracle Linux 5 / 6 : gimp (ELSA-2013-1778)

Oracle Linux 5 / 6 : gnupg2 (ELSA-2013-1459)

Oracle Linux 5 / 6 : gnutls (ELSA-2013-0588)

Oracle Linux 5 / 6 : gnutls (ELSA-2013-0883)

Oracle Linux 5 / 6 : hplip (ELSA-2011-0154)

Oracle Linux 5 / 6 : httpd (ELSA-2013-0815)

Oracle Linux 5 / 6 : httpd (ELSA-2013-1156)

Oracle Linux 5 / 6 : httpd (ELSA-2014-0920)

Oracle Linux 5 / 6 : httpd (ELSA-2016-1421) (httpoxy)

Oracle Linux 5 / 6 : icu (ELSA-2011-1815)

Oracle Linux 5 / 6 : jakarta-commons-httpclient (ELSA-2013-0270)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2011-0214)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2011-0281)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2011-1380) (BEAST)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2013-0770)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2013-1014)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2013-1505)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2014-0097)

Oracle Linux 5 / 6 : java-1.6.0-openjdk (ELSA-2014-0408)

Oracle Linux 5 / 6 : java-1.7.0-openjdk (ELSA-2013-0165)

Oracle Linux 5 / 6 : java-1.7.0-openjdk (ELSA-2013-0247)

Oracle Linux 5 / 6 : java-1.7.0-openjdk (ELSA-2013-0275)

Oracle Linux 5 / 6 : krb5 (ELSA-2013-0942)

Oracle Linux 5 / 6 : libexif (ELSA-2012-1255)

Oracle Linux 5 / 6 : libgcrypt (ELSA-2013-1457)

Oracle Linux 5 / 6 : libpng (ELSA-2012-0407)

Oracle Linux 5 / 6 : libpng (ELSA-2012-0523)

Oracle Linux 5 / 6 : libtiff (ELSA-2012-0468)

Oracle Linux 5 / 6 : libtiff (ELSA-2012-1054)

Oracle Linux 5 / 6 : libtiff (ELSA-2012-1590)

Oracle Linux 5 / 6 : libvirt (ELSA-2011-0391)

Oracle Linux 5 / 6 : libXfont (ELSA-2011-1154)

Oracle Linux 5 / 6 : libxfont (ELSA-2014-0018)

Oracle Linux 5 / 6 : libxml2 (ELSA-2012-0324)

Oracle Linux 5 / 6 : libxml2 (ELSA-2012-1288)

Oracle Linux 5 / 6 : libxml2 (ELSA-2012-1512)

Oracle Linux 5 / 6 : libxml2 (ELSA-2013-0581)

Oracle Linux 5 / 6 : libxslt (ELSA-2012-1265)

Oracle Linux 5 / 6 : logwatch (ELSA-2011-0324)

Oracle Linux 5 / 6 : mod\_nss (ELSA-2013-1779)

Oracle Linux 5 / 6 : nss (ELSA-2013-1861)

Oracle Linux 5 / 6 : openssl (ELSA-2012-0426)

Oracle Linux 5 / 6 : openssl (ELSA-2012-0518)

Oracle Linux 5 / 6 : openssl (ELSA-2012-0699)

Oracle Linux 5 / 6 : openssl (ELSA-2013-0587)

Oracle Linux 5 / 6 : openssl097a / openssl098e (ELSA-2014-0626)

Oracle Linux 5 / 6 : openswan (ELSA-2011-1422)

Oracle Linux 5 / 6 : openswan (ELSA-2013-0827)

Oracle Linux 5 / 6 : openswan (ELSA-2014-0185)

Oracle Linux 5 / 6 : perl (ELSA-2013-0685)

Oracle Linux 5 / 6 : perl-DBD-Pg (ELSA-2012-1116)

Oracle Linux 5 / 6 : php (ELSA-2012-0546)

Oracle Linux 5 / 6 : php (ELSA-2013-1049)

Oracle Linux 5 / 6 : php / php53 (ELSA-2011-1423)

Oracle Linux 5 / 6 : php / php53 (ELSA-2012-0019)

Oracle Linux 5 / 6 : php / php53 (ELSA-2013-1813)

Oracle Linux 5 / 6 : php / php53 (ELSA-2014-1012)

Oracle Linux 5 / 6 : php / php53 (ELSA-2014-1326)

Oracle Linux 5 / 6 : postgresql / postgresql84 (ELSA-2012-0678)

Oracle Linux 5 / 6 : postgresql / postgresql84 (ELSA-2012-1037)

Oracle Linux 5 / 6 : postgresql / postgresql84 (ELSA-2012-1263)

Oracle Linux 5 / 6 : postgresql / postgresql84 (ELSA-2013-1475)

Oracle Linux 5 / 6 : postgresql / postgresql84 (ELSA-2014-0211)

Oracle Linux 5 / 6 : rdesktop (ELSA-2011-0506)

Oracle Linux 5 / 6 : rpm (ELSA-2014-1974)

Oracle Linux 5 / 6 : rsyslog / rsyslog5 (ELSA-2014-1671)

Oracle Linux 5 / 6 : ruby (ELSA-2013-1090)

Oracle Linux 5 / 6 : samba (ELSA-2012-0465)

Oracle Linux 5 / 6 : samba / samba3x (ELSA-2012-0533)

Oracle Linux 5 / 6 : samba / samba3x (ELSA-2013-1806)

Oracle Linux 5 / 6 : samba / samba3x (ELSA-2014-0330)

Oracle Linux 5 / 6 : samba / samba3x (ELSA-2014-0866)

Oracle Linux 5 / 6 : scsi-target-utils (ELSA-2011-0332)

Oracle Linux 5 / 6 : squid (ELSA-2014-1148)

Oracle Linux 5 / 6 : subversion (ELSA-2011-0862)

Oracle Linux 5 / 6 : subversion (ELSA-2013-0737)

Oracle Linux 5 / 6 : subversion (ELSA-2014-0255)

Oracle Linux 5 / 6 : sudo (ELSA-2012-1081)

Oracle Linux 5 / 6 : systemtap (ELSA-2010-0894)

Oracle Linux 5 / 6 : systemtap (ELSA-2012-0376)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2010)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2014)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2015)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2016)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2019)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2021)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2025)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2029)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2033)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2037)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2011-2038)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2001)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2003)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2007)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2008)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2013)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2014)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2020)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2021)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2022)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2025)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2026)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2034)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2035)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2038)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2039)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2040)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2041)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2043)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2044)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2047)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2012-2048)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2503)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2504)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2507)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2511)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2512)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2513)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2519)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2520)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2523)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2524)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2525)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2534)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2537)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2538)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2542)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2013-2543)

Oracle Linux 5 / 6 : Unbreakable Enterprise Kernel (ELSA-2013-2546)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2013-2575)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2013-2576)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2013-2584)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2013-2585)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2013-2588)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2013-2589)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3009)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3010)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3015)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3016)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3019)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3022)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3023)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3038)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3039)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2014-3042)

Oracle Linux 5 / 6 : unbreakable enterprise kernel (ELSA-2014-3043)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3047)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3048)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3053)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3054)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3068)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3069)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3073)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3074)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3082)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3083)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3085)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3086)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3088)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3089)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3104)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3105)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3107)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2014-3108)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3004)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3005)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3014)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3015)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3020)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3021)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3033)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3034)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3036)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3042)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3043)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3046)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3047)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3049)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3050)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3054)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3055)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3067)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3068)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3072)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3073)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3093)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2015-3094)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3502)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3503)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3552)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3553)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3566)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3567)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3572)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3579)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3589)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3592)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3618)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3624)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3634) (Dirty COW)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3646)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3652)

Oracle Linux 5 / 6 : Unbreakable Enterprise kernel (ELSA-2016-3657)

Oracle Linux 5 / 6 : vino (ELSA-2013-1452)

Oracle Linux 5 / 6 : xalan-j2 (ELSA-2014-0348)

Oracle Linux 5 / 6 : xinetd (ELSA-2013-1409)

Oracle Linux 5 / 6 : xorg-x11-server (ELSA-2011-1359)

Oracle Linux 5 / 6 : xorg-x11-server (ELSA-2013-1426)

Oracle Linux 5 / 6 : xorg-x11-server (ELSA-2013-1868)

Oracle Linux 5 / 6 : xorg-x11-server-utils (ELSA-2011-0433)

Oracle Linux 5 / 6 : xulrunner (ELSA-2012-0143)

Oracle Linux 5 / 6 : xulrunner (ELSA-2012-1361)

Oracle Linux 5 / 6 : xulrunner (ELSA-2013-0614)

Oracle Linux 5 / 7 : java-1.7.0-openjdk (ELSA-2016-0054) (SLOTH)

Oracle Linux 5 / 7 : java-1.7.0-openjdk (ELSA-2016-0512)

Oracle Linux 5 / 7 : java-1.7.0-openjdk (ELSA-2016-0676)

Oracle Linux 5 / 7 : nspr / nss (ELSA-2014-0916)

Oracle Linux 5 : acpid (ELSA-2009-1642)

Oracle Linux 5 : aide (ELSA-2007-0539)

Oracle Linux 5 : autofs (ELSA-2007-1128)

Oracle Linux 5 : autofs (ELSA-2007-1176)

Oracle Linux 5 : autofs (ELSA-2013-0132)

Oracle Linux 5 : automake (ELSA-2014-1243)

Oracle Linux 5 : avahi (ELSA-2009-0013)

Oracle Linux 5 : avahi (ELSA-2010-0528)

Oracle Linux 5 : avahi (ELSA-2011-0436)

Oracle Linux 5 : axis (ELSA-2013-0683)

Oracle Linux 5 : bash (ELSA-2014-3077)

Oracle Linux 5 : bash (ELSA-2014-3094) (Shellshock)

Oracle Linux 5 : bind (ELSA-2007-0057)

Oracle Linux 5 : bind (ELSA-2009-1179)

Oracle Linux 5 : bind (ELSA-2009-1620)

Oracle Linux 5 : bind (ELSA-2010-0062)

Oracle Linux 5 : bind (ELSA-2010-0976)

Oracle Linux 5 : bind (ELSA-2012-1267)

Oracle Linux 5 : bind (ELSA-2015-1514)

Oracle Linux 5 : bind (ELSA-2015-1706)

Oracle Linux 5 : bind (ELSA-2015-2656)

Oracle Linux 5 : bind97 (ELSA-2011-1459)

Oracle Linux 5 : bind97 (ELSA-2012-0717)

Oracle Linux 5 : bind97 (ELSA-2012-1122)

Oracle Linux 5 : bind97 (ELSA-2012-1266)

Oracle Linux 5 : bind97 (ELSA-2012-1364)

Oracle Linux 5 : bind97 (ELSA-2013-0690)

Oracle Linux 5 : bind97 (ELSA-2013-1115)

Oracle Linux 5 : bind97 (ELSA-2014-1244)

Oracle Linux 5 : bind97 (ELSA-2014-1985)

Oracle Linux 5 : bind97 (ELSA-2015-1515)

Oracle Linux 5 : bind97 (ELSA-2015-1707)

Oracle Linux 5 : bind97 (ELSA-2015-2658)

Oracle Linux 5 : bind97 (ELSA-2016-0074)

Oracle Linux 5 : bind97 (ELSA-2016-0458)

Oracle Linux 5 : bind97 (ELSA-2016-1945)

Oracle Linux 5 : bind97 (ELSA-2016-2094)

Oracle Linux 5 : bind97 (ELSA-2016-2142)

Oracle Linux 5 : bind97 (ELSA-2017-0064)

Oracle Linux 5 : boost (ELSA-2012-0305)

Oracle Linux 5 : busybox (ELSA-2012-0308)

Oracle Linux 5 : ccid (ELSA-2013-1323)

Oracle Linux 5 : cman (ELSA-2007-0559-2)

Oracle Linux 5 : conga (ELSA-2011-0394)

Oracle Linux 5 : conga (ELSA-2012-0151)

Oracle Linux 5 : conga (ELSA-2013-0128)

Oracle Linux 5 : conga (ELSA-2014-1194)

Oracle Linux 5 : cpio (ELSA-2010-0144)

Oracle Linux 5 : cscope (ELSA-2009-1102)

Oracle Linux 5 : cups (ELSA-2007-1020)

Oracle Linux 5 : cups (ELSA-2008-0157)

Oracle Linux 5 : cups (ELSA-2008-0192)

Oracle Linux 5 : cups (ELSA-2008-1029)

Oracle Linux 5 : cups (ELSA-2009-1082)

Oracle Linux 5 : cups (ELSA-2009-1513)

Oracle Linux 5 : cups (ELSA-2009-1595)

Oracle Linux 5 : cups (ELSA-2010-0129)

Oracle Linux 5 : cups (ELSA-2010-0811)

Oracle Linux 5 : cups (ELSA-2012-0302)

Oracle Linux 5 : dbus (ELSA-2008-0159)

Oracle Linux 5 : dbus (ELSA-2009-0008)

Oracle Linux 5 : dbus (ELSA-2010-0018)

Oracle Linux 5 : dbus-glib (ELSA-2010-0616)

Oracle Linux 5 : dhcp (ELSA-2012-1140)

Oracle Linux 5 : dnsmasq (ELSA-2008-0789)

Oracle Linux 5 : dnsmasq (ELSA-2009-1238)

Oracle Linux 5 : dstat (ELSA-2009-1619)

Oracle Linux 5 : enscript (ELSA-2008-1016)

Oracle Linux 5 : evolution-data-server (ELSA-2007-0344)

Oracle Linux 5 : evolution-data-server (ELSA-2007-0510)

Oracle Linux 5 : firefox (ELSA-2008-0569)

Oracle Linux 5 : firefox (ELSA-2008-0597)

Oracle Linux 5 : firefox (ELSA-2008-0879)

Oracle Linux 5 : firefox (ELSA-2008-0978)

Oracle Linux 5 : firefox (ELSA-2010-0501)

Oracle Linux 5 : firefox (ELSA-2010-0556)

Oracle Linux 5 : freeradius (ELSA-2009-1451)

Oracle Linux 5 : freeradius2 (ELSA-2012-1327)

Oracle Linux 5 : freeradius2 (ELSA-2013-0134)

Oracle Linux 5 : freetype (ELSA-2009-1061)

Oracle Linux 5 : gdm (ELSA-2007-0777)

Oracle Linux 5 : gdm (ELSA-2013-1213)

Oracle Linux 5 : ghostscript (ELSA-2009-0421)

Oracle Linux 5 : giflib (ELSA-2009-0444)

Oracle Linux 5 : gimp (ELSA-2011-0838)

Oracle Linux 5 : gimp (ELSA-2012-1181)

Oracle Linux 5 : glib2 (ELSA-2009-0336)

Oracle Linux 5 : glibc (ELSA-2010-0787)

Oracle Linux 5 : glibc (ELSA-2010-0793)

Oracle Linux 5 : glibc (ELSA-2011-0412)

Oracle Linux 5 : glibc (ELSA-2012-0126)

Oracle Linux 5 : glibc (ELSA-2012-0397)

Oracle Linux 5 : glibc (ELSA-2012-1097)

Oracle Linux 5 : glibc (ELSA-2012-1207)

Oracle Linux 5 : glibc (ELSA-2013-0769)

Oracle Linux 5 : glibc (ELSA-2013-1411)

Oracle Linux 5 : glibc (ELSA-2015-0090) (GHOST)

Oracle Linux 5 : glibc (ELSA-2015-1627)

Oracle Linux 5 : gnome-screensaver (ELSA-2008-0197)

Oracle Linux 5 : gnome-vfs2 (ELSA-2013-0131)

Oracle Linux 5 : gnupg (ELSA-2007-0107)

Oracle Linux 5 : gnupg (ELSA-2013-1458)

Oracle Linux 5 : gnupg (ELSA-2014-0016)

Oracle Linux 5 : gnupg2 (ELSA-2010-0603)

Oracle Linux 5 : gnutls (ELSA-2008-0489)

Oracle Linux 5 : gnutls (ELSA-2008-0982)

Oracle Linux 5 : gnutls (ELSA-2010-0166)

Oracle Linux 5 : gnutls (ELSA-2012-0428)

Oracle Linux 5 : gnutls (ELSA-2014-0247)

Oracle Linux 5 : gnutls (ELSA-2014-0594)

Oracle Linux 5 : gstreamer-plugins-base (ELSA-2009-0352)

Oracle Linux 5 : gstreamer-plugins-good (ELSA-2009-0271)

Oracle Linux 5 : gstreamer-plugins-good (ELSA-2009-1123)

Oracle Linux 5 : gtk2 (ELSA-2013-0135)

Oracle Linux 5 : hplip (ELSA-2007-0960)

Oracle Linux 5 : hplip (ELSA-2008-0818)

Oracle Linux 5 : hplip3 (ELSA-2013-0133)

Oracle Linux 5 : httpd (ELSA-2007-0556)

Oracle Linux 5 : httpd (ELSA-2008-0008)

Oracle Linux 5 : httpd (ELSA-2009-1075)

Oracle Linux 5 : httpd (ELSA-2009-1148)

Oracle Linux 5 : httpd (ELSA-2010-0168)

Oracle Linux 5 : httpd (ELSA-2010-0659)

Oracle Linux 5 : httpd (ELSA-2012-0323)

Oracle Linux 5 : httpd (ELSA-2013-0130)

Oracle Linux 5 : httpd (ELSA-2014-0369)

Oracle Linux 5 : hypervkvpd (ELSA-2013-0807)

Oracle Linux 5 : ibutils (ELSA-2012-0311)

Oracle Linux 5 : icu (ELSA-2008-0090)

Oracle Linux 5 : icu (ELSA-2009-0296)

Oracle Linux 5 : icu (ELSA-2009-1122)

Oracle Linux 5 : ImageMagick (ELSA-2010-0652)

Oracle Linux 5 : ImageMagick (ELSA-2012-0301)

Oracle Linux 5 : ImageMagick (ELSA-2012-0545)

Oracle Linux 5 : initscripts (ELSA-2012-0312)

Oracle Linux 5 : ipa-client (ELSA-2013-0189)

Oracle Linux 5 : ipsec-tools (ELSA-2007-0342)

Oracle Linux 5 : ipsec-tools (ELSA-2009-1036)

Oracle Linux 5 : iscsi-initiator-utils (ELSA-2007-0497)

Oracle Linux 5 : jakarta-commons-collections (ELSA-2015-2671)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2009-0377)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2009-1201)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2009-1584)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2010-0339)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2010-0768)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2011-0176)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2011-0857)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2012-0322)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2012-0730)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2012-1222)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2012-1385) (ROBOT)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2013-0246)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2013-0274)

Oracle Linux 5 : java-1.6.0-openjdk (ELSA-2013-0604)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2013-0603)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2013-0752)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2013-0958)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2013-1447)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2014-0027)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2014-0407)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2014-0890)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2014-1633)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2015-0068) (POODLE)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2015-0807)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2015-1230) (Bar Mitzvah) (Logjam)

Oracle Linux 5 : java-1.7.0-openjdk (ELSA-2015-1921)

Oracle Linux 5 : kernel (ELSA-2007-0347)

Oracle Linux 5 : kernel (ELSA-2007-0376)

Oracle Linux 5 : kernel (ELSA-2007-0595)

Oracle Linux 5 : kernel (ELSA-2007-0705)

Oracle Linux 5 : kernel (ELSA-2007-0936)

Oracle Linux 5 : kernel (ELSA-2007-0940)

Oracle Linux 5 : kernel (ELSA-2007-0993)

Oracle Linux 5 : kernel (ELSA-2008-0089)

Oracle Linux 5 : kernel (ELSA-2008-0129)

Oracle Linux 5 : kernel (ELSA-2008-0154)

Oracle Linux 5 : kernel (ELSA-2008-0233)

Oracle Linux 5 : kernel (ELSA-2008-0275)

Oracle Linux 5 : kernel (ELSA-2008-0519)

Oracle Linux 5 : kernel (ELSA-2008-0612)

Oracle Linux 5 : kernel (ELSA-2008-0885)

Oracle Linux 5 : kernel (ELSA-2008-0957)

Oracle Linux 5 : kernel (ELSA-2008-1017)

Oracle Linux 5 : kernel (ELSA-2009-0264)

Oracle Linux 5 : kernel (ELSA-2009-0326)

Oracle Linux 5 : kernel (ELSA-2009-0473)

Oracle Linux 5 : kernel (ELSA-2009-1106)

Oracle Linux 5 : kernel (ELSA-2009-1193)

Oracle Linux 5 : kernel (ELSA-2009-1222)

Oracle Linux 5 : kernel (ELSA-2009-1455)

Oracle Linux 5 : kernel (ELSA-2009-1548)

Oracle Linux 5 : kernel (ELSA-2009-1670)

Oracle Linux 5 : kernel (ELSA-2010-0019)

Oracle Linux 5 : kernel (ELSA-2010-0046)

Oracle Linux 5 : kernel (ELSA-2010-0147)

Oracle Linux 5 : kernel (ELSA-2010-0398)

Oracle Linux 5 : kernel (ELSA-2010-0504)

Oracle Linux 5 : kernel (ELSA-2010-0610)

Oracle Linux 5 : kernel (ELSA-2010-0661)

Oracle Linux 5 : kernel (ELSA-2010-0704)

Oracle Linux 5 : kernel (ELSA-2010-0723)

Oracle Linux 5 : kernel (ELSA-2010-0792)

Oracle Linux 5 : kernel (ELSA-2010-0839)

Oracle Linux 5 : kernel (ELSA-2010-2010)

Oracle Linux 5 : kernel (ELSA-2011-0004)

Oracle Linux 5 : kernel (ELSA-2011-0163)

Oracle Linux 5 : kernel (ELSA-2011-0303)

Oracle Linux 5 : kernel (ELSA-2011-0429)

Oracle Linux 5 : kernel (ELSA-2011-0833)

Oracle Linux 5 : kernel (ELSA-2011-0927)

Oracle Linux 5 : kernel (ELSA-2011-1212)

Oracle Linux 5 : kernel (ELSA-2011-1386)

Oracle Linux 5 : kernel (ELSA-2011-1479)

Oracle Linux 5 : kernel (ELSA-2012-0007)

Oracle Linux 5 : kernel (ELSA-2012-0107)

Oracle Linux 5 : kernel (ELSA-2012-0150)

Oracle Linux 5 : kernel (ELSA-2012-0150-1)

Oracle Linux 5 : kernel (ELSA-2012-0480)

Oracle Linux 5 : kernel (ELSA-2012-0480-1)

Oracle Linux 5 : kernel (ELSA-2012-0690)

Oracle Linux 5 : kernel (ELSA-2012-0690-1)

Oracle Linux 5 : kernel (ELSA-2012-0721)

Oracle Linux 5 : kernel (ELSA-2012-0721-1)

Oracle Linux 5 : kernel (ELSA-2012-1061)

Oracle Linux 5 : kernel (ELSA-2012-1061-1)

Oracle Linux 5 : kernel (ELSA-2012-1174)

Oracle Linux 5 : kernel (ELSA-2012-1174-1)

Oracle Linux 5 : kernel (ELSA-2012-1323)

Oracle Linux 5 : kernel (ELSA-2012-1323-1)

Oracle Linux 5 : kernel (ELSA-2012-1445)

Oracle Linux 5 : kernel (ELSA-2012-1445-1)

Oracle Linux 5 : kernel (ELSA-2012-1540)

Oracle Linux 5 : kernel (ELSA-2012-1540-1)

Oracle Linux 5 : kernel (ELSA-2013-0168)

Oracle Linux 5 : kernel (ELSA-2013-0168-1)

Oracle Linux 5 : kernel (ELSA-2013-0594)

Oracle Linux 5 : kernel (ELSA-2013-0594-1)

Oracle Linux 5 : kernel (ELSA-2013-0621)

Oracle Linux 5 : kernel (ELSA-2013-0621-1)

Oracle Linux 5 : kernel (ELSA-2013-0747)

Oracle Linux 5 : kernel (ELSA-2013-0747-1)

Oracle Linux 5 : kernel (ELSA-2013-0847)

Oracle Linux 5 : kernel (ELSA-2013-0847-1)

Oracle Linux 5 : kernel (ELSA-2013-1034)

Oracle Linux 5 : kernel (ELSA-2013-1034-1)

Oracle Linux 5 : kernel (ELSA-2013-1166)

Oracle Linux 5 : kernel (ELSA-2013-1166-1)

Oracle Linux 5 : kernel (ELSA-2013-1292)

Oracle Linux 5 : kernel (ELSA-2013-1292-1)

Oracle Linux 5 : kernel (ELSA-2013-1348)

Oracle Linux 5 : kernel (ELSA-2013-1348-1)

Oracle Linux 5 : kernel (ELSA-2013-1449)

Oracle Linux 5 : kernel (ELSA-2013-1449-1)

Oracle Linux 5 : kernel (ELSA-2013-1790)

Oracle Linux 5 : kernel (ELSA-2013-1790-1)

Oracle Linux 5 : kernel (ELSA-2014-0108)

Oracle Linux 5 : kernel (ELSA-2014-0108-1)

Oracle Linux 5 : kernel (ELSA-2014-0285)

Oracle Linux 5 : kernel (ELSA-2014-0285-1)

Oracle Linux 5 : kernel (ELSA-2014-0433)

Oracle Linux 5 : kernel (ELSA-2014-0433-1)

Oracle Linux 5 : kernel (ELSA-2014-0740)

Oracle Linux 5 : kernel (ELSA-2014-0740-1)

Oracle Linux 5 : kernel (ELSA-2014-0926)

Oracle Linux 5 : kernel (ELSA-2014-0926-1)

Oracle Linux 5 : kernel (ELSA-2014-1143)

Oracle Linux 5 : kernel (ELSA-2014-1143-1)

Oracle Linux 5 : kernel (ELSA-2014-1959)

Oracle Linux 5 : kernel (ELSA-2014-1959-1)

Oracle Linux 5 : kernel (ELSA-2014-2008)

Oracle Linux 5 : kernel (ELSA-2014-2008-1)

Oracle Linux 5 : kernel (ELSA-2015-0164)

Oracle Linux 5 : kernel (ELSA-2015-0164-1)

Oracle Linux 5 : kernel (ELSA-2015-0783)

Oracle Linux 5 : kernel (ELSA-2015-0783-1)

Oracle Linux 5 : kernel (ELSA-2015-1042)

Oracle Linux 5 : kernel (ELSA-2015-1042-1)

Oracle Linux 5 : kernel (ELSA-2016-0045)

Oracle Linux 5 : kernel (ELSA-2016-0045-1)

Oracle Linux 5 : kernel (ELSA-2016-0450)

Oracle Linux 5 : kernel (ELSA-2016-0450-1)

Oracle Linux 5 : kernel (ELSA-2016-2124) (Dirty COW)

Oracle Linux 5 : kernel (ELSA-2016-2124-1)

Oracle Linux 5 : kernel (ELSA-2016-2962)

Oracle Linux 5 : kernel (ELSA-2016-2962-1)

Oracle Linux 5 : kernel (ELSA-2017-0323)

Oracle Linux 5 : kernel (ELSA-2017-0323-1)

Oracle Linux 5 : kexec-tools (ELSA-2012-0152)

Oracle Linux 5 : krb5 (ELSA-2007-0858)

Oracle Linux 5 : krb5 (ELSA-2007-0892)

Oracle Linux 5 : krb5 (ELSA-2008-0164)

Oracle Linux 5 : krb5 (ELSA-2009-0408)

Oracle Linux 5 : krb5 (ELSA-2010-0343)

Oracle Linux 5 : krb5 (ELSA-2011-0199)

Oracle Linux 5 : krb5 (ELSA-2012-0306)

Oracle Linux 5 : krb5 (ELSA-2014-1245)

Oracle Linux 5 : krb5 (ELSA-2014-1255)

Oracle Linux 5 : kvm (ELSA-2009-1465)

Oracle Linux 5 : kvm (ELSA-2009-1659)

Oracle Linux 5 : kvm (ELSA-2010-0088)

Oracle Linux 5 : kvm (ELSA-2010-0126)

Oracle Linux 5 : kvm (ELSA-2010-0627)

Oracle Linux 5 : kvm (ELSA-2010-0898)

Oracle Linux 5 : kvm (ELSA-2010-0998)

Oracle Linux 5 : kvm (ELSA-2012-0051)

Oracle Linux 5 : kvm (ELSA-2012-0149)

Oracle Linux 5 : kvm (ELSA-2012-0676)

Oracle Linux 5 : kvm (ELSA-2012-1235)

Oracle Linux 5 : kvm (ELSA-2013-0608)

Oracle Linux 5 : kvm (ELSA-2013-0727)

Oracle Linux 5 : kvm (ELSA-2014-0163)

Oracle Linux 5 : kvm (ELSA-2015-0869)

Oracle Linux 5 : kvm (ELSA-2015-1003) (Venom)

Oracle Linux 5 : kvm (ELSA-2015-1189)

Oracle Linux 5 : kvm (ELSA-2015-1925)

Oracle Linux 5 : kvm (ELSA-2016-1943)

Oracle Linux 5 : kvm (ELSA-2017-0454)

Oracle Linux 5 : lcms (ELSA-2009-0011)

Oracle Linux 5 : lcms (ELSA-2009-0339)

Oracle Linux 5 : lftp (ELSA-2010-0585)

Oracle Linux 5 : libexif (ELSA-2007-1165)

Oracle Linux 5 : libjpeg (ELSA-2013-1804)

Oracle Linux 5 : libpng (ELSA-2011-1104)

Oracle Linux 5 : libtiff (ELSA-2008-0847)

Oracle Linux 5 : libtiff (ELSA-2014-0223)

Oracle Linux 5 : libvirt (ELSA-2009-0382)

Oracle Linux 5 : libvirt (ELSA-2010-0615)

Oracle Linux 5 : libvirt (ELSA-2011-0478)

Oracle Linux 5 : libvirt (ELSA-2013-0127)

Oracle Linux 5 : libX11 / xorg-x11-apps (ELSA-2007-0157)

Oracle Linux 5 : libXfont (ELSA-2007-0132)

Oracle Linux 5 : libXfont (ELSA-2008-0064)

Oracle Linux 5 : libXfont (ELSA-2014-1893)

Oracle Linux 5 : libxml2 (ELSA-2012-0017)

Oracle Linux 5 : libxml2 (ELSA-2014-1885)

Oracle Linux 5 : lvm2-cluster (ELSA-2010-0567)

Oracle Linux 5 : mesa (ELSA-2013-0898)

Oracle Linux 5 : mod\_auth\_mysql (ELSA-2009-0259)

Oracle Linux 5 : mysql (ELSA-2010-0109)

Oracle Linux 5 : mysql (ELSA-2010-0442)

Oracle Linux 5 : mysql (ELSA-2010-0825)

Oracle Linux 5 : mysql (ELSA-2012-0127)

Oracle Linux 5 : mysql (ELSA-2013-0121)

Oracle Linux 5 : mysql (ELSA-2013-0180)

Oracle Linux 5 : mysql55-mysql (ELSA-2014-0186)

Oracle Linux 5 : mysql55-mysql (ELSA-2014-0536)

Oracle Linux 5 : mysql55-mysql (ELSA-2014-1859)

Oracle Linux 5 : mysql55-mysql (ELSA-2015-1628)

Oracle Linux 5 : net-snmp (ELSA-2013-0124)

Oracle Linux 5 : net-snmp (ELSA-2014-0322)

Oracle Linux 5 : NetworkManager (ELSA-2009-0361)

Oracle Linux 5 : NetworkManager (ELSA-2010-0108)

Oracle Linux 5 : nfs-utils (ELSA-2008-0486)

Oracle Linux 5 : nfs-utils (ELSA-2012-0310)

Oracle Linux 5 : nfs-utils-lib (ELSA-2007-0951)

Oracle Linux 5 : nspr / nss (ELSA-2012-1090)

Oracle Linux 5 : nspr / nss (ELSA-2013-0214)

Oracle Linux 5 : nspr / nss (ELSA-2013-1135)

Oracle Linux 5 : nspr / nss (ELSA-2013-1791)

Oracle Linux 5 : nspr / nss (ELSA-2014-1246)

Oracle Linux 5 : nspr / nss (ELSA-2015-1980)

Oracle Linux 5 : nspr / nss (ELSA-2016-0684)

Oracle Linux 5 : nss (ELSA-2015-1664)

Oracle Linux 5 : nss (ELSA-2016-0371)

Oracle Linux 5 : nss (ELSA-2017-1101)

Oracle Linux 5 : nss\_db (ELSA-2010-0347)

Oracle Linux 5 : ntp (ELSA-2009-1039)

Oracle Linux 5 : ntp (ELSA-2014-2025)

Oracle Linux 5 : OpenIPMI (ELSA-2013-0123)

Oracle Linux 5 : openldap (ELSA-2010-0542)

Oracle Linux 5 : openldap (ELSA-2011-0346)

Oracle Linux 5 : openldap (ELSA-2014-0206)

Oracle Linux 5 : openssh (ELSA-2009-1470)

Oracle Linux 5 : openssh (ELSA-2016-3521)

Oracle Linux 5 : openssh (ELSA-2016-3531)

Oracle Linux 5 : openssl (ELSA-2007-0964)

Oracle Linux 5 : openssl (ELSA-2010-0054)

Oracle Linux 5 : openssl (ELSA-2010-0162)

Oracle Linux 5 : openssl (ELSA-2010-0978)

Oracle Linux 5 : openssl (ELSA-2012-0060)

Oracle Linux 5 : openssl (ELSA-2014-0624)

Oracle Linux 5 : openssl (ELSA-2014-1053)

Oracle Linux 5 : openssl (ELSA-2014-1653) (POODLE)

Oracle Linux 5 : openssl (ELSA-2015-0800) (FREAK)

Oracle Linux 5 : openssl (ELSA-2015-1197) (Logjam)

Oracle Linux 5 : openssl (ELSA-2015-2616)

Oracle Linux 5 : openssl (ELSA-2015-3010)

Oracle Linux 5 : openssl (ELSA-2016-0302) (DROWN)

Oracle Linux 5 : openssl (ELSA-2016-1137)

Oracle Linux 5 : openssl (ELSA-2016-3576)

Oracle Linux 5 : openssl (ELSA-2016-3627)

Oracle Linux 5 : openssl097a (ELSA-2010-0164)

Oracle Linux 5 : openswan (ELSA-2009-0402)

Oracle Linux 5 : openswan (ELSA-2009-1138)

Oracle Linux 5 : pam (ELSA-2010-0819)

Oracle Linux 5 : pam\_krb5 (ELSA-2008-0907)

Oracle Linux 5 : pango (ELSA-2011-1326)

Oracle Linux 5 : pcre (ELSA-2007-0967)

Oracle Linux 5 : pcre (ELSA-2007-1059)

Oracle Linux 5 : pcsc-lite (ELSA-2010-0533)

Oracle Linux 5 : perl (ELSA-2010-0458)

Oracle Linux 5 : perl-DBD-Pg (ELSA-2009-0479)

Oracle Linux 5 : perl-Net-DNS (ELSA-2007-0674)

Oracle Linux 5 : php (ELSA-2007-0348)

Oracle Linux 5 : php (ELSA-2009-0338)

Oracle Linux 5 : php (ELSA-2012-0033)

Oracle Linux 5 : php (ELSA-2012-1045)

Oracle Linux 5 : php (ELSA-2013-1814)

Oracle Linux 5 : php (ELSA-2014-0311)

Oracle Linux 5 : php (ELSA-2014-1824)

Oracle Linux 5 : php53 (ELSA-2011-0196)

Oracle Linux 5 : php53 (ELSA-2012-0092)

Oracle Linux 5 : php53 (ELSA-2012-0547)

Oracle Linux 5 : php53 (ELSA-2012-1047)

Oracle Linux 5 : php53 (ELSA-2013-1050)

Oracle Linux 5 : php53 (ELSA-2013-1307)

Oracle Linux 5 : php53 (ELSA-2014-1768)

Oracle Linux 5 : piranha (ELSA-2014-0174)

Oracle Linux 5 : poppler (ELSA-2007-0732)

Oracle Linux 5 : poppler (ELSA-2007-1026)

Oracle Linux 5 : poppler (ELSA-2008-0239)

Oracle Linux 5 : poppler (ELSA-2009-0480)

Oracle Linux 5 : poppler (ELSA-2009-1504)

Oracle Linux 5 : poppler (ELSA-2010-0749)

Oracle Linux 5 : postgresql (ELSA-2010-0429)

Oracle Linux 5 : postgresql (ELSA-2012-0677)

Oracle Linux 5 : postgresql (ELSA-2012-1036)

Oracle Linux 5 : postgresql (ELSA-2012-1264)

Oracle Linux 5 : postgresql (ELSA-2014-0249)

Oracle Linux 5 : postgresql84 (ELSA-2010-0430)

Oracle Linux 5 : postgresql84 (ELSA-2011-0198)

Oracle Linux 5 : postgresql84 (ELSA-2011-1378)

Oracle Linux 5 : python (ELSA-2009-1176)

Oracle Linux 5 : python (ELSA-2011-0492)

Oracle Linux 5 : python (ELSA-2012-0745)

Oracle Linux 5 : qspice (ELSA-2010-0633)

Oracle Linux 5 : qspice (ELSA-2013-1474)

Oracle Linux 5 : qt4 (ELSA-2011-1324)

Oracle Linux 5 : quagga (ELSA-2012-1258)

Oracle Linux 5 : quota (ELSA-2013-0120)

Oracle Linux 5 : rdesktop (ELSA-2008-0575)

Oracle Linux 5 : rpm (ELSA-2010-0679)

Oracle Linux 5 : ruby (ELSA-2011-0909)

Oracle Linux 5 : ruby (ELSA-2013-0129)

Oracle Linux 5 : ruby (ELSA-2013-0611)

Oracle Linux 5 : samba (ELSA-2008-0290)

Oracle Linux 5 : samba (ELSA-2012-0313)

Oracle Linux 5 : samba (ELSA-2014-0305)

Oracle Linux 5 : samba (ELSA-2016-0621) (Badlock)

Oracle Linux 5 : samba3x (ELSA-2010-0698)

Oracle Linux 5 : samba3x (ELSA-2011-0306)

Oracle Linux 5 : samba3x (ELSA-2011-1220)

Oracle Linux 5 : samba3x (ELSA-2012-0466)

Oracle Linux 5 : samba3x (ELSA-2013-1310)

Oracle Linux 5 : samba3x (ELSA-2015-0249)

Oracle Linux 5 : samba3x (ELSA-2016-0613) (Badlock)

Oracle Linux 5 : samba3x (ELSA-2017-1272) (SambaCry)

Oracle Linux 5 : scsi-target-utils (ELSA-2010-0362)

Oracle Linux 5 : scsi-target-utils (ELSA-2010-0518)

Oracle Linux 5 : sos (ELSA-2012-0153)

Oracle Linux 5 : sos (ELSA-2013-1121)

Oracle Linux 5 : squid (ELSA-2007-0131)

Oracle Linux 5 : squirrelmail (ELSA-2013-0126)

Oracle Linux 5 : sssd (ELSA-2013-1319)

Oracle Linux 5 : struts (ELSA-2014-0474)

Oracle Linux 5 : subversion (ELSA-2011-0257)

Oracle Linux 5 : subversion (ELSA-2011-0327)

Oracle Linux 5 : sudo (ELSA-2009-0267)

Oracle Linux 5 : sudo (ELSA-2010-0122)

Oracle Linux 5 : sudo (ELSA-2010-0361)

Oracle Linux 5 : sudo (ELSA-2010-0475)

Oracle Linux 5 : sudo (ELSA-2010-0675)

Oracle Linux 5 : sudo (ELSA-2012-0309)

Oracle Linux 5 : sudo (ELSA-2012-1149)

Oracle Linux 5 : sudo (ELSA-2013-1353)

Oracle Linux 5 : sudo (ELSA-2014-0266)

Oracle Linux 5 : sudo (ELSA-2017-1381)

Oracle Linux 5 : systemtap (ELSA-2010-0124)

Oracle Linux 5 : systemtap (ELSA-2011-0841)

Oracle Linux 5 : systemtap (ELSA-2011-1089)

Oracle Linux 5 : tcl (ELSA-2013-0122)

Oracle Linux 5 : tetex (ELSA-2010-0400)

Oracle Linux 5 : tetex (ELSA-2012-1201)

Oracle Linux 5 : tk (ELSA-2008-0136)

Oracle Linux 5 : tog-pegasus (ELSA-2008-1001)

Oracle Linux 5 : tomcat (ELSA-2007-0327)

Oracle Linux 5 : tomcat (ELSA-2007-0569)

Oracle Linux 5 : tomcat (ELSA-2007-0871)

Oracle Linux 5 : tomcat (ELSA-2008-0042)

Oracle Linux 5 : tomcat (ELSA-2008-0648)

Oracle Linux 5 : tomcat (ELSA-2009-1164)

Oracle Linux 5 : tomcat5 (ELSA-2010-0580)

Oracle Linux 5 : tomcat5 (ELSA-2011-0336)

Oracle Linux 5 : tomcat5 (ELSA-2011-1845)

Oracle Linux 5 : tomcat5 (ELSA-2012-0474)

Oracle Linux 5 : tomcat5 (ELSA-2013-0640)

Oracle Linux 5 : tomcat5 (ELSA-2013-0870)

Oracle Linux 5 : udev (ELSA-2009-0427)

Oracle Linux 5 : Unbreakable Enterprise kernel (ELSA-2010-2008)

Oracle Linux 5 : Unbreakable Enterprise kernel (ELSA-2010-2009)

Oracle Linux 5 : Unbreakable Enterprise kernel (ELSA-2010-2011)

Oracle Linux 5 : util-linux (ELSA-2012-0307)

Oracle Linux 5 : vim (ELSA-2007-0346)

Oracle Linux 5 : vim (ELSA-2008-0580)

Oracle Linux 5 : vixie-cron (ELSA-2012-0304)

Oracle Linux 5 : w3m (ELSA-2010-0565)

Oracle Linux 5 : wireshark (ELSA-2013-0125)

Oracle Linux 5 : wireshark (ELSA-2014-0341)

Oracle Linux 5 : wireshark (ELSA-2014-1677)

Oracle Linux 5 : xen (ELSA-2007-0114)

Oracle Linux 5 : xen (ELSA-2007-0323)

Oracle Linux 5 : xen (ELSA-2008-0194)

Oracle Linux 5 : xen (ELSA-2008-0892)

Oracle Linux 5 : xen (ELSA-2009-0003)

Oracle Linux 5 : xen (ELSA-2009-1472)

Oracle Linux 5 : xen (ELSA-2011-0496)

Oracle Linux 5 : xen (ELSA-2011-1401)

Oracle Linux 5 : xen (ELSA-2012-0370)

Oracle Linux 5 : xen (ELSA-2012-1130)

Oracle Linux 5 : xen (ELSA-2012-1236)

Oracle Linux 5 : xen (ELSA-2013-0241)

Oracle Linux 5 : xen (ELSA-2013-0599)

Oracle Linux 5 : xen (ELSA-2015-1002) (Venom)

Oracle Linux 5 : xen (ELSA-2015-2065)

Oracle Linux 5 : xen (ELSA-2016-2963)

Oracle Linux 5 : xerces-j2 (ELSA-2009-1615)

Oracle Linux 5 : xinetd (ELSA-2013-1302)

Oracle Linux 5 : xorg-x11-server (ELSA-2007-0127)

Oracle Linux 5 : xorg-x11-server (ELSA-2008-0031)

Oracle Linux 5 : xorg-x11-server (ELSA-2008-0504)

Oracle Linux 5 : xorg-x11-server (ELSA-2010-0382)

Oracle Linux 5 : xorg-x11-server (ELSA-2012-0303)

Oracle Linux 5 : xorg-x11-server (ELSA-2014-1982)

Oracle Linux 5 : xorg-x11-xfs (ELSA-2007-0520)

Oracle Linux 5 : xulrunner (ELSA-2010-0809)

Oracle Linux 5 : yum-updatesd (ELSA-2014-1004)

Oracle Linux 6 / 7 : 389-ds-base (ELSA-2014-1031)

Oracle Linux 6 / 7 : apr (ELSA-2017-3270)

Oracle Linux 6 / 7 : bind (ELSA-2015-0672)

Oracle Linux 6 / 7 : bind (ELSA-2015-1513)

Oracle Linux 6 / 7 : bind (ELSA-2015-1705)

Oracle Linux 6 / 7 : bind (ELSA-2015-2655)

Oracle Linux 6 / 7 : bluez (ELSA-2017-2685) (BlueBorne)

Oracle Linux 6 / 7 : cups (ELSA-2015-1123)

Oracle Linux 6 / 7 : curl (ELSA-2019-4652)

Oracle Linux 6 / 7 : docker (ELSA-2014-3095)

Oracle Linux 6 / 7 : docker (ELSA-2014-3110)

Oracle Linux 6 / 7 : docker (ELSA-2015-3037)

Oracle Linux 6 / 7 : docker-engine (ELSA-2015-3085)

Oracle Linux 6 / 7 : docker-engine (ELSA-2016-3568)

Oracle Linux 6 / 7 : docker-engine / docker-engine-selinux (ELSA-2017-3511)

Oracle Linux 6 / 7 : dovecot (ELSA-2014-0790)

Oracle Linux 6 / 7 : expat (ELSA-2016-2824)

Oracle Linux 6 / 7 : firefox (ELSA-2017-1440)

Oracle Linux 6 / 7 : firefox (ELSA-2017-2456)

Oracle Linux 6 / 7 : firefox (ELSA-2017-2831)

Oracle Linux 6 / 7 : firefox (ELSA-2017-3247)

Oracle Linux 6 / 7 : firefox (ELSA-2017-3382)

Oracle Linux 6 / 7 : firefox (ELSA-2018-0122)

Oracle Linux 6 / 7 : firefox (ELSA-2018-0549)

Oracle Linux 6 / 7 : flac (ELSA-2015-0767)

Oracle Linux 6 / 7 : freetype (ELSA-2015-0696)

Oracle Linux 6 / 7 : gdk-pixbuf2 (ELSA-2015-1694)

Oracle Linux 6 / 7 : ghostscript (ELSA-2017-1230)

Oracle Linux 6 / 7 : git (ELSA-2016-0496)

Oracle Linux 6 / 7 : glibc (ELSA-2015-0092) (GHOST)

Oracle Linux 6 / 7 : gnutls (ELSA-2016-0012) (SLOTH)

Oracle Linux 6 / 7 : ImageMagick (ELSA-2016-0726) (ImageTragick)

Oracle Linux 6 / 7 : ImageMagick (ELSA-2016-1237)

Oracle Linux 6 / 7 : ipa (ELSA-2016-1797)

Oracle Linux 6 / 7 : jakarta-taglibs-standard (ELSA-2015-1695)

Oracle Linux 6 / 7 : jasper (ELSA-2014-2021)

Oracle Linux 6 / 7 : jasper (ELSA-2015-0074)

Oracle Linux 6 / 7 : jasper (ELSA-2017-1208)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2014-0889)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2014-1620)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2015-0067) (POODLE)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2015-0806)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2015-1229) (Bar Mitzvah) (Logjam)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2015-1920)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2017-1204)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2017-2424)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2017-3392)

Oracle Linux 6 / 7 : java-1.7.0-openjdk (ELSA-2018-0349)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2015-0809)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2015-1228) (Bar Mitzvah) (Logjam)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2015-1919)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2016-1458)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2016-2079)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2017-0180)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2017-1789)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2017-2998)

Oracle Linux 6 / 7 : java-1.8.0-openjdk (ELSA-2018-0095)

Oracle Linux 6 / 7 : kernel-uek (ELSA-2016-3529)

Oracle Linux 6 / 7 : kernel-uek (ELSA-2016-3587)

Oracle Linux 6 / 7 : libgcrypt (ELSA-2016-2674)

Oracle Linux 6 / 7 : libldb (ELSA-2016-0009)

Oracle Linux 6 / 7 : libreoffice (ELSA-2015-2619)

Oracle Linux 6 / 7 : libssh2 (ELSA-2016-0428)

Oracle Linux 6 / 7 : libtiff (ELSA-2017-0225)

Oracle Linux 6 / 7 : libvncserver (ELSA-2014-1826)

Oracle Linux 6 / 7 : libwmf (ELSA-2015-1917)

Oracle Linux 6 / 7 : libXfont (ELSA-2014-1870)

Oracle Linux 6 / 7 : libXfont (ELSA-2015-1708)

Oracle Linux 6 / 7 : libxml2 (ELSA-2014-1655)

Oracle Linux 6 / 7 : libxml2 (ELSA-2016-1292)

Oracle Linux 6 / 7 : libyaml (ELSA-2015-0100)

Oracle Linux 6 / 7 : lxc (ELSA-2015-3065)

Oracle Linux 6 / 7 : lxc (ELSA-2015-3087)

Oracle Linux 6 / 7 : lzo (ELSA-2014-0861)

Oracle Linux 6 / 7 : mailx (ELSA-2014-1999)

Oracle Linux 6 / 7 : mercurial (ELSA-2017-1576)

Oracle Linux 6 / 7 : microcode\_ctl (ELSA-2018-0093) (Spectre)

Oracle Linux 6 / 7 : mutt (ELSA-2018-2526)

Oracle Linux 6 / 7 : net-snmp (ELSA-2015-1636)

Oracle Linux 6 / 7 : nspr / nss / nss-util (ELSA-2015-1981)

Oracle Linux 6 / 7 : nss (ELSA-2015-1185) (Logjam)

Oracle Linux 6 / 7 : nss (ELSA-2016-0007) (SLOTH)

Oracle Linux 6 / 7 : nss (ELSA-2017-2832)

Oracle Linux 6 / 7 : nss / nss-util (ELSA-2017-1100)

Oracle Linux 6 / 7 : nss-softokn (ELSA-2015-1699)

Oracle Linux 6 / 7 : nss-util (ELSA-2016-0370)

Oracle Linux 6 / 7 : ntp (ELSA-2014-2024)

Oracle Linux 6 / 7 : ntp (ELSA-2015-1930)

Oracle Linux 6 / 7 : ntp (ELSA-2016-0063)

Oracle Linux 6 / 7 : ntp (ELSA-2016-1141)

Oracle Linux 6 / 7 : ntp (ELSA-2017-0252)

Oracle Linux 6 / 7 : openssl (ELSA-2014-1052)

Oracle Linux 6 / 7 : openssl (ELSA-2014-1652) (POODLE)

Oracle Linux 6 / 7 : openssl (ELSA-2015-0066) (FREAK)

Oracle Linux 6 / 7 : openssl (ELSA-2015-1072) (Logjam)

Oracle Linux 6 / 7 : openssl (ELSA-2015-1115)

Oracle Linux 6 / 7 : openssl (ELSA-2015-2617)

Oracle Linux 6 / 7 : openssl (ELSA-2016-0008) (SLOTH)

Oracle Linux 6 / 7 : openssl (ELSA-2016-0301) (DROWN)

Oracle Linux 6 / 7 : openssl (ELSA-2016-1940)

Oracle Linux 6 / 7 : openssl (ELSA-2017-0286)

Oracle Linux 6 / 7 : openssl098e (ELSA-2016-0372) (DROWN)

Oracle Linux 6 / 7 : pam (ELSA-2015-1640)

Oracle Linux 6 / 7 : php (ELSA-2014-1767)

Oracle Linux 6 / 7 : policycoreutils (ELSA-2016-2702)

Oracle Linux 6 / 7 : postgresql (ELSA-2015-0750)

Oracle Linux 6 / 7 : postgresql (ELSA-2015-1194)

Oracle Linux 6 / 7 : python (ELSA-2016-1626) (httpoxy)

Oracle Linux 6 / 7 : python-twisted-web (ELSA-2016-1978)

Oracle Linux 6 / 7 : rpcbind (ELSA-2016-0005)

Oracle Linux 6 / 7 : samba (ELSA-2016-0448)

Oracle Linux 6 / 7 : samba (ELSA-2017-1270) (SambaCry)

Oracle Linux 6 / 7 : samba / samba4 (ELSA-2016-0612) (Badlock)

Oracle Linux 6 / 7 : sudo (ELSA-2016-2872)

Oracle Linux 6 / 7 : sudo (ELSA-2017-1382)

Oracle Linux 6 / 7 : sudo (ELSA-2017-1574)

Oracle Linux 6 / 7 : thunderbird (ELSA-2015-0771)

Oracle Linux 6 / 7 : thunderbird (ELSA-2015-1012)

Oracle Linux 6 / 7 : thunderbird (ELSA-2015-1455)

Oracle Linux 6 / 7 : thunderbird (ELSA-2015-1682)

Oracle Linux 6 / 7 : thunderbird (ELSA-2015-1852)

Oracle Linux 6 / 7 : thunderbird (ELSA-2015-2519)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-0001)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-0258)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-0460)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-1041)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-1392)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-1809)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-1985)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-2825)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-2850)

Oracle Linux 6 / 7 : thunderbird (ELSA-2016-2973)

Oracle Linux 6 / 7 : thunderbird (ELSA-2017-0238)

Oracle Linux 6 / 7 : thunderbird (ELSA-2017-0498)

Oracle Linux 6 / 7 : thunderbird (ELSA-2017-1201)

Oracle Linux 6 / 7 : thunderbird (ELSA-2017-1561)

Oracle Linux 6 / 7 : thunderbird (ELSA-2017-2534)

Oracle Linux 6 / 7 : thunderbird (ELSA-2017-2885)

Oracle Linux 6 / 7 : thunderbird (ELSA-2017-3372)

Oracle Linux 6 / 7 : thunderbird (ELSA-2018-0061)

Oracle Linux 6 / 7 : thunderbird (ELSA-2018-0262)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3052)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3067)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3070)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3072)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3081)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3084)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3087)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3096)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3103)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2014-3106)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3003)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3012)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3013)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3019)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3032)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3035)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3041)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3045)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3048)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3053)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3064)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3066)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3071)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3078)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3092)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3098)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3101)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2015-3107)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3501)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3509)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3510)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3519)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3528)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3551)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3554)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3559)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3565)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3570)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3573)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3588)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3591)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3593)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3594)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3595)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3596)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3617)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3619)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3623)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3625)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3626)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3632) (Dirty COW)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3633) (Dirty COW)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3635)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3636)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3644)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3645)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3648)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3651)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3655)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2016-3656)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3508)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3509)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3514)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3515)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3520)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3521)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3533)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3534)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3537)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3539)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3565)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3566)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3574)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3575)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3579)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3580)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3587) (Stack Clash)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3589)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3590)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3595) (Stack Clash)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3596)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3605)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3606)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3609) (Stack Clash)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3620) (BlueBorne)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3621) (BlueBorne) (Stack Clash)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3629)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3631)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3632)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3635)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3636)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3640)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3651) (Dirty COW)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3657) (BlueBorne) (Stack Clash)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2017-3659) (BlueBorne) (Dirty COW) (Stack Clash)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4001)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4004) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4006) (Meltdown) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4011) (Meltdown) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4017) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4022) (Meltdown) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4025) (Meltdown)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4040)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4062)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4071) (Dirty COW) (Meltdown) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4084)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4087)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4089) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4096)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4098)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4108)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4109) (Meltdown) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4114) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4126) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4131)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4134)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4144)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4161)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4164)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4193)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4196) (Foreshadow)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4200)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4208)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4210) (Foreshadow)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4211)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4215) (Foreshadow)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4216)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4227)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4230)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4233)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4244)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4245) (Foreshadow)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4261)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4265)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4268)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4288)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4299)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4300)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2018-4307)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4315)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4316)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4510)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4528)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4531)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4532)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4575)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4576)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4594)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4596)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4600)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4619)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4629) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4636) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4642)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4644)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4669) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4670)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4672) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4684) (SACK Panic) (SACK Slowness)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4686) (SACK Panic) (SACK Slowness)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4703)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4710) (Spectre)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4729)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4735)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4739)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4741)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4775)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4800)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4808)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4810)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4823)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4837)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4838)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4850)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4854)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4870)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2019-4871)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5508)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5511)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5535)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5541)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5542)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5543)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5559)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5642)

Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2020-5644)

Oracle Linux 6 / 7 : unzip (ELSA-2015-0700)

Oracle Linux 6 / 7 : vim (ELSA-2016-2972)

Oracle Linux 6 / 7 : wget (ELSA-2014-1764)

Oracle Linux 6 / 7 : wireshark (ELSA-2014-1676)

Oracle Linux 6 / 7 : xerces-j2 (ELSA-2014-1319)

Oracle Linux 6 / 7 : xorg-x11-server (ELSA-2014-1983)

Oracle Linux 6 / 7 : xorg-x11-server (ELSA-2015-0797)

Oracle Linux 6 : 389-ds-base (ELSA-2012-0813)

Oracle Linux 6 : 389-ds-base (ELSA-2012-0997)

Oracle Linux 6 : 389-ds-base (ELSA-2013-0503)

Oracle Linux 6 : 389-ds-base (ELSA-2013-0628)

Oracle Linux 6 : 389-ds-base (ELSA-2013-0742)

Oracle Linux 6 : 389-ds-base (ELSA-2013-1119)

Oracle Linux 6 : 389-ds-base (ELSA-2013-1182)

Oracle Linux 6 : 389-ds-base (ELSA-2013-1752)

Oracle Linux 6 : 389-ds-base (ELSA-2014-0292)

Oracle Linux 6 : 389-ds-base (ELSA-2015-0628)

Oracle Linux 6 : 389-ds-base (ELSA-2016-2765)

Oracle Linux 6 : 389-ds-base (ELSA-2017-0893)

Oracle Linux 6 : 389-ds-base (ELSA-2018-0515)

Oracle Linux 6 : 389-ds-base (ELSA-2018-1364)

Oracle Linux 6 : abrt (ELSA-2015-1210)

Oracle Linux 6 : abrt / btparser / libreport / python-meh (ELSA-2012-0841)

Oracle Linux 6 : abrt / libreport (ELSA-2013-0215)

Oracle Linux 6 : augeas (ELSA-2013-1537)

Oracle Linux 6 : augeas (ELSA-2014-0044)

Oracle Linux 6 : autofs (ELSA-2015-1344)

Oracle Linux 6 : automake (ELSA-2013-0526)

Oracle Linux 6 : axis (ELSA-2013-0269)

Oracle Linux 6 : bash (ELSA-2014-3075)

Oracle Linux 6 : bash (ELSA-2014-3093) (Shellshock)

Oracle Linux 6 : bash (ELSA-2017-0725)

Oracle Linux 6 : bind (ELSA-2010-0975)

Oracle Linux 6 : bind (ELSA-2012-1268)

Oracle Linux 6 : bind (ELSA-2012-1549)

Oracle Linux 6 : bind (ELSA-2013-0550)

Oracle Linux 6 : bind (ELSA-2013-0689)

Oracle Linux 6 : bind (ELSA-2013-1114)

Oracle Linux 6 : bind (ELSA-2014-0043)

Oracle Linux 6 : bind (ELSA-2015-1471)

Oracle Linux 6 : bind (ELSA-2017-1105)

Oracle Linux 6 : bind (ELSA-2017-1202)

Oracle Linux 6 : bind (ELSA-2017-1679)

Oracle Linux 6 : bind (ELSA-2018-0101)

Oracle Linux 6 : bind (ELSA-2018-2571)

Oracle Linux 6 : bind (ELSA-2019-1492)

Oracle Linux 6 : bind-dyndb-ldap (ELSA-2012-0683)

Oracle Linux 6 : bind-dyndb-ldap (ELSA-2012-1139)

Oracle Linux 6 : busybox (ELSA-2012-0810)

Oracle Linux 6 : busybox (ELSA-2013-1732)

Oracle Linux 6 : bzip2 (ELSA-2010-0858)

Oracle Linux 6 : ca-certificates (ELSA-2011-1248)

Oracle Linux 6 : ca-certificates (ELSA-2013-1866)

Oracle Linux 6 : ccid (ELSA-2013-0523)

Oracle Linux 6 : cifs-utils (ELSA-2012-0902)

Oracle Linux 6 : cifs-utils / samba (ELSA-2011-1221)

Oracle Linux 6 : Core X11 clients (ELSA-2013-0502)

Oracle Linux 6 : coreutils (ELSA-2013-1652)

Oracle Linux 6 : coreutils (ELSA-2017-0654)

Oracle Linux 6 : cups (ELSA-2010-0866)

Oracle Linux 6 : cups (ELSA-2014-1388)

Oracle Linux 6 : curl (ELSA-2014-0561)

Oracle Linux 6 : curl (ELSA-2015-1254)

Oracle Linux 6 : curl (ELSA-2017-0847)

Oracle Linux 6 : curl (ELSA-2020-5561)

Oracle Linux 6 : cvs (ELSA-2010-0918)

Oracle Linux 6 : dbus (ELSA-2012-1261)

Oracle Linux 6 : dbus (ELSA-2019-1726)

Oracle Linux 6 : dhcp (ELSA-2010-0923)

Oracle Linux 6 : dhcp (ELSA-2011-0256)

Oracle Linux 6 : dhcp (ELSA-2011-1819)

Oracle Linux 6 : dhcp (ELSA-2012-1141)

Oracle Linux 6 : dhcp (ELSA-2013-0504)

Oracle Linux 6 : dhcp (ELSA-2018-0469)

Oracle Linux 6 : dhcp (ELSA-2018-1454)

Oracle Linux 6 : ding-libs / sssd (ELSA-2018-1877)

Oracle Linux 6 : dnsmasq (ELSA-2013-0277)

Oracle Linux 6 : dnsmasq (ELSA-2017-2838)

Oracle Linux 6 : dovecot (ELSA-2013-0520)

Oracle Linux 6 : dovecot (ELSA-2019-2885)

Oracle Linux 6 : dracut (ELSA-2013-1674)

Oracle Linux 6 : evince (ELSA-2011-0009)

Oracle Linux 6 : evolution (ELSA-2013-0516)

Oracle Linux 6 : evolution (ELSA-2013-1540)

Oracle Linux 6 : file (ELSA-2014-1606)

Oracle Linux 6 : file (ELSA-2016-0760)

Oracle Linux 6 : firefox (ELSA-2017-1104)

Oracle Linux 6 : firefox (ELSA-2018-0526)

Oracle Linux 6 : firefox (ELSA-2018-1098)

Oracle Linux 6 : firefox (ELSA-2018-1414)

Oracle Linux 6 : firefox (ELSA-2018-3006)

Oracle Linux 6 : firefox (ELSA-2018-3831)

Oracle Linux 6 : firefox (ELSA-2019-0218)

Oracle Linux 6 : firefox (ELSA-2019-0373)

Oracle Linux 6 : firefox (ELSA-2019-0623)

Oracle Linux 6 : firefox (ELSA-2019-0672)

Oracle Linux 6 : firefox (ELSA-2019-1267)

Oracle Linux 6 : firefox (ELSA-2019-1604)

Oracle Linux 6 : firefox (ELSA-2019-1765)

Oracle Linux 6 : firefox (ELSA-2019-2694)

Oracle Linux 6 : foomatic (ELSA-2011-1110)

Oracle Linux 6 : foomatic (ELSA-2016-0491)

Oracle Linux 6 : freeradius (ELSA-2012-1326)

Oracle Linux 6 : freeradius (ELSA-2015-1287)

Oracle Linux 6 : freeradius (ELSA-2017-1759)

Oracle Linux 6 : freetype (ELSA-2011-1085)

Oracle Linux 6 : freetype (ELSA-2019-4254)

Oracle Linux 6 : fuse (ELSA-2011-1083)

Oracle Linux 6 : gc (ELSA-2013-1500)

Oracle Linux 6 : gdb (ELSA-2013-0522)

Oracle Linux 6 : gdm (ELSA-2011-0395)

Oracle Linux 6 : gegl (ELSA-2012-1455)

Oracle Linux 6 : ghostscript (ELSA-2017-0014)

Oracle Linux 6 : ghostscript (ELSA-2018-3760)

Oracle Linux 6 : gimp (ELSA-2011-0839)

Oracle Linux 6 : gimp (ELSA-2012-1180)

Oracle Linux 6 : git (ELSA-2010-1003)

Oracle Linux 6 : git (ELSA-2013-0589)

Oracle Linux 6 : git (ELSA-2017-2485)

Oracle Linux 6 : git (ELSA-2020-0316)

Oracle Linux 6 : glibc (ELSA-2010-0872)

Oracle Linux 6 : glibc (ELSA-2011-0413)

Oracle Linux 6 : glibc (ELSA-2012-0058)

Oracle Linux 6 : glibc (ELSA-2012-0393)

Oracle Linux 6 : glibc (ELSA-2012-1098)

Oracle Linux 6 : glibc (ELSA-2012-1208)

Oracle Linux 6 : glibc (ELSA-2013-1605)

Oracle Linux 6 : glibc (ELSA-2014-1391)

Oracle Linux 6 : glibc (ELSA-2015-0016)

Oracle Linux 6 : glibc (ELSA-2015-0863)

Oracle Linux 6 : glibc (ELSA-2016-0175)

Oracle Linux 6 : glibc (ELSA-2017-0680)

Oracle Linux 6 : glibc (ELSA-2017-1480) (Stack Clash)

Oracle Linux 6 : glibc (ELSA-2018-1879)

Oracle Linux 6 : glusterfs (ELSA-2018-2892)

Oracle Linux 6 : gnupg2 (ELSA-2018-2180)

Oracle Linux 6 : gnutls (ELSA-2012-0429)

Oracle Linux 6 : gnutls (ELSA-2014-0246)

Oracle Linux 6 : gnutls (ELSA-2014-0595)

Oracle Linux 6 : gnutls (ELSA-2015-1457)

Oracle Linux 6 : gnutls (ELSA-2017-0574)

Oracle Linux 6 : grep (ELSA-2015-1447)

Oracle Linux 6 : gstreamer-plugins-bad-free (ELSA-2016-2974)

Oracle Linux 6 : gstreamer-plugins-good (ELSA-2016-2975)

Oracle Linux 6 : hivex (ELSA-2015-1378)

Oracle Linux 6 : hplip (ELSA-2013-0500)

Oracle Linux 6 : hplip (ELSA-2013-1274)

Oracle Linux 6 : httpd (ELSA-2011-1391)

Oracle Linux 6 : httpd (ELSA-2012-0128)

Oracle Linux 6 : httpd (ELSA-2013-0512)

Oracle Linux 6 : httpd (ELSA-2014-0370)

Oracle Linux 6 : httpd (ELSA-2015-1668)

Oracle Linux 6 : httpd (ELSA-2017-1721)

Oracle Linux 6 : httpd (ELSA-2017-2478)

Oracle Linux 6 : httpd (ELSA-2017-2972) (Optionsbleed)

Oracle Linux 6 : icedtea-web (ELSA-2011-1100)

Oracle Linux 6 : icedtea-web (ELSA-2011-1441)

Oracle Linux 6 : icedtea-web (ELSA-2012-1132)

Oracle Linux 6 : icedtea-web (ELSA-2012-1434)

Oracle Linux 6 : icedtea-web (ELSA-2013-0753)

Oracle Linux 6 : icedtea-web (ELSA-2016-0778)

Oracle Linux 6 : icu (ELSA-2020-0896)

Oracle Linux 6 : ImageMagick (ELSA-2012-0544)

Oracle Linux 6 : ipa (ELSA-2013-0188)

Oracle Linux 6 : ipa (ELSA-2013-0528)

Oracle Linux 6 : ipa (ELSA-2015-1462)

Oracle Linux 6 : ipmitool (ELSA-2011-1814)

Oracle Linux 6 : ipmitool (ELSA-2020-1331)

Oracle Linux 6 : jakarta-commons-collections (ELSA-2015-2521)

Oracle Linux 6 : jasper (ELSA-2011-1807)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2011-0856)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2012-0135)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2012-0729)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2012-1221)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2012-1384) (ROBOT)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2013-0245)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2013-0273)

Oracle Linux 6 : java-1.6.0-openjdk (ELSA-2013-0605)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2012-1009)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2012-1223)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2012-1386) (ROBOT)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2013-0602)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2013-0751)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2013-0957)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2013-1451)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2014-0026)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2014-0406)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2016-0053) (SLOTH)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2016-0511)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2016-0675)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2018-1270)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2018-1647) (Spectre)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2018-2283)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2018-3409)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2019-0462)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2019-0790)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2019-1840)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2019-3158)

Oracle Linux 6 : java-1.7.0-openjdk (ELSA-2020-0632)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2014-1636)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2015-0069) (POODLE)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2016-0050) (SLOTH)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2016-0514)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2016-0651)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2017-1109)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2018-1188)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2018-1650) (Spectre)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2018-2241)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2018-2943)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2019-0416)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2019-0774)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2019-1811)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2019-3136)

Oracle Linux 6 : java-1.8.0-openjdk (ELSA-2020-0157)

Oracle Linux 6 : kdelibs (ELSA-2011-0464)

Oracle Linux 6 : kdelibs (ELSA-2011-1364)

Oracle Linux 6 : kdelibs (ELSA-2012-1416)

Oracle Linux 6 : kdelibs (ELSA-2012-1418)

Oracle Linux 6 : kdenetwork (ELSA-2011-0465)

Oracle Linux 6 : kernel (ELSA-2011-0007)

Oracle Linux 6 : kernel (ELSA-2011-0283)

Oracle Linux 6 : kernel (ELSA-2011-0329)

Oracle Linux 6 : kernel (ELSA-2011-0421)

Oracle Linux 6 : kernel (ELSA-2011-0498)

Oracle Linux 6 : kernel (ELSA-2011-0836)

Oracle Linux 6 : kernel (ELSA-2011-0928)

Oracle Linux 6 : kernel (ELSA-2011-1189)

Oracle Linux 6 : kernel (ELSA-2011-1350)

Oracle Linux 6 : kernel (ELSA-2011-1465)

Oracle Linux 6 : kernel (ELSA-2011-1849)

Oracle Linux 6 : kernel (ELSA-2012-0052)

Oracle Linux 6 : kernel (ELSA-2012-0350)

Oracle Linux 6 : kernel (ELSA-2012-0481)

Oracle Linux 6 : kernel (ELSA-2012-0571)

Oracle Linux 6 : kernel (ELSA-2012-0743)

Oracle Linux 6 : kernel (ELSA-2012-0862)

Oracle Linux 6 : kernel (ELSA-2012-1064)

Oracle Linux 6 : kernel (ELSA-2012-1156)

Oracle Linux 6 : kernel (ELSA-2012-1304)

Oracle Linux 6 : kernel (ELSA-2012-1366)

Oracle Linux 6 : kernel (ELSA-2012-1426)

Oracle Linux 6 : kernel (ELSA-2012-1580)

Oracle Linux 6 : kernel (ELSA-2013-0223)

Oracle Linux 6 : kernel (ELSA-2013-0496)

Oracle Linux 6 : kernel (ELSA-2013-0567)

Oracle Linux 6 : kernel (ELSA-2013-0630)

Oracle Linux 6 : kernel (ELSA-2013-0744)

Oracle Linux 6 : kernel (ELSA-2013-0830)

Oracle Linux 6 : kernel (ELSA-2013-0911)

Oracle Linux 6 : kernel (ELSA-2013-1051)

Oracle Linux 6 : kernel (ELSA-2013-1173)

Oracle Linux 6 : kernel (ELSA-2013-1436)

Oracle Linux 6 : Kernel (ELSA-2013-1645)

Oracle Linux 6 : kernel (ELSA-2013-1801)

Oracle Linux 6 : kernel (ELSA-2014-0159)

Oracle Linux 6 : kernel (ELSA-2014-0328)

Oracle Linux 6 : kernel (ELSA-2014-0475)

Oracle Linux 6 : kernel (ELSA-2014-0771)

Oracle Linux 6 : kernel (ELSA-2014-0924)

Oracle Linux 6 : kernel (ELSA-2014-0981)

Oracle Linux 6 : kernel (ELSA-2014-1167)

Oracle Linux 6 : kernel (ELSA-2014-1392)

Oracle Linux 6 : kernel (ELSA-2014-1843)

Oracle Linux 6 : kernel (ELSA-2014-1997)

Oracle Linux 6 : kernel (ELSA-2015-0087)

Oracle Linux 6 : kernel (ELSA-2015-0674)

Oracle Linux 6 : kernel (ELSA-2015-0864)

Oracle Linux 6 : kernel (ELSA-2015-1081)

Oracle Linux 6 : kernel (ELSA-2015-1221)

Oracle Linux 6 : kernel (ELSA-2015-1272)

Oracle Linux 6 : kernel (ELSA-2015-1623)

Oracle Linux 6 : kernel (ELSA-2015-2636)

Oracle Linux 6 : kernel (ELSA-2016-0494)

Oracle Linux 6 : kernel (ELSA-2016-0715)

Oracle Linux 6 : kernel (ELSA-2016-0855)

Oracle Linux 6 : kernel (ELSA-2016-1406)

Oracle Linux 6 : kernel (ELSA-2016-1664)

Oracle Linux 6 : kernel (ELSA-2016-2006)

Oracle Linux 6 : kernel (ELSA-2016-2105) (Dirty COW)

Oracle Linux 6 : kernel (ELSA-2016-2766)

Oracle Linux 6 : kernel (ELSA-2017-0036)

Oracle Linux 6 : kernel (ELSA-2017-0293)

Oracle Linux 6 : kernel (ELSA-2017-0307)

Oracle Linux 6 : kernel (ELSA-2017-0817)

Oracle Linux 6 : kernel (ELSA-2017-0892)

Oracle Linux 6 : kernel (ELSA-2017-0892-1)

Oracle Linux 6 : kernel (ELSA-2017-1372)

Oracle Linux 6 : kernel (ELSA-2017-1486) (Stack Clash)

Oracle Linux 6 : kernel (ELSA-2017-1723)

Oracle Linux 6 : kernel (ELSA-2017-2681) (BlueBorne)

Oracle Linux 6 : kernel (ELSA-2017-2795)

Oracle Linux 6 : kernel (ELSA-2017-2863)

Oracle Linux 6 : kernel (ELSA-2017-3200)

Oracle Linux 6 : kernel (ELSA-2018-0008) (Meltdown) (Spectre)

Oracle Linux 6 : kernel (ELSA-2018-0512) (Meltdown) (Spectre)

Oracle Linux 6 : kernel (ELSA-2018-1319) (Meltdown)

Oracle Linux 6 : kernel (ELSA-2018-1651) (Spectre)

Oracle Linux 6 : kernel (ELSA-2018-1854) (Spectre)

Oracle Linux 6 : kernel (ELSA-2018-2164) (Spectre)

Oracle Linux 6 : kernel (ELSA-2018-2390) (Foreshadow)

Oracle Linux 6 : kernel (ELSA-2018-2846)

Oracle Linux 6 : kernel (ELSA-2019-0415)

Oracle Linux 6 : kernel (ELSA-2019-0717)

Oracle Linux 6 : kernel (ELSA-2019-1169) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 : kernel (ELSA-2019-1488) (SACK Panic) (SACK Slowness)

Oracle Linux 6 : kernel (ELSA-2019-2473)

Oracle Linux 6 : kernel (ELSA-2019-2736)

Oracle Linux 6 : kernel (ELSA-2019-2863)

Oracle Linux 6 : kernel (ELSA-2019-3836)

Oracle Linux 6 : kernel (ELSA-2019-3878)

Oracle Linux 6 : kernel (ELSA-2019-4256)

Oracle Linux 6 : kernel (ELSA-2020-0790)

Oracle Linux 6 : krb5 (ELSA-2011-0200)

Oracle Linux 6 : krb5 (ELSA-2011-0356)

Oracle Linux 6 : krb5 (ELSA-2011-0447)

Oracle Linux 6 : krb5 (ELSA-2011-1379)

Oracle Linux 6 : krb5 (ELSA-2011-1790)

Oracle Linux 6 : krb5 (ELSA-2012-1131)

Oracle Linux 6 : krb5 (ELSA-2013-0656)

Oracle Linux 6 : krb5 (ELSA-2013-0748)

Oracle Linux 6 : krb5 (ELSA-2014-1389)

Oracle Linux 6 : krb5 (ELSA-2015-0794)

Oracle Linux 6 : krb5 (ELSA-2016-0493)

Oracle Linux 6 : krb5-appl (ELSA-2011-0920)

Oracle Linux 6 : krb5-appl (ELSA-2011-1852)

Oracle Linux 6 : krb5-appl (ELSA-2020-1349)

Oracle Linux 6 : ksh (ELSA-2020-0515)

Oracle Linux 6 : libarchive (ELSA-2011-1507)

Oracle Linux 6 : libarchive (ELSA-2016-1850)

Oracle Linux 6 : libcgroup (ELSA-2011-0320)

Oracle Linux 6 : libguestfs (ELSA-2012-0774)

Oracle Linux 6 : libguestfs (ELSA-2013-1536)

Oracle Linux 6 : libguestfs (ELSA-2017-0564)

Oracle Linux 6 : libjpeg-turbo (ELSA-2013-1803)

Oracle Linux 6 : libpng (ELSA-2011-1105)

Oracle Linux 6 : libpng (ELSA-2015-2594)

Oracle Linux 6 : libproxy (ELSA-2012-1461)

Oracle Linux 6 : librelp (ELSA-2018-1225)

Oracle Linux 6 : libreoffice (ELSA-2012-1135)

Oracle Linux 6 : libreoffice (ELSA-2015-1458)

Oracle Linux 6 : libreoffice (ELSA-2017-0979)

Oracle Linux 6 : libreoffice (ELSA-2018-0517)

Oracle Linux 6 : libreport (ELSA-2015-2504)

Oracle Linux 6 : librsvg2 (ELSA-2011-1289)

Oracle Linux 6 : librsvg2 (ELSA-2014-0127)

Oracle Linux 6 : libsndfile (ELSA-2011-1084)

Oracle Linux 6 : libsoup (ELSA-2011-1102)

Oracle Linux 6 : libssh2 (ELSA-2019-1652)

Oracle Linux 6 : libssh2 (ELSA-2019-4693)

Oracle Linux 6 : libtar (ELSA-2013-1418)

Oracle Linux 6 : libtasn1 (ELSA-2012-0427)

Oracle Linux 6 : libtasn1 (ELSA-2014-0596)

Oracle Linux 6 : libtiff (ELSA-2011-0452)

Oracle Linux 6 : libtiff (ELSA-2014-0222)

Oracle Linux 6 : libtiff (ELSA-2016-1547)

Oracle Linux 6 : libtirpc (ELSA-2013-0884)

Oracle Linux 6 : libtirpc (ELSA-2017-1268)

Oracle Linux 6 : libuser (ELSA-2015-1482)

Oracle Linux 6 : libvirt (ELSA-2011-0479)

Oracle Linux 6 : libvirt (ELSA-2011-1197)

Oracle Linux 6 : libvirt (ELSA-2012-0748)

Oracle Linux 6 : libvirt (ELSA-2012-1202)

Oracle Linux 6 : libvirt (ELSA-2012-1359)

Oracle Linux 6 : libvirt (ELSA-2013-0199)

Oracle Linux 6 : libvirt (ELSA-2013-0276)

Oracle Linux 6 : libvirt (ELSA-2013-0831)

Oracle Linux 6 : libvirt (ELSA-2013-1272)

Oracle Linux 6 : libvirt (ELSA-2014-0103)

Oracle Linux 6 : libvirt (ELSA-2014-0560)

Oracle Linux 6 : libvirt (ELSA-2014-1873)

Oracle Linux 6 : libvirt (ELSA-2018-0030) (Spectre)

Oracle Linux 6 : libvirt (ELSA-2018-1669) (Spectre)

Oracle Linux 6 : libvirt (ELSA-2018-1929)

Oracle Linux 6 : libvirt (ELSA-2019-1180) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 : libvirt (ELSA-2019-1578)

Oracle Linux 6 : libvorbis (ELSA-2018-0649)

Oracle Linux 6 : libvpx (ELSA-2010-0999)

Oracle Linux 6 : libxml2 (ELSA-2012-0018)

Oracle Linux 6 : libxml2 (ELSA-2014-0513)

Oracle Linux 6 : libxml2 (ELSA-2015-1419)

Oracle Linux 6 : libxml2 (ELSA-2015-2549)

Oracle Linux 6 : logrotate (ELSA-2011-0407)

Oracle Linux 6 : mailman (ELSA-2011-0308)

Oracle Linux 6 : mailman (ELSA-2015-1417)

Oracle Linux 6 : mailman (ELSA-2018-0504)

Oracle Linux 6 : memcached (ELSA-2016-2820)

Oracle Linux 6 : mesa (ELSA-2013-0897)

Oracle Linux 6 : microcode\_ctl (ELSA-2018-0013) (Spectre)

Oracle Linux 6 : microcode\_ctl (ELSA-2018-4019) (Spectre)

Oracle Linux 6 : microcode\_ctl (ELSA-2019-4868)

Oracle Linux 6 : mingw32-libxml2 (ELSA-2013-0217)

Oracle Linux 6 : mod\_auth\_mellon (ELSA-2014-1803)

Oracle Linux 6 : mod\_auth\_mysql (ELSA-2010-1002)

Oracle Linux 6 : mod\_perl (ELSA-2018-2737)

Oracle Linux 6 : mod\_wsgi (ELSA-2014-0788)

Oracle Linux 6 : mutt (ELSA-2011-0959)

Oracle Linux 6 : mutt (ELSA-2014-0304)

Oracle Linux 6 : mysql (ELSA-2011-0164)

Oracle Linux 6 : mysql (ELSA-2012-0105)

Oracle Linux 6 : mysql (ELSA-2012-0874)

Oracle Linux 6 : mysql (ELSA-2012-1462)

Oracle Linux 6 : mysql (ELSA-2012-1551)

Oracle Linux 6 : mysql (ELSA-2013-0219)

Oracle Linux 6 : mysql (ELSA-2013-0772)

Oracle Linux 6 : mysql (ELSA-2014-0164)

Oracle Linux 6 : mysql (ELSA-2017-0184)

Oracle Linux 6 : net-snmp (ELSA-2012-0876)

Oracle Linux 6 : net-snmp (ELSA-2014-0321)

Oracle Linux 6 : net-snmp (ELSA-2015-1385)

Oracle Linux 6 : NetworkManager (ELSA-2011-0930)

Oracle Linux 6 : NetworkManager (ELSA-2011-1338)

Oracle Linux 6 : nspluginwrapper (ELSA-2012-1459)

Oracle Linux 6 : nspr / nss (ELSA-2014-0917)

Oracle Linux 6 : nspr / nss / nss-softokn / nss-util (ELSA-2013-1144)

Oracle Linux 6 : nspr / nss / nss-util (ELSA-2012-0973)

Oracle Linux 6 : nspr / nss / nss-util (ELSA-2012-1091)

Oracle Linux 6 : nspr / nss / nss-util (ELSA-2013-0213)

Oracle Linux 6 : nspr / nss / nss-util (ELSA-2013-1829)

Oracle Linux 6 : nspr / nss / nss-util (ELSA-2016-0591)

Oracle Linux 6 : nss (ELSA-2010-0862)

Oracle Linux 6 : nss (ELSA-2017-1364)

Oracle Linux 6 : nss (ELSA-2018-2898)

Oracle Linux 6 : nss-pam-ldapd (ELSA-2013-0590)

Oracle Linux 6 : nss-softokn (ELSA-2019-4152)

Oracle Linux 6 : ntp (ELSA-2015-1459)

Oracle Linux 6 : ntp (ELSA-2016-0780)

Oracle Linux 6 : ntp (ELSA-2016-3613)

Oracle Linux 6 : ntp (ELSA-2017-3071)

Oracle Linux 6 : ntp (ELSA-2018-3854)

Oracle Linux 6 : ocaml (ELSA-2017-0565)

Oracle Linux 6 : openchange (ELSA-2013-0515)

Oracle Linux 6 : openjpeg (ELSA-2012-1068)

Oracle Linux 6 : openjpeg (ELSA-2012-1283)

Oracle Linux 6 : openjpeg (ELSA-2013-1850)

Oracle Linux 6 : openjpeg (ELSA-2017-0559)

Oracle Linux 6 : openldap (ELSA-2011-0347)

Oracle Linux 6 : openldap (ELSA-2012-0899)

Oracle Linux 6 : openldap (ELSA-2012-1151)

Oracle Linux 6 : openldap (ELSA-2014-0126)

Oracle Linux 6 : openoffice.org (ELSA-2011-0183)

Oracle Linux 6 : openoffice.org (ELSA-2012-0705)

Oracle Linux 6 : openslp (ELSA-2018-2308)

Oracle Linux 6 : openslp (ELSA-2020-0199)

Oracle Linux 6 : openssh (ELSA-2012-0884)

Oracle Linux 6 : openssh (ELSA-2013-0519)

Oracle Linux 6 : openssh (ELSA-2013-1591)

Oracle Linux 6 : openssh (ELSA-2014-1552)

Oracle Linux 6 : openssh (ELSA-2016-0466)

Oracle Linux 6 : openssh (ELSA-2016-0741)

Oracle Linux 6 : openssh (ELSA-2017-0641)

Oracle Linux 6 : openssh (ELSA-2017-2563)

Oracle Linux 6 : openssh (ELSA-2019-0711)

Oracle Linux 6 : openssl (ELSA-2010-0979)

Oracle Linux 6 : openssl (ELSA-2011-1409)

Oracle Linux 6 : openssl (ELSA-2012-0059)

Oracle Linux 6 : openssl (ELSA-2014-0015)

Oracle Linux 6 : openssl (ELSA-2014-0376)

Oracle Linux 6 : openssl (ELSA-2014-0625)

Oracle Linux 6 : openssl (ELSA-2015-0715)

Oracle Linux 6 : openssl (ELSA-2016-0996)

Oracle Linux 6 : openssl (ELSA-2018-4228)

Oracle Linux 6 : openssl (ELSA-2018-4248)

Oracle Linux 6 : openssl (ELSA-2019-2471)

Oracle Linux 6 : openswan (ELSA-2010-0892)

Oracle Linux 6 : openswan (ELSA-2011-1356)

Oracle Linux 6 : pam (ELSA-2010-0891)

Oracle Linux 6 : pam (ELSA-2013-0521)

Oracle Linux 6 : pango (ELSA-2011-0309)

Oracle Linux 6 : patch (ELSA-2018-1199)

Oracle Linux 6 : pcsc-lite (ELSA-2013-0525)

Oracle Linux 6 : perl (ELSA-2011-1424)

Oracle Linux 6 : php (ELSA-2011-0195)

Oracle Linux 6 : php (ELSA-2012-1046)

Oracle Linux 6 : php (ELSA-2013-0514)

Oracle Linux 6 : php (ELSA-2013-1615)

Oracle Linux 6 : php (ELSA-2015-1218)

Oracle Linux 6 : php (ELSA-2016-1609) (httpoxy)

Oracle Linux 6 : php (ELSA-2019-3287)

Oracle Linux 6 : php-pecl-apc (ELSA-2012-0811)

Oracle Linux 6 : pidgin (ELSA-2010-0890)

Oracle Linux 6 : pidgin (ELSA-2011-1821)

Oracle Linux 6 : pidgin (ELSA-2012-1102)

Oracle Linux 6 : pidgin (ELSA-2013-0646)

Oracle Linux 6 : pidgin (ELSA-2014-0139)

Oracle Linux 6 : pixman (ELSA-2013-0687)

Oracle Linux 6 : pixman (ELSA-2013-1869)

Oracle Linux 6 : pki-core (ELSA-2013-0511)

Oracle Linux 6 : pki-core (ELSA-2015-1347)

Oracle Linux 6 : policycoreutils (ELSA-2011-0414)

Oracle Linux 6 : polkit (ELSA-2011-0455)

Oracle Linux 6 : polkit (ELSA-2013-1270)

Oracle Linux 6 : polkit (ELSA-2019-0420)

Oracle Linux 6 : poppler (ELSA-2010-0859)

Oracle Linux 6 : poppler (ELSA-2017-2550)

Oracle Linux 6 : postfix (ELSA-2011-0423)

Oracle Linux 6 : postgresql (ELSA-2015-2081)

Oracle Linux 6 : postgresql (ELSA-2016-0347)

Oracle Linux 6 : postgresql (ELSA-2017-2860)

Oracle Linux 6 : ppp (ELSA-2020-0631)

Oracle Linux 6 : procps (ELSA-2018-1777)

Oracle Linux 6 : python (ELSA-2012-0744)

Oracle Linux 6 : python (ELSA-2013-1582)

Oracle Linux 6 : python (ELSA-2015-1330)

Oracle Linux 6 : python (ELSA-2019-1467)

Oracle Linux 6 : python-imaging (ELSA-2020-0898)

Oracle Linux 6 : python-jinja2 (ELSA-2014-0747)

Oracle Linux 6 : python-paramiko (ELSA-2018-1124)

Oracle Linux 6 : python-paramiko (ELSA-2018-3406)

Oracle Linux 6 : python-paste-script (ELSA-2012-1206)

Oracle Linux 6 : python-reportlab (ELSA-2020-0197)

Oracle Linux 6 : python-sqlalchemy (ELSA-2012-0369)

Oracle Linux 6 : qemu-kvm (ELSA-2011-0345)

Oracle Linux 6 : qemu-kvm (ELSA-2011-0919)

Oracle Linux 6 : qemu-kvm (ELSA-2011-1777)

Oracle Linux 6 : qemu-kvm (ELSA-2012-0050)

Oracle Linux 6 : qemu-kvm (ELSA-2012-1234)

Oracle Linux 6 : qemu-kvm (ELSA-2013-0609)

Oracle Linux 6 : qemu-kvm (ELSA-2013-0896)

Oracle Linux 6 : qemu-kvm (ELSA-2013-1100)

Oracle Linux 6 : qemu-kvm (ELSA-2013-1553)

Oracle Linux 6 : qemu-kvm (ELSA-2014-0420)

Oracle Linux 6 : qemu-kvm (ELSA-2014-0743)

Oracle Linux 6 : qemu-kvm (ELSA-2014-1075)

Oracle Linux 6 : qemu-kvm (ELSA-2015-0867)

Oracle Linux 6 : qemu-kvm (ELSA-2015-0998) (Venom)

Oracle Linux 6 : qemu-kvm (ELSA-2015-1087)

Oracle Linux 6 : qemu-kvm (ELSA-2015-1833)

Oracle Linux 6 : qemu-kvm (ELSA-2015-1924)

Oracle Linux 6 : qemu-kvm (ELSA-2015-2694)

Oracle Linux 6 : qemu-kvm (ELSA-2016-0082)

Oracle Linux 6 : qemu-kvm (ELSA-2016-0997)

Oracle Linux 6 : qemu-kvm (ELSA-2016-1585)

Oracle Linux 6 : qemu-kvm (ELSA-2017-0309)

Oracle Linux 6 : qemu-kvm (ELSA-2017-0352)

Oracle Linux 6 : qemu-kvm (ELSA-2017-0621)

Oracle Linux 6 : qemu-kvm (ELSA-2017-1206)

Oracle Linux 6 : qemu-kvm (ELSA-2018-0024) (Spectre)

Oracle Linux 6 : qemu-kvm (ELSA-2018-0516)

Oracle Linux 6 : qemu-kvm (ELSA-2018-1660) (Spectre)

Oracle Linux 6 : qemu-kvm (ELSA-2018-2162) (Spectre)

Oracle Linux 6 : qemu-kvm (ELSA-2019-1181) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 : qemu-kvm (ELSA-2019-1650)

Oracle Linux 6 : qemu-kvm (ELSA-2019-2892)

Oracle Linux 6 : qemu-kvm (ELSA-2020-0775)

Oracle Linux 6 : qemu-kvm (ELSA-2020-1403)

Oracle Linux 6 : qpid (ELSA-2012-1269)

Oracle Linux 6 : qt (ELSA-2011-1323)

Oracle Linux 6 : qt (ELSA-2012-0880)

Oracle Linux 6 : qt (ELSA-2013-0669)

Oracle Linux 6 : quagga (ELSA-2010-0945)

Oracle Linux 6 : quagga (ELSA-2011-0406)

Oracle Linux 6 : quagga (ELSA-2012-1259)

Oracle Linux 6 : quagga (ELSA-2017-0794)

Oracle Linux 6 : raptor (ELSA-2012-0410)

Oracle Linux 6 : rdma (ELSA-2013-0509)

Oracle Linux 6 : RDMA / stack (ELSA-2013-1661)

Oracle Linux 6 : rpcbind (ELSA-2017-1267)

Oracle Linux 6 : rsync (ELSA-2011-0390)

Oracle Linux 6 : rsyslog (ELSA-2011-1247)

Oracle Linux 6 : rsyslog (ELSA-2012-0796)

Oracle Linux 6 : rsyslog7 (ELSA-2014-1654)

Oracle Linux 6 : rtkit (ELSA-2013-1282)

Oracle Linux 6 : ruby (ELSA-2011-0910)

Oracle Linux 6 : ruby (ELSA-2012-0069)

Oracle Linux 6 : ruby (ELSA-2013-0612)

Oracle Linux 6 : ruby (ELSA-2013-1764)

Oracle Linux 6 : ruby (ELSA-2014-1911)

Oracle Linux 6 : rubygems (ELSA-2013-1441)

Oracle Linux 6 : samba (ELSA-2010-0860)

Oracle Linux 6 : samba (ELSA-2013-1542)

Oracle Linux 6 : samba (ELSA-2015-0251)

Oracle Linux 6 : samba (ELSA-2016-0011)

Oracle Linux 6 : samba (ELSA-2016-0611) (Badlock)

Oracle Linux 6 : samba (ELSA-2017-0662)

Oracle Linux 6 : samba (ELSA-2017-2789)

Oracle Linux 6 : samba (ELSA-2018-1860)

Oracle Linux 6 : samba4 (ELSA-2013-0506)

Oracle Linux 6 : samba4 (ELSA-2013-1543)

Oracle Linux 6 : samba4 (ELSA-2013-1805)

Oracle Linux 6 : samba4 (ELSA-2014-0383)

Oracle Linux 6 : samba4 (ELSA-2014-1009)

Oracle Linux 6 : samba4 (ELSA-2015-0250)

Oracle Linux 6 : samba4 (ELSA-2016-0010)

Oracle Linux 6 : samba4 (ELSA-2016-0449)

Oracle Linux 6 : samba4 (ELSA-2016-1487)

Oracle Linux 6 : samba4 (ELSA-2017-0744)

Oracle Linux 6 : samba4 (ELSA-2017-1271) (SambaCry)

Oracle Linux 6 : samba4 (ELSA-2017-2791)

Oracle Linux 6 : samba4 (ELSA-2017-3278)

Oracle Linux 6 : samba4 (ELSA-2018-1883)

Oracle Linux 6 : sblim-cim-client2 (ELSA-2012-0987)

Oracle Linux 6 : setroubleshoot / setroubleshoot-plugins (ELSA-2016-1267)

Oracle Linux 6 : sos (ELSA-2012-0958)

Oracle Linux 6 : sos (ELSA-2016-0152)

Oracle Linux 6 : spice-gtk (ELSA-2012-1284)

Oracle Linux 6 : spice-gtk (ELSA-2013-1273)

Oracle Linux 6 : spice-gtk (ELSA-2020-0471)

Oracle Linux 6 : spice-gtk / spice-server (ELSA-2018-2732)

Oracle Linux 6 : spice-server (ELSA-2013-1192)

Oracle Linux 6 : spice-server (ELSA-2013-1473)

Oracle Linux 6 : spice-server (ELSA-2015-1715)

Oracle Linux 6 : spice-server (ELSA-2015-1889)

Oracle Linux 6 : spice-server (ELSA-2016-1204)

Oracle Linux 6 : spice-server (ELSA-2017-0253)

Oracle Linux 6 : spice-server (ELSA-2018-3522)

Oracle Linux 6 : spice-server (ELSA-2019-0232)

Oracle Linux 6 : spice-xpi (ELSA-2011-0426)

Oracle Linux 6 : sqlite (ELSA-2015-1634)

Oracle Linux 6 : squid (ELSA-2011-1293)

Oracle Linux 6 : squid (ELSA-2011-1791)

Oracle Linux 6 : squid (ELSA-2013-0505)

Oracle Linux 6 : squid (ELSA-2014-0597)

Oracle Linux 6 : squid (ELSA-2016-1138)

Oracle Linux 6 : squid (ELSA-2016-1573)

Oracle Linux 6 : squid34 (ELSA-2016-1140)

Oracle Linux 6 : squid34 (ELSA-2017-0183)

Oracle Linux 6 : sssd (ELSA-2013-0508)

Oracle Linux 6 : sssd (ELSA-2013-0663)

Oracle Linux 6 : sssd (ELSA-2015-2019)

Oracle Linux 6 : stunnel (ELSA-2013-0714)

Oracle Linux 6 : subversion (ELSA-2011-0258)

Oracle Linux 6 : subversion (ELSA-2011-0328)

Oracle Linux 6 : subversion (ELSA-2015-0165)

Oracle Linux 6 : subversion (ELSA-2015-1633)

Oracle Linux 6 : sudo (ELSA-2013-1701)

Oracle Linux 6 : sudo (ELSA-2015-1409)

Oracle Linux 6 : sudo (ELSA-2019-3755)

Oracle Linux 6 : sudo (ELSA-2020-0726)

Oracle Linux 6 : system-config-firewall (ELSA-2011-0953)

Oracle Linux 6 : systemtap (ELSA-2011-0842)

Oracle Linux 6 : systemtap (ELSA-2011-1088)

Oracle Linux 6 : t1lib (ELSA-2012-0062)

Oracle Linux 6 : telnet (ELSA-2020-1335)

Oracle Linux 6 : texlive (ELSA-2012-0137)

Oracle Linux 6 : thunderbird (ELSA-2010-0969)

Oracle Linux 6 : thunderbird (ELSA-2011-0311)

Oracle Linux 6 : thunderbird (ELSA-2011-0475)

Oracle Linux 6 : thunderbird (ELSA-2011-0886)

Oracle Linux 6 : thunderbird (ELSA-2011-1166)

Oracle Linux 6 : thunderbird (ELSA-2011-1342)

Oracle Linux 6 : thunderbird (ELSA-2011-1439)

Oracle Linux 6 : thunderbird (ELSA-2012-0080)

Oracle Linux 6 : thunderbird (ELSA-2012-0140)

Oracle Linux 6 : thunderbird (ELSA-2012-0388)

Oracle Linux 6 : thunderbird (ELSA-2012-0516)

Oracle Linux 6 : thunderbird (ELSA-2012-0715)

Oracle Linux 6 : thunderbird (ELSA-2012-1089)

Oracle Linux 6 : thunderbird (ELSA-2012-1211)

Oracle Linux 6 : thunderbird (ELSA-2012-1351)

Oracle Linux 6 : thunderbird (ELSA-2012-1362)

Oracle Linux 6 : thunderbird (ELSA-2012-1413)

Oracle Linux 6 : thunderbird (ELSA-2012-1483)

Oracle Linux 6 : thunderbird (ELSA-2013-0145)

Oracle Linux 6 : thunderbird (ELSA-2013-0272)

Oracle Linux 6 : thunderbird (ELSA-2013-0627)

Oracle Linux 6 : thunderbird (ELSA-2013-0697)

Oracle Linux 6 : thunderbird (ELSA-2013-0821)

Oracle Linux 6 : thunderbird (ELSA-2013-0982)

Oracle Linux 6 : thunderbird (ELSA-2013-1142)

Oracle Linux 6 : thunderbird (ELSA-2013-1269)

Oracle Linux 6 : thunderbird (ELSA-2013-1480)

Oracle Linux 6 : thunderbird (ELSA-2013-1823)

Oracle Linux 6 : thunderbird (ELSA-2014-0133)

Oracle Linux 6 : thunderbird (ELSA-2014-0316)

Oracle Linux 6 : thunderbird (ELSA-2014-0449)

Oracle Linux 6 : thunderbird (ELSA-2014-0742)

Oracle Linux 6 : thunderbird (ELSA-2014-0918)

Oracle Linux 6 : thunderbird (ELSA-2014-1145)

Oracle Linux 6 : thunderbird (ELSA-2014-1647)

Oracle Linux 6 : thunderbird (ELSA-2014-1924)

Oracle Linux 6 : thunderbird (ELSA-2015-0047)

Oracle Linux 6 : thunderbird (ELSA-2015-0266)

Oracle Linux 6 : thunderbird (ELSA-2018-0647)

Oracle Linux 6 : thunderbird (ELSA-2018-1726)

Oracle Linux 6 : thunderbird (ELSA-2018-2251)

Oracle Linux 6 : thunderbird (ELSA-2018-3531)

Oracle Linux 6 : thunderbird (ELSA-2019-0159)

Oracle Linux 6 : thunderbird (ELSA-2019-0269)

Oracle Linux 6 : thunderbird (ELSA-2019-0680)

Oracle Linux 6 : thunderbird (ELSA-2019-1310)

Oracle Linux 6 : thunderbird (ELSA-2019-1624)

Oracle Linux 6 : thunderbird (ELSA-2019-1777)

Oracle Linux 6 : thunderbird (ELSA-2019-2807)

Oracle Linux 6 : tigervnc (ELSA-2011-0871)

Oracle Linux 6 : tigervnc (ELSA-2017-0630)

Oracle Linux 6 : tomcat6 (ELSA-2011-0335)

Oracle Linux 6 : tomcat6 (ELSA-2011-1780)

Oracle Linux 6 : tomcat6 (ELSA-2012-0475)

Oracle Linux 6 : tomcat6 (ELSA-2013-0623)

Oracle Linux 6 : tomcat6 (ELSA-2013-0869)

Oracle Linux 6 : tomcat6 (ELSA-2013-0964)

Oracle Linux 6 : tomcat6 (ELSA-2014-0429)

Oracle Linux 6 : tomcat6 (ELSA-2014-0865)

Oracle Linux 6 : tomcat6 (ELSA-2014-1038)

Oracle Linux 6 : tomcat6 (ELSA-2015-0991)

Oracle Linux 6 : tomcat6 (ELSA-2016-0492)

Oracle Linux 6 : tomcat6 (ELSA-2016-2045) (httpoxy)

Oracle Linux 6 : tomcat6 (ELSA-2017-0527)

Oracle Linux 6 : tomcat6 (ELSA-2017-3080)

Oracle Linux 6 : tomcat6 (ELSA-2020-0912)

Oracle Linux 6 : trousers (ELSA-2014-1507)

Oracle Linux 6 : udisks (ELSA-2014-0293)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2011-2024)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2013-2577)

Oracle Linux 6 : unbreakable enterprise kernel (ELSA-2013-2583)

Oracle Linux 6 : unbreakable enterprise kernel (ELSA-2013-2587)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2014-3002)

Oracle Linux 6 : unbreakable enterprise kernel (ELSA-2014-3011)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2014-3014)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2014-3018)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2014-3021)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2014-3034)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2014-3037)

Oracle Linux 6 : unbreakable enterprise kernel (ELSA-2014-3041)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2014-3046)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3510)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3516)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3522)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3535)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3538)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3567)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3576)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3591)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3597)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3607)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3622) (BlueBorne) (Stack Clash)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3626)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3633)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3637)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2017-3658) (BlueBorne) (Stack Clash)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4020) (Meltdown) (Spectre)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4041)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4088) (Spectre)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4097)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4110) (Meltdown) (Spectre)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4145)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4172)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4214) (Foreshadow)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4234)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4250)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4269)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2018-4301)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4533)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4577)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4601)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4637) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4646)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4675) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4689) (SACK Panic) (SACK Slowness)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4742)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4777)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4812)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4839)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4855)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2019-4872)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2020-5512)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2020-5532)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2020-5560)

Oracle Linux 6 : Unbreakable Enterprise kernel (ELSA-2020-5645)

Oracle Linux 6 : util-linux-ng (ELSA-2013-0517)

Oracle Linux 6 : vim (ELSA-2019-1774)

Oracle Linux 6 : vino (ELSA-2013-0169)

Oracle Linux 6 : webkitgtk (ELSA-2011-0177)

Oracle Linux 6 : wget (ELSA-2014-0151)

Oracle Linux 6 : wireshark (ELSA-2011-0369)

Oracle Linux 6 : wireshark (ELSA-2012-0509)

Oracle Linux 6 : wireshark (ELSA-2013-1569)

Oracle Linux 6 : wireshark (ELSA-2014-0342)

Oracle Linux 6 : wireshark (ELSA-2015-1460)

Oracle Linux 6 : wireshark (ELSA-2017-0631)

Oracle Linux 6 : wpa\_supplicant (ELSA-2015-1439)

Oracle Linux 6 : wpa\_supplicant (ELSA-2017-2911) (KRACK)

Oracle Linux 6 : xerces-c (ELSA-2020-0702)

Oracle Linux 6 : xerces-j2 (ELSA-2011-0858)

Oracle Linux 6 : xinetd (ELSA-2013-0499)

Oracle Linux 6 : xmlrpc3 (ELSA-2018-1779)

Oracle Linux 6 : xorg-x11-drv-qxl (ELSA-2013-0218)

Oracle Linux 6 : xorg-x11-server (ELSA-2012-0939)

Oracle Linux 6 : xorg-x11-server (ELSA-2013-1620)

Oracle Linux 6 : yum-utils (ELSA-2018-2284)

Oracle Linux 6 : zsh (ELSA-2018-1932)

Oracle Linux 6 : zsh (ELSA-2020-0892)

Oracle Linux 7 / 8 : vim (ELSA-2019-1619)

Oracle Linux 7 : 389-ds-base (ELSA-2015-0416)

Oracle Linux 7 : 389-ds-base (ELSA-2015-0895)

Oracle Linux 7 : 389-ds-base (ELSA-2016-0204)

Oracle Linux 7 : 389-ds-base (ELSA-2016-2594)

Oracle Linux 7 : 389-ds-base (ELSA-2017-0920)

Oracle Linux 7 : 389-ds-base (ELSA-2017-2569)

Oracle Linux 7 : 389-ds-base (ELSA-2018-0163)

Oracle Linux 7 : 389-ds-base (ELSA-2018-0414)

Oracle Linux 7 : 389-ds-base (ELSA-2018-1380)

Oracle Linux 7 : 389-ds-base (ELSA-2018-2757)

Oracle Linux 7 : 389-ds-base (ELSA-2018-3127)

Oracle Linux 7 : 389-ds-base (ELSA-2019-1896)

Oracle Linux 7 : 389-ds-base (ELSA-2019-3981)

Oracle Linux 7 : abrt (ELSA-2015-1083)

Oracle Linux 7 : abrt / libreport (ELSA-2015-2505)

Oracle Linux 7 : apache-commons-beanutils (ELSA-2020-0194)

Oracle Linux 7 : apache-commons-collections (ELSA-2015-2522)

Oracle Linux 7 : augeas (ELSA-2017-2788)

Oracle Linux 7 : authconfig (ELSA-2017-2285)

Oracle Linux 7 : autofs (ELSA-2015-2417)

Oracle Linux 7 : bash (ELSA-2014-3076)

Oracle Linux 7 : bash (ELSA-2014-3092) (Shellshock)

Oracle Linux 7 : bash (ELSA-2017-1931)

Oracle Linux 7 : bind (ELSA-2015-1443)

Oracle Linux 7 : bind (ELSA-2016-2615)

Oracle Linux 7 : bind (ELSA-2017-0062)

Oracle Linux 7 : bind (ELSA-2017-0276)

Oracle Linux 7 : bind (ELSA-2017-1095)

Oracle Linux 7 : bind (ELSA-2017-1680)

Oracle Linux 7 : bind (ELSA-2018-0102)

Oracle Linux 7 : bind (ELSA-2018-2570)

Oracle Linux 7 : bind (ELSA-2019-0194)

Oracle Linux 7 : bind (ELSA-2019-1294)

Oracle Linux 7 : binutils (ELSA-2015-2079)

Oracle Linux 7 : binutils (ELSA-2018-3032)

Oracle Linux 7 : chrony (ELSA-2015-2241)

Oracle Linux 7 : cloud-init (ELSA-2019-0597)

Oracle Linux 7 : clutter (ELSA-2015-1510)

Oracle Linux 7 : cockpit (ELSA-2019-0482)

Oracle Linux 7 : corosync (ELSA-2018-1169)

Oracle Linux 7 : cpio (ELSA-2015-2108)

Oracle Linux 7 : cups-filters (ELSA-2014-1795)

Oracle Linux 7 : cups-filters (ELSA-2015-2360)

Oracle Linux 7 : curl (ELSA-2015-2159)

Oracle Linux 7 : curl (ELSA-2016-2575)

Oracle Linux 7 : curl (ELSA-2017-2016)

Oracle Linux 7 : curl (ELSA-2017-3263)

Oracle Linux 7 : curl (ELSA-2019-1880)

Oracle Linux 7 : curl (ELSA-2020-5562)

Oracle Linux 7 : curl / nss-pem (ELSA-2018-3157)

Oracle Linux 7 : dhcp (ELSA-2016-2590)

Oracle Linux 7 : dhcp (ELSA-2018-0158)

Oracle Linux 7 : dhcp (ELSA-2018-0483)

Oracle Linux 7 : dhcp (ELSA-2018-1453)

Oracle Linux 7 : dnsmasq (ELSA-2017-2836)

Oracle Linux 7 : docker-engine (ELSA-2019-4680)

Oracle Linux 7 : dovecot (ELSA-2019-2836)

Oracle Linux 7 : emacs (ELSA-2017-2771)

Oracle Linux 7 : evince (ELSA-2017-2388)

Oracle Linux 7 : file (ELSA-2015-2155)

Oracle Linux 7 : firefox (ELSA-2017-0461)

Oracle Linux 7 : firefox (ELSA-2017-0558)

Oracle Linux 7 : firefox (ELSA-2017-1106)

Oracle Linux 7 : firefox (ELSA-2018-0527)

Oracle Linux 7 : firefox (ELSA-2018-1099)

Oracle Linux 7 : firefox (ELSA-2018-1415)

Oracle Linux 7 : firefox (ELSA-2018-2113)

Oracle Linux 7 : firefox (ELSA-2018-2692)

Oracle Linux 7 : firefox (ELSA-2018-2835)

Oracle Linux 7 : firefox (ELSA-2018-2884)

Oracle Linux 7 : firefox (ELSA-2018-3005)

Oracle Linux 7 : firefox (ELSA-2018-3833)

Oracle Linux 7 : firefox (ELSA-2019-0219)

Oracle Linux 7 : firefox (ELSA-2019-0374)

Oracle Linux 7 : firefox (ELSA-2019-0622)

Oracle Linux 7 : firefox (ELSA-2019-0671)

Oracle Linux 7 : firefox (ELSA-2019-1265)

Oracle Linux 7 : firefox (ELSA-2019-1603)

Oracle Linux 7 : firefox (ELSA-2019-1763)

Oracle Linux 7 : firefox (ELSA-2019-2729)

Oracle Linux 7 : firefox (ELSA-2019-3193)

Oracle Linux 7 : firefox (ELSA-2019-4107)

Oracle Linux 7 : firefox (ELSA-2020-0085)

Oracle Linux 7 : firefox (ELSA-2020-0520)

Oracle Linux 7 : firefox (ELSA-2020-0815)

Oracle Linux 7 : firefox (ELSA-2020-1338)

Oracle Linux 7 : firefox (ELSA-2020-1420)

Oracle Linux 7 : firewalld (ELSA-2016-2597)

Oracle Linux 7 : flatpak (ELSA-2018-2766)

Oracle Linux 7 : flatpak (ELSA-2019-0375)

Oracle Linux 7 : flatpak (ELSA-2019-1024)

Oracle Linux 7 : fltk / tigervnc (ELSA-2017-2000)

Oracle Linux 7 : fontconfig (ELSA-2016-2601)

Oracle Linux 7 : freeradius (ELSA-2017-1581)

Oracle Linux 7 : freeradius (ELSA-2017-2389)

Oracle Linux 7 : freeradius (ELSA-2019-1131)

Oracle Linux 7 : freerdp (ELSA-2019-0697)

Oracle Linux 7 : fribidi (ELSA-2019-4326)

Oracle Linux 7 : gcab (ELSA-2018-0350)

Oracle Linux 7 : gcc (ELSA-2018-0849)

Oracle Linux 7 : gdm / gnome-session (ELSA-2017-2128)

Oracle Linux 7 : ghostscript (ELSA-2017-0013)

Oracle Linux 7 : ghostscript (ELSA-2017-2180)

Oracle Linux 7 : ghostscript (ELSA-2018-2918)

Oracle Linux 7 : ghostscript (ELSA-2018-3650)

Oracle Linux 7 : ghostscript (ELSA-2018-3761)

Oracle Linux 7 : ghostscript (ELSA-2018-3834)

Oracle Linux 7 : ghostscript (ELSA-2019-0229)

Oracle Linux 7 : ghostscript (ELSA-2019-0633)

Oracle Linux 7 : ghostscript (ELSA-2019-1017)

Oracle Linux 7 : ghostscript (ELSA-2019-2462)

Oracle Linux 7 : ghostscript (ELSA-2019-2586)

Oracle Linux 7 : ghostscript (ELSA-2019-3888)

Oracle Linux 7 : gimp (ELSA-2016-2589)

Oracle Linux 7 : git (ELSA-2015-2561)

Oracle Linux 7 : git (ELSA-2017-2004)

Oracle Linux 7 : git (ELSA-2017-2484)

Oracle Linux 7 : git (ELSA-2018-1957)

Oracle Linux 7 : git (ELSA-2018-3408)

Oracle Linux 7 : git (ELSA-2020-0124)

Oracle Linux 7 : glibc (ELSA-2014-2023)

Oracle Linux 7 : glibc (ELSA-2015-0327)

Oracle Linux 7 : glibc (ELSA-2015-2172)

Oracle Linux 7 : glibc (ELSA-2015-2199)

Oracle Linux 7 : glibc (ELSA-2016-0176)

Oracle Linux 7 : glibc (ELSA-2016-2573)

Oracle Linux 7 : glibc (ELSA-2017-1481) (Stack Clash)

Oracle Linux 7 : glibc (ELSA-2017-1916)

Oracle Linux 7 : glibc (ELSA-2018-0805)

Oracle Linux 7 : glusterfs (ELSA-2018-3242)

Oracle Linux 7 : GNOME / Shell (ELSA-2015-0535)

Oracle Linux 7 : gnupg2 (ELSA-2018-2181)

Oracle Linux 7 : gnutls (ELSA-2014-0684)

Oracle Linux 7 : gnutls (ELSA-2014-1846)

Oracle Linux 7 : gnutls (ELSA-2017-2292)

Oracle Linux 7 : gnutls (ELSA-2018-3050)

Oracle Linux 7 : golang (ELSA-2016-1538) (httpoxy)

Oracle Linux 7 : golang (ELSA-2017-1859)

Oracle Linux 7 : graphite2 (ELSA-2016-0594)

Oracle Linux 7 : graphite2 (ELSA-2017-1793)

Oracle Linux 7 : grep (ELSA-2015-2111)

Oracle Linux 7 : groovy (ELSA-2017-2486)

Oracle Linux 7 : grub2 (ELSA-2015-2401)

Oracle Linux 7 : grub2 (ELSA-2015-2623)

Oracle Linux 7 : gstreamer-plugins-bad-free (ELSA-2017-0018)

Oracle Linux 7 : gstreamer-plugins-good (ELSA-2017-0019)

Oracle Linux 7 : gstreamer1-plugins-bad-free (ELSA-2017-0021)

Oracle Linux 7 : gstreamer1-plugins-good (ELSA-2017-0020)

Oracle Linux 7 : gtk-vnc (ELSA-2017-2258)

Oracle Linux 7 : haproxy (ELSA-2014-1292)

Oracle Linux 7 : haproxy (ELSA-2015-1741)

Oracle Linux 7 : hivex (ELSA-2015-0301)

Oracle Linux 7 : http-parser (ELSA-2020-0703)

Oracle Linux 7 : httpcomponents-client (ELSA-2014-1146)

Oracle Linux 7 : httpd (ELSA-2014-0921)

Oracle Linux 7 : httpd (ELSA-2015-0325)

Oracle Linux 7 : httpd (ELSA-2015-1667)

Oracle Linux 7 : httpd (ELSA-2016-1422) (httpoxy)

Oracle Linux 7 : httpd (ELSA-2017-0906)

Oracle Linux 7 : httpd (ELSA-2017-2479)

Oracle Linux 7 : httpd (ELSA-2017-2882) (Optionsbleed)

Oracle Linux 7 : httpd (ELSA-2019-1898)

Oracle Linux 7 : icedtea-web (ELSA-2019-2003)

Oracle Linux 7 : icoutils (ELSA-2017-0837)

Oracle Linux 7 : icu (ELSA-2020-0897)

Oracle Linux 7 : ipa (ELSA-2015-0442)

Oracle Linux 7 : ipa (ELSA-2017-0001)

Oracle Linux 7 : ipa (ELSA-2017-0388)

Oracle Linux 7 : ipa (ELSA-2020-0378)

Oracle Linux 7 : ipa / slapi-nis (ELSA-2015-0728)

Oracle Linux 7 : ipmitool (ELSA-2020-0984)

Oracle Linux 7 : ipsilon (ELSA-2016-2809)

Oracle Linux 7 : jasper (ELSA-2018-3253)

Oracle Linux 7 : java-1.6.0-openjdk (ELSA-2014-0685)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2014-0675)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2018-1278)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2018-1648) (Spectre)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2018-2286)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2018-3350)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2019-0464)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2019-0791)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2019-1839)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2019-3157)

Oracle Linux 7 : java-1.7.0-openjdk (ELSA-2020-0541)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2016-0049) (SLOTH)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2016-0513)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2016-0650)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2017-1108)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2018-1191)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2018-1649) (Spectre)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2018-2242)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2018-2942)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2019-0435)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2019-0775)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2019-1815)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2019-3128)

Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2020-0196)

Oracle Linux 7 : java-11-openjdk (ELSA-2018-3521)

Oracle Linux 7 : java-11-openjdk (ELSA-2019-0436)

Oracle Linux 7 : java-11-openjdk (ELSA-2019-0778)

Oracle Linux 7 : java-11-openjdk (ELSA-2019-1810)

Oracle Linux 7 : java-11-openjdk (ELSA-2019-3127)

Oracle Linux 7 : java-11-openjdk (ELSA-2020-0122)

Oracle Linux 7 : json-c (ELSA-2014-0703)

Oracle Linux 7 : jss (ELSA-2019-3067)

Oracle Linux 7 : kde-settings / kdelibs (ELSA-2019-2606)

Oracle Linux 7 : kdelibs (ELSA-2017-1264)

Oracle Linux 7 : kdenetwork (ELSA-2014-1827)

Oracle Linux 7 : keepalived (ELSA-2019-0022)

Oracle Linux 7 : kernel (ELSA-2014-0678)

Oracle Linux 7 : kernel (ELSA-2014-0786)

Oracle Linux 7 : kernel (ELSA-2014-0923)

Oracle Linux 7 : kernel (ELSA-2014-1023)

Oracle Linux 7 : kernel (ELSA-2014-1281)

Oracle Linux 7 : kernel (ELSA-2014-1724)

Oracle Linux 7 : kernel (ELSA-2014-1971)

Oracle Linux 7 : kernel (ELSA-2014-2010)

Oracle Linux 7 : kernel (ELSA-2015-0102)

Oracle Linux 7 : kernel (ELSA-2015-0290)

Oracle Linux 7 : kernel (ELSA-2015-0726)

Oracle Linux 7 : kernel (ELSA-2015-0987)

Oracle Linux 7 : kernel (ELSA-2015-1137)

Oracle Linux 7 : kernel (ELSA-2015-1534)

Oracle Linux 7 : kernel (ELSA-2015-1778)

Oracle Linux 7 : kernel (ELSA-2015-1978)

Oracle Linux 7 : kernel (ELSA-2015-2152)

Oracle Linux 7 : kernel (ELSA-2015-2552)

Oracle Linux 7 : kernel (ELSA-2016-0064)

Oracle Linux 7 : kernel (ELSA-2016-0185)

Oracle Linux 7 : kernel (ELSA-2016-1033)

Oracle Linux 7 : kernel (ELSA-2016-1277)

Oracle Linux 7 : kernel (ELSA-2016-1539)

Oracle Linux 7 : kernel (ELSA-2016-1633)

Oracle Linux 7 : kernel (ELSA-2016-1847)

Oracle Linux 7 : kernel (ELSA-2016-2047)

Oracle Linux 7 : kernel (ELSA-2016-2098) (Dirty COW)

Oracle Linux 7 : kernel (ELSA-2016-2574)

Oracle Linux 7 : kernel (ELSA-2017-0086)

Oracle Linux 7 : kernel (ELSA-2017-0294)

Oracle Linux 7 : kernel (ELSA-2017-0294-1)

Oracle Linux 7 : kernel (ELSA-2017-0386)

Oracle Linux 7 : kernel (ELSA-2017-0386-1)

Oracle Linux 7 : kernel (ELSA-2017-0933)

Oracle Linux 7 : kernel (ELSA-2017-0933-1)

Oracle Linux 7 : kernel (ELSA-2017-1308)

Oracle Linux 7 : kernel (ELSA-2017-1308-1)

Oracle Linux 7 : kernel (ELSA-2017-1484) (Stack Clash)

Oracle Linux 7 : kernel (ELSA-2017-1484-1)

Oracle Linux 7 : kernel (ELSA-2017-1615)

Oracle Linux 7 : kernel (ELSA-2017-1615-1) (Stack Clash)

Oracle Linux 7 : kernel (ELSA-2017-1842) (Stack Clash)

Oracle Linux 7 : kernel (ELSA-2017-1842-1) (Stack Clash)

Oracle Linux 7 : kernel (ELSA-2017-2473)

Oracle Linux 7 : kernel (ELSA-2017-2473-1)

Oracle Linux 7 : kernel (ELSA-2017-2679) (BlueBorne)

Oracle Linux 7 : kernel (ELSA-2017-2679-1)

Oracle Linux 7 : kernel (ELSA-2017-2930)

Oracle Linux 7 : kernel (ELSA-2017-2930-1) (BlueBorne)

Oracle Linux 7 : kernel (ELSA-2017-3315)

Oracle Linux 7 : kernel (ELSA-2017-3315-1)

Oracle Linux 7 : kernel (ELSA-2018-0007) (Meltdown) (Spectre)

Oracle Linux 7 : kernel (ELSA-2018-0151) (Meltdown) (Spectre)

Oracle Linux 7 : kernel (ELSA-2018-0395)

Oracle Linux 7 : kernel (ELSA-2018-1062)

Oracle Linux 7 : kernel (ELSA-2018-1318)

Oracle Linux 7 : kernel (ELSA-2018-1629) (Spectre)

Oracle Linux 7 : kernel (ELSA-2018-1852)

Oracle Linux 7 : kernel (ELSA-2018-1965) (Spectre)

Oracle Linux 7 : kernel (ELSA-2018-2384) (Foreshadow)

Oracle Linux 7 : kernel (ELSA-2018-2748)

Oracle Linux 7 : kernel (ELSA-2018-3083)

Oracle Linux 7 : kernel (ELSA-2018-3651)

Oracle Linux 7 : kernel (ELSA-2019-0163)

Oracle Linux 7 : kernel (ELSA-2019-0512)

Oracle Linux 7 : kernel (ELSA-2019-0818)

Oracle Linux 7 : kernel (ELSA-2019-1168) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 7 : kernel (ELSA-2019-1481) (SACK Panic) (SACK Slowness)

Oracle Linux 7 : kernel (ELSA-2019-1873)

Oracle Linux 7 : kernel (ELSA-2019-2600)

Oracle Linux 7 : kernel (ELSA-2019-2829)

Oracle Linux 7 : kernel (ELSA-2019-3055)

Oracle Linux 7 : kernel (ELSA-2019-3834)

Oracle Linux 7 : kernel (ELSA-2019-3872)

Oracle Linux 7 : kernel (ELSA-2019-3979)

Oracle Linux 7 : kernel (ELSA-2020-0374)

Oracle Linux 7 : kernel (ELSA-2020-0834)

Oracle Linux 7 : kexec-tools (ELSA-2015-0986)

Oracle Linux 7 : krb5 (ELSA-2015-0439)

Oracle Linux 7 : krb5 (ELSA-2015-2154)

Oracle Linux 7 : krb5 (ELSA-2016-0532)

Oracle Linux 7 : krb5 (ELSA-2016-2591)

Oracle Linux 7 : krb5 (ELSA-2018-0666)

Oracle Linux 7 : krb5 (ELSA-2018-3071)

Oracle Linux 7 : ksh (ELSA-2020-0568)

Oracle Linux 7 : kubernetes (ELSA-2018-4061)

Oracle Linux 7 : libarchive (ELSA-2016-1844)

Oracle Linux 7 : libarchive (ELSA-2020-0203)

Oracle Linux 7 : libcdio (ELSA-2018-3246)

Oracle Linux 7 : libguestfs (ELSA-2016-2576)

Oracle Linux 7 : libkdcraw (ELSA-2018-3065)

Oracle Linux 7 : liblouis (ELSA-2017-3111)

Oracle Linux 7 : liblouis (ELSA-2017-3384)

Oracle Linux 7 : libmspack (ELSA-2018-3327)

Oracle Linux 7 : libndp (ELSA-2016-1086)

Oracle Linux 7 : libpng (ELSA-2015-2596)

Oracle Linux 7 : libpng12 (ELSA-2015-2595)

Oracle Linux 7 : librelp (ELSA-2018-1223)

Oracle Linux 7 : libreoffice (ELSA-2015-0377)

Oracle Linux 7 : libreoffice (ELSA-2016-2579)

Oracle Linux 7 : libreoffice (ELSA-2017-0914)

Oracle Linux 7 : libreoffice (ELSA-2017-1975)

Oracle Linux 7 : libreoffice (ELSA-2018-0418)

Oracle Linux 7 : libreswan (ELSA-2015-1154)

Oracle Linux 7 : libreswan (ELSA-2015-1979)

Oracle Linux 7 : libreswan (ELSA-2016-2603)

Oracle Linux 7 : libsoup (ELSA-2017-2459)

Oracle Linux 7 : libssh2 (ELSA-2015-2140)

Oracle Linux 7 : libssh2 (ELSA-2019-0679)

Oracle Linux 7 : libssh2 (ELSA-2019-1884)

Oracle Linux 7 : libssh2 (ELSA-2019-4692)

Oracle Linux 7 : libtasn1 (ELSA-2014-0687)

Oracle Linux 7 : libtasn1 (ELSA-2017-1860)

Oracle Linux 7 : libtiff (ELSA-2016-1546)

Oracle Linux 7 : libtirpc (ELSA-2017-1263)

Oracle Linux 7 : libuser (ELSA-2015-1483)

Oracle Linux 7 : libvirt (ELSA-2014-0914)

Oracle Linux 7 : libvirt (ELSA-2014-1352)

Oracle Linux 7 : libvirt (ELSA-2015-0008)

Oracle Linux 7 : libvirt (ELSA-2015-0323)

Oracle Linux 7 : libvirt (ELSA-2016-2577)

Oracle Linux 7 : libvirt (ELSA-2018-0029) (Spectre)

Oracle Linux 7 : libvirt (ELSA-2018-1396)

Oracle Linux 7 : libvirt (ELSA-2018-1632) (Spectre)

Oracle Linux 7 : libvirt (ELSA-2018-1997) (Spectre)

Oracle Linux 7 : libvirt (ELSA-2018-3113)

Oracle Linux 7 : libvirt (ELSA-2019-1177) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 7 : libvirt (ELSA-2019-1264)

Oracle Linux 7 : libvirt (ELSA-2019-1579)

Oracle Linux 7 : libvirt (ELSA-2019-4714) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 7 : libvncserver (ELSA-2018-1055)

Oracle Linux 7 : libvncserver (ELSA-2019-0059)

Oracle Linux 7 : libvncserver (ELSA-2020-0913)

Oracle Linux 7 : libvorbis (ELSA-2018-1058)

Oracle Linux 7 : libxml2 (ELSA-2015-0749)

Oracle Linux 7 : libxml2 (ELSA-2015-2550)

Oracle Linux 7 : log4j (ELSA-2017-2423)

Oracle Linux 7 : mailman (ELSA-2015-1153)

Oracle Linux 7 : mailman (ELSA-2018-0505)

Oracle Linux 7 : mariadb (ELSA-2014-0702)

Oracle Linux 7 : mariadb (ELSA-2014-1861)

Oracle Linux 7 : mariadb (ELSA-2015-0118)

Oracle Linux 7 : mariadb (ELSA-2015-1665) (BACKRONYM)

Oracle Linux 7 : mariadb (ELSA-2016-0534)

Oracle Linux 7 : mariadb (ELSA-2016-1602)

Oracle Linux 7 : mariadb (ELSA-2016-2595)

Oracle Linux 7 : mariadb (ELSA-2017-2192)

Oracle Linux 7 : mariadb (ELSA-2018-2439)

Oracle Linux 7 : memcached (ELSA-2016-2819)

Oracle Linux 7 : mercurial (ELSA-2016-0706)

Oracle Linux 7 : mercurial (ELSA-2017-2489)

Oracle Linux 7 : microcode\_ctl (ELSA-2018-0012) (Spectre)

Oracle Linux 7 : microcode\_ctl (ELSA-2018-4018) (Spectre)

Oracle Linux 7 : microcode\_ctl (ELSA-2019-4867)

Oracle Linux 7 : mod\_auth\_mellon (ELSA-2019-0766)

Oracle Linux 7 : mod\_nss (ELSA-2016-2602)

Oracle Linux 7 : mod\_wsgi (ELSA-2014-1091)

Oracle Linux 7 : nautilus (ELSA-2018-0223)

Oracle Linux 7 : net-snmp (ELSA-2015-2345)

Oracle Linux 7 : netcf (ELSA-2015-2248)

Oracle Linux 7 : nettle (ELSA-2016-2582)

Oracle Linux 7 : NetworkManager (ELSA-2015-2315)

Oracle Linux 7 : NetworkManager (ELSA-2016-2581)

Oracle Linux 7 : NetworkManager (ELSA-2018-3665)

Oracle Linux 7 : NetworkManager / libnl3 (ELSA-2017-2299)

Oracle Linux 7 : nspr / nss / nss-softokn / nss-util (ELSA-2016-0685)

Oracle Linux 7 : nss (ELSA-2017-1365)

Oracle Linux 7 : nss (ELSA-2018-2768)

Oracle Linux 7 : nss / nss-softokn / nss-util (ELSA-2014-1073)

Oracle Linux 7 : nss / nss-softokn / nss-util (ELSA-2019-4190)

Oracle Linux 7 : ntp (ELSA-2015-2231)

Oracle Linux 7 : ntp (ELSA-2016-2583)

Oracle Linux 7 : ntp (ELSA-2016-3612)

Oracle Linux 7 : ntp (ELSA-2018-0855)

Oracle Linux 7 : ocaml (ELSA-2016-1296)

Oracle Linux 7 : openhpi (ELSA-2015-2369)

Oracle Linux 7 : openjpeg (ELSA-2017-0838)

Oracle Linux 7 : openjpeg2 (ELSA-2020-0262)

Oracle Linux 7 : openjpeg2 (ELSA-2020-0550)

Oracle Linux 7 : openldap (ELSA-2015-2131)

Oracle Linux 7 : openldap (ELSA-2017-1852)

Oracle Linux 7 : openslp (ELSA-2018-2240)

Oracle Linux 7 : openslp (ELSA-2019-4240)

Oracle Linux 7 : openssh (ELSA-2015-0425)

Oracle Linux 7 : openssh (ELSA-2015-2088)

Oracle Linux 7 : openssh (ELSA-2016-0043)

Oracle Linux 7 : openssh (ELSA-2016-0465)

Oracle Linux 7 : openssh (ELSA-2016-2588)

Oracle Linux 7 : openssh (ELSA-2017-2029)

Oracle Linux 7 : openssh (ELSA-2018-0980)

Oracle Linux 7 : openssl (ELSA-2014-0679)

Oracle Linux 7 : openssl (ELSA-2015-0716)

Oracle Linux 7 : openssl (ELSA-2016-0722)

Oracle Linux 7 : openssl (ELSA-2018-0998)

Oracle Linux 7 : openssl (ELSA-2018-3221)

Oracle Linux 7 : openssl (ELSA-2018-4249)

Oracle Linux 7 : openssl (ELSA-2019-0483)

Oracle Linux 7 : openssl098e (ELSA-2014-0680)

Oracle Linux 7 : openwsman (ELSA-2019-0638)

Oracle Linux 7 : ovmf (ELSA-2018-3090)

Oracle Linux 7 : ovmf (ELSA-2019-0809)

Oracle Linux 7 : PackageKit (ELSA-2018-1224)

Oracle Linux 7 : pango (ELSA-2019-2571)

Oracle Linux 7 : patch (ELSA-2018-1200)

Oracle Linux 7 : patch (ELSA-2019-2964)

Oracle Linux 7 : pcre (ELSA-2015-0330)

Oracle Linux 7 : pcre (ELSA-2016-1025)

Oracle Linux 7 : pcs (ELSA-2018-1060)

Oracle Linux 7 : perl (ELSA-2019-0109)

Oracle Linux 7 : php (ELSA-2014-1013)

Oracle Linux 7 : php (ELSA-2014-1327)

Oracle Linux 7 : php (ELSA-2015-1135)

Oracle Linux 7 : php (ELSA-2016-1613) (httpoxy)

Oracle Linux 7 : php (ELSA-2016-2598)

Oracle Linux 7 : php (ELSA-2017-3221)

Oracle Linux 7 : php (ELSA-2018-0406)

Oracle Linux 7 : php (ELSA-2019-3286)

Oracle Linux 7 : pidgin (ELSA-2017-1854)

Oracle Linux 7 : pki-core (ELSA-2017-2335)

Oracle Linux 7 : pki-core (ELSA-2018-1979)

Oracle Linux 7 : plexus-archiver (ELSA-2018-1836)

Oracle Linux 7 : policycoreutils (ELSA-2018-0913)

Oracle Linux 7 : polkit (ELSA-2016-0189)

Oracle Linux 7 : polkit (ELSA-2019-0230)

Oracle Linux 7 : polkit-qt (ELSA-2014-1359)

Oracle Linux 7 : poppler (ELSA-2016-2580)

Oracle Linux 7 : poppler (ELSA-2017-2551)

Oracle Linux 7 : postgresql (ELSA-2015-2078)

Oracle Linux 7 : postgresql (ELSA-2016-0346)

Oracle Linux 7 : postgresql (ELSA-2016-2606)

Oracle Linux 7 : postgresql (ELSA-2017-1983)

Oracle Linux 7 : postgresql (ELSA-2017-2728)

Oracle Linux 7 : postgresql (ELSA-2017-3402)

Oracle Linux 7 : postgresql (ELSA-2018-2557)

Oracle Linux 7 : ppp (ELSA-2020-0630)

Oracle Linux 7 : procmail (ELSA-2017-3269)

Oracle Linux 7 : procps-ng (ELSA-2018-1700)

Oracle Linux 7 : python (ELSA-2015-2101)

Oracle Linux 7 : python (ELSA-2016-2586)

Oracle Linux 7 : python (ELSA-2017-1868)

Oracle Linux 7 : python (ELSA-2018-2123)

Oracle Linux 7 : python (ELSA-2018-3041)

Oracle Linux 7 : python (ELSA-2019-0710)

Oracle Linux 7 : python (ELSA-2019-1587)

Oracle Linux 7 : python-jinja2 (ELSA-2019-1022)

Oracle Linux 7 : python-paramiko (ELSA-2018-3347)

Oracle Linux 7 : python-pillow (ELSA-2020-0578)

Oracle Linux 7 : python-pip (ELSA-2020-0850)

Oracle Linux 7 : python-reportlab (ELSA-2020-0195)

Oracle Linux 7 : python-virtualenv (ELSA-2020-0851)

Oracle Linux 7 : qemu (ELSA-2019-4713) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 7 : qemu-kvm (ELSA-2014-0704)

Oracle Linux 7 : qemu-kvm (ELSA-2014-0927)

Oracle Linux 7 : qemu-kvm (ELSA-2014-1669)

Oracle Linux 7 : qemu-kvm (ELSA-2015-0349)

Oracle Linux 7 : qemu-kvm (ELSA-2015-0999) (Venom)

Oracle Linux 7 : qemu-kvm (ELSA-2015-1507)

Oracle Linux 7 : qemu-kvm (ELSA-2015-1793)

Oracle Linux 7 : qemu-kvm (ELSA-2015-1943)

Oracle Linux 7 : qemu-kvm (ELSA-2016-0083)

Oracle Linux 7 : qemu-kvm (ELSA-2016-0724)

Oracle Linux 7 : qemu-kvm (ELSA-2016-1606)

Oracle Linux 7 : qemu-kvm (ELSA-2016-2585)

Oracle Linux 7 : qemu-kvm (ELSA-2017-0083)

Oracle Linux 7 : qemu-kvm (ELSA-2017-0396)

Oracle Linux 7 : qemu-kvm (ELSA-2017-0987)

Oracle Linux 7 : qemu-kvm (ELSA-2017-1430)

Oracle Linux 7 : qemu-kvm (ELSA-2017-1681)

Oracle Linux 7 : qemu-kvm (ELSA-2017-1856)

Oracle Linux 7 : qemu-kvm (ELSA-2017-2445)

Oracle Linux 7 : qemu-kvm (ELSA-2017-3368)

Oracle Linux 7 : qemu-kvm (ELSA-2018-0023) (Spectre)

Oracle Linux 7 : qemu-kvm (ELSA-2018-0816)

Oracle Linux 7 : qemu-kvm (ELSA-2018-1416)

Oracle Linux 7 : qemu-kvm (ELSA-2018-1633) (Spectre)

Oracle Linux 7 : qemu-kvm (ELSA-2018-2001) (Spectre)

Oracle Linux 7 : qemu-kvm (ELSA-2018-2462)

Oracle Linux 7 : qemu-kvm (ELSA-2019-1178) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 7 : qemu-kvm (ELSA-2019-1883)

Oracle Linux 7 : qemu-kvm (ELSA-2019-2607)

Oracle Linux 7 : qemu-kvm (ELSA-2020-0366)

Oracle Linux 7 : qemu-kvm (ELSA-2020-1208)

Oracle Linux 7 : quagga (ELSA-2018-0377)

Oracle Linux 7 : rest (ELSA-2015-2237)

Oracle Linux 7 : resteasy-base (ELSA-2014-1011)

Oracle Linux 7 : resteasy-base (ELSA-2016-2604)

Oracle Linux 7 : rpcbind (ELSA-2017-1262)

Oracle Linux 7 : rpm (ELSA-2014-1976)

Oracle Linux 7 : rsyslog (ELSA-2014-1397)

Oracle Linux 7 : ruby (ELSA-2014-1912)

Oracle Linux 7 : ruby (ELSA-2018-0378)

Oracle Linux 7 : ruby (ELSA-2018-3738)

Oracle Linux 7 : ruby (ELSA-2019-1235)

Oracle Linux 7 : rubygem-bundler / rubygem-thor (ELSA-2015-2180)

Oracle Linux 7 : samba (ELSA-2014-0867)

Oracle Linux 7 : samba (ELSA-2014-1008)

Oracle Linux 7 : samba (ELSA-2015-0252)

Oracle Linux 7 : samba (ELSA-2016-0006)

Oracle Linux 7 : samba (ELSA-2016-1486)

Oracle Linux 7 : samba (ELSA-2017-1265)

Oracle Linux 7 : samba (ELSA-2017-1950)

Oracle Linux 7 : samba (ELSA-2017-2790)

Oracle Linux 7 : samba (ELSA-2017-3260)

Oracle Linux 7 : samba (ELSA-2018-3056)

Oracle Linux 7 : SDL (ELSA-2019-4024)

Oracle Linux 7 : setroubleshoot / setroubleshoot-plugins (ELSA-2016-1293)

Oracle Linux 7 : setup (ELSA-2018-3249)

Oracle Linux 7 : shim (ELSA-2014-1801)

Oracle Linux 7 : slf4j (ELSA-2018-0592)

Oracle Linux 7 : sos (ELSA-2016-0188)

Oracle Linux 7 : sos-collector (ELSA-2018-3663)

Oracle Linux 7 : spamassassin (ELSA-2018-2916)

Oracle Linux 7 : spice (ELSA-2015-1714)

Oracle Linux 7 : spice (ELSA-2015-1890)

Oracle Linux 7 : spice (ELSA-2016-1205)

Oracle Linux 7 : spice (ELSA-2017-0254)

Oracle Linux 7 : spice (ELSA-2017-2471)

Oracle Linux 7 : spice (ELSA-2019-0231)

Oracle Linux 7 : spice / spice-gtk (ELSA-2018-2731)

Oracle Linux 7 : sqlite (ELSA-2015-1635)

Oracle Linux 7 : sqlite (ELSA-2020-0227)

Oracle Linux 7 : squid (ELSA-2014-1147)

Oracle Linux 7 : squid (ELSA-2015-2378)

Oracle Linux 7 : squid (ELSA-2016-1139)

Oracle Linux 7 : squid (ELSA-2016-2600)

Oracle Linux 7 : squid (ELSA-2017-0182)

Oracle Linux 7 : sssd (ELSA-2015-2355)

Oracle Linux 7 : sssd (ELSA-2017-3379)

Oracle Linux 7 : sssd (ELSA-2018-3158)

Oracle Linux 7 : subversion (ELSA-2015-0166)

Oracle Linux 7 : subversion (ELSA-2015-1742)

Oracle Linux 7 : subversion (ELSA-2017-2480)

Oracle Linux 7 : sudo (ELSA-2016-2593)

Oracle Linux 7 : sudo (ELSA-2019-4821)

Oracle Linux 7 : sudo (ELSA-2020-0540)

Oracle Linux 7 : systemd (ELSA-2016-2610)

Oracle Linux 7 : systemd (ELSA-2018-0260)

Oracle Linux 7 : systemd (ELSA-2019-0049)

Oracle Linux 7 : systemd (ELSA-2019-0201)

Oracle Linux 7 : systemd (ELSA-2019-0368)

Oracle Linux 7 : tcpdump (ELSA-2017-1871)

Oracle Linux 7 : tcpdump (ELSA-2019-3976)

Oracle Linux 7 : telnet (ELSA-2020-1334)

Oracle Linux 7 : thunderbird (ELSA-2015-0642)

Oracle Linux 7 : thunderbird (ELSA-2018-0648)

Oracle Linux 7 : thunderbird (ELSA-2018-1725)

Oracle Linux 7 : thunderbird (ELSA-2018-2252)

Oracle Linux 7 : thunderbird (ELSA-2018-3458)

Oracle Linux 7 : thunderbird (ELSA-2018-3532)

Oracle Linux 7 : thunderbird (ELSA-2019-0160)

Oracle Linux 7 : thunderbird (ELSA-2019-0270)

Oracle Linux 7 : thunderbird (ELSA-2019-0681)

Oracle Linux 7 : thunderbird (ELSA-2019-1309)

Oracle Linux 7 : thunderbird (ELSA-2019-1626)

Oracle Linux 7 : thunderbird (ELSA-2019-1775)

Oracle Linux 7 : thunderbird (ELSA-2019-2773)

Oracle Linux 7 : thunderbird (ELSA-2019-3210)

Oracle Linux 7 : thunderbird (ELSA-2019-4148)

Oracle Linux 7 : thunderbird (ELSA-2020-0120)

Oracle Linux 7 : thunderbird (ELSA-2020-0576)

Oracle Linux 7 : thunderbird (ELSA-2020-0905)

Oracle Linux 7 : thunderbird (ELSA-2020-1489)

Oracle Linux 7 : tigervnc (ELSA-2015-2233)

Oracle Linux 7 : tomcat (ELSA-2014-0686)

Oracle Linux 7 : tomcat (ELSA-2014-0827)

Oracle Linux 7 : tomcat (ELSA-2014-1034)

Oracle Linux 7 : tomcat (ELSA-2015-0983)

Oracle Linux 7 : tomcat (ELSA-2016-2046) (httpoxy)

Oracle Linux 7 : tomcat (ELSA-2016-2599)

Oracle Linux 7 : tomcat (ELSA-2017-0935)

Oracle Linux 7 : tomcat (ELSA-2017-1809)

Oracle Linux 7 : tomcat (ELSA-2017-2247)

Oracle Linux 7 : tomcat (ELSA-2017-3081)

Oracle Linux 7 : tomcat (ELSA-2018-2921)

Oracle Linux 7 : tomcat (ELSA-2019-0485)

Oracle Linux 7 : tomcat (ELSA-2020-0855)

Oracle Linux 7 : unbound (ELSA-2015-2455)

Oracle Linux 7 : unbreakable enterprise kernel (ELSA-2014-3049)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2018-4189)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2018-4195) (Foreshadow)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2018-4242) (Foreshadow)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2018-4270)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2018-4304)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4509)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4541)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4570)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4612)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4628) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4643) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4685) (SACK Panic) (SACK Slowness)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4708)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4746)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4789)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4799)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4820)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4836)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2019-4878)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2020-5526)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2020-5528)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2020-5533)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2020-5540)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2020-5569)

Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2020-5649)

Oracle Linux 7 : util-linux (ELSA-2016-2605)

Oracle Linux 7 : util-linux (ELSA-2017-0907)

Oracle Linux 7 : wget (ELSA-2016-2587)

Oracle Linux 7 : wget (ELSA-2017-3075)

Oracle Linux 7 : wget (ELSA-2018-3052)

Oracle Linux 7 : wget (ELSA-2019-1228)

Oracle Linux 7 : wireshark (ELSA-2015-2393)

Oracle Linux 7 : wpa\_supplicant (ELSA-2014-1956)

Oracle Linux 7 : wpa\_supplicant (ELSA-2015-1090)

Oracle Linux 7 : wpa\_supplicant (ELSA-2017-2907) (KRACK)

Oracle Linux 7 : wpa\_supplicant (ELSA-2018-3107)

Oracle Linux 7 : X.org / X11 / libraries (ELSA-2017-1865)

Oracle Linux 7 : xdg-user-dirs (ELSA-2018-0842)

Oracle Linux 7 : xerces-c (ELSA-2015-1193)

Oracle Linux 7 : xerces-c (ELSA-2016-0430)

Oracle Linux 7 : xerces-c (ELSA-2018-3335)

Oracle Linux 7 : xerces-c (ELSA-2020-0704)

Oracle Linux 7 : xfsprogs (ELSA-2015-2151)

Oracle Linux 7 : xmlrpc (ELSA-2018-1780)

Oracle Linux 7 : xmlsec1 (ELSA-2017-2492)

Oracle Linux 7 : xorg-x11-server (ELSA-2018-3410)

Oracle Linux 7 : yum-utils (ELSA-2018-2285)

Oracle Linux 7 : zsh (ELSA-2018-3073)

Oracle Linux 7 : zsh (ELSA-2020-0853)

Oracle Linux 7 : zziplib (ELSA-2018-3229)

Oracle Linux 8 : .NET / Core / Enterprise / Hat / Linux / Red / on (ELSA-2019-2731)

Oracle Linux 8 : .NET / Core / Enterprise / Hat / Linux / Red / on (ELSA-2020-0130)

Oracle Linux 8 : bind (ELSA-2019-1145)

Oracle Linux 8 : bind (ELSA-2019-1714)

Oracle Linux 8 : container-tools:1.0 (ELSA-2019-4273) (Ping Flood) (Reset Flood)

Oracle Linux 8 : container-tools:ol8 (ELSA-2019-4269) (Ping Flood) (Reset Flood)

Oracle Linux 8 : container-tools:ol8 (ELSA-2020-1379)

Oracle Linux 8 : container-tools:rhel8 (ELSA-2019-0975)

Oracle Linux 8 : cyrus-imapd (ELSA-2019-1771)

Oracle Linux 8 : dotnet (ELSA-2019-1259)

Oracle Linux 8 : dovecot (ELSA-2019-2822)

Oracle Linux 8 : edk2 (ELSA-2019-0968)

Oracle Linux 8 : firefox (ELSA-2019-1269)

Oracle Linux 8 : firefox (ELSA-2019-1696)

Oracle Linux 8 : firefox (ELSA-2019-1764)

Oracle Linux 8 : firefox (ELSA-2019-2663)

Oracle Linux 8 : firefox (ELSA-2019-3196)

Oracle Linux 8 : firefox (ELSA-2019-4111)

Oracle Linux 8 : firefox (ELSA-2020-0111)

Oracle Linux 8 : firefox (ELSA-2020-1341)

Oracle Linux 8 : firefox (ELSA-2020-1406)

Oracle Linux 8 : flatpak (ELSA-2019-1143)

Oracle Linux 8 : freeradius:3.0 (ELSA-2019-1142)

Oracle Linux 8 : fribidi (ELSA-2019-4361)

Oracle Linux 8 : ghostscript (ELSA-2019-0971)

Oracle Linux 8 : ghostscript (ELSA-2019-2465)

Oracle Linux 8 : ghostscript (ELSA-2019-2591)

Oracle Linux 8 : ghostscript (ELSA-2019-3890)

Oracle Linux 8 : git (ELSA-2019-4356)

Oracle Linux 8 : go-toolset:ol8 (ELSA-2019-2726) (Ping Flood) (Reset Flood)

Oracle Linux 8 : grub2 (ELSA-2019-4869)

Oracle Linux 8 : grub2 (ELSA-2020-0335)

Oracle Linux 8 : gvfs (ELSA-2019-1517)

Oracle Linux 8 : haproxy (ELSA-2020-1288)

Oracle Linux 8 : http-parser (ELSA-2020-0708)

Oracle Linux 8 : httpd:2.4 (ELSA-2019-0980)

Oracle Linux 8 : httpd:2.4 (ELSA-2019-2893) (Internal Data Buffering)

Oracle Linux 8 : icedtea-web (ELSA-2019-2004)

Oracle Linux 8 : ipmitool (ELSA-2020-0981)

Oracle Linux 8 : java-1.8.0-openjdk (ELSA-2019-1146)

Oracle Linux 8 : java-1.8.0-openjdk (ELSA-2019-1816)

Oracle Linux 8 : java-1.8.0-openjdk (ELSA-2020-0202)

Oracle Linux 8 : java-11-openjdk (ELSA-2019-1518)

Oracle Linux 8 : java-11-openjdk (ELSA-2019-1817)

Oracle Linux 8 : java-11-openjdk (ELSA-2020-0128)

Oracle Linux 8 : kernel (ELSA-2019-1167) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 8 : kernel (ELSA-2019-1479) (SACK Panic) (SACK Slowness)

Oracle Linux 8 : kernel (ELSA-2019-1959)

Oracle Linux 8 : kernel (ELSA-2019-2411)

Oracle Linux 8 : kernel (ELSA-2019-2703)

Oracle Linux 8 : kernel (ELSA-2019-2827)

Oracle Linux 8 : kernel (ELSA-2019-3832)

Oracle Linux 8 : kernel (ELSA-2019-3871)

Oracle Linux 8 : kernel (ELSA-2020-0339)

Oracle Linux 8 : kernel (ELSA-2020-1372)

Oracle Linux 8 : libarchive (ELSA-2020-0271)

Oracle Linux 8 : libvncserver (ELSA-2020-0920)

Oracle Linux 8 : libwmf (ELSA-2019-2722)

Oracle Linux 8 : mod\_auth\_mellon (ELSA-2019-0985)

Oracle Linux 8 : mysql:8.0 (ELSA-2019-2511)

Oracle Linux 8 : nghttp2 (ELSA-2019-2692) (Data Dribble) (Resource Loop)

Oracle Linux 8 : nginx:1.14 (ELSA-2019-2799) (0-Length Headers Leak) (Data Dribble) (Resource Loop)

Oracle Linux 8 : nodejs:10 (ELSA-2019-2925) (0-Length Headers Leak) (Data Dribble) (Empty Frames Flood) (Internal Data Buffering) (Ping Flood) (Reset Flood) (Resource Loop) (Settings Flood)

Oracle Linux 8 : nodejs:10 (ELSA-2020-1317)

Oracle Linux 8 : nodejs:12 (ELSA-2020-1293)

Oracle Linux 8 : nspr / nss (ELSA-2019-1951)

Oracle Linux 8 : nss (ELSA-2019-4114)

Oracle Linux 8 : openjpeg2 (ELSA-2020-0274)

Oracle Linux 8 : pacemaker (ELSA-2019-1279)

Oracle Linux 8 : pango (ELSA-2019-2582)

Oracle Linux 8 : patch (ELSA-2019-2798)

Oracle Linux 8 : php:7.2 (ELSA-2019-3735)

Oracle Linux 8 : php:7.3 (ELSA-2019-3736)

Oracle Linux 8 : pki-deps:10.6 (ELSA-2019-1529)

Oracle Linux 8 : poppler (ELSA-2019-2713)

Oracle Linux 8 : ppp (ELSA-2020-0633)

Oracle Linux 8 : python-jinja2 (ELSA-2019-1152)

Oracle Linux 8 : python-pillow (ELSA-2020-0580)

Oracle Linux 8 : python-reportlab (ELSA-2020-0201)

Oracle Linux 8 : python27:2.7 (ELSA-2019-0981)

Oracle Linux 8 : python3 (ELSA-2019-0997)

Oracle Linux 8 : python36:3.6 (ELSA-2019-0984)

Oracle Linux 8 : redis:5 (ELSA-2019-2002)

Oracle Linux 8 : ruby:2.5 (ELSA-2019-1972)

Oracle Linux 8 : SDL (ELSA-2019-3951)

Oracle Linux 8 : squid:4 (ELSA-2019-2593)

Oracle Linux 8 : subversion:1.10 (ELSA-2019-2512)

Oracle Linux 8 : sudo (ELSA-2019-3694)

Oracle Linux 8 : sudo (ELSA-2019-4822)

Oracle Linux 8 : systemd (ELSA-2019-0990)

Oracle Linux 8 : systemd (ELSA-2020-0575)

Oracle Linux 8 : telnet (ELSA-2020-1318)

Oracle Linux 8 : thunderbird (ELSA-2019-1144)

Oracle Linux 8 : thunderbird (ELSA-2019-1308)

Oracle Linux 8 : thunderbird (ELSA-2019-1623)

Oracle Linux 8 : thunderbird (ELSA-2019-1799)

Oracle Linux 8 : thunderbird (ELSA-2019-2774)

Oracle Linux 8 : thunderbird (ELSA-2019-3237)

Oracle Linux 8 : thunderbird (ELSA-2019-4195)

Oracle Linux 8 : thunderbird (ELSA-2020-0127)

Oracle Linux 8 : thunderbird (ELSA-2020-0919)

Oracle Linux 8 : virt:ol (ELSA-2020-1358)

Oracle Linux 8 : virt:rhel (ELSA-2019-1175) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Oracle Linux 8 : virt:rhel (ELSA-2019-1268)

Oracle Linux 8 : WALinuxAgent (ELSA-2019-1527)

Oracle Linux 8 : wget (ELSA-2019-0983)

Oracle Linux Update Release

# NewStart CGSL Local Security Checks

NewStart CGSL CORE 5.04 / MAIN 5.04 : 389-ds-base Multiple Vulnerabilities (NS-SA-2019-0038)

NewStart CGSL CORE 5.04 / MAIN 5.04 : 389-ds-base Vulnerability (NS-SA-2019-0062)

NewStart CGSL CORE 5.04 / MAIN 5.04 : 389-ds-base Vulnerability (NS-SA-2019-0181)

NewStart CGSL CORE 5.04 / MAIN 5.04 : 389-ds-base Vulnerability (NS-SA-2019-0261)

NewStart CGSL CORE 5.04 / MAIN 5.04 : apache-commons-beanutils Vulnerability (NS-SA-2020-0011)

NewStart CGSL CORE 5.04 / MAIN 5.04 : bind Vulnerability (NS-SA-2019-0031)

NewStart CGSL CORE 5.04 / MAIN 5.04 : bind Vulnerability (NS-SA-2019-0063)

NewStart CGSL CORE 5.04 / MAIN 5.04 : bind Vulnerability (NS-SA-2019-0158)

NewStart CGSL CORE 5.04 / MAIN 5.04 : bind Vulnerability (NS-SA-2019-0191)

NewStart CGSL CORE 5.04 / MAIN 5.04 : binutils Multiple Vulnerabilities (NS-SA-2019-0060)

NewStart CGSL CORE 5.04 / MAIN 5.04 : binutils Multiple Vulnerabilities (NS-SA-2019-0187)

NewStart CGSL CORE 5.04 / MAIN 5.04 : blktrace Vulnerability (NS-SA-2019-0198)

NewStart CGSL CORE 5.04 / MAIN 5.04 : cockpit Vulnerability (NS-SA-2019-0066)

NewStart CGSL CORE 5.04 / MAIN 5.04 : compat-libtiff3 Vulnerability (NS-SA-2019-0194)

NewStart CGSL CORE 5.04 / MAIN 5.04 : corosync Vulnerability (NS-SA-2019-0046)

NewStart CGSL CORE 5.04 / MAIN 5.04 : curl Multiple Vulnerabilities (NS-SA-2019-0039)

NewStart CGSL CORE 5.04 / MAIN 5.04 : curl Vulnerability (NS-SA-2019-0182)

NewStart CGSL CORE 5.04 / MAIN 5.04 : curl Vulnerability (NS-SA-2019-0193)

NewStart CGSL CORE 5.04 / MAIN 5.04 : dhcp Multiple Vulnerabilities (NS-SA-2019-0021)

NewStart CGSL CORE 5.04 / MAIN 5.04 : dhcp Vulnerability (NS-SA-2019-0190)

NewStart CGSL CORE 5.04 / MAIN 5.04 : dovecot Vulnerability (NS-SA-2019-0220)

NewStart CGSL CORE 5.04 / MAIN 5.04 : elfutils Multiple Vulnerabilities (NS-SA-2019-0209)

NewStart CGSL CORE 5.04 / MAIN 5.04 : exempi Multiple Vulnerabilities (NS-SA-2019-0186)

NewStart CGSL CORE 5.04 / MAIN 5.04 : exiv2 Multiple Vulnerabilities (NS-SA-2019-0188)

NewStart CGSL CORE 5.04 / MAIN 5.04 : fence-agents Vulnerability (NS-SA-2019-0214)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0032)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0039)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0053)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0056)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0064)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0159)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0161)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0181)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0192)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0216)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0261)

NewStart CGSL CORE 5.04 / MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2020-0011)

NewStart CGSL CORE 5.04 / MAIN 5.04 : flatpak Vulnerability (NS-SA-2019-0042)

NewStart CGSL CORE 5.04 / MAIN 5.04 : flatpak Vulnerability (NS-SA-2019-0056)

NewStart CGSL CORE 5.04 / MAIN 5.04 : flatpak Vulnerability (NS-SA-2019-0080)

NewStart CGSL CORE 5.04 / MAIN 5.04 : freeradius Multiple Vulnerabilities (NS-SA-2019-0079)

NewStart CGSL CORE 5.04 / MAIN 5.04 : freerdp Multiple Vulnerabilities (NS-SA-2019-0074)

NewStart CGSL CORE 5.04 / MAIN 5.04 : freerdp Vulnerability (NS-SA-2019-0204)

NewStart CGSL CORE 5.04 / MAIN 5.04 : fribidi Vulnerability (NS-SA-2019-0264)

NewStart CGSL CORE 5.04 / MAIN 5.04 : fuse Vulnerability (NS-SA-2019-0073)

NewStart CGSL CORE 5.04 / MAIN 5.04 : gcab Vulnerability (NS-SA-2019-0020)

NewStart CGSL CORE 5.04 / MAIN 5.04 : gcc Vulnerability (NS-SA-2019-0023)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ghostscript Multiple Vulnerabilities (NS-SA-2019-0035)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ghostscript Multiple Vulnerabilities (NS-SA-2019-0046)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ghostscript Multiple Vulnerabilities (NS-SA-2019-0054)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ghostscript Multiple Vulnerabilities (NS-SA-2019-0071)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ghostscript Multiple Vulnerabilities (NS-SA-2019-0203)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ghostscript Vulnerability (NS-SA-2019-0081)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ghostscript Vulnerability (NS-SA-2019-0265)

NewStart CGSL CORE 5.04 / MAIN 5.04 : git Vulnerability (NS-SA-2019-0027)

NewStart CGSL CORE 5.04 / MAIN 5.04 : git Vulnerability (NS-SA-2019-0047)

NewStart CGSL CORE 5.04 / MAIN 5.04 : glibc Multiple Vulnerabilities (NS-SA-2019-0024)

NewStart CGSL CORE 5.04 / MAIN 5.04 : glibc Multiple Vulnerabilities (NS-SA-2019-0040)

NewStart CGSL CORE 5.04 / MAIN 5.04 : glibc Vulnerability (NS-SA-2019-0194)

NewStart CGSL CORE 5.04 / MAIN 5.04 : glusterfs Vulnerability (NS-SA-2019-0064)

NewStart CGSL CORE 5.04 / MAIN 5.04 : gnupg2 Vulnerability (NS-SA-2019-0023)

NewStart CGSL CORE 5.04 / MAIN 5.04 : gnutls Multiple Vulnerabilities (NS-SA-2019-0068)

NewStart CGSL CORE 5.04 / MAIN 5.04 : golang Multiple Vulnerabilities (NS-SA-2019-0047)

NewStart CGSL CORE 5.04 / MAIN 5.04 : gvfs Vulnerability (NS-SA-2019-0224)

NewStart CGSL CORE 5.04 / MAIN 5.04 : http-parser Multiple Vulnerabilities (NS-SA-2019-0208)

NewStart CGSL CORE 5.04 / MAIN 5.04 : httpd Multiple Vulnerabilities (NS-SA-2019-0202)

NewStart CGSL CORE 5.04 / MAIN 5.04 : httpd Vulnerability (NS-SA-2019-0182)

NewStart CGSL CORE 5.04 / MAIN 5.04 : jasper Multiple Vulnerabilities (NS-SA-2019-0069)

NewStart CGSL CORE 5.04 / MAIN 5.04 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0032)

NewStart CGSL CORE 5.04 / MAIN 5.04 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0040)

NewStart CGSL CORE 5.04 / MAIN 5.04 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0027)

NewStart CGSL CORE 5.04 / MAIN 5.04 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0035)

NewStart CGSL CORE 5.04 / MAIN 5.04 : jss Vulnerability (NS-SA-2019-0219)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kdelibs Vulnerability (NS-SA-2019-0223)

NewStart CGSL CORE 5.04 / MAIN 5.04 : keepalived Vulnerability (NS-SA-2019-0051)

NewStart CGSL CORE 5.04 / MAIN 5.04 : keepalived Vulnerability (NS-SA-2019-0219)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0025)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0034)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0044)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0070)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0077)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0078)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0162)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0180)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0200)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0221)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0264)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2020-0010)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Vulnerability (NS-SA-2019-0053)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel Vulnerability (NS-SA-2019-0057)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0028)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0049)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0074)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0076)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0162)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0183)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0189)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0222)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0266)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Vulnerability (NS-SA-2019-0055)

NewStart CGSL CORE 5.04 / MAIN 5.04 : kernel-rt Vulnerability (NS-SA-2019-0058)

NewStart CGSL CORE 5.04 / MAIN 5.04 : krb5 Multiple Vulnerabilities (NS-SA-2019-0025)

NewStart CGSL CORE 5.04 / MAIN 5.04 : krb5 Multiple Vulnerabilities (NS-SA-2019-0067)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libarchive Multiple Vulnerabilities (NS-SA-2019-0201)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libcdio Multiple Vulnerabilities (NS-SA-2019-0043)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libcgroup Vulnerability (NS-SA-2019-0186)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libgxps Multiple Vulnerabilities (NS-SA-2019-0044)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libjpeg-turbo Multiple Vulnerabilities (NS-SA-2019-0185)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libkdcraw Multiple Vulnerabilities (NS-SA-2019-0068)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libmspack Multiple Vulnerabilities (NS-SA-2019-0217)

NewStart CGSL CORE 5.04 / MAIN 5.04 : librelp Vulnerability (NS-SA-2019-0050)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libsoup Vulnerability (NS-SA-2019-0048)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libssh2 Multiple Vulnerabilities (NS-SA-2019-0073)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libssh2 Multiple Vulnerabilities (NS-SA-2019-0205)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libssh2 Vulnerability (NS-SA-2019-0183)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libtiff Multiple Vulnerabilities (NS-SA-2019-0185)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libvncserver Multiple Vulnerabilities (NS-SA-2019-0052)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libvorbis Vulnerability (NS-SA-2019-0026)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libwpd Vulnerability (NS-SA-2019-0207)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libX11 Multiple Vulnerabilities (NS-SA-2019-0196)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libXcursor Vulnerability (NS-SA-2019-0048)

NewStart CGSL CORE 5.04 / MAIN 5.04 : libxkbcommon Multiple Vulnerabilities (NS-SA-2019-0199)

NewStart CGSL CORE 5.04 / MAIN 5.04 : linux-firmware Vulnerability (NS-SA-2019-0204)

NewStart CGSL CORE 5.04 / MAIN 5.04 : mariadb Multiple Vulnerabilities (NS-SA-2019-0034)

NewStart CGSL CORE 5.04 / MAIN 5.04 : mariadb Multiple Vulnerabilities (NS-SA-2019-0197)

NewStart CGSL CORE 5.04 / MAIN 5.04 : mercurial Multiple Vulnerabilities (NS-SA-2019-0216)

NewStart CGSL CORE 5.04 / MAIN 5.04 : mod\_auth\_mellon Multiple Vulnerabilities (NS-SA-2019-0077)

NewStart CGSL CORE 5.04 / MAIN 5.04 : mod\_auth\_openidc Multiple Vulnerabilities (NS-SA-2019-0220)

NewStart CGSL CORE 5.04 / MAIN 5.04 : mutt Multiple Vulnerabilities (NS-SA-2019-0038)

NewStart CGSL CORE 5.04 / MAIN 5.04 : NetworkManager Vulnerability (NS-SA-2019-0049)

NewStart CGSL CORE 5.04 / MAIN 5.04 : nss Multiple Vulnerabilities (NS-SA-2019-0033)

NewStart CGSL CORE 5.04 / MAIN 5.04 : nss Multiple Vulnerabilities (NS-SA-2019-0193)

NewStart CGSL CORE 5.04 / MAIN 5.04 : nss Multiple Vulnerabilities (NS-SA-2019-0262)

NewStart CGSL CORE 5.04 / MAIN 5.04 : nss-softokn Vulnerability (NS-SA-2019-0262)

NewStart CGSL CORE 5.04 / MAIN 5.04 : nss-util Vulnerability (NS-SA-2019-0263)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ntp Multiple Vulnerabilities (NS-SA-2019-0029)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ntp Vulnerability (NS-SA-2019-0206)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ntp Vulnerability (NS-SA-2019-0267)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openjpeg2 Vulnerability (NS-SA-2020-0012)

NewStart CGSL CORE 5.04 / MAIN 5.04 : opensc Multiple Vulnerabilities (NS-SA-2019-0222)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openslp Vulnerability (NS-SA-2019-0022)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openslp Vulnerability (NS-SA-2019-0260)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openssh Multiple Vulnerabilities (NS-SA-2019-0036)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openssh Multiple Vulnerabilities (NS-SA-2019-0060)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openssl Multiple Vulnerabilities (NS-SA-2019-0033)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openssl Multiple Vulnerabilities (NS-SA-2019-0065)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openssl Multiple Vulnerabilities (NS-SA-2019-0206)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openssl098e Multiple Vulnerabilities (NS-SA-2019-0020)

NewStart CGSL CORE 5.04 / MAIN 5.04 : openwsman Vulnerability (NS-SA-2019-0061)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ovmf Multiple Vulnerabilities (NS-SA-2019-0218)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ovmf Vulnerability (NS-SA-2019-0066)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ovmf Vulnerability (NS-SA-2019-0076)

NewStart CGSL CORE 5.04 / MAIN 5.04 : pacemaker Multiple Vulnerabilities (NS-SA-2019-0224)

NewStart CGSL CORE 5.04 / MAIN 5.04 : PackageKit Vulnerability (NS-SA-2019-0028)

NewStart CGSL CORE 5.04 / MAIN 5.04 : pam Multiple Vulnerabilities (NS-SA-2019-0198)

NewStart CGSL CORE 5.04 / MAIN 5.04 : pango Vulnerability (NS-SA-2019-0191)

NewStart CGSL CORE 5.04 / MAIN 5.04 : patch Multiple Vulnerabilities (NS-SA-2019-0205)

NewStart CGSL CORE 5.04 / MAIN 5.04 : patch Multiple Vulnerabilities (NS-SA-2019-0223)

NewStart CGSL CORE 5.04 / MAIN 5.04 : patch Vulnerability (NS-SA-2019-0029)

NewStart CGSL CORE 5.04 / MAIN 5.04 : pcs Multiple Vulnerabilities (NS-SA-2019-0042)

NewStart CGSL CORE 5.04 / MAIN 5.04 : perl Vulnerability (NS-SA-2019-0054)

NewStart CGSL CORE 5.04 / MAIN 5.04 : perl-Archive-Tar Vulnerability (NS-SA-2019-0188)

NewStart CGSL CORE 5.04 / MAIN 5.04 : php Multiple Vulnerabilities (NS-SA-2019-0019)

NewStart CGSL CORE 5.04 / MAIN 5.04 : php Vulnerability (NS-SA-2019-0214)

NewStart CGSL CORE 5.04 / MAIN 5.04 : pki-core Vulnerability (NS-SA-2019-0063)

NewStart CGSL CORE 5.04 / MAIN 5.04 : plexus-archiver Vulnerability (NS-SA-2019-0041)

NewStart CGSL CORE 5.04 / MAIN 5.04 : policycoreutils Vulnerability (NS-SA-2019-0030)

NewStart CGSL CORE 5.04 / MAIN 5.04 : polkit Vulnerability (NS-SA-2019-0055)

NewStart CGSL CORE 5.04 / MAIN 5.04 : polkit Vulnerability (NS-SA-2019-0207)

NewStart CGSL CORE 5.04 / MAIN 5.04 : poppler Multiple Vulnerabilities (NS-SA-2019-0045)

NewStart CGSL CORE 5.04 / MAIN 5.04 : poppler Multiple Vulnerabilities (NS-SA-2019-0202)

NewStart CGSL CORE 5.04 / MAIN 5.04 : postgresql Vulnerability (NS-SA-2019-0036)

NewStart CGSL CORE 5.04 / MAIN 5.04 : procps-ng Multiple Vulnerabilities (NS-SA-2019-0019)

NewStart CGSL CORE 5.04 / MAIN 5.04 : procps-ng Vulnerability (NS-SA-2019-0184)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python Multiple Vulnerabilities (NS-SA-2019-0061)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python Multiple Vulnerabilities (NS-SA-2019-0187)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python Vulnerability (NS-SA-2019-0022)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python Vulnerability (NS-SA-2019-0160)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python Vulnerability (NS-SA-2019-0260)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python-jinja2 Vulnerability (NS-SA-2019-0078)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python-reportlab Vulnerability (NS-SA-2020-0012)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python-requests Vulnerability (NS-SA-2019-0189)

NewStart CGSL CORE 5.04 / MAIN 5.04 : python-urllib3 Multiple Vulnerabilities (NS-SA-2019-0199)

NewStart CGSL CORE 5.04 / MAIN 5.04 : qt5-qtbase Multiple Vulnerabilities (NS-SA-2019-0217)

NewStart CGSL CORE 5.04 / MAIN 5.04 : rsyslog Vulnerability (NS-SA-2019-0209)

NewStart CGSL CORE 5.04 / MAIN 5.04 : rsyslog Vulnerability (NS-SA-2019-0225)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ruby Multiple Vulnerabilities (NS-SA-2019-0080)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ruby Multiple Vulnerabilities (NS-SA-2019-0221)

NewStart CGSL CORE 5.04 / MAIN 5.04 : ruby Vulnerability (NS-SA-2019-0043)

NewStart CGSL CORE 5.04 / MAIN 5.04 : samba Multiple Vulnerabilities (NS-SA-2019-0069)

NewStart CGSL CORE 5.04 / MAIN 5.04 : samba Vulnerability (NS-SA-2019-0197)

NewStart CGSL CORE 5.04 / MAIN 5.04 : SDL Vulnerability (NS-SA-2019-0263)

NewStart CGSL CORE 5.04 / MAIN 5.04 : setup Vulnerability (NS-SA-2019-0075)

NewStart CGSL CORE 5.04 / MAIN 5.04 : sox Vulnerability (NS-SA-2019-0203)

NewStart CGSL CORE 5.04 / MAIN 5.04 : spamassassin Multiple Vulnerabilities (NS-SA-2019-0041)

NewStart CGSL CORE 5.04 / MAIN 5.04 : spice-gtk Vulnerability (NS-SA-2019-0208)

NewStart CGSL CORE 5.04 / MAIN 5.04 : sssd Multiple Vulnerabilities (NS-SA-2019-0195)

NewStart CGSL CORE 5.04 / MAIN 5.04 : sssd Vulnerability (NS-SA-2019-0067)

NewStart CGSL CORE 5.04 / MAIN 5.04 : sudo Vulnerability (NS-SA-2019-0215)

NewStart CGSL CORE 5.04 / MAIN 5.04 : systemd Multiple Vulnerabilities (NS-SA-2019-0051)

NewStart CGSL CORE 5.04 / MAIN 5.04 : systemd Multiple Vulnerabilities (NS-SA-2019-0057)

NewStart CGSL CORE 5.04 / MAIN 5.04 : systemd Multiple Vulnerabilities (NS-SA-2019-0196)

NewStart CGSL CORE 5.04 / MAIN 5.04 : tcpdump Multiple Vulnerabilities (NS-SA-2019-0071)

NewStart CGSL CORE 5.04 / MAIN 5.04 : tcpdump Vulnerability (NS-SA-2019-0266)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0037)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0052)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0062)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0158)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0160)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0180)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0190)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0215)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0265)

NewStart CGSL CORE 5.04 / MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2020-0010)

NewStart CGSL CORE 5.04 / MAIN 5.04 : tomcat Vulnerability (NS-SA-2019-0031)

NewStart CGSL CORE 5.04 / MAIN 5.04 : tomcat Vulnerability (NS-SA-2019-0059)

NewStart CGSL CORE 5.04 / MAIN 5.04 : udisks2 Vulnerability (NS-SA-2019-0201)

NewStart CGSL CORE 5.04 / MAIN 5.04 : unixODBC Multiple Vulnerabilities (NS-SA-2019-0195)

NewStart CGSL CORE 5.04 / MAIN 5.04 : unzip Vulnerability (NS-SA-2019-0192)

NewStart CGSL CORE 5.04 / MAIN 5.04 : uriparser Multiple Vulnerabilities (NS-SA-2019-0218)

NewStart CGSL CORE 5.04 / MAIN 5.04 : vim Vulnerability (NS-SA-2019-0161)

NewStart CGSL CORE 5.04 / MAIN 5.04 : wget Vulnerability (NS-SA-2019-0065)

NewStart CGSL CORE 5.04 / MAIN 5.04 : wget Vulnerability (NS-SA-2019-0079)

NewStart CGSL CORE 5.04 / MAIN 5.04 : wpa\_supplicant Vulnerability (NS-SA-2019-0072)

NewStart CGSL CORE 5.04 / MAIN 5.04 : xdg-user-dirs Vulnerability (NS-SA-2019-0026)

NewStart CGSL CORE 5.04 / MAIN 5.04 : xerces-c Vulnerability (NS-SA-2019-0072)

NewStart CGSL CORE 5.04 / MAIN 5.04 : xmlrpc Vulnerability (NS-SA-2019-0037)

NewStart CGSL CORE 5.04 / MAIN 5.04 : xorg-x11-server Vulnerability (NS-SA-2019-0045)

NewStart CGSL CORE 5.04 / MAIN 5.04 : yum-utils Vulnerability (NS-SA-2019-0024)

NewStart CGSL CORE 5.04 / MAIN 5.04 : zsh Multiple Vulnerabilities (NS-SA-2019-0070)

NewStart CGSL CORE 5.04 / MAIN 5.04 : zsh Vulnerability (NS-SA-2019-0200)

NewStart CGSL CORE 5.04 / MAIN 5.04 : zziplib Multiple Vulnerabilities (NS-SA-2019-0059)

NewStart CGSL CORE 5.04 / MAIN 5.04 : zziplib Multiple Vulnerabilities (NS-SA-2019-0184)

NewStart CGSL CORE 5.05 / MAIN 5.05 : 389-ds-base Vulnerability (NS-SA-2019-0170)

NewStart CGSL CORE 5.05 / MAIN 5.05 : 389-ds-base Vulnerability (NS-SA-2020-0003)

NewStart CGSL CORE 5.05 / MAIN 5.05 : bind Vulnerability (NS-SA-2019-0087)

NewStart CGSL CORE 5.05 / MAIN 5.05 : bind Vulnerability (NS-SA-2019-0232)

NewStart CGSL CORE 5.05 / MAIN 5.05 : binutils Multiple Vulnerabilities (NS-SA-2019-0228)

NewStart CGSL CORE 5.05 / MAIN 5.05 : blktrace Vulnerability (NS-SA-2019-0245)

NewStart CGSL CORE 5.05 / MAIN 5.05 : compat-libtiff3 Vulnerability (NS-SA-2019-0238)

NewStart CGSL CORE 5.05 / MAIN 5.05 : curl Vulnerability (NS-SA-2019-0171)

NewStart CGSL CORE 5.05 / MAIN 5.05 : curl Vulnerability (NS-SA-2019-0235)

NewStart CGSL CORE 5.05 / MAIN 5.05 : dhcp Vulnerability (NS-SA-2019-0231)

NewStart CGSL CORE 5.05 / MAIN 5.05 : dovecot Vulnerability (NS-SA-2019-0244)

NewStart CGSL CORE 5.05 / MAIN 5.05 : elfutils Multiple Vulnerabilities (NS-SA-2019-0258)

NewStart CGSL CORE 5.05 / MAIN 5.05 : exempi Multiple Vulnerabilities (NS-SA-2019-0228)

NewStart CGSL CORE 5.05 / MAIN 5.05 : exiv2 Multiple Vulnerabilities (NS-SA-2019-0229)

NewStart CGSL CORE 5.05 / MAIN 5.05 : fence-agents Vulnerability (NS-SA-2019-0226)

NewStart CGSL CORE 5.05 / MAIN 5.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0087)

NewStart CGSL CORE 5.05 / MAIN 5.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0164)

NewStart CGSL CORE 5.05 / MAIN 5.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0171)

NewStart CGSL CORE 5.05 / MAIN 5.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0233)

NewStart CGSL CORE 5.05 / MAIN 5.05 : firefox Multiple Vulnerabilities (NS-SA-2020-0004)

NewStart CGSL CORE 5.05 / MAIN 5.05 : flatpak Vulnerability (NS-SA-2019-0084)

NewStart CGSL CORE 5.05 / MAIN 5.05 : freeradius Multiple Vulnerabilities (NS-SA-2019-0083)

NewStart CGSL CORE 5.05 / MAIN 5.05 : freerdp Vulnerability (NS-SA-2019-0255)

NewStart CGSL CORE 5.05 / MAIN 5.05 : fribidi Vulnerability (NS-SA-2020-0006)

NewStart CGSL CORE 5.05 / MAIN 5.05 : gcc Multiple Vulnerabilities (NS-SA-2019-0233)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ghostscript Multiple Vulnerabilities (NS-SA-2019-0250)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ghostscript Vulnerability (NS-SA-2019-0085)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ghostscript Vulnerability (NS-SA-2020-0007)

NewStart CGSL CORE 5.05 / MAIN 5.05 : glibc Vulnerability (NS-SA-2019-0237)

NewStart CGSL CORE 5.05 / MAIN 5.05 : gvfs Vulnerability (NS-SA-2019-0238)

NewStart CGSL CORE 5.05 / MAIN 5.05 : http-parser Multiple Vulnerabilities (NS-SA-2019-0257)

NewStart CGSL CORE 5.05 / MAIN 5.05 : httpd Multiple Vulnerabilities (NS-SA-2019-0250)

NewStart CGSL CORE 5.05 / MAIN 5.05 : httpd Vulnerability (NS-SA-2019-0172)

NewStart CGSL CORE 5.05 / MAIN 5.05 : jss Vulnerability (NS-SA-2019-0240)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kdelibs Vulnerability (NS-SA-2019-0254)

NewStart CGSL CORE 5.05 / MAIN 5.05 : keepalived Vulnerability (NS-SA-2019-0240)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0085)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0165)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0247)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel Multiple Vulnerabilities (NS-SA-2020-0002)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0086)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0165)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel-rt Multiple Vulnerabilities (NS-SA-2019-0253)

NewStart CGSL CORE 5.05 / MAIN 5.05 : kernel-rt Multiple Vulnerabilities (NS-SA-2020-0008)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libarchive Multiple Vulnerabilities (NS-SA-2019-0248)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libcgroup Vulnerability (NS-SA-2019-0235)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libjpeg-turbo Multiple Vulnerabilities (NS-SA-2019-0227)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libmspack Multiple Vulnerabilities (NS-SA-2019-0237)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libssh2 Multiple Vulnerabilities (NS-SA-2019-0252)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libssh2 Vulnerability (NS-SA-2019-0172)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libtiff Multiple Vulnerabilities (NS-SA-2019-0227)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libwpd Vulnerability (NS-SA-2019-0256)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libX11 Multiple Vulnerabilities (NS-SA-2019-0242)

NewStart CGSL CORE 5.05 / MAIN 5.05 : libxkbcommon Multiple Vulnerabilities (NS-SA-2019-0246)

NewStart CGSL CORE 5.05 / MAIN 5.05 : linux-firmware Vulnerability (NS-SA-2019-0251)

NewStart CGSL CORE 5.05 / MAIN 5.05 : mariadb Multiple Vulnerabilities (NS-SA-2019-0243)

NewStart CGSL CORE 5.05 / MAIN 5.05 : mercurial Multiple Vulnerabilities (NS-SA-2019-0234)

NewStart CGSL CORE 5.05 / MAIN 5.05 : mod\_auth\_openidc Multiple Vulnerabilities (NS-SA-2019-0243)

NewStart CGSL CORE 5.05 / MAIN 5.05 : nss Multiple Vulnerabilities (NS-SA-2019-0236)

NewStart CGSL CORE 5.05 / MAIN 5.05 : nss Multiple Vulnerabilities (NS-SA-2020-0005)

NewStart CGSL CORE 5.05 / MAIN 5.05 : nss-softokn Vulnerability (NS-SA-2020-0005)

NewStart CGSL CORE 5.05 / MAIN 5.05 : nss-util Vulnerability (NS-SA-2020-0006)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ntp Vulnerability (NS-SA-2019-0255)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ntp Vulnerability (NS-SA-2020-0009)

NewStart CGSL CORE 5.05 / MAIN 5.05 : opensc Multiple Vulnerabilities (NS-SA-2019-0249)

NewStart CGSL CORE 5.05 / MAIN 5.05 : openslp Vulnerability (NS-SA-2020-0001)

NewStart CGSL CORE 5.05 / MAIN 5.05 : openssl Multiple Vulnerabilities (NS-SA-2019-0254)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ovmf Multiple Vulnerabilities (NS-SA-2019-0239)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ovmf Vulnerability (NS-SA-2019-0083)

NewStart CGSL CORE 5.05 / MAIN 5.05 : pacemaker Multiple Vulnerabilities (NS-SA-2019-0258)

NewStart CGSL CORE 5.05 / MAIN 5.05 : pango Vulnerability (NS-SA-2019-0232)

NewStart CGSL CORE 5.05 / MAIN 5.05 : patch Multiple Vulnerabilities (NS-SA-2019-0253)

NewStart CGSL CORE 5.05 / MAIN 5.05 : perl-Archive-Tar Vulnerability (NS-SA-2019-0230)

NewStart CGSL CORE 5.05 / MAIN 5.05 : php Vulnerability (NS-SA-2020-0001)

NewStart CGSL CORE 5.05 / MAIN 5.05 : polkit Vulnerability (NS-SA-2019-0256)

NewStart CGSL CORE 5.05 / MAIN 5.05 : poppler Multiple Vulnerabilities (NS-SA-2019-0249)

NewStart CGSL CORE 5.05 / MAIN 5.05 : procps-ng Vulnerability (NS-SA-2019-0252)

NewStart CGSL CORE 5.05 / MAIN 5.05 : python Multiple Vulnerabilities (NS-SA-2019-0229)

NewStart CGSL CORE 5.05 / MAIN 5.05 : python Vulnerability (NS-SA-2019-0163)

NewStart CGSL CORE 5.05 / MAIN 5.05 : python Vulnerability (NS-SA-2020-0002)

NewStart CGSL CORE 5.05 / MAIN 5.05 : python-jinja2 Vulnerability (NS-SA-2019-0082)

NewStart CGSL CORE 5.05 / MAIN 5.05 : python-requests Vulnerability (NS-SA-2019-0230)

NewStart CGSL CORE 5.05 / MAIN 5.05 : python-urllib3 Multiple Vulnerabilities (NS-SA-2019-0246)

NewStart CGSL CORE 5.05 / MAIN 5.05 : qt5-qtbase Multiple Vulnerabilities (NS-SA-2019-0236)

NewStart CGSL CORE 5.05 / MAIN 5.05 : rsyslog Vulnerability (NS-SA-2019-0259)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ruby Multiple Vulnerabilities (NS-SA-2019-0084)

NewStart CGSL CORE 5.05 / MAIN 5.05 : ruby Multiple Vulnerabilities (NS-SA-2019-0245)

NewStart CGSL CORE 5.05 / MAIN 5.05 : samba Vulnerability (NS-SA-2019-0244)

NewStart CGSL CORE 5.05 / MAIN 5.05 : SDL Vulnerability (NS-SA-2020-0007)

NewStart CGSL CORE 5.05 / MAIN 5.05 : sox Vulnerability (NS-SA-2019-0251)

NewStart CGSL CORE 5.05 / MAIN 5.05 : spice-gtk Vulnerability (NS-SA-2019-0257)

NewStart CGSL CORE 5.05 / MAIN 5.05 : sssd Multiple Vulnerabilities (NS-SA-2019-0241)

NewStart CGSL CORE 5.05 / MAIN 5.05 : sudo Vulnerability (NS-SA-2020-0004)

NewStart CGSL CORE 5.05 / MAIN 5.05 : systemd Multiple Vulnerabilities (NS-SA-2019-0242)

NewStart CGSL CORE 5.05 / MAIN 5.05 : tcpdump Vulnerability (NS-SA-2020-0008)

NewStart CGSL CORE 5.05 / MAIN 5.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0088)

NewStart CGSL CORE 5.05 / MAIN 5.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0163)

NewStart CGSL CORE 5.05 / MAIN 5.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0170)

NewStart CGSL CORE 5.05 / MAIN 5.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0231)

NewStart CGSL CORE 5.05 / MAIN 5.05 : thunderbird Multiple Vulnerabilities (NS-SA-2020-0003)

NewStart CGSL CORE 5.05 / MAIN 5.05 : udisks2 Vulnerability (NS-SA-2019-0248)

NewStart CGSL CORE 5.05 / MAIN 5.05 : unixODBC Multiple Vulnerabilities (NS-SA-2019-0241)

NewStart CGSL CORE 5.05 / MAIN 5.05 : unzip Vulnerability (NS-SA-2019-0234)

NewStart CGSL CORE 5.05 / MAIN 5.05 : uriparser Multiple Vulnerabilities (NS-SA-2019-0239)

NewStart CGSL CORE 5.05 / MAIN 5.05 : vim Vulnerability (NS-SA-2019-0164)

NewStart CGSL CORE 5.05 / MAIN 5.05 : wget Vulnerability (NS-SA-2019-0082)

NewStart CGSL CORE 5.05 / MAIN 5.05 : zsh Vulnerability (NS-SA-2019-0247)

NewStart CGSL CORE 5.05 / MAIN 5.05 : zziplib Multiple Vulnerabilities (NS-SA-2019-0226)

NewStart CGSL MAIN 4.05 : 389-ds-base Multiple Vulnerabilities (NS-SA-2019-0123)

NewStart CGSL MAIN 4.05 : 389-ds-base Vulnerability (NS-SA-2019-0101)

NewStart CGSL MAIN 4.05 : 389-ds-base Vulnerability (NS-SA-2019-0140)

NewStart CGSL MAIN 4.05 : apr Vulnerability (NS-SA-2019-0115)

NewStart CGSL MAIN 4.05 : bash Multiple Vulnerabilities (NS-SA-2019-0108)

NewStart CGSL MAIN 4.05 : bind Multiple Vulnerabilities (NS-SA-2019-0102)

NewStart CGSL MAIN 4.05 : bind Vulnerability (NS-SA-2019-0123)

NewStart CGSL MAIN 4.05 : bind Vulnerability (NS-SA-2019-0130)

NewStart CGSL MAIN 4.05 : bind Vulnerability (NS-SA-2019-0167)

NewStart CGSL MAIN 4.05 : bluez Vulnerability (NS-SA-2019-0117)

NewStart CGSL MAIN 4.05 : coreutils Vulnerability (NS-SA-2019-0107)

NewStart CGSL MAIN 4.05 : curl Vulnerability (NS-SA-2019-0104)

NewStart CGSL MAIN 4.05 : dbus Vulnerability (NS-SA-2020-0016)

NewStart CGSL MAIN 4.05 : dhcp Multiple Vulnerabilities (NS-SA-2019-0127)

NewStart CGSL MAIN 4.05 : dhcp Vulnerability (NS-SA-2019-0129)

NewStart CGSL MAIN 4.05 : dnsmasq Vulnerability (NS-SA-2019-0112)

NewStart CGSL MAIN 4.05 : dovecot Vulnerability (NS-SA-2020-0020)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0103)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0116)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0124)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0130)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0141)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0148)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0153)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2019-0167)

NewStart CGSL MAIN 4.05 : firefox Multiple Vulnerabilities (NS-SA-2020-0017)

NewStart CGSL MAIN 4.05 : freeradius Multiple Vulnerabilities (NS-SA-2019-0107)

NewStart CGSL MAIN 4.05 : ghostscript Vulnerability (NS-SA-2019-0097)

NewStart CGSL MAIN 4.05 : ghostscript Vulnerability (NS-SA-2019-0145)

NewStart CGSL MAIN 4.05 : git Vulnerability (NS-SA-2019-0120)

NewStart CGSL MAIN 4.05 : git Vulnerability (NS-SA-2020-0023)

NewStart CGSL MAIN 4.05 : glibc Multiple Vulnerabilities (NS-SA-2019-0099)

NewStart CGSL MAIN 4.05 : glibc Multiple Vulnerabilities (NS-SA-2019-0142)

NewStart CGSL MAIN 4.05 : glusterfs Vulnerability (NS-SA-2019-0141)

NewStart CGSL MAIN 4.05 : gnupg2 Vulnerability (NS-SA-2019-0135)

NewStart CGSL MAIN 4.05 : gnutls Multiple Vulnerabilities (NS-SA-2019-0109)

NewStart CGSL MAIN 4.05 : httpd Multiple Vulnerabilities (NS-SA-2019-0118)

NewStart CGSL MAIN 4.05 : httpd Vulnerability (NS-SA-2019-0156)

NewStart CGSL MAIN 4.05 : jasper Multiple Vulnerabilities (NS-SA-2019-0109)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0105)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0116)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0124)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0131)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0142)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0154)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2020-0017)

NewStart CGSL MAIN 4.05 : java-1.7.0-openjdk Vulnerability (NS-SA-2019-0148)

NewStart CGSL MAIN 4.05 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0111)

NewStart CGSL MAIN 4.05 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0119)

NewStart CGSL MAIN 4.05 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0126)

NewStart CGSL MAIN 4.05 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0137)

NewStart CGSL MAIN 4.05 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0146)

NewStart CGSL MAIN 4.05 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0157)

NewStart CGSL MAIN 4.05 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2020-0022)

NewStart CGSL MAIN 4.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0098)

NewStart CGSL MAIN 4.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0099)

NewStart CGSL MAIN 4.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0113)

NewStart CGSL MAIN 4.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0143)

NewStart CGSL MAIN 4.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0152)

NewStart CGSL MAIN 4.05 : kernel Multiple Vulnerabilities (NS-SA-2019-0168)

NewStart CGSL MAIN 4.05 : kernel Multiple Vulnerabilities (NS-SA-2020-0021)

NewStart CGSL MAIN 4.05 : kernel Vulnerability (NS-SA-2019-0125)

NewStart CGSL MAIN 4.05 : kernel Vulnerability (NS-SA-2019-0149)

NewStart CGSL MAIN 4.05 : libguestfs Vulnerability (NS-SA-2019-0110)

NewStart CGSL MAIN 4.05 : librelp Vulnerability (NS-SA-2019-0147)

NewStart CGSL MAIN 4.05 : libssh2 Multiple Vulnerabilities (NS-SA-2019-0169)

NewStart CGSL MAIN 4.05 : libtirpc Vulnerability (NS-SA-2019-0106)

NewStart CGSL MAIN 4.05 : libvirt Multiple Vulnerabilities (NS-SA-2019-0132)

NewStart CGSL MAIN 4.05 : libvirt Multiple Vulnerabilities (NS-SA-2019-0152)

NewStart CGSL MAIN 4.05 : libvirt Vulnerability (NS-SA-2019-0166)

NewStart CGSL MAIN 4.05 : libvorbis Vulnerability (NS-SA-2019-0122)

NewStart CGSL MAIN 4.05 : mailman Vulnerability (NS-SA-2019-0122)

NewStart CGSL MAIN 4.05 : mercurial Vulnerability (NS-SA-2019-0104)

NewStart CGSL MAIN 4.05 : mod\_perl Vulnerability (NS-SA-2019-0134)

NewStart CGSL MAIN 4.05 : mutt Multiple Vulnerabilities (NS-SA-2019-0140)

NewStart CGSL MAIN 4.05 : nss Multiple Vulnerabilities (NS-SA-2019-0105)

NewStart CGSL MAIN 4.05 : nss Vulnerability (NS-SA-2019-0112)

NewStart CGSL MAIN 4.05 : nss Vulnerability (NS-SA-2019-0131)

NewStart CGSL MAIN 4.05 : nss-softokn Vulnerability (NS-SA-2020-0018)

NewStart CGSL MAIN 4.05 : ntp Multiple Vulnerabilities (NS-SA-2019-0114)

NewStart CGSL MAIN 4.05 : ntp Multiple Vulnerabilities (NS-SA-2019-0127)

NewStart CGSL MAIN 4.05 : ntp Vulnerability (NS-SA-2019-0150)

NewStart CGSL MAIN 4.05 : openjpeg Multiple Vulnerabilities (NS-SA-2019-0129)

NewStart CGSL MAIN 4.05 : openslp Vulnerability (NS-SA-2019-0128)

NewStart CGSL MAIN 4.05 : openssh Multiple Vulnerabilities (NS-SA-2019-0139)

NewStart CGSL MAIN 4.05 : openssh Vulnerability (NS-SA-2019-0155)

NewStart CGSL MAIN 4.05 : openssh-latest Multiple Vulnerabilities (NS-SA-2019-0146)

NewStart CGSL MAIN 4.05 : openssh-latest Vulnerability (NS-SA-2019-0137)

NewStart CGSL MAIN 4.05 : openssh-latest Vulnerability (NS-SA-2019-0157)

NewStart CGSL MAIN 4.05 : openssl Vulnerability (NS-SA-2020-0019)

NewStart CGSL MAIN 4.05 : patch Vulnerability (NS-SA-2019-0138)

NewStart CGSL MAIN 4.05 : pcs Vulnerability (NS-SA-2019-0143)

NewStart CGSL MAIN 4.05 : php Vulnerability (NS-SA-2020-0018)

NewStart CGSL MAIN 4.05 : polkit Vulnerability (NS-SA-2019-0151)

NewStart CGSL MAIN 4.05 : poppler Vulnerability (NS-SA-2019-0118)

NewStart CGSL MAIN 4.05 : postgresql Vulnerability (NS-SA-2019-0121)

NewStart CGSL MAIN 4.05 : procps Multiple Vulnerabilities (NS-SA-2019-0135)

NewStart CGSL MAIN 4.05 : procps Multiple Vulnerabilities (NS-SA-2019-0155)

NewStart CGSL MAIN 4.05 : python Vulnerability (NS-SA-2019-0166)

NewStart CGSL MAIN 4.05 : python-paramiko Vulnerability (NS-SA-2019-0138)

NewStart CGSL MAIN 4.05 : python-paramiko Vulnerability (NS-SA-2019-0147)

NewStart CGSL MAIN 4.05 : python-reportlab Vulnerability (NS-SA-2020-0021)

NewStart CGSL MAIN 4.05 : qemu-kvm Multiple Vulnerabilities (NS-SA-2019-0108)

NewStart CGSL MAIN 4.05 : qemu-kvm Multiple Vulnerabilities (NS-SA-2019-0133)

NewStart CGSL MAIN 4.05 : qemu-kvm Multiple Vulnerabilities (NS-SA-2019-0154)

NewStart CGSL MAIN 4.05 : qemu-kvm Multiple Vulnerabilities (NS-SA-2020-0019)

NewStart CGSL MAIN 4.05 : qemu-kvm Vulnerability (NS-SA-2019-0125)

NewStart CGSL MAIN 4.05 : qemu-kvm Vulnerability (NS-SA-2019-0168)

NewStart CGSL MAIN 4.05 : quagga Multiple Vulnerabilities (NS-SA-2019-0101)

NewStart CGSL MAIN 4.05 : rpcbind Vulnerability (NS-SA-2019-0100)

NewStart CGSL MAIN 4.05 : samba Multiple Vulnerabilities (NS-SA-2019-0096)

NewStart CGSL MAIN 4.05 : samba Multiple Vulnerabilities (NS-SA-2019-0113)

NewStart CGSL MAIN 4.05 : samba Vulnerability (NS-SA-2019-0134)

NewStart CGSL MAIN 4.05 : samba4 Multiple Vulnerabilities (NS-SA-2019-0100)

NewStart CGSL MAIN 4.05 : samba4 Multiple Vulnerabilities (NS-SA-2019-0115)

NewStart CGSL MAIN 4.05 : samba4 Vulnerability (NS-SA-2019-0128)

NewStart CGSL MAIN 4.05 : spice-server Multiple Vulnerabilities (NS-SA-2019-0144)

NewStart CGSL MAIN 4.05 : spice-server Vulnerability (NS-SA-2019-0149)

NewStart CGSL MAIN 4.05 : sssd Vulnerability (NS-SA-2019-0132)

NewStart CGSL MAIN 4.05 : sudo Vulnerability (NS-SA-2019-0097)

NewStart CGSL MAIN 4.05 : sudo Vulnerability (NS-SA-2019-0102)

NewStart CGSL MAIN 4.05 : sudo Vulnerability (NS-SA-2020-0016)

NewStart CGSL MAIN 4.05 : tar Multiple Vulnerabilities (NS-SA-2019-0153)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0110)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0119)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0126)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0136)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0145)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0150)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0156)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0169)

NewStart CGSL MAIN 4.05 : thunderbird Multiple Vulnerabilities (NS-SA-2020-0022)

NewStart CGSL MAIN 4.05 : tigervnc Multiple Vulnerabilities (NS-SA-2019-0106)

NewStart CGSL MAIN 4.05 : tomcat6 Multiple Vulnerabilities (NS-SA-2019-0117)

NewStart CGSL MAIN 4.05 : vim Vulnerability (NS-SA-2020-0020)

NewStart CGSL MAIN 4.05 : wireshark Multiple Vulnerabilities (NS-SA-2019-0103)

NewStart CGSL MAIN 4.05 : wpa\_supplicant Multiple Vulnerabilities (NS-SA-2019-0120)

NewStart CGSL MAIN 4.05 : xmlrpc3 Vulnerability (NS-SA-2019-0136)

NewStart CGSL MAIN 4.05 : yum-utils Vulnerability (NS-SA-2019-0133)

NewStart CGSL MAIN 4.05 : zsh Multiple Vulnerabilities (NS-SA-2019-0144)

NewStart CGSL MAIN 4.06 : bind Vulnerability (NS-SA-2019-0174)

NewStart CGSL MAIN 4.06 : dbus Vulnerability (NS-SA-2019-0173)

NewStart CGSL MAIN 4.06 : dovecot Vulnerability (NS-SA-2019-0211)

NewStart CGSL MAIN 4.06 : firefox Multiple Vulnerabilities (NS-SA-2019-0090)

NewStart CGSL MAIN 4.06 : firefox Multiple Vulnerabilities (NS-SA-2019-0095)

NewStart CGSL MAIN 4.06 : firefox Multiple Vulnerabilities (NS-SA-2019-0175)

NewStart CGSL MAIN 4.06 : firefox Multiple Vulnerabilities (NS-SA-2019-0210)

NewStart CGSL MAIN 4.06 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0090)

NewStart CGSL MAIN 4.06 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0175)

NewStart CGSL MAIN 4.06 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0210)

NewStart CGSL MAIN 4.06 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0093)

NewStart CGSL MAIN 4.06 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0178)

NewStart CGSL MAIN 4.06 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0213)

NewStart CGSL MAIN 4.06 : kernel Multiple Vulnerabilities (NS-SA-2019-0092)

NewStart CGSL MAIN 4.06 : kernel Multiple Vulnerabilities (NS-SA-2019-0177)

NewStart CGSL MAIN 4.06 : kernel Multiple Vulnerabilities (NS-SA-2019-0212)

NewStart CGSL MAIN 4.06 : libssh2 Multiple Vulnerabilities (NS-SA-2019-0179)

NewStart CGSL MAIN 4.06 : libvirt Multiple Vulnerabilities (NS-SA-2019-0089)

NewStart CGSL MAIN 4.06 : libvirt Vulnerability (NS-SA-2019-0173)

NewStart CGSL MAIN 4.06 : openssh Vulnerability (NS-SA-2019-0091)

NewStart CGSL MAIN 4.06 : openssh-latest Vulnerability (NS-SA-2019-0094)

NewStart CGSL MAIN 4.06 : openssl Vulnerability (NS-SA-2019-0176)

NewStart CGSL MAIN 4.06 : polkit Vulnerability (NS-SA-2019-0094)

NewStart CGSL MAIN 4.06 : python Vulnerability (NS-SA-2019-0174)

NewStart CGSL MAIN 4.06 : qemu-kvm Multiple Vulnerabilities (NS-SA-2019-0091)

NewStart CGSL MAIN 4.06 : qemu-kvm Multiple Vulnerabilities (NS-SA-2019-0211)

NewStart CGSL MAIN 4.06 : qemu-kvm Vulnerability (NS-SA-2019-0176)

NewStart CGSL MAIN 4.06 : spice-server Vulnerability (NS-SA-2019-0092)

NewStart CGSL MAIN 4.06 : tar Multiple Vulnerabilities (NS-SA-2019-0089)

NewStart CGSL MAIN 4.06 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0093)

NewStart CGSL MAIN 4.06 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0095)

NewStart CGSL MAIN 4.06 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0178)

NewStart CGSL MAIN 4.06 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0212)

NewStart CGSL MAIN 4.06 : vim Vulnerability (NS-SA-2019-0177)

NewStart CGSL MAIN 5.04 : 389-ds-base Multiple Vulnerabilities (NS-SA-2019-0009)

NewStart CGSL MAIN 5.04 : apr Vulnerability (NS-SA-2019-0001)

NewStart CGSL MAIN 5.04 : bind Vulnerability (NS-SA-2019-0011)

NewStart CGSL MAIN 5.04 : curl Vulnerability (NS-SA-2019-0002)

NewStart CGSL MAIN 5.04 : dhcp Multiple Vulnerabilities (NS-SA-2019-0010)

NewStart CGSL MAIN 5.04 : dracut Vulnerability (NS-SA-2019-0016)

NewStart CGSL MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0001)

NewStart CGSL MAIN 5.04 : firefox Multiple Vulnerabilities (NS-SA-2019-0011)

NewStart CGSL MAIN 5.04 : glibc Multiple Vulnerabilities (NS-SA-2019-0012)

NewStart CGSL MAIN 5.04 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0003)

NewStart CGSL MAIN 5.04 : java-1.7.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0012)

NewStart CGSL MAIN 5.04 : java-1.8.0-openjdk Multiple Vulnerabilities (NS-SA-2019-0016)

NewStart CGSL MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0004)

NewStart CGSL MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0007)

NewStart CGSL MAIN 5.04 : kernel Multiple Vulnerabilities (NS-SA-2019-0014)

NewStart CGSL MAIN 5.04 : kernel-rt Vulnerability (NS-SA-2019-0018)

NewStart CGSL MAIN 5.04 : liblouis Vulnerability (NS-SA-2019-0004)

NewStart CGSL MAIN 5.04 : libreoffice Vulnerability (NS-SA-2019-0013)

NewStart CGSL MAIN 5.04 : mailman Vulnerability (NS-SA-2019-0008)

NewStart CGSL MAIN 5.04 : nautilus Vulnerability (NS-SA-2019-0015)

NewStart CGSL MAIN 5.04 : net-snmp Multiple Vulnerabilities (NS-SA-2019-0017)

NewStart CGSL MAIN 5.04 : postgresql Multiple Vulnerabilities (NS-SA-2019-0006)

NewStart CGSL MAIN 5.04 : procmail Vulnerability (NS-SA-2019-0005)

NewStart CGSL MAIN 5.04 : python Multiple Vulnerabilities (NS-SA-2019-0008)

NewStart CGSL MAIN 5.04 : qemu-kvm Multiple Vulnerabilities (NS-SA-2019-0005)

NewStart CGSL MAIN 5.04 : quagga Vulnerability (NS-SA-2019-0010)

NewStart CGSL MAIN 5.04 : ruby Multiple Vulnerabilities (NS-SA-2019-0013)

NewStart CGSL MAIN 5.04 : samba Multiple Vulnerabilities (NS-SA-2019-0003)

NewStart CGSL MAIN 5.04 : slf4j Vulnerability (NS-SA-2019-0015)

NewStart CGSL MAIN 5.04 : sssd Vulnerability (NS-SA-2019-0002)

NewStart CGSL MAIN 5.04 : systemd Vulnerability (NS-SA-2019-0014)

NewStart CGSL MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0006)

NewStart CGSL MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0009)

NewStart CGSL MAIN 5.04 : thunderbird Multiple Vulnerabilities (NS-SA-2019-0017)

# Netware

Novell Groupwise Servlet Manager Default Password

Novell NetBasic Scripting Server Encoded Traversal Arbitrary File Access

Novell NetWare 6.0 Tomcat source.jsp Traversal Arbitrary File Access

Novell NetWare 6.5 OpenSSH Remote Stack Buffer Overflow

Novell NetWare 6.5 Support Pack 1.1 Admin/Install Local Information Disclosure

Novell NetWare FTPServ Malformed Input Remote DoS

Novell NetWare LDAP Server Anonymous Bind

Novell NetWare Management Portal Unrestricted Access

Novell NetWare ncp Service NDS Object Enumeration

Novell NetWare Web Handler Multiple Vulnerabilities

Novell NetWare Web Server CGI2PERL.NLM PERL Handler Remote Overflow

Novell NetWare Web Server sewse.nlm (viewcode.jse) Traversal Arbitrary File Access

Novonyx Web Server Multiple Sample Application Files Present

Unsupported Novell NetWare Operating System

# Misc

3com RAS 1500 Configuration Disclosure

3Com Superstack 3 Switch Multiple Default Accounts

3Com Switch Default Admin Credentials

4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0 Multiple Vulnerabilities

4.10.0 < 4.10.5 AC DC LDAP Server Denial of Service Vulnerability (CVE-2019-12436)

4.5.x < 4.5.15 / 4.6.x < 4.6.11 / 4.7.x < 4.7.3 Multiple Vulnerabilities

4.6.x < 4.6.16 / 4.7.x < 4.7.9 / 4.8.x < 4.8.4 Multiple Vulnerabilities

A10 Networks Advanced Core OS Device Detection

A10 Networks Remote Buffer Overflow

Ability Mail Server < 2.70 IMAP4 FETCH DoS

ACAP Cleartext Authentication

ACAP Service STARTTLS Plaintext Command Injection

ACC Tigris Access Terminal Configuration Disclosure

Adobe Experience Manager 6.1.x / 6.2.x / 6.3.x < 6.3.3.8 / 6.4.x < 6.4.8.0 / 6.5.x < 6.5.4.0 (APSB20-15)

Adobe Experience Manager 6.4 and 6.5 DoS (APSB20-08)

Adobe Experience Manager Installed (Windows)

Adobe Flash Media Server < 3.0.5 / 3.5.3 Multiple Vulnerabilities (APSB09-18)

Adobe Flash Media Server < 3.0.6 / 3.5.4 Multiple Vulnerabilities (APSB10-19)

Adobe Flash Media Server < 3.0.7 / 3.5.5 / 4.0.1 Multiple Vulnerabilities (APSB10-27)

Adobe Flash Media Server < 3.5.6 / 4.0.2 Multiple Vulnerabilities (APSB11-11)

Adobe Flash Media Server < 3.5.7 / 4.0.3 Denial of Service (APSB11-20)

Adobe Flash Media Server RPC Privilege Escalation (APSB09-05)

Adobe Flash Media Server Version Detection

Adobe Media Server Unsupported Version Detection

Advanced Message Queuing Protocol Detection STARTTLS Support

AFP Server Directory Traversal

AFP Server Network Interface Enumeration

AFP Server Share Enumeration (guest)

AirConnect Default Password

akfingerd 0.5 Multiple Vulnerabilities

Alcatel ADSL Modem Unpassworded Access

Alcatel ADSL Modem Unrestricted Remote Access

AlienVault OSSIM get\_fqdn() RCE

Allied Telesyn Router/Switch Default Password

Alvarion Multiple Products Default Telnet Credentials

AMQP Cleartext Authentication

Android Emulator Telnet Port on Remote Host

Anonymous NNTP Authentication Enabled

AOST Network Video Recorder Detection

Apache Jetspeed Detection

Apache Nifi Web Interface Detection

Apache Pluto Web Interface Detection

Apache Solr Detection

Apache Storm < 1.1.3 / 1.2.x < 1.2.2 arbitrary file write vulnerability

Apache Storm Version Detection

Apache Struts 2 CookieInterceptor Unspecified Security Bypass (S2-022)

Apache Struts 2 Multiple Vulnerabilities (S2-023) (S2-025)

Apache Struts 2.0.x < 2.0.12 / 2.1.x < 2.1.6 Directory Traversal Vulnerability (S2-004)

Apache Struts 2.0.x < 2.0.9 RCE (S2-001)

Apache Struts 2.0.x < 2.2.1 <s:url> and <s:a> Tag XSS (S2-002)

Apache Struts 2.0.x < 2.2.1 Security Bypass Vulnerability (S2-003)

Apache Struts 2.1.x >= 2.1.2 / 2.2.x / 2.3.x < 2.3.34 / 2.5.x < 2.5.13 Multiple Vulnerabilities (S2-050 - S2-053)

Apache Struts 2.3.1 < 2.3.31 / 2.5.x < 2.5.5 Convention Plugin Path Traversal RCE (S2-042)

Apache Struts 2.3.20 < 2.3.29 / 2.5.x < 2.5.13 Denial of Service Vulnerability (S2-041)

Apache Struts 2.3.20 Incorrect Default Exclude Pattern (S2-024)

Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (S2-045) (S2-046)

Apache Struts 2.3.x < 2.3.33 Denial of Service (S2-049)

Apache Struts 2.3.x Showcase App Struts 1 Plugin ActionMessage Class Error Message Input Handling RCE (S2-048)

Apache Struts 2.5.x < 2.5.12 Multiple DoS (S2-047) (S2-049)

Apache Struts 2.5.x < 2.5.13 URLValidator Form Field Handling Remote DoS (S2-044)

Apache Struts 2.5.x < 2.5.14.1 Json-lib JSON Parsing Unspecified DoS (S2-054) (S2-055)

Apache Struts 2.x < 2.2.1 OGNL RCE (S2-005)

Apache Struts 2.x < 2.2.3 Multiple XSS (S2-006)

Apache Struts 2.x < 2.2.3.1 RCE (S2-007)

Apache Struts 2.x < 2.3.1.2 RCE (S2-009)

Apache Struts 2.x < 2.3.14.2 Multiple Vulnerabilities (S2-014)

Apache Struts 2.x < 2.3.14.2 Remote Code Execution Vulnerability (S2-013)

Apache Struts 2.x < 2.3.14.3 RCE (S2-015)

Apache Struts 2.x < 2.3.14.3 Remote Code Execution Vulnerability (S2-012)

Apache Struts 2.x < 2.3.15.1 Multiple Vulnerabilities (S2-016) (S2-017)

Apache Struts 2.x < 2.3.15.2 Dynamic Method Invocation Multiple Vulnerabilities (S2-019)

Apache Struts 2.x < 2.3.15.3 Broken Access Control Vulnerability (S2-018)

Apache Struts 2.x < 2.3.16.2 Multiple Vulnerabilities (S2-020)

Apache Struts 2.x < 2.3.18 Multiple Critical Vulnerabilities (S2-008)

Apache Struts 2.x < 2.3.20 Multiple ClassLoader Manipulation Vulnerabilities (S2-021)

Apache Struts 2.x < 2.3.24.1 Multiple Vulnerabilities (S2-026) (S2-027)

Apache Struts 2.x < 2.3.28 Multiple Vulnerabilities (S2-028) (S2-029) (S2-030) (S2-034)

Apache Struts 2.x < 2.3.28.1 Multiple Vulnerabilities

Apache Struts 2.x < 2.3.29 Multiple Vulnerabilities (S2-035 - S2-040)

Apache Struts 2.x < 2.3.4.1 Multiple Vulnerabilities (S2-010) (S2-011)

Apache Struts <= 2.3.36 FileUpload Deserialization Vulnerability

Apache Struts CVE-2018-11776 Results With No Namespace Possible Remote Code Execution (S2-057)

Apache Struts Detection for Linux/UNIX

Apache Struts Unsupported Version Detection

Apache Struts XStream Handler REST Plugin XML Request Handling Remote DoS (S2-056)

Apache ZooKeeper 3.4.0 < 3.4.10 / 3.5.x < 3.5.3 Multiple Vulnerabilities

Apache ZooKeeper < 3.4.14 / 3.5.x < 3.5.5 Information Disclosure

Apache Zookeeper x < 3.4.10 / 3.5.x < 3.5.4 Missing Authentication Remote Quorum Joining Vulnerability

APC SmartSlot Web/SNMP Management Card Default Password

Apple AirPort Base Station (802.11n) Firmware < 7.6.4 Remote DoS (APPLE-SA-2013-09-06-1)

Apple AirPort Base Station Authentication Credential Encryption Weakness

Apple Boot Camp Support Software Installed

Apple Time Capsule and AirPort Base Station (802.11n) Firmware < 7.6 (APPLE-SA-2011-11-10-2)

Apple Time Capsule and AirPort Base Station Firmware < 7.5.2 (APPLE-SA-2010-12-16-1)

Apple TV < 10 Multiple Vulnerabilities

Apple TV < 10.0.1 Multiple Vulnerabilities

Apple TV < 10.1.1 Multiple Vulnerabilities

Apple TV < 10.2 Multiple Vulnerabilities

Apple TV < 10.2.1 Multiple Vulnerabilities

Apple TV < 11 Multiple Vulnerabilities

Apple TV < 11.1 Multiple Vulnerabilities

Apple TV < 11.2 Multiple Vulnerabilities

Apple TV < 11.2.6 Telugu Character Handling Remote Memory Corruption Vulnerability

Apple TV < 11.3 Multiple Vulnerabilities

Apple TV < 11.4 Multiple Vulnerabilities

Apple TV < 11.4.1 Multiple Vulnerabilities

Apple TV < 12 Multiple Vulnerabilities

Apple TV < 12.1 Multiple Vulnerabilities

Apple TV < 12.1.1 Multiple Vulnerabilities

Apple TV < 12.3 Multiple Vulnerabilities

Apple TV < 12.4 Multiple Vulnerabilities

Apple TV < 12.4.1 A Use-After-Free Vulnerability

Apple TV < 13.3 Multiple Vulnerabilities

Apple TV < 13.3.1 Multiple Vulnerabilities

Apple TV < 5.2 Multiple Vulnerabilities

Apple TV < 6.0 Multiple Vulnerabilities

Apple TV < 6.1 Multiple Vulnerabilities

Apple TV < 7 Multiple Vulnerabilities

Apple TV < 7.0.1 Multiple Vulnerabilities (POODLE)

Apple TV < 7.0.2 Multiple Vulnerabilities

Apple TV < 7.0.3 Multiple Vulnerabilities

Apple TV < 7.1 Multiple Vulnerabilities (FREAK)

Apple TV < 7.2 Multiple Vulnerabilities

Apple TV < 7.2.1 Multiple Vulnerabilities

Apple TV < 9.1 Multiple Vulnerabilities

Apple TV < 9.1.1 Multiple Vulnerabilities

Apple TV < 9.2 Multiple Vulnerabilities

Apple TV < 9.2.1 Multiple Vulnerabilities

Apple TV < 9.2.2 Multiple Vulnerabilities

Apple TV <= 7.2.2 Bluetooth Remote Code Execution (BlueBorne)

ArcSight Enterprise Security Management (ESM) Installed

ArcSight Logger Installed (Linux)

ArGoSoft Mail Server \_DUMP Command System Information Disclosure

ArGoSoft Mail Server Pro IMAP RENAME Command Traversal Arbitrary Directory Creation

Arista Networks Device Detection

Arista Networks EOS 4.17 Multiple Vulnerabilities (SA0024) (SWEET32)

Arista Networks EOS 802.1x authentication DoS (SA0038)

Arista Networks EOS ASN.1 Encoder RCE (SA0020)

Arista Networks EOS Control Plane Packet Handling DoS (SA0025)

Arista Networks EOS DNS 2 byte heap based overflow RCE (SA0030)

Arista Networks EOS DoS (SA0039)

Arista Networks EOS IPv6 Neighbor Discovery Packet DoS (SA0022)

Arista Networks EOS kernel DoS (SA0040)

Arista Networks EOS LDP DoS (SA0042)

Arista Networks EOS libresolv Overflow RCE (SA0017)

Arista Networks EOS Linux Kernel TCP Multiple DoS (SA0041)

Arista Networks EOS Mlag agent DOS (SA0032)

Arista Networks EOS MPBGP Denial of Service (SA0029)

Arista Networks EOS Multiple Vulnerabilities (SA0018) (DROWN)

Arista Networks EOS Multiple Vulnerabilities (SA0019)

Arista Networks EOS Multiple Vulnerabilities (SA0024) (SWEET32)

Arista Networks EOS Multiple Vulnerabilities (SA0043)

Arista Networks EOS ngx\_chain\_to\_iovec NULL Pointer Deference DoS (SA0021)

Arista Networks EOS tcp\_input Challenge ACKs Shared Counter Disclosure (SA0023)

Arista Networks EOS/vEOS IP fragment DoS (SA0037)

Arista Networks EOS/vEOS SegmentSmack TCP DoS (SA0036)

Arista Networks Rib agent DoS (SA0033)

Arista Networks tcpmss\_mangle\_packet DoS (SA0034)

ARRIS Touchstone Cable Modem Detection

Aruba ClearPass Policy Manager Detection

Aruba VAN SDN Controller Detection

ArubaOS 6.3.1.11 / 6.4.2.1 SSH Authentication Bypass

ArubaOS Detection

ArubaOS Multiple Vulnerabilities (2017-006)

ArubaOS Remote Access Point Command Injection

ArubaOS WPA2 Key Reinstallation Vulnerabilities (KRACK)

Asterisk 'res\_http\_websocket' Double-Free DoS (AST-2014-019)

Asterisk 11.x < 11.25.2 / 11.6 < 11.6-cert17 / 13.x < 13.17.1 / 14.x < 14.6.1 / 13.13 < 13.13-cert5 Multiple Vulnerabilities (AST-2017-005 - AST-2017-007)

Asterisk 11.x < 11.25.3 / 13.x < 13.17.2 / 14.x < 14.6.2 / 11.6 < 11.6-cert18 / 13.13 < 13.13-cert6 RTP/RTCP information leak (AST-2017-008)

Asterisk 13.10.x < 13.11.1 ACK Handling Unrecognized Username NULL Pointer Dereference DoS (AST-2016-006)

Asterisk 13.13 < 13.13-cert3 / 13.x < 13.14.1 / 14.x < 14.3.1 CDR user Field RCE (AST-2017-001)

Asterisk 13.13 < 13.13-cert4 / 13.x < 13.15.1 / 14.x < 14.4.1 Multiple Vulnerabilities (AST-2017-002 - AST-2017-004)

Asterisk 13.x < 13.18.1 / 14.x < 14.7.1 / 15.x < 15.1.1 / 13.13 < 13.13-cert7 Multiple Vulnerabilities (AST-2017-009 - AST-2017-011)

Asterisk 13.x < 13.18.3 / 14.x < 14.7.3 / 15.x < 15.1.3 / 13.13 < 13.13-cert8 Memory Exhaustion Remote DoS (AST-2017-013)

Asterisk 13.x < 13.18.4 / 14.x < 14.7.4 / 15.x < 15.1.4 / 13.13 < 13.13-cert9 Improper Memory Storage Remote DoS (AST-2017-012)

Asterisk 13.x < 13.18.5 / 14.x < 14.7.5 / 15.x < 15.1.5 / 13.13 < 13.18-cert2 Crash in PJSIP (AST-2017-014)

Asterisk 13.x < 13.19.2 / 14.x < 14.7.6 / 13.13 < 13.18-cert3 Multiple DoS Vulnerabilities (AST-2018-002, AST-2018-003, AST-2018-004, & AST-2018-005)

Asterisk 13.x < 13.21.1 / 14.x < 14.7.7 / 13.13 < 13.18-cert4 / 13.21 < 13.21-cert2 Information Disclosure Vulnerability (AST-2018-008)

Asterisk 13.x < 13.23.1 / 14.x < 14.7.8 / 15.x < 15.6.1 / 13.21 < 13.21-cert3 HTTP Websocket Stack Overflow (AST-2018-009)

Asterisk 15.x < 15.2.2 Denial of Service Vulnerability (AST-2018-006)

Asterisk 15.x < 15.2.2 Multiple Vulnerabilities (AST-2018-001 - AST-2018-006)

Asterisk 15.x < 15.4.1 Multiple Vulnerabilities (AST-2018-007 - AST-2018-008)

Asterisk 15.x < 15.6.2 / 16.x < 16.0.1 DoS (AST-2018-010)

Asterisk 15.x < 15.7.2 / 16.x < 16.2.1 DoS (AST-2019-001)

Asterisk ast\_parse\_digest Function HTTP Digest Authentication String Parsing Remote Overflow (AST-2012-003)

Asterisk chan\_pjsip Incompatible Codecs DoS (AST-2015-001)

Asterisk chan\_sip Overlap Dialing Feature DoS (AST-2016-007)

Asterisk ConfBridge 'dialplan' Privilege Escalation (AST-2014-017)

Asterisk ConfBridge State Transitions DoS (AST-2014-014)

Asterisk Detection

Asterisk Endpoint Provisional Response Parsing RTP Port Consumption Remote DoS (AST-2012-010)

Asterisk Heap-Based Buffer Overflow in Skinny Channel Driver (AST-2012-005)

Asterisk HTTP Content-Length Header DoS (AST-2013-002)

Asterisk HTTP Session Handling DoS (AST-2014-007)

Asterisk Information Disclosure (AST-2014-011) (POODLE)

Asterisk Invalid INVITE / REGISTER SIP Request Username Enumeration (AST-2011-011)

Asterisk libcURL HTTP Request Injection (AST-2015-002)

Asterisk main/http.c DoS (AST-2014-001)

Asterisk Manager Interface ExternalIVR Application Originate Action Remote Shell Command Execution (AST-2012-012)

Asterisk Manager Interface MixMonitor Privilege Escalation (AST-2014-006)

Asterisk Manager User Unauthorized Shell Access (AST-2012-004)

Asterisk milliwatt\_generate Function Internal Data Sample Packet Parsing Remote DoS (AST-2012-002)

Asterisk Multiple Caller Simultaneous Voicemail Account Manipulation Double-free Remote DoS (AST-2012-011)

Asterisk Multiple Vulnerabilities (AST-2011-013 / AST-2011-014)

Asterisk Multiple Vulnerabilities (AST-2012-014 / AST-2012-015)

Asterisk Multiple Vulnerabilities (AST-2013-006 / AST-2013-007)

Asterisk Multiple Vulnerabilities (AST-2014-012 / AST-2014-018)

Asterisk Multiple Vulnerabilities (AST-2016-001 - AST-2016-003) (BEAST)

Asterisk Opus Codec DoS (AST-2016-008)

Asterisk Peer IAX2 Call Handling ACL Rule Bypass (AST-2012-013)

Asterisk PJProject TCP Connection DoS (AST-2016-005)

Asterisk PJSIP Channel Driver DoS (AST-2014-009)

Asterisk PJSIP Channel Driver Multiple DoS Vulnerabilities (AST-2014-005 / AST-2014-008)

Asterisk PJSIP Channel Driver Options DoS (AST-2014-003)

Asterisk PJSIP Channel Driver Subscription DoS (AST-2014-004)

Asterisk PJSIP Multiple Vulnerabilities (AST-2014-013 / AST-2014-015 / AST-2014-016)

Asterisk ReceiveFax Dialplan Application Remote DoS (AST-2014-010)

Asterisk REGISTER Request Contact URI Handling DoS (AST-2016-004)

Asterisk Remote Crash Vulnerability in IAX2 Channel Driver (AST-2012-007)

Asterisk Remote Crash Vulnerability in SIP Channel Driver (AST-2012-006)

Asterisk Remote Crash Vulnerability in Skinny Channel Driver (AST-2012-008)

Asterisk Remote Crash Vulnerability in Skinny Channel Driver (AST-2012-009)

Asterisk SIP Channel Authentication Bypass (AST-2016-009)

Asterisk SIP Channel Driver ACK with SDP Denial of Service (AST-2013-004)

Asterisk SIP Channel Driver Invalid SDP Denial of Service (AST-2013-005)

Asterisk SIP Channel Driver Username Disclosure (AST-2013-003)

Asterisk SIP File Descriptor Exhaustion with chan\_sip Session-Timers DoS (AST-2014-002)

Asterisk SIP Remote Authentication Bypass

Asterisk SIP SDP Buffer Overflow (AST-2013-001)

Asterisk SRTP Video Stream Negotiation Remote Crash (AST-2012-001)

Asterisk TLS Certificate Common Name NULL Byte Vulnerability (AST-2015-003)

ASUS RT-N13U Router Built-in Admin Telnet Account with Unchangeable Password

at32 Reverse Proxy Admin Portal No Password

at32 Reverse Proxy Detection

Atlassian HipChat Server 1.0 < 2.2.4 Image Upload RCE

Attachmate Reflection for Secure IT UNIX server < 7.0 SP1 Multiple Vulnerabilities

AttachmateWRQ Reflection for Secure IT Server < 6.0 Build 24 Multiple Vulnerabilities

AttachmateWRQ Reflection for Secure IT Server SFTP Format String

Avaya P330 Stackable Switch Default Password

AVG Internet Security Out-of-Date

Avocent KVM Over IP Switch Detection

Avotus CDR mm Arbitrary File Retrieval

AVTech Web Interface Detection

Axis Camera Default Password

AXIS Camera Unconfigured Password Detection

AXIS Camera Unsecured Feed Detection

AXIS FTP Server Detection

AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)

AXIS Multiple Vulnerabilities (ACV-128401)

AXIS Web Interface Detection

Bay Networks Accelar 1200 Switch Default Password (password) for 'usrname' Account

Beanstalkd < 1.4.6 Remote Beanstalkd Command Injection

Belkin Web Interface Detection

Bitdefender GravityZone Detection

Bitvise SSH Server < 7.41 Multiple Vulnerabilities (remote)

BlackBerry Enterprise Service (BES) Management Console Detection

Blackboard LC3000 Laundry Reader Default Telnet Password

Blind Command Injection Vulnerability in Grandstream Products

BMC BladeLogic Server Automation RSCD Agent Detection

BMC Server Automation RSCD Agent ACL Bypass

BMC Server Automation RSCD Agent Weak ACL NSH Arbitrary Command Execution

BMC Server Automation RSCD Agent Weak ACL XML-RPC Arbitrary Command Execution

BMC Server Automation rscd Service Authentication Bypass RCE

BNC IRC Server Incorrect Password Authentication Bypass

Brocade Fabric OS Default Credentials

Brother Printer Debut Embedded HTTP Server Detection

Buffalo TeraStation Web detection

CA eTrust Directory SNMP Packet Parsing Denial of Service

CA Unified Infrastructure Management < 8.4 SP2 Multiple Information Disclosure Vulnerabilities (CA20161109-01)

CA Unified Infrastructure Management < 8.48 / 8.53 Multiple Vulnerabilities (CA20180829-02)

Cayman DSL Router Single Character String Authentication Bypass.

Cayman DSL Router Unauthenticated Access

cfingerd < 1.4.4 Multiple Vulnerabilities

cfingerd Version Detection

cfingerd Wildcard Argument Information Disclosure

Charybdis IRCd m\_capab.c Denial of Service

Check Point Secure Platform Detection

Check\_MK Agent Detection

Cheops NG Unauthenticated Access

Cheops-ng Cleartext Authentication Information Disclosure

Cisco Aironet 1240 AG Unsupported Device Detection

Cisco CallManager TFTP File Detection

Cisco Energy Management Web Detection

Cisco Identity Services Engine (ISE) Unsupported Version Detection

Cisco IOS Device TFTP Certificate Authority (CA) File Detection

Cisco IOS TFTP File Disclosure

Cisco Prime Data Center Network Manager Installed (Linux)

Cisco Prime LAN Management Solution Java Object Deserialization RCE (CSCux34647)

Cisco Security Manager Java Object Deserialization RCE (CSCux34671)

Cisco SPA ATA SIP Detection

Cisco SPA ATA Web Interface Detection

Cisco TelePresence VX Clinical Assistant WIL-A Module Reboot Admin Password Removal

Cisco UCS Director Default Credentials (SSH)

Cisco Wireless Control System Installed (Linux)

Citrix CloudPlatform Detection

Citrix NetScaler Application Delivery Controller Multiple Vulnerabilities

Citrix NetScaler Gateway XSS (CTX140291)

Citrix NetScaler Multiple Vulnerabilities (CTX140651)

Citrix NetScaler nsconfigd Remote DoS (CTX139017)

Citrix NetScaler Version Detection

Citrix Provisioning Services Unspecified Request Parsing Remote Code Execution (CTX133039) (uncredentialed check)

Citrix Published Applications Remote Enumeration

Citrix SD-WAN Center Detection

Citrix SD-WAN Detection

Citrix Studio < 7.6.1000 Insecure Access Policy Configuration (CTX213045)

Citrix XenServer Active Directory Authentication Incorrect Host Management Security Bypass (CTX213549, CTX213769)

Citrix XenServer Detection

Citrix XenServer Guest-to-host DoS (CTX230624)

Citrix XenServer Information Disclosure Vulnerability (CTX235225)

Citrix XenServer Local Memory Disclosure Vulnerability (CTX235225)

Citrix XenServer Microarchitectural Data Sampling Speculative Side-Channel Vulnerabilities (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (CTX2251995)

Citrix XenServer Multiple Infinite Loop Guest-to-Host DoS (CTX202583)

Citrix XenServer Multiple memory\_exchange() Hypercall Error Handling DoS (CTX203451)

Citrix XenServer Multiple Vulnerabilities (CTX140984)

Citrix XenServer Multiple Vulnerabilities (CTX200288)

Citrix XenServer Multiple Vulnerabilities (CTX200892)

Citrix XenServer Multiple Vulnerabilities (CTX212736)

Citrix XenServer Multiple Vulnerabilities (CTX214954) (Bunker Buster)

Citrix XenServer Multiple Vulnerabilities (CTX216071)

Citrix XenServer Multiple Vulnerabilities (CTX218775)

Citrix XenServer Multiple Vulnerabilities (CTX219378)

Citrix XenServer Multiple Vulnerabilities (CTX220112)

Citrix XenServer Multiple Vulnerabilities (CTX220771)

Citrix XenServer multiple vulnerabilities (CTX222565)

Citrix XenServer Multiple Vulnerabilities (CTX223291)

Citrix XenServer Multiple Vulnerabilities (CTX224740)

Citrix XenServer Multiple Vulnerabilities (CTX225941)

Citrix XenServer Multiple Vulnerabilities (CTX227185)

Citrix XenServer Multiple Vulnerabilities (CTX228867)

Citrix XenServer Multiple Vulnerabilities (CTX230138)

Citrix XenServer Multiple Vulnerabilities (CTX231390) (Meltdown)(Spectre)

Citrix XenServer Multiple Vulnerabilities (CTX232096)

Citrix XenServer Multiple Vulnerabilities (CTX232655)

Citrix XenServer Multiple Vulnerabilities (CTX234679)

Citrix XenServer Multiple Vulnerabilities (CTX235748)

Citrix XenServer Multiple Vulnerabilities (CTX239432)

Citrix XenServer Multiple Vulnerabilities (Foreshadow) (CTX236548)

Citrix XenServer Nested VT-x Instruction Guest-to-Host DoS (CTX239100)

Citrix XenServer Pin Count / Page Reference Grant Table Code Guest-to-Host Memory Corruption Vulnerability (CTX229057)

Citrix XenServer QEMU Display Geometry Resize Handling Guest-to-Host Code Execution (CTX221578)

Citrix XenServer QEMU FDC Buffer Overflow RCE (CTX201078) (VENOM)

Citrix XenServer QEMU IDE Buffer Overflow Code Execution (CTX201593)

Citrix XenServer QEMU ioport Array Overflow Guest-to-Host Privilege Escalation (CTX219136)

Citrix XenServer QEMU RTL8139 Guest Network Device Information Disclosure (CTX201717)

ClamAV < 0.100.1 Multiple Vulnerabilities

ClamAV < 0.95 Scan Evasion

ClamAV < 0.95.1 Multiple Vulnerabilities

ClamAV < 0.95.2 Multiple Scan Evasion Vulnerabilities

ClamAV < 0.96 Multiple Vulnerabilities

ClamAV < 0.96.1 Multiple Vulnerabilities

ClamAV < 0.96.3 Multiple Vulnerabilities

ClamAV < 0.96.5 Multiple Vulnerabilities

ClamAV < 0.97 Multiple Vulnerabilities

ClamAV < 0.97.2 'cli\_hm\_scan' Denial of Service

ClamAV < 0.97.5 Multiple Vulnerabilities

ClamAV < 0.97.7 Multiple Vulnerabilities

ClamAV < 0.97.8 Multiple Vulnerabilities

ClamAV < 0.98.5 Multiple Vulnerabilities

ClamAV < 0.98.6 Multiple Vulnerabilities

ClamAV < 0.98.7 Multiple Vulnerabilities

ClamAV < 0.99.2 Multiple libclamav DoS

ClamAV < 0.99.3 Multiple libclamav DoS

ClamAV Antivirus Detection and Status

ClamAV Unsupported Version Detection

ClamAV Version Detection

ClarkConnect Linux clarkconnectd Remote Information Disclosure

Clearswift MIMEsweeper Manager Console Detection

ClusterLabs Pacemaker PCS Daemon Default Password

ClusterLabs Pacemaker PCS Daemon Detection

Comelit Actuator Detection

Comelit Camera Detection

Comelit Intercom Detection

Comelit Intercom Master Detection

Commvault 11 < 11 SP7 Multiple Vulnerabilities

CoSoSys Endpoint Protector 4 Predictable Password

Countertack Sentinel Detection

Countertack Sentinel User Interface Detection

CUPS 1.6.x >= 1.6.4 / 1.7.x < 1.7.1 lppasswd Information Disclosure

CUPS 1.7.x < 1.7.4 'get\_file' Function Symlink Handling Info Disclosure

CUPS 1.7.x < 1.7.5 'get\_file' Function Symlink Handling Info Disclosure

CUPS < 1.1.18 Multiple Vulnerabilities

CUPS < 1.1.23 Multiple Vulnerabilities

CUPS < 1.3.10 Multiple Vulnerabilities

CUPS < 1.3.6 process\_browse\_data() Function Double Free DoS

CUPS < 1.3.7 Multiple Vulnerabilities

CUPS < 1.3.8 PNG File Handling Multiple Overflows

CUPS < 1.3.9 Multiple Vulnerabilities

CUPS < 1.4.2 kerberos Parameter XSS

CUPS < 1.4.3 Multiple Vulnerabilities

CUPS < 1.4.4 Multiple Vulnerabilities

CUPS < 1.4.5 Multiple Vulnerabilities

CUPS < 1.4.7 'gif\_read\_lzw' Buffer Overflow

CUPS < 1.6.2 Multiple Vulnerabilities

CUPS < 1.7.2 is\_path\_absolute Function XSS

CUPS < 2.0.1 SSLv3 Legacy Encryption Vulnerability (POODLE)

CUPS < 2.0.3 Multiple Vulnerabilities

CUPS cups/ipp.c ippReadIO Function IPP Tag Handling Overflow

CUPS Incomplete SSL Negotiation Remote DoS

CUPS Internet Printing Protocol (IPP) Implementation Empty UDP Datagram Remote DoS

CUPS Printer List Disclosure

CUPS Remote Command Execution via Shellshock

CUPS SNMP Back End (backend/snmp.c) asn1\_get\_string Function Crafted SNMP Response Remote Overflow

CVS < 1.11.17 / 1.12.9 Multiple Vulnerabilities

CVS < 1.11.20 / 1.12.12 Multiple Unspecified Vulnerabilities

CVS Client Traversal Arbitrary File Retrieval

CVS history.c File Existence Information Disclosure

CVS Malformed Directory Request Double-free Privilege Escalation

CVS pserver Brute Force Access

CVS pserver Crafted Module Request Arbitrary File / Directory Creation

CVS PServer CVSROOT Passwd File Arbitrary Code Execution

CVS pserver Line Entry Handling Overflow

D-Link DCC Protocol Security Bypass

D-Link DIR Router Web Interface Detection

Danware NetOp Host HELO Request Remote Information Disclosure

Default Password (0000) for 'user' on WIP5000 IP Phone

Default Password (000000) for 'admin' on WIP5000 IP Phone

Dell EMC Data Protection Central 1.0, 1.0.1, 18.1, 18.2, 19.1 Improper Certificate Chain of Trust (DSA-2019-135)

Dell KACE K2000 Appliance Hidden CIFS Fileshare Information Disclosure

Deprecated / Disabled Plugins in Scan Policy - Notice

DHCP server Detection (Linux)

DISA Security Readiness Review Scripts Detection

DISA Security Readiness Review Scripts for Solaris Local Privilege Escalation

Docker Container Number of Changed Files

Dovecot Multiple Command Traversal Arbitrary Directory Listing

Dovecot passdbs Argument Injection Authentication Bypass

Dropbear SSH Server < 2013.59 Multiple Vulnerabilities

Dropbear SSH Server < 2016.72 Multiple Vulnerabilities

Dropbear SSH Server < 2016.72 xauth Command Injection

Dropbear SSH Server Channel Concurrency Use-after-free Remote Code Execution

Dropbear SSH Server svr\_ses.childpidsize Remote Overflow

Dropbear SSH Server Username Remote Format String

EgoSecure EndPoint Service Installed

Ekiga SIP Detection

EMC AutoStart < 5.5.0 HF4 ftAgent Remote Code Execution

EMC Avamar ADS / AVE 7.2.x < 7.2.1 Hotfix 277897 / 7.3.x < 7.3.1 Hotfix 276676 / 7.4.x < 7.4.1 Hotfix 279294 Multiple Vulnerabilities (ESA-2017-054)

EMC Avamar ADS / AVE 7.2.x < 7.2.1 Hotfix HOTFIX 300440 / 7.3.x < 7.3.1 Hotfix 300439 / 7.4.x < 7.4.1 Hotfix 300438 / 7.5.0 < 7.5.0 Hotfix 300441 / 7.5.1 < 7.5.1 Hotfix 300442 / 18.1 < 18.1 Hotfix 300443 Multiple Vulnerabilities (DSA-2018-145)

EMC Avamar ADS / AVE 7.3.0.x < 7.3.0 Hotfix 268253 / 7.3.1.x < 7.3.1 Hotfix 272363 Incorrect File Ownership Local Privilege Escalation (ESA-2016-146)

EMC Avamar ADS / AVE 7.3.x < 7.3.1 Hotfix HOTFIX 290316 / 7.4.x < 7.4.1 Hotfix 291882 / 7.5.x < 7.5.0 Hotfix 291881 Missing Access Control Check Vulnerability (DSA-2018-025)

EMC Avamar ADS / AVE < 7.3.0 Hotfix 263301 PostgreSQL Command Local Privilege Escalation (ESA-2016-111)

EMC Avamar ADS / AVE Installed (credentialed check)

EMC Avamar Server Incorrect Permission Assignment Vulnerability (DSA-2019-138)

EMC Cloud Tiering Appliance Web Interface Detection

EMC Data Protection Advisor 6.2 < 6.4 Patch B180 / < 6.5 patch B51 (DSA-2018-112).

EMC Documentum D2 4.1 / 4.2.x < 4.2 P16 / 4.5.x < 4.5 P03 Multiple DQL Injection Vulnerabilities

EMC Documentum D2 4.1.x < 4.5 XSS (ESA-2015-109)

EMC Documentum D2 4.5.x < 4.5 P15 / 4.6.x < 4.6 P03 r\_object\_id Handling Unauthenticated Document Disclosure (ESA-2016-108)

EMC Documentum D2 4.5.x and 4.6.x < 4.7 Multiple Vulnerabilities (ESA-2016-167)

EMC Documentum D2 < 4.1 P22 / 4.2 P11 Multiple Vulnerabilities (ESA-2015-010)

EMC Documentum D2 < 4.6 Insufficient ACL Remote Object Manipulation (ESA-2016-034)

EMC Documentum D2 Detection (credentialed)

EMC Documentum D2 Privilege Escalation (ESA-2014-045)

EMC Documentum D2 Privilege Escalation (ESA-2014-067)

EMC Legato Networker Multiple Vulnerabilities

EMC RepliStor rep\_srv.exe Crafted TCP Packet Remote DoS (ESA-09-019)

EMC RSA Authentication Manager 8.x < 8.1 Patch 6 Unspecified URI Redirection

EMC RSA Authentication Manager Version

Emerson Network Power Avocent MergePoint Unity KVM Switch < 1.14 / 1.18 download.php filename Parameter Directory Traversal

Emerson Network Power Avocent MergePoint Unity KVM Switch Detection

ESET NOD32 Antivirus for Linux Installed

eStara SoftPhone Detection

eStara SoftPhone SIP Packet SDP Data attribute Field Overflow

ESXi 5.0 / 5.1 / 5.5 / 6.0 Multiple Vulnerabilities (VMSA-2016-0010) (remote check)

ESXi 5.0 < Build 1022489 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 1197855 NFC Traffic Denial of Service (remote check)

ESXi 5.0 < Build 1311175 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 1749766 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 1918656 OpenSSL Library Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 3086167 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)

ESXi 5.0 < Build 515841 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 608089 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 702118 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 721882 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 764879 Multiple Vulnerabilities (remote check)

ESXi 5.0 < Build 912577 Multiple Vulnerabilities (remote check)

ESXi 5.1 < Build 1063671 Multiple Vulnerabilities (remote check)

ESXi 5.1 < Build 1142907 NFC Traffic Denial of Service (remote check)

ESXi 5.1 < Build 1312873 File Descriptors Privilege Escalation (remote check)

ESXi 5.1 < Build 1483097 Multiple Vulnerabilities (remote check)

ESXi 5.1 < Build 1743201 Multiple Vulnerabilities (remote check)

ESXi 5.1 < Build 1900470 OpenSSL Library Multiple Vulnerabilities (remote check)

ESXi 5.1 < Build 2323231 glibc Library Multiple Vulnerabilities (remote check)

ESXi 5.1 < Build 2323236 Third-Party Libraries Multiple Vulnerabilities (remote check) (BEAST)

ESXi 5.1 < Build 3070626 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)

ESXi 5.1 < Build 911593 Multiple Vulnerabilities (remote check)

ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)

ESXi 5.5 / 6.0 / 6.5 / Hypervisor-Assisted Guest Remediation for Speculative Execution (VMSA-2018-0004) (Spectre) (remote check)

ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check)

ESXi 5.5 < Build 1474526 File Descriptors Privilege Escalation (remote check)

ESXi 5.5 < Build 1623387 Multiple Vulnerabilities (remote check)

ESXi 5.5 < Build 1746974 / 5.5 Update 1 < Build 1746018 OpenSSL Library Multiple Vulnerabilities (remote check) (Heartbleed)

ESXi 5.5 < Build 1881737 OpenSSL Library Multiple Vulnerabilities (remote check)

ESXi 5.5 < Build 1980513 glibc Library Multiple Vulnerabilities (remote check)

ESXi 5.5 < Build 2352327 Multiple Vulnerabilities (remote check) (POODLE)

ESXi 5.5 < Build 3248547 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)

ESXi 5.5 < Build 3568722 / 6.0 < Build 3568940 glibc DNS Resolver RCE (VMSA-2016-0002) (remote check)

ESXi 5.5 < Build 5230635 Multiple Vulnerabilities (VMSA-2017-0006) (remote check)

ESXi 5.5 < Build 6480267 RPC NULL Pointer Dereference Vulnerability (VMSA-2017-0015) (remote check)

ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)

ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)

ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0008)(MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)(Remote Check)

ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0013)

ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)

ESXi 6.0 / 6.5 / 6.7 Use-After-Free (VMSA-2019-0014)

ESXi 6.0 < Build 3380124 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)

ESXi 6.0 < Build 5485776 Multiple Vulnerabilities (VMSA-2017-0015) (remote check)

ESXi 6.0 U1 < Build 5251621 / 6.0 U2 < Build 5251623 / 6.0 U3 < Build 5224934 Multiple Vulnerabilities (VMSA-2017-0006) (remote check)

ESXi 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0006) (Remote Check)

ESXi 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0012)

ESXi 6.5 < Build 5224529 Multiple Vulnerabilities (VMSA-2017-0006) (remote check)

ESXi 6.5 < Build 5969300 Multiple Vulnerabilities (VMSA-2017-0015) (remote check)

ESXi 6.5 < Build 6765664 Heap Buffer Overflow (VMSA-2017-0021) (remote check)

Ethernet Card Manufacturer Detection

Eudora WorldMail Unsupported

F5 Device Default Support Password

F5 Networks BIG-IP Detection

F5 Networks BIG-IQ Detection

F5 Networks rsync RCE

FasterXML Jackson Databind Detection for Linux/UNIX

FileMaker Pro Client Request User Passwords Remote Disclosure

Finger .@host Unused Account Disclosure

Finger 0@host Unused Account Disclosure

Finger Recursive Request Arbitrary Site Redirection

Finger Service Remote Information Disclosure

fingerd Remote Overflow

Firebird SQL Server for Linux Installed (credentialed check)

FKey Arbitrary Remote File Disclosure

Flexense Enterprise Products Detection

Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities

Flexera FlexNet Publisher lmadmin < 11.16.5.1 Multiple Vulnerabilities

Fortinet FortiOS SSH Undocumented Interactive Login Vulnerability

Fortinet OpenSSL Information Disclosure (Heartbleed)

Fortinet OpenSSL Multiple Vulnerabilities

FortressSSH SSH\_MSG\_KEXINIT Logging Remote Overflow

Foxit Reader Installed (Linux)

FreeBSD 4.1.1 Finger Arbitrary Remote File Access

FreeSWITCH < 1.4.26 / 1.6.x < 1.6.5 JSON Parser RCE

FreeSWITCH Detection

FreeSWITCH Route Header Value Handling DoS

Generic Format String Detection

GitHub Enterprise Detection

GPON ONT Home Gateway Router Detection

Grandstream Phone Web Interface Default Credentials

Grandstream Phone Web Interface Detection

Grandstream SIP Detection

Groovy Shell Unauthenticated Remote Command Execution

H3C / HPE Intelligent Management Center accessMgrServlet Java Object Deserialization RCE

H3C / HPE Intelligent Management Center Java Object Deserialization RCE

H3C / HPE Intelligent Management Center PLAT < 7.3 E0504P04 Multiple Vulnerabilities

H3C / HPE Intelligent Management Center PLAT < 7.3 E0506 Multiple Vulnerabilities

H3C / HPE Intelligent Management Center PLAT < 7.3 E0506P03 Multiple RCE

H3C / HPE Intelligent Management Center PLAT < 7.3 E0506P03 Multiple Vulnerabilities

H3C / HPE Intelligent Management Center PLAT < 7.3 E0605P06 Multiple Vulnerabilities

H3C / HPE Intelligent Management Center PLAT <= 7.3 E0501P01 Multiple Vulnerabilities

H3C / HPE Intelligent Management Center RMI Java Object Deserialization RCE

HAProxy Trash Buffer Overflow Vulnerability

Hazelcast REST Interface Detection

Hikvision IP Camera Web Interface Detection

Hobbit Monitor config Method Traversal Arbitrary File Access

HooToo TripMate Web Interface Detection

Host Asset Information

Host Unique Identifiers

HP ArcSight ESM 6.x < 6.9.1.2377.4 / 6.11.0.2385.1 Multiple Vulnerabilities

HP ArcSight ESM < 5.6 / 6.0 / 6.5c SP1 P2 / 6.8c Multiple Vulnerabilities

HP ArcSight ESM < 6.5c SP1 P1 / 6.8c Multiple Vulnerabilities

HP ArcSight ESM < 6.8c Information Disclosure

HP ArcSight Logger < 5.3 Multiple Vulnerabilities (credentialed check)

HP ArcSight Logger < 6.0 P2 Multiple Vulnerabilities

HP ArcSight Logger < 6.0P1 Multiple Vulnerabilities

HP ArcSight Logger < 6.1 Management Center XSS

HP ArcSight Logger < 6.1P1 Multiple Vulnerabilities

HP BladeSystem c-Class Onboard Administrator 4.11 / 4.20 Heartbeat Information Disclosure (Heartbleed)

HP Data Protector 'EXEC\_INTEGUTIL' Arbitrary Command Execution

HP Data Protector 7.0x < 7.03 build 108 / 8.1x < 8.15 / 9.0x < 9.06 Multiple Vulnerabilities (HPSBGN03580) (Bar Mitzvah)

HP Data Protector 8.x < 8.17 / 9.x < 9.09 Multiple Vulnerabilities (HPSBGN03732)

HP Data Protector 8.x Arbitrary Command Execution (HPSBMU03072)

HP Data Protector < A.06.20 Multiple Vulnerabilities

HP Data Protector Components Version Detection

HP Data Protector Hard-coded Cryptographic Key (HPSBGN03580)

HP Data Protector Local Privilege Escalation

HP Data Protector Media Operations DBServer opcode 0x10 Traversal Arbitrary File Access

HP Data Protector Multiple RCE Vulnerabilities

HP Data Protector Multiple Vulnerabilities (HPSBMU02895 SSRT101253)

HP Data Protector Multiple Vulnerabilities (HPSBMU03321 SSRT101677)

HP Data Protector Unspecified Local Unauthorized Access

HP Data Protector Unsupported

HP Ignite-UX TFTP /etc/pass File Disclosure

HP Ignite-UX TFTP File Access Information Disclosure

HP Ink Printers Multiple Vulnerabilities (HPSBHF03589)

HP Intelligent Management Center 7.x < 7.0-E0202P03 Multiple Vulnerabilities

HP Intelligent Management Center < 7.0 E0102 DES / ECB Weak Decryption Key

HP Intelligent Management Center APM Module < 7.0 E0101 SQL Injection

HP Intelligent Management Center BIMS Module Information Disclosure

HP Intelligent Management Center Branch Intelligent Management Module 7.x < 7.0-E0201P02 Multiple Vulnerabilities

HP Intelligent Management Center Branch Intelligent Management Module Multiple Vulnerabilities

HP Intelligent Management Center SOM Module < 7.0 E0101 Multiple Vulnerabilities

HP Intelligent Management Center SOM Module filePath Information Disclosure

HP Intelligent Management Center SOM Module Information Disclosure

HP Intelligent Management Center Web Administration Interface Default Credentials

HP Intelligent Management Center Web Administration Interface Detection

HP JetDirect < Q.24.09 Multiple Vulnerabilities

HP LaserJet Direct Print Filter Bypass

HP LaserJet LCD Display Modification

HP LaserJet Printer Unauthenticated Access

HP LaserJet Printers Multiple Vulnerabilities

HP LaserJet Printers RCE (HPSBPI03569)

HP LaserJet Printers Remote Unauthorized Access, DoS (HPSBPI03147)

HP LaserJet Printers Unspecified Denial of Service (HPSBPI02938)

HP LaserJet Printers Unspecified Information Disclosure (HPSBPI03546)

HP LaserJet Pro Printers Multiple Information Disclosures (July 2013)

HP LaserJet Pro Printers OpenSSL Heartbeat Information Disclosure (HPSBPI03014) (Heartbleed)

HP LaserJet Pro Printers Unauthorized Data Access

HP LaserJet Pro Printers Unauthorized Data Access (April 2013)

HP LeftHand OS Unmanaged Host Detection

HP Mercury LoadRunner Agent Remote Command Execution

HP Multiple Network Products Remote Information Disclosure and DoS (HPSBHF02912)

HP Multiple Network Products Unspecified Information Disclosure and Remote Code Execution (HPSBHF02888)

HP Network Automation Detection

HP Network Automation Remote Unauthorized Access (HPSBMU02738)

HP OfficeJet Printers RCE (HPSBPI03569)

HP OfficeJet Printers Unspecified Information Disclosure (HPSBPI03546)

HP Onboard Administrator < 4.22 Remote Information Disclosure

HP OpenView Communication Broker Arbitrary File Deletion (HPSBMU02691)

HP Operations Manager / Operations Agent < 11.13 XSS (HPSBMU03126)

HP Operations Manager 9.10 / 9.11 / 9.20 Multiple RCE

HP Operations Manager i (OMi) Unspecified RCE

HP Operations Manager Installed (Linux)

HP Operations Orchestration Detection

HP Printer Firmware Signing Disabled

HP Printers Security Bypass (HPSBPI03107)

HP ProCurve 5400 zl Switches Compact Flash Card Security Issue

HP ProCurve Switches Remote Unauthorized Information Disclosure

HP Service Manager Detection

HP StorageWorks File Migration Agent Unauthorized Access

HP StoreVirtual 4000 and StoreVirtual VSA Software < 11.5 Multiple Vulnerabilities

HP StoreVirtual 4000 and StoreVirtual VSA Software dbd\_manager RCE

HP Universal Configuration Management Database Server (UCMDB) Local Information Disclosure (HPSBGN03504)

HP Version Control Repository Manager for Linux < 7.5.0 Multiple Vulnerabilities (HPSBMU03396) (FREAK)

HP Version Control Repository Manager for Linux < 7.6.0 Multiple Vulnerabilities

HP Version Control Repository Manager Linux Detection (credentialed check)

HP-UX Ignite-UX TFTP Service Remote File Manipulation

HPE Intelligent Management Center 7.2 E0403P06 Multiple Vulnerabilities

HPE Intelligent Management Center dbman Command 10001 Information Disclosure

HPE Intelligent Management Center dbman Command 10018 Multiple Vulnerabilities

HPE Intelligent Management Center dbman Detection

HPE Intelligent Management Center dbman Multiple Vulnerabilities

HPE Intelligent Management Center dbman Opcode 10008 Command Injection

HPE Moonshot Provisioning Manager Detection

HPE Network Node Manager i (NNMi) Linux Detection (credentialed check)

HPE UCMDB 'UploadFileOnUIServerServlet' Servlet Path Handling RCE (HPESBGN03758)

HTTP Host Information via NTLM SSP over HTTP(S)

Huawei HG532e Home Gateway Command Injection

Huawei Versatile Routing Platform Version Detection

Huawei Versatile Security / Storage Platform Version Detection

HylaFAX hfaxd with PAM Password Policy Bypass

HylaFAX Installed

HylaFAX Remote Access Control Bypass

HylaFAX+ 5.2.4 < 5.5.4 Remote Buffer Overflow

IBM AS400 and iSeries POP3 Server Remote Information Disclosure

IBM Baseboard Management Controller Default Credentials

IBM BigFix Compliance 1.9.70 Multiple Vulnerabilities

IBM BigFix Platform 9.x < 9.1.9 / 9.2.x < 9.2.9 / 9.5.x < 9.5.4 Multiple Vulnerabilities

IBM DataPower Gateway < 7.5.2.2 Default Admin Password Security Bypass

IBM DataPower Gateway Detection

IBM Domino 8.5.3 FP6 / 9.0.1 < 8.5.3 FP6 IF2 / 9.0.1 FP1 iNotes XSS

IBM Domino 8.5.x / 9.0.x < 9.0.1 Fix Pack 8 TLS Server Diffie-Hellman Key Validation MitM

IBM Domino 8.5.x < 8.5.3 Fix Pack 5 Interim Fix 1 iNotes Buffer Overflow

IBM Domino 8.5.x < 8.5.3 Fix Pack 6 Interim Fix 13 Multiple Vulnerabilities

IBM Domino 8.5.x < 8.5.3 Fix Pack 6 Interim Fix 15 / 9.0.x < 9.0.1 Fix Pack 7 Interim Fix 1 Multiple Vulnerabilities

IBM Domino 8.5.x < 8.5.3 Fix Pack 6 Interim Fix 2 NX Memory Protection Disabled

IBM Domino 8.5.x < 8.5.3 Fix Pack 6 Interim Fix 4 GIF Code Execution

IBM Domino 8.5.x < 8.5.3 FP 5 Multiple Vulnerabilities

IBM Domino 8.5.x < 8.5.3 FP6 iNotes Multiple XSS (uncredentialed check)

IBM Domino 9.0 < 9.0.0 Interim Fix 4 iNotes Buffer Overflow

IBM Domino 9.0.x < 9.0.1 Fix Pack 3 Interim Fix 2 GIF Code Execution

IBM Domino 9.0.x < 9.0.1 Fix Pack 6 Multiple Vulnerabilities

IBM Domino 9.x < 9.0.1 Fix Pack 1 Multiple Vulnerabilities (uncredentialed check)

IBM Domino 9.x < 9.0.1 Fix Pack 2 Multiple Vulnerabilities (uncredentialed check)

IBM Domino 9.x < 9.0.1 Multiple Vulnerabilities (uncredentialed check)

IBM Domino < 8.5.3 FP 6 IF 1 / 9.0.1 IF 2 DoS

IBM Domino IMAP EXAMINE Command Handling RCE (EMPHASISMINE)

IBM Domino Unsupported Version Detection

IBM GCM16 / GCM32 Global Console Manager KVM Switch Detection

IBM GCM16 / GCM32 Global Console Manager KVM Switch Firmware Version < 1.20.0.22575 Remote Code Execution

IBM GCM16 / GCM32 Global Console Manager KVM Switch Firmware Version < 1.20.20.23447 Multiple Vulnerabilities

IBM Installation Manager Detection (Linux)

IBM Installed Software Enumeration

IBM Inventory Scout < 2.2.0.19 Symlink Vulnerability

IBM iSeries Default Password

IBM iSeries Login

IBM Lotus Sametime Multiplexer Buffer Overflow

IBM Netezza Platform Software Detection (Linux)

IBM Network Security Protection XGS Remote Code Execution (swg21690823) (credentialed check)

IBM Network Security Protection XGS WebUI Detection

IBM Rational Software Architect Design Manager / Engineering Lifecycle Manager / Rhapsody Design Manager < 4.0.7 XSRF

IBM Rational Software Architect Design Manager and Rhapsody Design Manager < 4.0.6000 Unspecified Vulnerability

IBM Rational Software Architect Design Manager and Rhapsody Design Manager < 4.0.7 Unspecified Vulnerability

IBM San Volume Controller / Storwize / FlashSystem 8.1.x < 8.1.0.1 privilege escalation vulnerability

IBM San Volume Controller / Storwize / FlashSystem Arbitrary File Read (CVE-2018-1775)

IBM Spectrum Protect Client Instrumentation Log Credentials Disclosure

IBM Spectrum Protect Client VM Backup INCLUDE.VMTSMVSS Option Credentials Disclosure

IBM Spectrum Protect Client Windows Registry Credentials Disclosure

IBM Storwize 1.3.x < 1.4.3.4 / 1.5.x < 1.5.0.2 Multiple Vulnerabilities

IBM Storwize 1.5.x / 1.6.x < 1.6.2.0 RC4 Initial Keystream Bias Vulnerability (CVE-2017-1375)

IBM Storwize Authenticated Information Disclosure

IBM Storwize Detection

IBM Storwize SSL/TLS RC4 Stream Cipher Key Invariance (Bar Mitzvah)

IBM Storwize V7000 Unified 1.3.x < 1.4.3.5 / 1.5.x < 1.5.0.4 Multiple Vulnerabilities (Shellshock)

IBM Storwize V7000 Unified ACL Security Bypass

IBM Storwize V7000 Unified Service Account Unspecified Local Privilege Escalation

IBM Tivoli Access Manager for e-Business / IBM Security Access Manager for Web Installed Components

IBM Tivoli Access Manager for e-Business < 6.0.0.31 / 6.1.0.12 / 6.1.1.8 or GSKit < 7.0.4.47 SSL/TLS Handshake Processing DoS

IBM Tivoli Access Manager for e-Business < 6.0.0.33 / 6.1.0.14 / 6.1.1.10 SSL Multiple Vulnerabilities

IBM Tivoli Access Manager for e-Business WebSEAL Multiple Vulnerabilities

IBM Tivoli NetView for z/OS Privilege Escalation

IBM Tivoli Storage FlashCopy Manager for VMware 3.1.x < 3.1.1.3 / 3.2.x < 3.2.0.6 / 4.1.x < 4.1.3.0 XSS

IBM Tivoli Storage FlashCopy Manager for VMware 3.1.x < 3.1.1.3 / 3.2.x < 3.2.0.6 / 4.1.x < 4.1.4.0 Command Execution

IBM Tivoli Storage FlashCopy Manager Installed (Linux)

IBM Tivoli Storage Manager Client DSO Local Privilege Escalation

IBM Tivoli Storage Manager Client Installed (Linux)

IBM Tivoli Storage Manager Client Local Buffer Overrun

IBM Tivoli Storage Manager Client Metadata Local File Access Information Disclosure

IBM Tivoli Storage Manager Client Symlink Cross-User Information Disclosure

IBM Tivoli Storage Manager for Virtual Environments Installed (Linux)

IBM TSM for Virtual Environments 6.3.x < 6.3.2.5 / 6.4.x < 6.4.3.1 / 7.1.x < 7.1.3.0 XSS

IBM TSM for Virtual Environments 6.3.x < 6.3.2.5 / 6.4.x < 6.4.3.1 / 7.1.x < 7.1.4.0 RCE

IBM TSM for Virtual Environments 6.4.x < 6.4.3.4 / 7.1.x < 7.1.6.0 RCE

IBM TSM for Virtual Environments 7.1.3.0 < 7.1.6.4 Windows Domain Credential Disclosure

ignitionServer < 0.3.6-P1 Multiple Vulnerabilities

ignitionServer SERVER Command Spoofed Server Saturation DoS

ignitionServer umode Command Global Operator Privilege Escalation

iLO 3 < 1.50 / iLO 4 < 1.13 Unspecified Information Disclosure

IMAP Service Cleartext Login Permitted

IMAP Service STARTTLS Command Support

IMAP Service STARTTLS Plaintext Command Injection

in.fingerd Pipe Input Arbitrary Command Execution

Informix Server GSKit 7.x < 7.0.4.50 / 8.0.50.x < 8.0.50.20 SSL CPU Utilization DoS

Informix Server GSKit 7.x <= 7.0.4.47 / 8.0.50.x <= 8.0.50.13 X.509 Certificate Chain DoS

Informix Server GSKit < 7.0.4.47 / 8.0.50.13 SSL/TLS DoS

INN < 2.2.2 Crafted Article Handling Remote Overflow

Intel Desktop Board Bitmap Processing Buffer Overflow (INTEL-SA-00020)

Intel Desktop Boards BIOS Unauthorized BIOS Flash (INTEL-SA-00019)

Intel Desktop Boards Privilege Escalation (INTEL-SA-00022)

Intel Multiple Products Crafted UEFI Variable Handling Security Bypass

Intel System Management Mode Local Privilege Escalation (INTEL-SA-00017)

Intel System Management Mode Local Privilege Escalation (INTEL-SA-00018)

Intel UEFI EFI S3 Resume Boot Path Script Privilege Escalation (INTEL-SA-00041)

Intel Xeon Baseboard Management Component (BMC) Privilege Escalation (INTEL-SA-00026)

Intellipeer POP3 Server User Account Enumeration

Internet Gateway Device WAN Interface UPnP Access

ipop2d fold Command Arbitrary File Access

Ipswitch IMail Server 11.x / 12.x < 12.3 Information Disclosure

Ipswitch IMail Server 11.x / 12.x < 12.4.1.15 Multiple Vulnerabilities (Heartbleed)

Ipswitch IMail Server < 11.02 Multiple Vulnerabilities

IRC Daemon STARTTLS Command Support

ircd-ratbox m\_capab.c Denial of Service

Irix Performance Copilot Service Information Disclosure

ISC DHCP 4.1.0 to 4.1-ESV-R15 / 4.2.0 to 4.2.8 / 4.3.0 to 4.3.6 DoS vulnerability

iSCSI Unauthenticated Target Detection

JAR File Detection for Linux/UNIX

Java JMX Agent Insecure Configuration

JBoss Detection

JBoss Remoting Detection

Juniper IVE OS Unintentionally Trusted Certificate Authorities

Juniper Junos Pulse Secure Access Service IVE OS (SSL VPN) Linux Network Connect Client Local Privilege Escalation (JSA10616)

Juniper Junos Pulse Secure Access Service IVE OS (SSL VPN) Multiple XSS (JSA10589)

Juniper Junos Pulse Secure Access Service IVE OS (SSL VPN) XSS (JSA10602)

Juniper Junos Pulse Secure Access Service IVE OS (SSL VPN) XSS (JSA10617)

Juniper JUNOSe IPv6 Packet Handling Line Card Reset Remote DoS (JSA10767)

Juniper JunosE Malformed ICMP Remote DoS (JSA10651)

Juniper NSM < 2012.2R11 Multiple OpenSSL Vulnerabilities (JSA10679) (FREAK)

Juniper NSM < 2012.2R14 OpenSSL Multiple Vulnerabilities (JSA10851)

Juniper NSM < 2012.2R9 Apache HTTP Server Multiple Vulnerabilities (JSA10685)

Juniper NSM < 2012.2R9 Apache HTTP Server Multiple Vulnerabilities (JSA10685) (credentialed check)

Juniper NSM < 2012.2R9 Multiple Java and Apache Vulnerabilities (JSA10642)

Juniper NSM Linux Kernel TCP Sequence Number Generation Issue (PSN-2012-08-688)

Juniper NSM Remote Code Execution (JSA10625)

Juniper NSM Servers < 2012.1 Multiple Vulnerabilities

Juniper NSM Servers < 2012.2R5 Multiple Vulnerabilities

Juniper NSM Servers Detection (credentialed check)

Juniper NSM Servers Multiple Java JDK/JRE Vulnerabilities (PSN-2012-08-689)

Juniper NSM Web Proxy Detection

Juniper NSM Web Proxy SOAP Interface Detection

Juniper Steel-Belted Radius Multiple OpenSSL Vulnerabilities

Junos Pulse Secure Access IVE / UAC OS Multiple OpenSSL Vulnerabilities (JSA10629)

Junos Pulse Secure Access IVE / UAC OS OpenSSL Heartbeat Information Disclosure (JSA10623) (Heartbleed)

Junos Pulse Secure Access IVE / UAC OS Weak Cipher Information Disclosure (JSA10628)

Junos Pulse Secure Access IVE / UAC OS XSS (JSA10645)

Junos Pulse Secure Access IVE OS Clickjacking (JSA10647)

Junos Pulse Secure Access IVE OS XSS (JSA10646)

Junos Pulse Secure Access Service (SSL VPN) Multiple XSS (JSA10554)

Junos Pulse Secure IVE / UAC OS DoS (JSA10590)

Junos Pulse Secure IVE / UAC OS Multiple SSL Vulnerabilities

K2 KeyServer Default Credentials

Kerberos 4 Realm Principle Impersonation

Kerberos 5 < 1.3.5 Multiple Vulnerabilities

Kerberos Information Disclosure

Kerberos Server Spoofed Packet Amplification DoS (PingPong)

Kerio Connect 8.2.x < 8.2.4 Heartbeat Information Disclosure (Heartbleed)

Kerio Connect < 7.0.0 Products Administration Console File Disclosure and Corruption Vulnerabilities

Kerio Connect < 8.1.0 SSL/TLS Information Disclosure (BEAST)

Kismet Server Information Disclosure

Kiwi CatTools < 3.2.9 TFTP Server Traversal Arbitrary File Manipulation

Knox Arkeia Backup Service Buffer Overflow

Knox Arkeia Network Backup Agent Default Account

Kubernetes 1.11.x < 1.11.9 / 1.12.x < 1.12.7 / 1.13.x < 1.13.5 kubectl directory traversal

Kubernetes 1.12.x < 1.12.9 / 1.13.x < 1.13.6 / 1.14.x < 1.14.2 kubectl directory traversal

Kubernetes 1.13.x < 1.13.10 / 1.14.x < 1.14.6 / 1.15.x < 1.15.3 DoS

Kubernetes 1.3.x < 1.7.14 / 1.8.x < 1.8.9 / 1.9.x < 1.9.4 multiple vulnerabilities

KVM / QEMU Guest Detection (credentialed check)

KVM / QEMU Guest Detection (uncredentialed check)

Lantronix Universal Device Server UDS1100 Version

LDAP 'Domain Admins' Group Membership Enumeration

LDAP Crafted Search Request Server Information Disclosure

LDAP Group Enumeration

LDAP NULL BASE Search Access

LDAP Server NULL Bind Connection Information Disclosure

LDAP Service STARTTLS Command Support

LDAP User Enumeration

leafnode Cross-Posted Article Group Name Prefix DoS

leafnode fetchnews DoS

Lenel OnGuard License Administrator

Lexmark / Dell Printer Unauthenticated Access

Lexmark MarkVision Enterprise < 2.1 Multiple Vulnerabilities

Lexmark Markvision Enterprise Java Object Deserialization RCE

Lexmark Markvision Enterprise Remote Command Execution

Lexmark MarkVision Enterprise ReportDownloadServlet Information Disclosure

Lexmark Printer config.html Administrator Authentication Bypass

Lexmark Printer config.html Administrator Authentication Bypass (FREAK)

Lexmark Printer Configuration Persistent XSS

libssh 0.6.x / 0.7.x < 0.7.6 / 0.8.x < 0.8.4 Authentication Bypass (Remote Version Check)

Lime Wire Multiple Remote Unauthorized Access

Linksys Router Detection

Linksys Smart Wi-Fi Web Interface Detection

Linux /proc/cpuinfo

Linux Daemons with Broken Links to Executables

Linux Kernel Detection of MDS vulnerabilities (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Linux Kernel IP Stack ICMP Error Response Arbitrary Memory Information Disclosure

Loxone Smart Home Miniserver < 6.3 Multiple Vulnerabilities

Loxone Smart Home Miniserver Web Server Version Detection

LSH Daemon < 1.4.3 / 1.5.3 lshd Remote Overflow

Mac OS X 10.7 / 10.8 Unauthorized File Access (remote check)

Mac OS X AFP Shared Folders Unauthenticated Access (Security Update 2010-006) (uncredentialed check)

Mac OS X Directory Service Buffer Overflow

Macallan IMAP Server Multiple Traversals Arbitrary File/Directory Manipulation

macOS 10.13 Authentication Bypass Remote Check (CVE-2017-13872)

MacOS Process Code Signing: Invalid

MacOS Process Code Signing: Invalid Apple

MacOS Process Code Signing: Misc

MacOS Process Code Signing: Not Apple

MacOS Process Code Signing: Not Signed

MacOS Process Code Signing: Signed

MacOS root Authentication Bypass Direct check over VNC Server (unauthenticated)

MagniComp SysInfo Agent Accessible

MagniComp SysInfo Installed (Linux/UNIX)

MagniComp SysInfo Privilege Escalation Vulnerability (Linux/UNIX)

Mailman Crated Email Remote User Password Disclosure

MAILsweeper Archive File Filtering Bypass

McAfee Agent 5.0.x / 5.5.0 / 5.5.1 Multiple Vulnerabilities (SB10260)

McAfee Agent 5.0.x < 5.0.6 HF1267994 / 5.5.x < 5.5.1 HF1267991 / 5.6.x < 5.6.1 UDP DoS (SB10272)

McAfee Agent 5.0.x < 5.0.6 HF1267994 / 5.5.x < 5.5.1 HF1267994 / 5.6.x < 5.6.0 Use-After-Free Vulnerability (SB10258)

McAfee Agent 5.5.x prior to 5.5.4 / 5.6.x prior to 5.6.4 Improper Access Control Vulnerability (SB10312)

McAfee Agent 5.6.x < 5.6.1 HF3 Privilege Escalation Vulnerability (SB10288)

McAfee Agent < 5.6.1 Information Disclosure Vulnerability (SB10271)

McAfee Agent Detection (Linux/MacOS)

McAfee Agent Unsupported Version Detection

McAfee Cloud Single Sign On < 4.0.1 Information Disclosure (SB10066) (McAfee Linux OS)

McAfee Drive Encryption 7.1 < 7.1.3 HF1241165 or 7.2.x < 7.2.6 Authentication Bypass vulnerability

McAfee Email Gateway Detection

McAfee Email Gateway Digest Token Reflected XSS (SB10099)

McAfee Email Gateway File Attachment Name NULL Character Handling Filter Bypass (SB10161)

McAfee Email Gateway GNU Bash Code Injection (SB10085) (Shellshock)

McAfee Email Gateway OpenSSL Information Disclosure (SB10071) (Heartbleed)

McAfee Email Gateway OpenSSL Multiple Vulnerabilities (SB10075)

McAfee Email Gateway Version

McAfee ePolicy Orchestrator Agent < 5.0.4.449 Log Viewer DoS

McAfee ePolicy Orchestrator Agent Remote Log Detection

McAfee ePolicy Orchestrator CSV File Handling Arbitrary Command Execution (SB10227)

McAfee ePolicy Orchestrator Insufficient Transport Layer Protection (SB10286)

McAfee ePolicy Orchestrator Multiple OpenSSL Vulnerabilities (SB10075)

McAfee ePolicy Orchestrator OpenSSL Information Disclosure (SB10071) (Heartbleed)

McAfee Next Generation Firewall GNU Bash Code Injection (SB10085) (Shellshock)

McAfee Next Generation Firewall OpenSSL Information Disclosure (SB10071) (Heartbleed)

McAfee Security Information and Event Management 9.3.x < 9.3.2.19 / 9.4.x < 9.4.2.9 / 9.5.x < 9.5.0.8 Authentication Bypass (SB10137)

McAfee Security Information and Event Management 9.5.x / 9.6.x < 9.6.0.3 ESM Authentication Bypass (KB87744)

McAfee VirusScan Enterprise for Linux <= 2.0.3 Multiple vulnerabilities (SB10181)

McAfee VirusScan Enterprise for Linux Detection

McAfee VirusScan Enterprise for Linux Detection and Status

McAfee VirusScan Enterprise for Linux Multiple OpenSSL Vulnerabilities (SB10075)

McAfee VirusScan Enterprise for Linux OpenSSL Information Disclosure (SB10071) (Heartbleed)

McAfee VirusScan Enterprise for Linux Unsupported Version Detection

McAfee Web Gateway 7.6.x < 7.6.2.15 / 7.7.x < 7.7.2.3 Multiple Vulnerabilities (SB10205)

McAfee Web Gateway < 7.3.2.2 DoS (SB10052)

McAfee Web Gateway < 7.3.2.6 / 7.4.1 Information Disclosure (SB10063)

McAfee Web Gateway Detection

McAfee Web Gateway GNU Bash Code Injection (SB10085) (Shellshock)

McAfee Web Gateway Information Disclosure (SB10080)

McAfee Web Gateway Multiple OpenSSL Vulnerabilities (SB10075)

McAfee Web Gateway OpenSSL Information Disclosure (SB10071) (Heartbleed)

Memcached / MemcacheDB ASLR Bypass Weakness

memcached SASL Authentication Security Bypass

MERCUR Mailserver Local Traversal Arbitrary File Access

MiCasaVerde VeraLite UPnP RCE

Microsoft Exchange Server Detection (Uncredentialed)

Microsoft SQL Server STARTTLS Support

MikroTik RouterOS 5.x < 5.26 / 6.x < 6.3 sshd Unspecified Remote Heap Corruption

MikroTik RouterOS < 6.40.9 / 6.42.7 / 6.43 multiple vulnerabilities.

MikroTik RouterOS < 6.39.3 / 6.40.4 / 6.41rc (KRACK)

MikroTik RouterOS < 6.40.7 or 6.41.x < 6.41.3 SMB Buffer Overflow

MikroTik RouterOS < 6.44.6 LTS or 6.45.x < 6.45.7 Multiple Vulnerabilities

MikroTik RouterOS DNS Cache Poisoning (CVE-2019-3978)

MikroTik RouterOS HTTP Server Arbitrary Write RCE (ChimayRed)

MikroTik RouterOS Unauthenticated Intermediary

MikroTik RouterOS Winbox Unauthenticated Arbitrary File Read/Write Vulnerability

MikroTik RouterOS with Blank Password (telnet check)

MikroTik Winbox < 5.17 File Download DoS

MiniUPnP < 1.9 Multiple Vulnerabilities

MiniUPnP DNS Rebind Vulnerability

Motorola Vanguard with No Password (telnet check)

Mount iSCSI Targets with 'None' Authentication

Moxa MiiNePort Blank Default Telnet Password

MSSQL Host Information in NTLM SSP

Multiple Command Injection Vulnerabilities in Grandstream Products

Multiple Command Injection Vulnerabilities in Grandstream Products

Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

Multiple Unix Netstat Service Remote Information Disclosure

Multiple Vendors EAS Authentication Bypass

Nagios NRPE Command Argument Processing Enabled

Nagios NRPE nrpe.c Arbitrary Command Execution

NAI WebShield SMTP GET\_CONFIG Information Disclosure

NAS4Free Version

NAS4Free Web UI Detection

NCR Aloha POS SOAP API Detection

NCR Aloha POS VNC Server 'aloha' Default Password

Nessus 5.x < 5.2.12 / 6.x < 6.4 Multiple OpenSSL Vulnerabilities

Nessus SQLite Multiple RCE

Nessus Unsupported Version Detection

NetApp Clustered Data ONTAP 8.x < 8.3.2P12 (NTAP-20170831-0002)

NetApp Clustered Data ONTAP 8.x < 8.3.2P8 / 9.x < 9.0P2 (NTAP-20170814-0001)

NetApp Clustered Data ONTAP < 8.2.5 / 8.3.x < 8.3.2P12 (NTAP-20170831-0003)

NetApp Data ONTAP (7-Mode) < 8.2.5P3 Multiple Vulnerabilities (ntap-20190801-0001)(ntap-20190801-0002)(ntap-20190802-0002)

NetApp ONTAP 8.x.x < 8.2.5 (NTAP-20170815-0002)

NetApp ONTAP Device Detection

NETGEAR DGN2200 Multiple Vulnerabilities

NETGEAR FM114P ProSafe Router Multiple Vulnerabilities

NETGEAR Hard-coded Telnet Unlock Credentials

NETGEAR Web Interface Detection

NetInfo Arbitrary Remote File Access

NetIQ Sentinel < 7.4.1 Multiple Vulnerabilities

NetIQ Sentinel Java Object Deserialization RCE

NetIQ Sentinel Java Object Deserialization RCE

Netopia Router Crafted SNMP Request Remote Admin Password Disclosure

Netscape Messenging Server POP3 Error Message User Account Enumeration

Netstat Active Connections

Network daemons not managed by the package system

Network Time Protocol (NTP) Mode 6 Scanner

Network Time Protocol Daemon (ntpd) 3.x / 4.x < 4.2.8p2 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 3.x / 4.x < 4.2.8p3 Denial Of Service Vulnerability

Network Time Protocol Daemon (ntpd) 3.x / 4.x < 4.2.8p4 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 3.x / 4.x < 4.2.8p5 Denial Of Service Vulnerability

Network Time Protocol Daemon (ntpd) 3.x / 4.x < 4.2.8p6 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 3.x / 4.x < 4.2.8p7 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 4.x < 4.2.4p7 / 4.x < 4.2.5p74 crypto\_recv() Function RCE

Network Time Protocol Daemon (ntpd) 4.x < 4.2.8p1 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 4.x < 4.2.8p10 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 4.x < 4.2.8p11 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 4.x < 4.2.8p12 / 4.3.x < 4.3.94 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 4.x < 4.2.8p13 / 4.3.x < 4.3.94 DoS

Network Time Protocol Daemon (ntpd) 4.x < 4.2.8p8 / 4.3.x < 4.3.93 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) 4.x < 4.2.8p9 Multiple Vulnerabilities

Network Time Protocol Daemon (ntpd) < 4.2.1 -u Group Permission Weakness Privilege Escalation

Network Time Protocol Daemon (ntpd) Information Disclosure

Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS

Network Time Protocol Daemon (ntpd) read\_mru\_list() Remote DoS

Network UPS Tools < 2.6.4 addchar() Function Buffer Overflow

Network UPS Tools Cleartext Authentication

Network UPS Tools Service STARTTLS Command Support

NNTP Authentication Methods

NNTP Service Cleartext Login Permitted

NNTP Service STARTTLS Plaintext Command Injection

Node.js multiple vulnerabilities (August 2018 Security Releases).

Node.js multiple vulnerabilities (July 2018 Security Releases).

Node.js multiple vulnerabilities (March 2018 Security Releases).

Node.js multiple vulnerabilities (November 2018 Security Releases).

Nokia VitalQIP Web Client Default Credentials

Nokia VitalQIP Web Client Detection

Nortel Baystack Default Password

Nortel CS Signaling Server Default Admin Credentials

Nortel Meridian Integrated RAN Default Admin Credentials

Nortel Multiple Default Accounts

Nortel Networks Router Unpassworded Account (manager Level)

Nortel Networks Router Unpassworded Account (User Level)

Nortel/Bay Networks Default Password

Nortel/Bay Networks/Xylogics Annex Default Password

Novell eDirectory 8.8.x Multiple Security Vulnerabilities

Novell eDirectory < 8.7.3 SP10 FTF1 Multiple Vulnerabilities

Novell eDirectory < 8.8 SP3 Multiple Vulnerabilities (OF, XSS, MC)

Novell eDirectory < 8.8 SP5 Multiple Vulnerabilities

Novell eDirectory < 8.8 SP5 Patch 3 eMBox SOAP Request DoS

Novell eDirectory < 8.8 SP5 Patch 4 Multiple Vulnerabilities

Novell eDirectory < 8.8 SP6 Patch 5 Multiple Vulnerabilities

Novell eDirectory < 8.8.5.2 / 8.7.3.10 ftf2 'NDS Verb' Request Buffer Overflow

Novell eDirectory eMBox Utility Unauthorized Access (uncredentialed check)

Novell File Reporter Agent FSFUI UICMD 126 Arbitrary File Download

Novell NetIQ Access Manager Installed (Linux)

Novell NetIQ Identity Manager Installed (Linux)

Novell ZENworks ChangePassword RPC XPath Injection

NSClient Default Password

NTP ntpd Mode 7 Error Response Packet Loop Remote DoS

NUUO NVR Web Interface Detection

NUUO NVRMini2 Authenticated Command Injection

NUUO NVRMini2 Multiple Vulnerabilities

NVIDIA Graphics Card Driver Detection (Unix / Linux)

NVIDIA Graphics Driver NVAPI Support Layer Integer Overflow Privilege Escalation (Unix / Linux)

NVIDIA Graphics Driver Pointer Dereference Privilege Escalation (Unix / Linux)

NVIDIA Graphics Driver Unspecified Privilege Escalation (Unix / Linux)

NVIDIA Linux GPU Display Driver 304.x < 304.132 / 340.x < 340.98 / 361.93.x < 361.93.03 / 367.x < 367.55 / 370.x < 370.28 Multiple Vulnerabilities

NVIDIA Linux GPU Display Driver 304.x < 304.134 / 340.x < 340.101 / 361.x < 361.107 / 375.x < 375.26 GPU Interrupt Saturation DoS

NVIDIA Linux GPU Display Driver 304.x < 304.135 / 340.x < 340.102 / 361.x < 361.119 / 375.x < 375.39 / 378.x < 378.13 Multiple Vulnerabilities

NVIDIA Linux GPU Display Driver 375.8x < 375.82 / 375.7x < 375.74 / 384.x < 384.59 Multiple Vulnerabilities

NVIDIA Linux GPU Display Driver 375.x < 375.66 / 381.x < 381.22 Multiple Vulnerabilities

NVIDIA Linux GPU Display Driver 375.x < 375.88 / 384.x < 384.90 Multiple Vulnerabilities

NVIDIA Linux GPU Display Driver 384.x < 384.111 / 390.x < 390.12 Multiple Vulnerabilities (Meltdown)(Spectre)

NVIDIA Linux GPU Display Driver Information Disclosure Vulnerability (CVE-2018-6260)

NVIDIA Linux GPU Display Driver Multiple Vulnerabilities

ONVIF Camera Snapshot

ONVIF Device Information

ONVIF Device Services

ONVIF Get Device User List

ONVIF Stream URI

OpenBSD 6.6 Multiple Authentication Bypass Vulnerabilties

OpenNMS Java Object Deserialization RCE

OpenSSH < 4.3 scp Command Line Filename Processing Command Injection

OpenSSH 2.3.1 SSHv2 Public Key Authentication Bypass

OpenSSH 2.5.x - 2.9 Multiple Vulnerabilities

OpenSSH 5.4 < 7.1p2 Multiple Vulnerabilities

OpenSSH 6.2 and 6.3 AES-GCM Cipher Memory Corruption

OpenSSH 6.8p1 - 7.x < 7.1p2 ssh\_packet\_read\_poll2() Packet Handling DoS

OpenSSH 7.7 < 8.1

OpenSSH 7.x < 7.1 PermitRootLogin Security Bypass

OpenSSH < 1.2.2 sshd Local TCP Redirection Connection Masking Weakness

OpenSSH < 1.2.3 xauth Session Highjacking

OpenSSH < 2.1.0 /dev/random Check Failure

OpenSSH < 2.1.1 UseLogin Local Privilege Escalation

OpenSSH < 2.1.1p3 Format String Privilege Escalation

OpenSSH < 2.5.2 / 2.5.2p2 Multiple Information Disclosure Vulnerabilities

OpenSSH < 2.9.9 / 2.9p2 Symbolic Link 'cookies' File Removal

OpenSSH < 2.9.9p1 Resource Limit Bypass

OpenSSH < 2.9.9p2 echo simulation Information Disclosure

OpenSSH < 3.0.1 Multiple Flaws

OpenSSH < 3.0.2 Multiple Vulnerabilities

OpenSSH < 3.4p1 scp Traversal Arbitrary File Overwrite

OpenSSH < 3.6.2 Reverse DNS Lookup Bypass

OpenSSH < 4.0 known\_hosts Plaintext Host Information Disclosure

OpenSSH < 4.2 Multiple Vulnerabilities

OpenSSH < 4.4 Multiple Vulnerabilities

OpenSSH < 4.5 Multiple Vulnerabilities

OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass

OpenSSH < 4.9 'ForceCommand' Directive Bypass

OpenSSH < 5.2 CBC Plaintext Disclosure

OpenSSH < 5.7 Multiple Vulnerabilities

OpenSSH < 6.6 Multiple Vulnerabilities

OpenSSH < 6.9 Multiple Vulnerabilities

OpenSSH < 7.0 Multiple Vulnerabilities

OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security Bypass

OpenSSH < 7.2p2 X11Forwarding xauth Command Injection

OpenSSH < 7.3 Multiple Vulnerabilities

OpenSSH < 7.4 Multiple Vulnerabilities

OpenSSH < 7.5

OpenSSH < 7.6

OpenSSH >= 2.3.0 AllowTcpForwarding Port Bouncing

OpenSSH Client Unauthorized X11 Remote Forwarding

OpenSSH Legacy Certificate Signing Information Disclosure

OpenSSH MaxAuthTries Bypass

OpenSSH S/KEY Authentication Account Enumeration

OpenSSH SSHFP Record Verification Weakness

OpenSSH w/ PAM Multiple Timing Attack Weaknesses

OpenSSH X11 Forwarding Session Hijacking

OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking

OpenSSL 'ChangeCipherSpec' MiTM Potential Vulnerability

OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

OpenSSL ASN.1 Parser Multiple Remote DoS

OpenSSL Heartbeat Information Disclosure (Heartbleed)

Openswan < 2.6.36 IKE Packet NULL Pointer Dereference Remote DoS

Openswan < 2.6.37 Cryptographic Helper Use-After-Free Remote DoS

OpenVAS Administrator / Manager Authentication Bypass

OpenVPN Heartbeat Information Disclosure (Heartbleed)

OpenVPN Unprotected Management Interface

OpenVZ Guest Detection

OPIE w/ OpenSSH Account Enumeration

Oracle Access Manager (October 2013 CPU)

Oracle Access Manager (October 2014 CPU)

Oracle Access Manager Information Disclosure (October 2015 CPU)

Oracle Access Manager Multiple Vulnerabilities (Apr 2018 CPU)

Oracle Access Manager Multiple Vulnerabilities (Apr 2020 CPU)

Oracle Access Manager Multiple Vulnerabilities (Jan 2018 CPU)

Oracle Access Manager Multiple Vulnerabilities (January 2015 CPU)

Oracle Access Manager Multiple Vulnerabilities (July 2015 CPU)

Oracle Access Manager Server Installation Detection (credentialed check)

Oracle Access Manager Unspecified WebGate Webserver Plugin Vulnerability

Oracle Access Manager Webgate Information Disclosure (July 2016 CPU)

Oracle Adaptive Access Manager Server Arbitrary Code Execution (October 2014 CPU)

Oracle Adaptive Access Manager Server Detection

Oracle Adaptive Access Manager Unspecified Remote Vulnerability (January 2015 CPU)

Oracle Application Express (APEX) / REST Data Services Listener Installation Detection

Oracle Application Express Listener Remote Information Disclosure Vulnerability (July 2012 CPU)

Oracle Application Testing Suite (Apr 2020 CPU)

Oracle Application Testing Suite Detection

Oracle Application Testing Suite Java Object Deserialization RCE (April 2016 CPU)

Oracle Application Testing Suite Multiple Vulnerabilities (April / July 2018 CPU)

Oracle Application Testing Suite Multiple Vulnerabilities (Jan 2019 CPU)

Oracle Application Testing Suite Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Application Testing Suite Multiple Vulnerabilities (Jul 2019 CPU)

Oracle BI Publisher Installation Detection

Oracle Database Management Plug-In Unix (October 2013 CPU) (credentialed check)

Oracle E-Business (January 2014 CPU)

Oracle E-Business (July 2013 CPU)

Oracle E-Business (July 2014 CPU)

Oracle E-Business (October 2013 CPU)

Oracle E-Business Multiple Vulnerabilities (April 2015 CPU)

Oracle E-Business Multiple Vulnerabilities (April 2016 CPU)

Oracle E-Business Multiple Vulnerabilities (April 2017 CPU)

Oracle E-Business Multiple Vulnerabilities (April 2018 CPU)

Oracle E-Business Multiple Vulnerabilities (Jan 2019 CPU)

Oracle E-Business Multiple Vulnerabilities (January 2015 CPU)

Oracle E-Business Multiple Vulnerabilities (January 2016 CPU)

Oracle E-Business Multiple Vulnerabilities (January 2017 CPU)

Oracle E-Business Multiple Vulnerabilities (January 2018 CPU)

Oracle E-Business Multiple Vulnerabilities (July 2015 CPU)

Oracle E-Business Multiple Vulnerabilities (July 2016 CPU)

Oracle E-Business Multiple Vulnerabilities (July 2017 CPU) (SWEET32)

Oracle E-Business Multiple Vulnerabilities (July 2018 CPU)

Oracle E-Business Multiple Vulnerabilities (Oct 2018 CPU)

Oracle E-Business Multiple Vulnerabilities (October 2014 CPU)

Oracle E-Business Multiple Vulnerabilities (October 2015 CPU)

Oracle E-Business Multiple Vulnerabilities (October 2016 CPU)

Oracle E-Business Multiple Vulnerabilities (October 2017 CPU)

Oracle E-Business Suite Multiple Vulnerabilities (Apr 2019 CPU)

Oracle E-Business Suite Multiple Vulnerabilities (Jan 2020 CPU)

Oracle E-Business Suite Multiple Vulnerabilities (Jul 2019 CPU)

Oracle E-Business Suite Multiple Vulnerabilities (Oct 2019 CPU)

Oracle E-Business Version and Patch Info

Oracle Enterprise Manager Agent Installation Detection (credentialed check)

Oracle Enterprise Manager Agent Unspecified Vulnerabilities (October 2015 CPU)

Oracle Enterprise Manager Cloud Control (Apr 2019 CPU)

Oracle Enterprise Manager Cloud Control (Apr 2020 CPU)

Oracle Enterprise Manager Cloud Control (Jan 2020 CPU)

Oracle Enterprise Manager Cloud Control (January 2019 CPU)

Oracle Enterprise Manager Cloud Control (Jul 2019 CPU)

Oracle Enterprise Manager Cloud Control (Oct 2019 CPU)

Oracle Enterprise Manager Cloud Control (October 2018 CPU)

Oracle Enterprise Manager Cloud Control Installation Detection (credentialed check)

Oracle Enterprise Manager Cloud Control Multiple Vulnerabilities (Apr 2018 CPU)

Oracle Enterprise Manager Cloud Control Multiple Vulnerabilities (January 2015 CPU)

Oracle Enterprise Manager Cloud Control Multiple Vulnerabilities (January 2016 CPU)

Oracle Enterprise Manager Cloud Control Multiple Vulnerabilities (January 2017 CPU)

Oracle Enterprise Manager Cloud Control Multiple Vulnerabilities (July 2015 CPU)

Oracle Enterprise Manager Cloud Control Multiple Vulnerabilities (July 2016 CPU)

Oracle Enterprise Manager Cloud Control Multiple Vulnerabilities (July 2018 CPU)

Oracle Enterprise Manager Cloud Control Plugins Detection (credentialed check)

Oracle Enterprise Manager Cloud Control Security Framework Vulnerability (October 2016 CPU)

Oracle Enterprise Manager Cloud Control Unspecified Vulnerability (April 2015 CPU)

Oracle Enterprise Manager Content Management Sub-Component Unspecified Vulnerability (October 2014 CPU)

Oracle Enterprise Manager Grid Control Multiple Vulnerabilities (April 2017 CPU) (SWEET32)

Oracle Enterprise Manager Grid Control Multiple Vulnerabilities (July 2017 CPU) (httpoxy)

Oracle Enterprise Manager Ops Center (Apr 2019 CPU)

Oracle Enterprise Manager Ops Center (Jan 2019 CPU)

Oracle Enterprise Manager Ops Center (Jan 2020 CPU)

Oracle Enterprise Manager Ops Center (Jul 2019 CPU)

Oracle Enterprise Manager Ops Center (Oct 2019 CPU)

Oracle Enterprise Manager Ops Center Installed (Linux / Unix)

Oracle Enterprise Manager Ops Center Remote Code Execution (October 2017 CPU)

Oracle Event Processing CVE-2014-2424 Unspecified Vulnerability (April 2014 CPU)

Oracle Event Processing Installation Detection (credentialed check)

Oracle Forms and Reports Multiple Unspecified Vulnerabilities (January 2015 CPU)

Oracle Glassfish Installed (Linux/UNIX)

Oracle GoldenGate for Big Data 12.2.0.1.x < 12.2.0.1.10 / 12.3.1.1.x < 12.3.1.1.6 Multiple Vulnerabilities (Oct 2018 CPU)

Oracle GoldenGate for Big Data 12.3.1.1.x < 12.3.1.1.6 / 12.3.2.1.x < 12.3.2.1.5 Spring Framework DoS (Oct 2019 CPU)

Oracle GoldenGate for Big Data 12.3.2.1.x < 12.3.2.1.2 Apache Log4j Insecure Deserialization RCE (Jan 2019 CPU)

Oracle GoldenGate for Big Data JAR Detection

Oracle GoldenGate Information Disclosure (April 2018 CPU)

Oracle GoldenGate Installation Detection

Oracle GoldenGate Manager < 12.2.0.1.1 OBEY Command ggserr.log File Handling RCE

Oracle GoldenGate Multiple Vulnerabilities (October 2018 CPU)

Oracle HTTP Server Installed

Oracle Identity Manager (April 2012 CPU)

Oracle Identity Manager (October 2013 CPU

Oracle Identity Manager (October 2014 CPU

Oracle Identity Manager Default Account Local Check (CVE-2017-10151)

Oracle Identity Manager Detection

Oracle Identity Manager End User Self Service (January 2014 CPU)

Oracle Identity Manager Identity Console (January 2014 CPU)

Oracle Identity Manager Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Identity Manager Multiple Vulnerabilities (January 2018 CPU)

Oracle Identity Manager Multiple Vulnerabilities (October 2018 CPU)

Oracle Identity Manager OIM Legacy UI Unspecified Vulnerability (October 2015 CPU)

Oracle Identity Manager Remote Security Vulnerability (Jul 2019 CPU)

Oracle Identity Manager Rules Engine Vulnerability (April 2017 CPU)

Oracle Installed Software Enumeration (Linux / Unix)

Oracle Integrated Lights Out Manager Default Credentials

Oracle Internet Directory LDAP Server Unspecified Remote Information Disclosure

Oracle Java JDK / JRE 5 < Update 41 Remote Code Execution (Unix)

Oracle Java JDK / JRE 6 < Update 20 Multiple Vulnerabilities (Unix)

Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities (Unix)

Oracle Java JDK / JRE 6 < Update 35 Multiple Vulnerabilities

Oracle Java JDK / JRE 6 < Update 43 Remote Code Execution (Unix)

Oracle Java JDK / JRE 7 < Update 17 Remote Code Execution (Unix)

Oracle Java JRE Premier Support and Extended Support Version Detection (Unix)

Oracle Java JRE Unsupported Version Detection (Unix)

Oracle Java SE 1.7.0\_221 / 1.8.0\_211 / 1.11.0\_3 / 1.12.0\_1 Multiple Vulnerabilities (Apr 2019 CPU) (Unix)

Oracle Java SE 1.7.0\_231 / 1.8.0\_221 / 1.11.0\_4 / 1.12.0\_2 Multiple Vulnerabilities (Jul 2019 CPU) (Unix)

Oracle Java SE 1.7.0\_241 / 1.8.0\_231 / 1.11.0\_5 / 1.13.0\_1 Multiple Vulnerabilities (Oct 2019 CPU) (Unix)

Oracle Java SE 1.7.0\_251 / 1.8.0\_241 / 1.11.0\_6 / 1.13.0\_2 Multiple Vulnerabilities (Jan 2020 CPU) (Unix)

Oracle Java SE 1.7.0\_261 / 1.8.0\_251 / 1.11.0\_7 / 1.14.0\_1 Multiple Vulnerabilities (Apr 2020 CPU) (Unix)

Oracle Java SE 1.7.x < 1.7.0\_211 / 1.8.x < 1.8.0\_201 / 1.11.x < 1.11.0\_2 Multiple Vulnerabilities (January 2019 CPU) (Unix)

Oracle Java SE 7 < Update 11 Multiple Vulnerabilities (Unix)

Oracle Java SE 7 < Update 7 Multiple Vulnerabilities (Unix)

Oracle Java SE Multiple Vulnerabilities (April 2013 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (April 2014 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (April 2015 CPU) (Unix) (FREAK)

Oracle Java SE Multiple Vulnerabilities (April 2016 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (April 2017 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (April 2018 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (February 2011 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (February 2012 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (February 2013 CPU Update 1) (Unix)

Oracle Java SE Multiple Vulnerabilities (February 2013 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (January 2014 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (January 2015 CPU) (Unix) (POODLE)

Oracle Java SE Multiple Vulnerabilities (January 2016 CPU) (SLOTH) (Unix)

Oracle Java SE Multiple Vulnerabilities (January 2017 CPU) (Unix) (SWEET32)

Oracle Java SE Multiple Vulnerabilities (January 2018 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (July 2014 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (July 2015 CPU) (Unix) (Bar Mitzvah)

Oracle Java SE Multiple Vulnerabilities (July 2016 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (July 2017 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (July 2018 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (June 2011 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (June 2012 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (June 2013 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (March 2010 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2010 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2011 CPU) (BEAST) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2012 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2013 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2014 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2015 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2016 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2017 CPU) (Unix)

Oracle Java SE Multiple Vulnerabilities (October 2018 CPU) (Unix)

Oracle JDeveloper ADF Faces DoS (July 2015 CPU)

Oracle JDeveloper ADF Faces goButton XSS (October 2014 CPU)

Oracle JDeveloper ADF Faces Unspecified Remote Code Execution (October 2017 CPU)

Oracle JDeveloper ADF Faces Unspecified Remote Information Disclosure (January 2017 CPU)

Oracle JDeveloper Information Disclosure Vulnerability (July 2018 CPU)

Oracle JDeveloper Installation Detection

Oracle JDeveloper Multiple RCE (July 2016 CPU)

Oracle JDeveloper Multiple Vulnerabilities (January 2018 CPU)

Oracle JDeveloper Multiple Vulnerabilities (October 2015 CPU)

Oracle MySQL Connectors (Apr 2020 CPU)

Oracle MySQL Connectors DoS (Jul 2018 CPU)

Oracle MySQL Connectors Multiple Vulnerabilities (Apr 2019 CPU)

Oracle MySQL Connectors Multiple Vulnerabilities (Jan 2018 CPU)

Oracle MySQL Connectors Multiple Vulnerabilities (Oct 2019 CPU)

Oracle MySQL Connectors OpenSSL (Jan 2020 CPU)

Oracle MySQL Connectors Unspecified Vulnerability (Jan 2019 CPU)

Oracle Oracle E-Business Suite (Apr 2020 CPU)

Oracle Primavera Gateway Detection

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Detection

Oracle Primavera Unifier Detection

Oracle Secure Global Desktop Linux Installation Detection

Oracle Secure Global Desktop Multiple DoS Vulnerabilities (October 2014 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (April 2014 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (April 2017 CPU) (SWEET32)

Oracle Secure Global Desktop Multiple Vulnerabilities (April 2018 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (January 2014 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (January 2015 CPU) (POODLE)

Oracle Secure Global Desktop Multiple Vulnerabilities (January 2016 CPU) (Logjam)

Oracle Secure Global Desktop Multiple Vulnerabilities (January 2018 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (January 2019 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (January 2020 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (July 2014 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (July 2015 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (July 2016 CPU)

Oracle Secure Global Desktop Multiple Vulnerabilities (July 2018 CPU)

Oracle Secure Global Desktop ttaauxserv Remote Denial of Service (credentialed check)

Oracle Secure Global Desktop ttaauxserv Remote Denial of Service (remote check)

Oracle Secure Global Desktop Unspecified Vulnerability (October 2016 CPU)

Oracle Secure Global Desktop Unsupported Version Detection

Oracle Secure Global Desktop Web Services Component Remote Authentication Bypass (October 2017 CPU)

Oracle Traffic Director Multiple Vulnerabilities (July 2014 CPU)

Oracle Tuxedo Installation Detection

Oracle Tuxedo Installed (Linux/UNIX)

Oracle Tuxedo Jolt Server Multiple Vulnerabilities (CVE-2017-10269)

Oracle Tuxedo Multiple Vulnerabilities (Apr 2019 CPU)

Oracle Tuxedo Multiple Vulnerabilities (July 2018 CPU)

Oracle Tuxedo Remote Code Execution Vulnerability (Jan 2020 CPU)

Oracle VM VirtualBox (Apr 2020 CPU)

Oracle VM VirtualBox 5.0.x < 5.0.28 / 5.1.x < 5.1.8 Multiple Vulnerabilities (October 2016 CPU)

Oracle VM VirtualBox 5.0.x < 5.0.32 / 5.1.x < 5.1.14 Multiple Vulnerabilities (January 2017 CPU)

Oracle VM VirtualBox 5.0.x < 5.0.34 / 5.1.x < 5.1.16 Shared Folder Implementation Information Disclosure

Oracle VM VirtualBox 5.0.x < 5.0.38 / 5.1.x < 5.1.20 (April 2017 CPU)

Oracle VM VirtualBox 5.1.x < 5.1.24 (July 2017 CPU)

Oracle VM VirtualBox 5.1.x < 5.1.30 (October 2017 CPU)

Oracle VM VirtualBox 5.1.x < 5.1.32 / 5.2.x < 5.2.6 (January 2018 CPU)

Oracle VM VirtualBox 5.1.x < 5.1.36 / 5.2.x < 5.2.10 (April 2018 CPU)

Oracle VM VirtualBox 5.2.x < 5.2.24 / 6.0.x < 6.0.2 (Jan 2019 CPU)

Oracle VM VirtualBox 5.2.x < 5.2.28 / 6.0.x < 6.0.6 (Apr 2019 CPU)

Oracle VM VirtualBox 5.2.x < 5.2.32 / 6.0.x < 6.0.10 (Jul 2019 CPU)

Oracle VM VirtualBox 5.2.x < 5.2.36 / 6.0.x < 6.0.16 / 6.1.x < 6.1.2 (Jan 2020 CPU)

Oracle VM VirtualBox < 4.0.30 / 4.1.38 / 4.2.30 / 4.3.26 / 5.0.0 Core DoS (October 2015 CPU)

Oracle VM VirtualBox < 4.0.32 / 4.1.40 / 4.2.32 / 4.3.30 Core Unspecified Vulnerability (July 2015 CPU)

Oracle VM VirtualBox < 4.0.34 / 4.1.42 / 4.2.34 / 4.3.32 / 5.0.8 Multiple Core DoS (October 2015 CPU)

Oracle VM VirtualBox < 4.0.36 / 4.1.44 / 4.2.36 / 4.3.34 / 5.0.10 Multiple Vulnerabilities (January 2016 CPU)

Oracle VM VirtualBox < 4.3.36 / 5.0.14 Multiple Vulnerabilities (January 2016 CPU)

Oracle VM VirtualBox < 4.3.36 / 5.0.18 Multiple Vulnerabilities (April 2016 CPU)

Oracle VM VirtualBox < 5.0.22 Multiple Vulnerabilities (July 2016 CPU)

Oracle VM VirtualBox < 5.0.26 Core Subcomponent DoS (July 2016 CPU)

Oracle VM VirtualBox < 5.2.16 Multiple Vulnerabilities (July 2018 CPU)

Oracle VM VirtualBox < 5.2.20 Multiple Vulnerabilities (Oct 2018 CPU)

Oracle WebCenter Portal Arbitrary File Read (Oct 2019 CPU)

Oracle WebCenter Portal Installation Detection

Oracle WebCenter Portal Multiple Vulnerabilities (Apr 2019 CPU)

Oracle WebCenter Portal Multiple Vulnerabilities (April 2018 CPU)

Oracle WebCenter Portal Multiple Vulnerabilities (Jan 2019 CPU)

Oracle WebCenter Portal Multiple Vulnerabilities (January 2018 CPU)

Oracle WebCenter Portal Multiple Vulnerabilities (July 2015 CPU)

Oracle WebCenter Portal Multiple Vulnerabilities (July 2018 CPU)

Oracle WebCenter Portal Multiple Vulnerabilities (Oct 2018 CPU)

Oracle WebCenter Portal Page Service Subcomponent Unspecified Information Disclosure

Oracle WebCenter Portal People Connection Subcomponent Unspecified Information Disclosure (April 2014 CPU)

Oracle WebCenter Portal Unspecified Remote Information Disclosure (July 2014 CPU)

Oracle WebCenter Portal Unspecified Remote Vulnerabilities (April 2015 CPU)

Oracle WebLogic Portal Apache Commons File Upload (January 2016 CPU)

Oracle WebLogic Portal Detection

Oracle WebLogic Server (Apr 2020 CPU)

Oracle WebLogic Server Detection

Oracle WebLogic Server Java Object Deserialization RCE (Local Check)

Oracle WebLogic Server Java Object RMI Connect-Back Deserialization RCE (January 2017 CPU)

Oracle WebLogic Server Multiple Vulnerabilities

Oracle WebLogic Server Multiple Vulnerabilities (Apr 2019 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (April 2015 CPU) (POODLE)

Oracle WebLogic Server Multiple Vulnerabilities (April 2016 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (April 2017 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (April 2018 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (Jan 2020 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (January 2015 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (January 2016 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (January 2019 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (Jul 2019 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (July 2014 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (July 2015 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (July 2016 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (July 2017 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (July 2018 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (Oct 2019 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (October 2014 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (October 2016 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (October 2017 CPU)

Oracle WebLogic Server Multiple Vulnerabilities (October 2018 CPU)

Oracle WebLogic Server Node Manager Remote Command Execution

Oracle WebLogic Server Security Subcomponent Unspecified Vulnerability (April 2014 CPU)

Oracle WebLogic Server Web Services Remote Code Execution Vulnerability

Oracle WebLogic Server wls9\_async\_response / wls-wsat Remote Code Execution

Oracle WebLogic Unsupported Version Detection

OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

pam\_ssh Login Prompt Remote Username Enumeration

Patch Management: Dell KACE K1000 Computer Info Initialization

Patch Management: Dell KACE K1000 Report

Patch Management: Get Packages from Symantec Altiris

Patch Management: Host information from VMware Go (deprecated)

Patch Management: Missing updates from Dell KACE K1000

Patch Management: Missing updates from SCCM

Patch Management: Missing Updates from Symantec Altiris

Patch Management: Missing updates from Tivoli Endpoint Manager

Patch Management: Missing updates from VMware Go (deprecated)

Patch Management: Missing updates from WSUS

Patch Management: Red Hat Satellite 6 Report

Patch Management: Red Hat Satellite Get Installed Packages

Patch Management: SCCM Computer Info Initialization

Patch Management: SCCM Report

Patch Management: Symantec Altiris Computer Info Initialization

Patch Management: Symantec Altiris Report

Patch Management: Tivoli Endpoint Manager Computer Info Initialization

Patch Management: Tivoli Endpoint Manager Get Installed Packages

Patch Management: Tivoli Endpoint Manager Report

Patch Management: WSUS Report

pfSense Detection

Pgbouncer 1.6 Invalid User Authentication Bypass

PII Information Removed From Scan Results

Pirelli AGE mB Router Default Password (microbusiness) for 'admin' Account

Pivotal Software Redis 2.0.x < 3.2.12 / 4.0.x < 4.0.3 DoS

Pivotal Software Redis 2.8.x < 2.8.24 / 3.x < 3.0.6 DoS

Pivotal Software Redis 3.2.x < 3.2.4 RCE

Pivotal Software Redis < 2.8.21 / 3.x < 3.0.2 RCE

Pivotal Software Redis < 3.2.3 Local Information Disclosure

Pivotal Software Redis LUA < 3.2.12 / 4.0.x < 4.0.10 / 5.0 < 5.0rc2 Multiple Vulnerabilities

Pocsag POC32 Remote Service Default Password (password)

Polycom HDX < 3.1.1.2 Multiple Vulnerabilities

Polycom SIP Detection

POP Password Changer (poppassd\_pam) Arbitrary User Remote Password Modification

POP2 Cleartext Logins Permitted

POP3 Cleartext Logins Permitted

POP3 Host Information in NTLM SSP

POP3 Service STLS Command Support

POP3 Service STLS Plaintext Command Injection

Poppler 0.74 Multiple Vulnerabilities

Poppler < 0.56.0 Multiple Vulnerabilities

Poppler < 0.70.0 Denial of Service Vulnerability (CVE-2018-19149)

Poppler < 0.79 Integer Overflow Vulnerability

Poppler <= 0.72.0 Multiple Vulnerabilities

Poppler <= 0.74.0 Multiple Vulnerabilities

Poppler <= 0.76.1 Heap Buffer Overflow Vulnerability

Portable OpenSSH < 3.8p1 Multiple Vulnerabilities

Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure

Portable SDK for UPnP Devices (libupnp) HTTP Arbitrary File Write

PostgreSQL STARTTLS Support

PowerFolder Java Object Deserialization RCE

Processor Speculative Execution Vulnerabilities (Linux)

Pulse Connect Secure Arbitrary File Read Vulnerability (CVE-2019-11510)

Pulse Connect Secure Cross-Site Request Forgery (SA40793)

Pulse Connect Secure Cross-Site Scripting Vulnerability (SA43018)

Pulse Connect Secure Insecure Cookie Handling (SA44114)

Pulse Connect Secure Multiple Vulnerabilities (SA43730)

Pulse Connect Secure Multiple Vulnerabilities (SA44101)

Pulse Connect Secure Unsupported Version Detection

Pulse Connect Secure XSS (SA3877)

Pulse Policy Secure Cross-Site Request Forgery (SA40793)

Pulse Policy Secure Cross-Site Scripting Vulnerability (SA43018)

Pulse Policy Secure Multiple Vulnerabilities (SA43730)

Pulse Policy Secure Multiple Vulnerabilities (SA44101)

QlikView Server Web UI Detection

QLogic QConvergeConsole (QCC) GUI Web Interface Default Credentials

QMTP Open Relay

Qpopper .qpopper-options Username Handling Overflow

Qpopper < 3.0.2 LIST Command Local Overflow

Qpopper < 4.0.6 Multiple Insecure File Handling Local Privilege Escalation

Qpopper Authentication Timing Response Account Enumeration

Qpopper EUIDL Arbitrary Command Execution

Qpopper PASS Command Remote Overflow

Qpopper pop\_msg() Macroname Remote Overflow

Quagga 0.99.21 bgp\_attr.c BGP Update DoS

Quagga < 0.96.4 Zebra Denial of Service Vulnerability

Quagga < 0.98.6 / 0.99.4 Multiple Vulnerabilities

Quagga < 0.98.7 / 0.99.7 BGPD Denial of Service Vulnerability

Quagga < 0.99.12 BGPD Denial of Service Vulnerability

Quagga < 0.99.17 BGPD Multiple Vulnerabilities

Quagga < 0.99.18 BGPD Multiple Denial of Service Vulnerabilities

Quagga < 0.99.19 Multiple Vulnerabilities

Quagga < 0.99.20.1 Multiple Vulnerabilities

Quagga < 0.99.21 BGP Denial of Service Vulnerability

Quagga < 0.99.22.2 OSPF API Buffer Overflow

Quagga < 0.99.9 BGPD Multiple Denial of Service Vulnerabilities

Quagga Zebra Detection

Quest NetVault Backup Server < 11.4.5 Process Manager Service SQL Injection Remote Code Execution Vulnerability (ZDI-17-982)

Rancher 1.6.x < 1.6.28 / 2.0.x < 2.0.15 / 2.1.x < 2.1.10 / 2.2.x < 2.2.4 Arbitrary Files Read Vulnerability

Rancher 2.0.x < 2.0.15 / 2.1.x < 2.1.10 / 2.2.x < 2.2.4 Command Injection Vulnerability

Rancher < 1.6.25 / 2.0.9 / 2.1.3 Kubernetes Proxy Request Handling Vulnerability

Rancher < 2.2.4 Web Parameter Tampering Vulnerability

RealNetworks Helix Server 11.x / 12.x / 13.x Multiple Vulnerabilities

RealNetworks Helix Server 14.x < 14.3.x Multiple Vulnerabilities

RealNetworks Helix Server < 13.0.0 Multiple Remote DoS

RealServer /admin/includes/ Remote Memory Content Disclosure

Realtek SDK miniigd SOAP Service RCE

RealVNC < 5.0.7 Multiple Local Privilege Escalations

Red Hat 6.2 inetd Internal Service Connections Remote DoS

Red Hat Enterprise Linux OpenSSH ChrootDirectory Local Privilege Escalation

Red Hat JBoss Operations Network Java Object Deserialization RCE

Redis EVAL Lua Sandbox Escape

Redis Server Unprotected by Password Authentication

Retrospect Backup Client Multiple Vulnerabilities (ESA-08-009)

Retrospect Client Malformed Packet DoS

RHEL / CentOS 6.x (64-bit) Malicious Kernel Module Detection (OutlawCountry)

RIP Poisoning Routing Table Modification

RIP Poisoning Routing Table Modification (Adjacent Network)

RIP-1 Poisoning Routing Table Modification

RIP-2 Poisoning Routing Table Modification

RSA Authentication Agent for Web for Apache 8.x < 8.0.1 Build 618 Filter Bypass

RSA Authentication Agent for Web for Apache 8.x < 8.0.2 Multiple Vulnerabilities

RSA Authentication Agent for Web for Apache Installed

RSA SecurID Software Token Converter Buffer Overflow

rsync STARTTLS Command Support

rsync Traversal Arbitrary File Creation

Samba 'AndX' Request Heap-Based Buffer Overflow

Samba 'CAP\_DAC\_OVERRIDE' File Permission Security Bypass

Samba 'CAP\_DAC\_OVERRIDE' File Permission Security Bypass (version check)

Samba 3.0.0 'SamrChangePassword' RCE

Samba 3.0.29 - 3.2.4 Potential Memory Disclosure

Samba 3.2.0 - 3.2.6 Unauthorized Access

Samba 3.2.x < 3.2.3 Privilege Escalation Vulnerability

Samba 3.2.x < 4.1.23 / 4.2.x < 4.2.9 / 4.3.x < 4.3.6 / 4.4.0 < 4.4.0rc4 Multiple Vulnerabilities

Samba 3.4.x < 3.6.23 / 4.0.x < 4.0.16 / 4.1.x < 4.1.6 Multiple Vulnerabilities

Samba 3.5.x / 3.6.x < 3.6.25 / 4.1.x < 4.1.8 Multiple Vulnerabilities

Samba 3.5.x < 3.5.22 / 3.6.x < 3.6.25 / 4.0.x < 4.0.25 / 4.1.x < 4.1.17 TALLOC\_FREE() RCE

Samba 3.5.x < 4.4 / 4.4.x < 4.4.14 / 4.5.x < 4.5.10 / 4.6.x < 4.6.4 Shared Library RCE

Samba 3.6.x < 3.6.24 / 4.0.x < 4.0.19 / 4.1.x < 4.1.9 Multiple Vulnerabilities

Samba 3.6.x < 3.6.3 Denial of Service

Samba 3.6.x < 3.6.6 Remote Security Bypass

Samba 3.x < 3.3.13 SMB1 Packet Chaining Memory Corruption

Samba 3.x < 3.3.15 / 3.4.12 / 3.5.7 'FD\_SET' Memory Corruption

Samba 3.x < 3.3.16 / 3.4.14 / 3.5.10 Multiple Vulnerabilities

Samba 3.x < 3.4.17 / 3.5.15 / 3.6.5 Security Bypass

Samba 3.x < 3.5.22 / 3.6.x < 3.6.17 / 4.0.x < 4.0.8 read\_nttrans\_ea\_lis DoS

Samba 3.x < 3.5.5 / 3.4.9 / 3.3.14 sid\_parse Buffer Overflow

Samba 3.x < 3.6.20 / 4.0.x < 4.0.11 / 4.1.x < 4.1.1 Multiple Vulnerabilities

Samba 3.x < 3.6.22 / 4.0.x < 4.0.13 / 4.1.x < 4.1.3 Multiple Vulnerabilities

Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows

Samba 3.x < 4.2.10 / 4.2.x < 4.2.10 / 4.3.x < 4.3.7 / 4.4.x < 4.4.1 Multiple Vulnerabilities (Badlock)

Samba 4.2.x < 4.2.7 / 4.3.x < 4.3.3 Multiple Vulnerabilities

Samba 4.3.x < 4.3.13 / 4.4.x < 4.4.8 / 4.5.x < 4.5.3 Multiple Vulnerabilities

Samba 4.4.x < 4.4.12 / 4.5.x < 4.5.7 / 4.6.x < 4.6.1 Path Renaming Symlink Local File Disclosure

Samba 4.4.x < 4.4.15 / 4.5.x < 4.5.12 / 4.6.x < 4.6.6 KDC-REP Service Name Validation (Orpheus' Lyre)

Samba 4.4.x < 4.4.16 / 4.5.x < 4.5.14 / 4.6.x < 4.6.8 Multiple Vulnerabilities

Samba 4.5.x / 4.6.x / 4.7.x / 4.8.x / 4.9.x < 4.9.15 / 4.10.x < 4.10.10 / 4.11.x < 4.11.2 Password Complexity Check Bypass (CVE-2019-14833)

Samba 4.5.x < 4.5.16 / 4.6.x < 4.6.14 / 4.7.x < 4.7.6 Multiple Vulnerabilities

Samba 4.7.x / 4.8.x / 4.9.x < 4.9.5 / 4.10.0rc < 4.10.0rc4 LDAP Search Expression Denial of Service Vulnerability (CVE-2019-3824)

Samba 4.7.x < 4.7.12 / 4.8.x < 4.8.7 / 4.9.x < 4.9.3 Multiple Vulnerabilities

Samba 4.8.0 < 4.8.10 / 4.9.x < 4.9.6 / 4.10.0 < 4.10.2 Path/Symlink Traversal Vulnerability (CVE-2019-3890)

Samba 4.9.x < 4.9.13 / 4.10.x < 4.10.8 / 4.11.0rc3 Security Bypass (CVE-2019-10197)

Samba 4.9.x < 4.9.6 / 4.10.0 < 4.10.2 World-Writable Files Vulnerability (CVE-2019-3870)

Samba 4.9.x < 4.9.9 / 4.10.0 < 4.10.5 AC DC DNS Management Server Denial of Service Vulnerability (CVE-2019-12435)

Samba 4.x < 4.0.1 AD DC LDAP Directory Objects Security Bypass

Samba 4.x < 4.0.18 Multiple Vulnerabilities

Samba 4.x < 4.0.21 / 4.1.11 nmbd Remote Code Execution

Samba 4.x < 4.0.24 / 4.1.16 UF\_SERVER\_TRUST\_ACCOUNT AD DC Privilege Escalation

Samba 4.x < 4.0.4 AD DC File Permissions

Samba 4.x < 4.1.22 Multiple Vulnerabilities

Samba 4.x < 4.2.14 / 4.3.x < 4.3.11 / 4.4.x < 4.4.5 SMB2/3 Client Connection Required Signing Downgrade

Samba 4.x < 4.8.12 / 4.9.x < 4.9.8 / 4.10.x < 4.10.3 Man in the Middle Vulnerability (CVE-2018-16860)

Samba 4.x < 4.9.15 / 4.10.x < 4.10.10 AD DC LDAP Server Denial of Service (CVE-2019-14847)

Samba 4.x < 4.9.17 / 4.10.x < 4.10.11 / 4.11.x < 4.11.3 Multiple Vulnerabilities

Samba 4.x < 4.9.18 / 4.10.x < 4.10.12 / 4.11.x < 4.11.5 Multiple Vulnerabilities

Samba < 2.2.8a Remote Code Execution Vulnerability

Samba < 3.0.2 mksmbpasswd.sh Uninitialized Passwords

Samba < 3.0.24 Multiple Flaws

Samba < 3.0.25 Multiple Vulnerabilities

Samba < 3.0.27 Multiple Vulnerabilities

Samba < 3.0.28 send\_mailslot Function Remote Buffer Overflow

Samba < 3.0.30 receive\_smb\_raw Function Remote Buffer Overflow

Samba < 3.0.35 / 3.2.13 / 3.3.6 Multiple Vulnerabilities

Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities

Samba < 3.0.6 Unspecified Remote Memory Leak Information Disclosure

Samba < 3.4.0 Remote Code Execution Vulnerability

Samba < 3.4.8 / 3.5.2 Session Setup AndX DoS

Samba < 3.5.21 / 3.6.12 / 4.0.2 SWAT Multiple Vulnerabilities

Samba idmap\_ad.so Winbind nss\_info Extension Local Privilege Escalation

Samba MS-DOS Path Request Arbitrary File Retrieval

Samba Multiple Remote Vulnerabilities

Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

Samba smbmnt Local Privilege Escalation

Samba SWAT 3.0.2 - 3.0.4 HTTP Basic Auth base64 Buffer Overflow

Samba Symlink Traversal Arbitrary File Access (unsafe check)

Samba Unsupported Version Detection

Samba Version

Samba winbindd Debug Log Server Credentials Local Disclosure

Samhain SRP Protocol Implementation Authentication Bypass

SAPlpd < 6.29 Multiple Vulnerabilities

Scanner Env. Variables Setup

SCO OpenServer Multiple Local Privilege Escalation Vulnerabilities

Security Updates for RancherOS Dirty COW Vulnerability

Security Updates for RancherOS Information Disclosure

Security Updates for RancherOS Information Disclosure Vulnerabilitn

Security Updates for RancherOS Information Disclosure Vulnerability

Security Updates for RancherOS Information Disclosure Vulnerabily

Security Updates for RancherOS Intel Microarchitectural Data Sampling Multiple Local Information Disclosure Vulnerabilities

Security Updates for RancherOS Local Command Execution Vulnerability

Security Updates for RancherOS Local Memory Corruption Vulnerability

Security Updates for RancherOS Local Privilege Escalation Vulnerablity

Security Updates for RancherOS Local privilege-escalation

Security Updates for RancherOS The TCP SACK panic

Serv-U < 10.3.0.1 SFTP Authentication Bypass

Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

ShadowIRCd m\_capab.c Denial of Service

ShareMailPro POP3 Interface Error Message Account Enumeration

Shibboleth Identity Provider Installed (Linux)

Shiva Integrator Default Password

Shiva LanRover Blank Password

SIP Username Enumeration

sipXtapi INVITE Message CSeq Field Header Remote Overflow

Skype for Mac 5.x < 5.1.0.922 Unspecified Remote Code Execution (uncredentialed check)

Skype for Windows < 5.8.0.154 Unspecified Vulnerability (uncredentialed check)

Skype for Windows < 6.3.0.105 Multiple Vulnerabilities (uncredentialed check)

SMB Signing not required

SMC2804WBR Router Default Password (smcadmin)

SNMPc Management Server Default Credentials

Solaris in.fingerd Unused Accounts Disclosure

SolarWinds Server & Application Monitor (SAM) Alert Handling Local Privilege Escalation

SolarWinds Virtualization Manager Java Object Deserialization RCE

Sonatype Nexus Repository Manager Java Object Deserialization RCE

Sonatype Nexus Repository Manager Missing Access Controls RCE

Sophos Anti-Virus Detection and Status (Linux)

Sophos Anti-Virus Installed (Linux)

Sophos Web Appliance < 4.3.1.2 Multiple Vulnerabilities

Splunk Non-root Configuration Local Privilege Escalation

Spring AMQP Installed

Spring Batch Installed

Spring Boot Installed

Spring Data Commons Installed

Spring Data JPA Installed

Spring Data REST Installed

Spring Framework 4.3.x < 4.3.16 / 5.0.x < 5.0.5 Remote Code Execution with spring-messaging (CVE-2018-1270)

Spring Framework 5.0.x < 5.0.16 / 5.1.x < 5.1.13 / 5.2.x < 5.2.3 Spring Framework Reflected File Download Vulnerability. (CVE-2020-5398)

Spring Framework JAR Detection

Spring Integration Installed

Spring Projects Linux Detection

Spring Projects Windows Detection

Spring Security Installed

Spring Security OAuth Installed

SSH 3 AllowedAuthentications Remote Bypass

SSH 3.0.0 Locked Account Remote Authentication Bypass

SSH Algorithms and Languages Supported

SSH CBC/CFB Data Stream Injection

SSH Compression Error Checking

SSH CRC-32 Compensation Attack Remote Overflow

SSH Diffie-Hellman Modulus <= 1024 Bits (Logjam)

SSH Known Hard Coded Private Keys

SSH Multiple Device Default Credentials

SSH Multiple Device Default Credentials (PCI)

SSH Multiple Remote Vulnerabilities

SSH Protocol Authentication Bypass (Remote Exploit Check)

SSH Rate Limited Device

SSH RSAREF Library Multiple Functions Local Overflow

SSH SCP Protocol Detection

SSH Secure Shell without PTY setsid() Function Privilege Escalation

SSH Server CBC Mode Ciphers Enabled

SSH ssh-keygen with Secure-RPC SUN-DES-1 Phrase Recovery

SSH Tectia Server Host Authentication Authorization Bypass Vulnerability

SSH Tectia Server SFTP Filename Logging Format String

SSH Weak Algorithms Supported

SSH Weak MAC Algorithms Enabled

SSH with Kerberos NFS Share Ticket Disclosure

SSL / TLS Certificate Known Hard Coded Private Keys

SSL Certificate Chain Contains Certificates Expiring Soon

SSL Custom CA Setup

SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

SSL/TLS EXPORT\_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK)

SSL/TLS Service Requires Client Certificate

Standard & Poor's ComStock MultiCSP Detection

StarWind Control Port Default Credentials

StreamSets Data Collector Web Detection

Subversion < 1.0.3 apr\_time\_t data Conversion Remote Overflow

Subversion < 1.0.4 Pre-Commit-Hook Remote Overflow

Subversion < 1.0.5 svnserver svn:// Protocol Handler Remote Overflow

Subversion < 1.0.6 mod\_authz\_svn Restricted File Access Bypass

Subversion < 1.0.8 / 1.1.0-rc4 mod\_authz\_svn Unreadable Path Metadata Information Disclosure

Subversion Cleartext Authentication

suidperl Privilege Escalation (PROCSUID)

Sun Java J2SE 1.4.2 < Update 18 Multiple Vulnerabilities (Unix)

Sun Java JDK/JRE 5 < Update 16 Multiple Vulnerabilities (Unix)

Sun Java JDK/JRE 6 < Update 7 Multiple Vulnerabilities (Unix)

Sun Java JRE / Web Start Java Plug-in Untrusted Applet Privilege Escalation (Unix)

Sun Java JRE / Web Start Multiple Vulnerabilities (103072, 103073, 103078, 103079, 103112) (Unix)

Sun Java JRE Applet Handling Privilege Escalation (231261) (Unix)

Sun Java JRE External XML Entities Restriction Bypass (231246) (Unix)

Sun Java JRE Font Parsing Privilege Escalation (103024) (Unix)

Sun Java JRE GIF Image Handling Buffer Overflow (102760) (Unix)

Sun Java JRE Image Parsing Vulnerabilities (102934) (Unix)

Sun Java JRE Multiple Vulnerabilities (102729 / 102732) (Unix)

Sun Java JRE Multiple Vulnerabilities (233321-233327) (Unix)

Sun Java JRE Multiple Vulnerabilities (244986 et al) (Unix)

Sun Java JRE Multiple Vulnerabilities (254569 / 254611 / 254608 ..) (Unix)

Sun Java JRE Multiple Vulnerabilities (263408 / 263409 / 263428 ..) (Unix)

Sun Java JRE Multiple Vulnerabilities (269868 / 269869 / 270476 ...) (Unix)

Sun Java JRE Plug-in Capability Arbitrary Package Access (Unix)

Sun Java JRE XML Signature Command Injection (102993) (Unix)

Sun Java System Directory Proxy Server 6.x < 6.3.1.1 Multiple Vulnerabilities.

Sun Java System Directory Server bind-dn Remote Privilege Escalation

Sun Java Web Start JNLP File Handling Overflow (102996) (Unix)

Sun Java Web Start Unauthorized Access (102881) (Unix)

SunSSH < 1.1.1 / 1.3 CBC Plaintext Disclosure

Supermicro IPMI Baseboard Management Controller Default Credentials

SurgeMail IMAP Server SEARCH Command Remote Buffer Overflow

SurgeMail IMAP Service APPEND Command Remote DoS

Symantec Backup Exec RALUS Code Execution (SYM13-009)

Symantec Backup Exec Remote Agent for Linux and UNIX Servers (RALUS) Installed

Symantec Content Analysis 2.3 < 2.3.1.1 affected by Multiple Vulnerabilities (SYMSA1377)

Symantec Content Analysis < 2.3.1.1 affected by Multiple Vulnerabilities (SYMSA1410)

Symantec Content Analysis < 2.3.5.1 affected by Multiple Vulnerabilities (SYMSA1419)

Symantec Content Analysis < 2.3.5.1 affected by Multiple Vulnerabilities (SYMSA1451)

Symantec Content Analysis < 2.3.5.1 affected by Multiple Vulnerabilities (SYMSA1463)

Symantec Data Insight Management Console Detection

Symantec Encryption Management Server 3.3.2 < 3.3.2 MP12 Multiple Vulnerabilities (SYM16-002)

Symantec Encryption Management Server < 3.3.2 Information Disclosure

Symantec Encryption Management Server < 3.3.2 MP7 Multiple Vulnerabilities

Symantec Encryption Management Server < 3.4.2 MP1 Denial of Service Vulnerability (SYMSA1458)

Symantec Encryption Management Server Remote Administrator Enumeration

Symantec Encryption Server Detection

Symantec Endpoint Protection Installed (Unix Credentialed Check)

Symantec Endpoint Protection Small Business Edition Unsupported Version Detection

Symantec pcAnywhere Default Accounts

Symantec pcAnywhere Unsupported

Symantec Protection Engine 7.0.x < 7.0.5 HF01 / 7.5.x < 7.5.3 HF03 / 7.8.x < 7.8.0 HF01 Multiple Vulnerabilities (SYM16-010) (\*nix check)

Symantec Protection Engine 7.0.x < 7.0.5 HF02 / 7.5.x < 7.5.5 HF01 / 7.8.x < 7.8.0 HF03 Multiple DoS (SYM16-015) (Linux)

Symantec Protection Engine Detection

Systat Service Remote Information Disclosure

Telnet Service START\_TLS Support

Tenable Log Correlation Engine (LCE) < 4.8.0 Libxml2 DoS

Tenable Log Correlation Engine (LCE) < 4.8.1 Multiple Vulnerabilities

Tenable Log Correlation Engine (LCE) < 5.1.1 (TNS-2018-13)

Tenable Log Correlation Engine (LCE) Server Installed (credentialed check)

Tenable Log Correlation Engine (LCE) Unix / Linux Client Installed (credentialed check)

Tenable Log Correlation Engine Server Unsupported Version Detection

Tenable Log Correlation Engine Unix / Linux Clients Unsupported Version Detection

Tenable Nessus < 7.1.0 Multiple Vulnerabilities (TNS-2018-05)

Tenable Nessus < 7.1.4 Multiple Vulnerabilities (TNS-2018-17)

Tenable Nessus < 8.0.0 Multiple Vulnerabilities (TNS-2018-14)

Tenable Nessus < 8.1.1 Multiple Vulnerabilities (TNS-2018-16)

Tenable Nessus < 8.2.2 Stored XSS Vulnerability (TNS-2019-01)

Tenable Nessus < 8.3.0 Multiple Vulnerabilities (TNS-2019-02)

Tenable Nessus < 8.5.0 Multiple Vulnerabilities (TNS-2019-04)

Tenable Nessus < 8.6.0 Denial of Service vulnerability (TNS-2019-05)

Tenable Nessus < 8.7.0 DoS (TNS-2019-06)

Tenable Nessus Agent 6.10.x < 6.10.5 Multiple Vulnerabilities (TNS-2017-10)

Tenable Nessus Agent 6.x < 6.11 MITM Vulnerability During Linking (TNS-2017-11)

Tenable Nessus Agent < 7.4.0 Third Party Vulnerability (OpenSSL) (TNS-2019-03)

Tenable Nessus Agent Installed (Linux)

Tenable Passive Vulnerability Scanner 5.x < 5.2.0 Multiple Vulnerabilities (SWEET32)

Tenable Passive Vulnerability Scanner Installed (Linux credentialed check)

Tenable Passive Vulnerability Scanner Unsupported Version Detection (credentialed check)

Tenable Passive Vulnerability Scanner Unsupported Version Detection (remote check)

Tenable SecurityCenter 5.0.2 Audit File XSS (TNS-2015-12)

Tenable SecurityCenter 5.2.x / 5.3.x < 5.3.1 Multiple Vulnerabilities (TNS-2016-07)

Tenable SecurityCenter 5.4.x <= 5.4.3 PHP Object Deserialization Remote File Deletion (TNS-2017-05)

Tenable SecurityCenter 5.5.0 <= 5.5.2 SQLi (TNS-2017-13)

Tenable SecurityCenter 5.x < 5.4.3 Multiple Vulnerabilities (TNS-2017-04) (httpoxy)

Tenable SecurityCenter < 5.0.1 Multiple RCE (TNS-2015-10)

Tenable SecurityCenter < 5.3.0 Multiple Vulnerabilities (TNS-2016-04)

Tenable SecurityCenter < 5.3.2 Multiple Vulnerabilities (TNS-2016-09)

Tenable SecurityCenter < 5.4.0 Multiple Vulnerabilities (TNS-2016-12)

Tenable SecurityCenter < 5.4.1 Multiple Vulnerabilities (TNS-2016-19)

Tenable SecurityCenter < 5.7.0 Multiple Vulnerabilites (TNS-2018-11)

Tenable SecurityCenter < 5.7.1 Multiple Vulnerabilities (TNS-2018-12)

Tenable SecurityCenter < 5.8.0 Multiple Vulnerabilities (TNS-2018-15)

Tenable SecurityCenter Alternative Certificate Validation Bypass Vulnerability (TNS-2015-08)

Tenable SecurityCenter Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (TNS-2017-04) (httpoxy)

Tenable SecurityCenter Installed

Tenable SecurityCenter Multiple DoS (TNS-2014-11)

Tenable SecurityCenter Multiple PHP Vulnerabilities (TNS-2015-06)

Tenable SecurityCenter OpenSSL 1.0.1 < 1.0.1u Multiple Vulnerabilities (SWEET32)

Tenable SecurityCenter OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities (TNS-2017-04)

Tenable SecurityCenter OpenSSL 1.0.2 < 1.0.2m Multiple Vulnerabilities

Tenable SecurityCenter OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities

Tenable SecurityCenter OpenSSL ASN.1 Signature Verification Routine DoS (TNS-2016-01)

Tenable SecurityCenter PHP < 5.6.25 Multiple Vulnerabilities (TNS-2016-09)

Tenable SecurityCenter PHP < 5.6.26 Multiple Vulnerabilities

Tenable SecurityCenter PHP < 5.6.27 Multiple Vulnerabilities

Tenable SecurityCenter PHP < 5.6.30 Multiple Vulnerabilities (TNS-2017-04)

Tenable SecurityCenter PHP < 5.6.31 Multiple Vulnerabilities (TNS-2017-12

Tenable SecurityCenter PHP < 5.6.32 PCRE DoS

Tenable SecurityCenter PHP Character Handling (TNS-2015-09)

Tenable SecurityCenter Unsupported Version Detection

Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Terminal Services Encryption Level is Medium or Low

Terminal Services Encryption Level is not FIPS-140 Compliant

Terminal Services Use SSL/TLS

TFTP Traversal Arbitrary File Access

Tivoli Storage Manager Server Unauthorized Access Vulnerability

Tivoli Storage Manager Server Unauthorized Backup File Displacement

Tivoli Storage Manager Server Unsupported Product

TLS ALPN Supported Protocol Enumeration

TLS NPN Supported Protocol Enumeration

Trend Micro Control Manager Detection (uncredentialed)

Trend Micro SafeSync for Enterprise (SSFE) Detection

Trend Micro SafeSync for Enterprise Authentication Bypass

Trend Micro Smart Protection Server Detection

Ubiquiti airCam < 1.2.0 ubnt-streamer RTSP Service Remote Code Execution

Ubiquiti airCam Detection

Ubiquiti Networks UniFi < 3.9.3.7537 (KRACK)

Unencrypted Telnet Server

Unitrends Backup Detection

Unix / Linux - Local Users Information : Passwords Never Expire

UnrealIRCd IP Cloaking Weakness Information Disclosure

UnrealIRCd OperServ Raw Channel Join DoS

UnrealIRCd Unspecified DoS

Unsupported Brocade Fabric OS

Unsupported Fortinet Hardware and Operating System

UoW imap Server (uw-imapd) Arbitrary Remote File Access

UPnP API Listing

UPnP File Share Detection

UPnP Internet Gateway Device (IGD) External IP Address Reachable

UPnP Internet Gateway Device (IGD) Port Mapping Listing

UPnP Internet Gateway Device (IGD) Port Mapping Manipulation

UPnP Internet Gateway Device (IGD) Protocol Detection

UPnP WFA Device Detection

UW-IMAP CRAM-MD5 Remote Authentication Bypass

Vacron NVR Web Interface Detection

Vanilla Forums Detection

VERITAS Backup Exec Remote Agent Static Password Arbitrary File Download

Visualware MyConnection Server Remote Agent Default Password

Visualware MyConnection Server Web Default Credentials

VMware Carbon Black Cloud Endpoint Standard Inactive

VMware Carbon Black Cloud Endpoint Standard Inactive (macOS)

VMware ESX / ESXi Arbitrary File Modification (VMSA-2013-0016) (remote check)

VMware ESX / ESXi Authentication Service and Third-Party Libraries Multiple Vulnerabilities (VMSA-2013-0001) (remote check)

VMware ESX / ESXi Descheduled Time Accounting DoS (VMSA-2009-0007) (remote check)

VMware ESX / ESXi Guest OS Local Privilege Escalation (VMSA-2013-0014) (remote check)

VMware ESX / ESXi libxml2 Multiple Vulnerabilities (VMSA-2012-0012) (remote check)

VMware ESX / ESXi libxml2 RCE (VMSA-2013-0004) (remote check)

VMware ESX / ESXi Multiple DoS (VMSA-2014-0001)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2009-0014) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2009-0016) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2011-0007) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2011-0008) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2011-0009) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2012-0005) (BEAST) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2012-0006) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2012-0009) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2012-0011) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2012-0016) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2013-0012) (remote check)

VMware ESX / ESXi Multiple Vulnerabilities (VMSA-2014-0002)

VMware ESX / ESXi NFC and Third-Party Libraries Multiple Vulnerabilities (VMSA-2013-0003) (remote check)

VMware ESX / ESXi NFC Traffic Handling DoS (VMSA-2013-0011) (remote check)

VMware ESX / ESXi Service Console and Third-Party Libraries Multiple Vulnerabilities (VMSA-2012-0001) (remote check)

VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0003) (remote check)

VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0004) (remote check)

VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0012) (remote check)

VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0013) (remote check)

VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2012-0013) (remote check)

VMware ESX / ESXi Third-Party Libraries Multiple Vulnerabilities (VMSA-2013-0009) (remote check)

VMware ESX / ESXi Tools Folder Incorrect ACL Privilege Escalation (VMSA-2012-0007) (remote check)

VMware ESX / ESXi VMCI Privilege Escalation (VMSA-2013-0002) (remote check)

VMware ESX / ESXi vSphere Client RCE (VMSA-2014-0003)

VMware ESX Multiple Bash Vulnerabilities (VMSA-2014-0010) (Shellshock)

VMware ESX Multiple Vulnerabilities (VMSA-2009-0004) (remote check)

VMware ESX Multiple Vulnerabilities (VMSA-2009-0008) (remote check)

VMware ESX Multiple Vulnerabilities (VMSA-2009-0009) (remote check)

VMware ESX Service Console Multiple Vulnerabilities (VMSA-2012-0008) (remote check)

VMware ESX sudo Package Multiple Vulnerabilities (VMSA-2013-0007) (remote check)

VMware ESX Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0001) (remote check)

VMware ESX Third-Party Libraries Multiple Vulnerabilities (VMSA-2011-0010) (remote check)

VMware ESX Third-Party Libraries Multiple Vulnerabilities (VMSA-2013-0015) (remote check)

VMware ESX WebWorks Help Multiple XSS (VMSA-2009-0017) (remote check)

VMware ESXi 5.0 < Build 3021432 OpenSLP RCE (VMSA-2015-0007)

VMware ESXi 5.1 < Build 3021178 OpenSLP RCE (VMSA-2015-0007)

VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)

VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 Information Disclosure (VMSA-2018-0012) (Spectre) (remote check)

VMware ESXi 5.5 / 6.0 XSS (VMSA-2016-0023) (remote check)

VMware ESXi 5.5 < Build 3029944 OpenSLP RCE (VMSA-2015-0007)

VMware ESXi Multiple DoS (VMSA-2014-0008)

VMware ESXi Multiple OpenSSL Vulnerabilities (VMSA-2014-0004) (Heartbleed)

VMware ESXi Multiple OpenSSL Vulnerabilities (VMSA-2014-0006)

VMware ESXi Multiple Vulnerabilities (VMSA-2014-0012)

VMware ESXi Tools Guest OS Privilege Escalation (VMSA-2014-0005)

VMware Harbor 1.7.x < 1.7.6, 1.8.x < 1.8.3 (VMSA-2019-0015)

VMware Harbor 1.7.x, 1.8.x < 1.8.6 / 1.9.x < 1.9.3

VMware Harbor 1.8.x < 1.8.4 (VMSA-2019-0016)

VMware Harbor Privilege Escalation (VMSA-2019-0015) (CVE-2019-16097)

VMware Horizon View Client 4.x < 4.8.0 Privilege Escalation Vulnerability (VMSA-2018-0014)

VMware Horizon View Client 5.x < 5.2.0 Use-After-Free (VMSA-2019-0014)

VMware Horizon Workspace 1.8 < 1.8.1 OpenSSL Library Multiple Vulnerabilities (VMSA-2014-0004) (Heartbleed)

VMware NSX Bash Environment Variable Command Injection (VMSA-2014-0010) (Shellshock)

VMware NSX Edge Information Disclosure (VMSA-2016-0007)

VMware NSX Edge Unspecified Information Disclosure (VMSA-2014-0009)

VMware NSX Installed

VMware Security Updates for vCenter Server (VMSA-2013-0006)

VMware Security Updates for vCenter Server (VMSA-2013-0012)

VMware Security Updates for vCenter Server (VMSA-2014-0006)

VMware Security Updates for vCenter Server (VMSA-2014-0008)

VMware Security Updates for vCenter Server (VMSA-2014-0012)

VMware Security Updates for vCenter Server (VMSA-2015-0001) (POODLE)

VMWare STARTTLS Support

VMware Studio 2.x < 2.1 Multiple Vulnerabilities

VMware vCenter / vRealize Orchestrator 4.2.x / 5.x / 6.x Java Object Deserialization RCE (VMSA-2015-0009)

VMware vCenter / vRealize Orchestrator Appliance 4.2.x / 5.x / 6.x Java Object Deserialization RCE (VMSA-2015-0009)

VMware vCenter 5.5 LDAP Certificate Validation MitM Spoofing (VMSA-2015-0006)

VMware vCenter 6.0 LDAP Certificate Validation MitM Spoofing (VMSA-2015-0006)

VMware vCenter Multiple Vulnerabilities (VMSA-2012-0013)

VMware vCenter Multiple Vulnerabilities (VMSA-2015-0007)

VMware vCenter Multiple Vulnerabilities (VMSA-2015-0008)

VMware vCenter Operations Management Bash Vulnerabilities (VMSA-2014-0010) (Shellshock)

VMware vCenter Operations Management Linux JRE Update 1.7.0\_76-b13 (VMSA-2015-0003) (POODLE)

VMware vCenter Operations Management Suite Multiple Vulnerabilities (VMSA-2014-0007)

VMware vCenter Operations Management vApp JRE Update 1.7.0\_76-b13 (VMSA-2015-0003) (POODLE)

VMware vCenter Operations Management Windows JRE Update 1.7.0\_76-b13 (VMSA-2015-0003) (POODLE)

VMware vCenter Operations Manager Arbitrary File Upload (VMSA-2012-0013)

VMware vCenter Operations Manager Installed (Linux)

VMware vCenter Operations Manager Multiple OpenSSL Vulnerabilities (VMSA-2014-0006)

VMware vCenter Operations Manager Web UI Detection

VMware vCenter Orchestrator 5.5.x < 5.5.2 DoS (VMSA-2014-0007)

VMware vCenter Orchestrator Appliance 5.5.x < 5.5.2 DoS (VMSA-2014-0007)

VMware vCenter Server 5.0.x < 5.0u3e / 5.1.x < 5.1u3b / 5.5.x < 5.5u3 (Linux) / 5.5.x < 5.5u3b (Windows) / 6.0.x < 6.0.0b JMX Deserialization RCE (VMSA-2016-0005)

VMware vCenter Server 5.5.x / 6.0.x / 6.5.x / 6.7.x Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020)

VMware vCenter Server 5.5.x < 5.5u3d / 6.0.x < 6.0u2 Client Integration Plugin Session Hijacking (VMSA-2016-0004)

VMware vCenter Server 5.5.x < 5.5u3e / 6.0.x < 6.0u2a Multiple XXE Vulnerabilities (VMSA-2016-0022)

VMware vCenter Server 5.5.x < 5.5u3f / 6.0.x < 6.0u3c / 6.5.x < 6.5u1 Multiple Vulnerabilities (VMSA-2017-0017)

VMware vCenter Server 5.5.x < 5.5U3g / 6.0.x < 6.0U3d / 6.5.x < 6.5U1e Hypervisor-Assisted Guest Remediation (VMSA-2018-0004) (Spectre)

VMware vCenter Server 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0013)

VMware vCenter Server 6.0.x < 6.0u2 Unspecified HTTP Header Injection (VMSA-2016-0010)

VMware vCenter Server 6.0.x < 6.0u3b / 6.5.x < 6.5c BlazeDS AMF3 RCE (VMSA-2017-0007)

VMware vCenter Server 6.5.x < 6.5u1 H5 Client Stored XSS (VMSA-2017-0015)

VMware vCenter Server 6.5.x < 6.5u1f Multiple Vulnerabilities (VMSA-2018-0007) (Spectre-1) (Meltdown)

VMware vCenter Server 6.7 Sensitive Information Disclosure Vulnerability (VMSA-2020-0006)

VMware vCenter Server Appliance 6.0 / 6.5 / 6.7 Information Disclosure vulnerability (VMSA-2018-0021)

VMware vCenter Server Appliance 6.5 < 6.5 U1 Multiple Vulnerabilities (VMSA-2017-0013)

VMware vCenter Server Appliance 6.5 < 6.5 U1d Local Privilege Escalation (VMSA-2017-0021)

VMware vCenter Server Appliance Bash Remote Code Execution (VMSA-2014-0010) (Shellshock)

VMware vCenter Server Appliance BlazeDS AMF3 RCE (VMSA-2017-0007)

VMware vCenter Server Appliance Multiple Vulnerabilities (VMSA-2013-0006)

VMware vCenter Server Appliance Multiple Vulnerabilities (VMSA-2014-0006)

VMware vCenter Server Appliance Unspecified XSS (VMSA-2014-0012)

VMware vCenter Server Denial of Service (VMSA-2012-0018)

VMware vCenter Server Multiple Java Vulnerabilities (VMSA-2015-0003) (POODLE)

VMware vCenter Server Multiple Vulnerabilities (VMSA-2012-0005)

VMware vCenter Server NFC Protocol Code Execution (VMSA-2013-0003)

VMware vCenter Support Assistant Multiple Vulnerabilities (VMSA-2014-0006)

VMware vCloud Director 5.1.x < 5.1.3 Logout XSRF (VMSA-2014-0001)

VMware vCloud Director 5.5.x < 5.5.6 Client Integration Plugin Session Hijacking (VMSA-2016-0004)

VMware vCloud Director 5.5.x < 5.5.6.1 / 5.6.x < 5.6.5.1 / 8.0.x < 8.0.1.1 JMX Deserialization RCE (VMSA-2016-0005)

VMware vCloud Director Installed

VMware vRealize Automation 6.x / 7.x Information Disclosure Vulnerability (VMSA-2018-0021

VMware vRealize Automation 7.0.x / 7.1.x / 7.2.x / 7.3.x Session IDs Handling Vulnerability (VMSA-2018-0009)

VMware vRealize Automation 7.0.x < 7.1 Multiple Vulnerabilities (VMSA-2016-0013)

VMware vRealize Automation Deserialization Vulnerability (VMSA-2018-0006)

VMware vRealize Automation Web UI Detection

VMware vRealize Business Web UI Detection

VMware vRealize Log Insight Web UI Detection

VMware vRealize Operations Manager 6.6.x < 6.6.1.11286876 / 6.7.x < 6.7.0.11286837 / 7.x < 7.0.0.11287810 Local Privilege Escalation Vulnerability (VMSA-2018-0031)

VMware VRealize Operations Manager 6.x Oracle JRE JMX Deserialization RCE (VMSA-2016-0005)

VMware vSphere Data Protection 5.5.x / 5.8.x / 6.0.x < 6.0.5 / 6.1.x < 6.1.4 Multiple Vulnerabilities (VMSA-2017-0010

VMware vSphere Data Protection 5.x / 6.0.x < 6.0.7 / 6.1.x < 6.1.6 Multiple Vulnerabilities (VMSA-2018-0001

VMware vSphere Data Protection 6.0.x < 6.0.9 / 6.1.x < 6.1.10 Multiple Vulnerabilities (VMSA-2018-0029)

VMware vSphere Data Protection 6.x Information Disclosure Vulnerability (VMSA-2018-0021

VMware vSphere Data Protection Certificate Validation (VMSA-2015-0002)

VMware vSphere Data Protection Private SSH Key Authentication Bypass (VMSA-2016-0024)

VMware vSphere Replication Bash Environment Variable Command Injection Vulnerability (VMSA-2014-0010) (Shellshock)

VMware vSphere Replication Multiple OpenSSL Vulnerabilities (VMSA-2014-0006)

VMware vSphere Replication Oracle JRE JMX Deserialization RCE (VMSA-2016-0005)

VMware Workspace Portal Multiple Bash Shell Vulnerabilities (VMSA-2014-0010) (Shellshock)

VMware Workspace Portal Multiple Java Vulnerabilities (VMSA-2015-0003) (POODLE)

VNC Security Type Enforcement Failure Remote Authentication Bypass

VNC Server Unauthenticated Access

VNC Server Unauthenticated Access: Screenshot

VxWorks 5.5 through 6.9 Multiple Vulnerabilities

Web Application Default Username ('super'/'1502') / Password ('super'/'1502')

Webmin < 1.930 Remote Code Execution Vulnerability

Websense TRITON Detection

WebTitan Default Credentials (ssh)

Western Digital MyCloud Web Interface Detection

Western Digital TV Web Interface Detection

WinComLPD LPD Monitoring Server Authentication Bypass

WinComLPD LPD Monitoring Server Default Credentials

Wind River VxWorks Multiple Vulnerabilities (URGENT/11)

Wind River VxWorks TCP Predictability Vulnerability

Wing FTP Server < 3.6.1 Multiple Flaws

Wireshark / Ethereal Unsupported Version Detection

X Server Unauthenticated Access: Screenshot

X11 Server Unauthenticated Access

Xen 32-bit Arm Guest OS Denial Of Service vulnerability (XSA-307)

Xen arch/x86/x86\_64/entry.S Exception Handling Guest-to-host DoS (XSA-259)

Xen arch\_domain\_create() Function Local APIC Assumption NULL Pointer Dereference Guest-to-host DoS (XSA-256)

Xen Arm-Based CPU Speculation past the ERET Instruction (XSA-312)

Xen Asynchronous Modification EFLAGS.IF Clearing DoS (XSA-202)

Xen CDROM Image Handling Local File Disclosure Vulnerability (XSA-258)

Xen CMPXCHG8B Emulation Information Disclosure (XSA-200)

Xen Denial of Service Vulnerability (XSA-301)

Xen Denial of Service Vulnerability (XSA-304)

Xen Denial of Service vulnerability (XSA-304)

Xen Device Quarantine for Alternate PCI Assignment Methods Privilege Escalation Vulnerability (XSA-306)

Xen Function M2P Entry Access Handling Guest-to-Host DoS (XSA-251)

Xen Function Page Use Shadow Mode Reference Counting Improper Overflow Check Guest-to-Host DoS (XSA-249)

Xen gnttab\_map\_frame() Function Missing Mapping Check Upgrade Guest-to-host DoS (XSA-255)

Xen Grant Table Transfer Issues on Large Hosts Denial of Service Vulnerability (XSA-284)

Xen Guest Destruction Memory Leak DoS (XSA-207)

Xen Guest Detection

Xen guest\_remove\_page() Function Pagetable Unpinning Handling Guest-to-host DoS (XSA-252)

Xen Hypervisor Detection

Xen Hypervisor Function Error Condition Handling Lock Release Failure Guest-to-Host DoS (XSA-235)

Xen Hypervisor Guest-to-Host Privilege Escalation (XSA-247)

Xen Hypervisor I/O Intercept Code Hypervisor Stack Guest-to-Host Information Disclosure (XSA-239)

Xen Hypervisor Infinite Loop Guest-to-Host DoS (XSA-246)

Xen Hypervisor Memory Leak on Boot (XSA-235)

Xen Hypervisor Multiple Functions DMOP Handling Guest-to-Host DoS (XSA-238)

Xen Hypervisor Multiple Vulnerabilities (XSA-213 - XSA-215)

Xen Hypervisor Multiple Vulnerabilities (XSA-226 - XSA-230)

Xen Hypervisor Multiple Vulnerabilities (XSA-231 - XSA-234)

Xen Hypervisor New CPU Interrupt Descriptor Table (IDT) Copy Handling Guest-to-Host Privilege Escalation (XSA-244)

Xen Hypervisor Page Type Reference Handling Memory Exhaustion Guest-to-Host DoS (XSA-242)

Xen Hypervisor Pagetable De-typing Recursion Handling Guest-to-Host DoS (XSA-240)

Xen Hypervisor PCI MSI Interrupt Setup Multiple Guest-to-Host Privilege Escalation (XSA-237)

Xen Hypervisor Pin Count / Page Reference Grant Table Code Guest-to-Host Memory Corruption (XSA-236)

Xen Hypervisor TLB Flush Request Handling Race Condition System Memory Access Guest-to-Host Privilege Escalation (XSA-241)

Xen Hypervisor Translated Guest Self-linear Shadow Mapping Handling Guest-to-Host Privilege Escalation (XSA-243)

Xen Hypervisor XENMEM\_exchange Memory Disclosure (XSA-212)

Xen Hypervisor xenstored Write Saturation DoS (XSA-206)

Xen Information Disclosure Vulnerability (XSA-305)

Xen Intel Architecture Debug Exception Handling Local Privilege Escalation (XSA-260)

Xen Intel VMX hvmemul\_vmfunc() NULL Pointer Dereference DoS (XSA-203)

Xen Multiple Vulnerabilities (Spectre) (Meltdown) (XSA-254)

Xen Multiple Vulnerabilities (XSA-186, XSA-187)

Xen Multiple Vulnerabilities (XSA-191 - XSA-198)

Xen PCI Pass-Through Elevation of Privilege vulnerability (XSA-302)

Xen Privilege Escalation (XSA-182) (Bunker Buster)

Xen Project ARM Grant Table v2 DoS (XSA-268)

Xen Project Denial of Service (XSA-295)

Xen Project Descriptor Table Limit Checking Privilege Escalation Vulnerability (XSA-298)

Xen Project Dynamic Height Handling Elevation of Privilege Vulnerability (XSA-311)

Xen Project fsgsbase CPU Feature Privilege Escalation Vulnerability (XSA-293)

Xen Project Guest p2m Page Removal Error Handling DoS (XSA-277)

Xen Project HLE Transaction 'XACQUIRE' DoS (XSA-282)

Xen Project Insufficient TLB Flushing Vulnerability (XSA-275)

Xen Project INVPCID with Non-Canonical Addresses DoS (XSA-279)

Xen Project Local Security Bypass Vulnerability (XSA-266)

Xen Project Microarchitectural Data Sampling Speculative Side-Channel Vulnerabilities (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (XSA-297)

Xen Project MSR\_DEBUGCTL 'Branch Trace Store' DoS (XSA-269)

Xen Project Nested VT-x Instruction Guest-to-Host DoS (XSA-278)

Xen Project Oxenstored Quota-maxentity DoS (XSA-272)

Xen Project Pass-through PCI Device Guest-to-Host Privilege Escalation (XSA-285)

Xen Project PCI Pass-through Device Denial of Service Vulnerability (XSA-291)

Xen Project PCI Pass-through DMA Privilege Escalation (XSA-288)

Xen Project Preemtible Linear Pagetable Denial of Service Vulnerability (XSA-290)

Xen Project Process Context Identifiers Shadow Pagetables Denial of Service Vulnerability (XSA-294)

Xen Project Process Context Identifiers TLB Flushing Multiple Vulnerabilities (XSA-292)

Xen Project Restartable PV Type Change Operations Elevation of Privilege Vulnerability (XSA-310)

Xen Project Speculative Execution Side Channel Vulnerability (XSA-273) (Foreshadow)

Xen Project steal\_page Race Condition Multiple Vulnerabilities (XSA-287)

Xen Project VCPUOP\_initialise DoS (XSA-296)

Xen Project x86 Debug Exception Handling Local DoS (XSA-265)

Xen Project x86 IOREQ Server Resource Accounting DoS (XSA-276)

Xen Project x86 Paravirtualization Local DoS (XSA-264)

Xen Project XSA-240 Mitigation Shadow Paging Conflict Vulnerability (XSA-280)

Xen PV Guests Internally Used Pages Access Handling Guest-to-Host Privilege Escalation (XSA-248)

Xen Restartable PV Type Change Operations Elevation of Privilege Vulnerability (XSA-299)

Xen Shadow Mode Page Use Reference Counting Error Handling Guest-to-Host DoS (XSA-250)

Xen SYSCALL singlestep Handling Privilege Escalation (XSA-204)

Xen vcpu Destruction Handling Memory Exhaustion Guest-to-Host DoS (XSA-253)

Xen VMentry Failure Denial Of Service vulnerability (XSA-308)

Xen x86 CR0.TS and CR0.EM Honoring Cross-task Register State Information Disclosure (XSA-190)

Xerox ColorQube 8570 / 8870 Multiple Vulnerabilities (XRX15OA)

Xerox ColorQube 92XX Multiple OpenSSL Vulnerabilities (XRX15AD) (FREAK) (GHOST) (POODLE)

Xerox ColorQube ConnectKey Controller Multiple Unspecified Vulnerabilities (XRX14-001)

XEROX ColorQube Device Detection

Xerox ColorQube Multiple Unspecified Vulnerabilities (XRX13-006)

Xerox ColorQube Unspecified Remote Protocol Authorization Bypass (XRX13-008)

Xerox DocuCentre / WorkCentre Postscript Interpreter Traversal (XRX05-001)

Xerox Document Centre Device Detection

Xerox Document Centre MicroServer Web Server Directory Navigation Crafted URL DoS (XRX05-004)

Xerox Document Centre MicroServer Web Server Multiple Vulnerabilities (XRX05-008)

Xerox Document Centre Web Server Unspecified Unauthorized Access (XRX05-003)

Xerox Printer SNMP Detection

Xerox WorkCentre 3025 / 3215 / 3225 OpenSSL Multiple Vulnerabilities (XRX15AM) (FREAK) (POODLE)

Xerox WorkCentre 3550 OpenSSL Multiple Vulnerabilities (XRX15AJ) (FREAK) (POODLE)

Xerox WorkCentre 4260 / 4265 Multiple Vulnerabilities (XRX15AV) (FREAK) (Logjam)

Xerox WorkCentre 6400 OpenSSL RSA Temporary Key Handling EXPORT\_RSA Ciphers Downgrade MitM (XRX15AP) (FREAK)

Xerox WorkCentre 77XX Multiple Vulnerabilities (XRX15R) (FREAK) (GHOST)

Xerox WorkCentre Authorization Bypass Vulnerabilities (XRX10-002)

Xerox WorkCentre Command Injection (XRX11-001)

Xerox WorkCentre Crafted PostScript File Handling Directory Access (XRX10-001)

Xerox WorkCentre Device Detection

Xerox WorkCentre Extensible Interface Platform Unspecified Security Bypass (XRX08-006)

Xerox WorkCentre MicroServer Multiple Vulnerabilities (XRX05-005)

Xerox WorkCentre Multi-Page Document Scan/Fax Information Disclosure (XRX05-002)

Xerox WorkCentre Multiple OpenSSL Vulnerabilities (XRX07-001)

Xerox WorkCentre Multiple Samba Vulnerabilities (XRX08-001)

Xerox WorkCentre Multiple Unspecified Vulnerabilities (XRX10-003)

Xerox WorkCentre Multiple Unspecified Vulnerabilities (XRX13-006)

Xerox WorkCentre Multiple Vulnerabilities (XRX05-006)

Xerox WorkCentre Multiple Vulnerabilities (XRX06-001)

Xerox WorkCentre Multiple Vulnerabilities (XRX06-002)

Xerox WorkCentre Multiple Vulnerabilities (XRX06-006)

Xerox WorkCentre Multiple Vulnerabilities (XRX19-016) (URGENT/11)

Xerox WorkCentre Samba Overflow (XRX08-009)

Xerox WorkCentre Unspecified Remote Protocol Authorization Bypass (XRX13-008)

Xerox WorkCentre Web Server Unspecified Command Injection (XRX09-001)

Xerox WorkCentre Web Server Unspecified Command Injection (XRX09-002)

Xerox WorkCentre Web Services Extensible Interface Platform Unauthorized Access (XRX09-003)

Xerox WorkCentre WebUI Arbitrary Command Execution (XRX06-005)

XLight FTP Server 3.x SFTP Directory Traversal

XMail < 1.27 Insecure Temporary File Creation

XMPP Cleartext Authentication

XMPP Service STARTTLS Command Support

XMPP Service STARTTLS Plaintext Command Injection

XtraMail Control Service Username Overflow

Zabbix node\_process\_command() Function Crafted Request Arbitrary Command Execution

Zabbix Server 'active checks' Command Injection

Zabbix Server send\_history\_last\_id() SQL Injection

Zabbix Unsupported Version Detection

Zend Server Java Bridge Arbitrary Java Code Execution

ZTE ZXV10 W300 Wireless Router Hard-coded Password

Zyxel D1000 CWMP Get Default Password

ZyXEL Prestige Router Configuration Reset

ZyXEL Router Default Telnet Password Present

ZyXEL Routers Default Web Account

# Mandriva Local Security Checks

Mandrake Linux Security Advisory : a2ps (MDKSA-2004:140)

Mandrake Linux Security Advisory : a2ps (MDKSA-2005:097)

Mandrake Linux Security Advisory : apache (MDKSA-2000:060-2)

Mandrake Linux Security Advisory : apache (MDKSA-2001:077-1)

Mandrake Linux Security Advisory : apache (MDKSA-2002:039-2)

Mandrake Linux Security Advisory : apache (MDKSA-2002:068)

Mandrake Linux Security Advisory : apache (MDKSA-2003:103)

Mandrake Linux Security Advisory : apache (MDKSA-2004:065)

Mandrake Linux Security Advisory : apache (MDKSA-2004:134)

Mandrake Linux Security Advisory : apache (MDKSA-2005:130)

Mandrake Linux Security Advisory : apache (MDKSA-2006:133)

Mandrake Linux Security Advisory : apache (MDKSA-2007:127)

Mandrake Linux Security Advisory : apache (MDKSA-2007:140)

Mandrake Linux Security Advisory : apache (MDKSA-2007:235)

Mandrake Linux Security Advisory : apache-mod\_auth\_shadow (MDKSA-2005:200)

Mandrake Linux Security Advisory : apache-mod\_perl (MDKSA-2004:046-1)

Mandrake Linux Security Advisory : apache-mod\_perl (MDKSA-2007:083)

Mandrake Linux Security Advisory : apache2 (MDKSA-2003:050)

Mandrake Linux Security Advisory : apache2 (MDKSA-2003:063-1)

Mandrake Linux Security Advisory : apache2 (MDKSA-2003:075-1)

Mandrake Linux Security Advisory : apache2 (MDKSA-2003:096-1)

Mandrake Linux Security Advisory : apache2 (MDKSA-2004:043)

Mandrake Linux Security Advisory : apache2 (MDKSA-2004:055)

Mandrake Linux Security Advisory : apache2 (MDKSA-2004:064)

Mandrake Linux Security Advisory : apache2 (MDKSA-2004:096)

Mandrake Linux Security Advisory : apache2 (MDKSA-2004:135)

Mandrake Linux Security Advisory : apache2 (MDKSA-2005:129)

Mandrake Linux Security Advisory : apache2 (MDKSA-2005:155)

Mandrake Linux Security Advisory : apache2 (MDKSA-2005:161)

Mandrake Linux Security Advisory : apache2 (MDKSA-2005:233)

Mandrake Linux Security Advisory : apache2 (MDKSA-2006:007)

Mandrake Linux Security Advisory : apache2-mod\_auth\_pgsql (MDKSA-2006:009)

Mandrake Linux Security Advisory : apcupsd (MDKSA-2000:077)

Mandrake Linux Security Advisory : apcupsd (MDKSA-2003:018)

Mandrake Linux Security Advisory : arpwatch (MDKSA-2001:002)

Mandrake Linux Security Advisory : arts (MDKSA-2006:107)

Mandrake Linux Security Advisory : aspell (MDKSA-2004:153)

Mandrake Linux Security Advisory : at (MDKSA-2002:007)

Mandrake Linux Security Advisory : avahi (MDKSA-2006:215)

Mandrake Linux Security Advisory : avahi (MDKSA-2007:003)

Mandrake Linux Security Advisory : avahi (MDKSA-2007:185)

Mandrake Linux Security Advisory : bash1 (MDKSA-2000:075)

Mandrake Linux Security Advisory : bind (MDKSA-2000:010)

Mandrake Linux Security Advisory : bind (MDKSA-2000:067)

Mandrake Linux Security Advisory : bind (MDKSA-2001:017)

Mandrake Linux Security Advisory : bind (MDKSA-2002:001)

Mandrake Linux Security Advisory : bind (MDKSA-2002:038-1)

Mandrake Linux Security Advisory : bind (MDKSA-2002:043)

Mandrake Linux Security Advisory : bind (MDKSA-2005:023)

Mandrake Linux Security Advisory : bind (MDKSA-2006:163)

Mandrake Linux Security Advisory : bind (MDKSA-2006:207)

Mandrake Linux Security Advisory : bind (MDKSA-2007:030)

Mandrake Linux Security Advisory : bind (MDKSA-2007:100)

Mandrake Linux Security Advisory : bind (MDKSA-2007:149)

Mandrake Linux Security Advisory : binutils (MDKSA-2005:215)

Mandrake Linux Security Advisory : BitchX (MDKSA-2000:017)

Mandrake Linux Security Advisory : BitchX (MDKSA-2000:079)

Mandrake Linux Security Advisory : BitchX (MDKSA-2003:069)

Mandrake Linux Security Advisory : bluez-hcidump (MDKSA-2006:041)

Mandrake Linux Security Advisory : bluez-utils (MDKSA-2005:150)

Mandrake Linux Security Advisory : bluez-utils (MDKSA-2007:014)

Mandrake Linux Security Advisory : bzip2 (MDKSA-2005:091)

Mandrake Linux Security Advisory : bzip2 (MDKSA-2006:026)

Mandrake Linux Security Advisory : cairo (MDKSA-2006:057)

Mandrake Linux Security Advisory : cdrdao (MDKSA-2005:089)

Mandrake Linux Security Advisory : cdrecord (MDKSA-2000:009)

Mandrake Linux Security Advisory : cdrecord (MDKSA-2003:058-1)

Mandrake Linux Security Advisory : cdrecord (MDKSA-2004:091)

Mandrake Linux Security Advisory : cdrecord (MDKSA-2005:077)

Mandrake Linux Security Advisory : cfengine (MDKSA-2000:061)

Mandrake Linux Security Advisory : cfengine (MDKSA-2005:184)

Mandrake Linux Security Advisory : chbg (MDKSA-2005:027)

Mandrake Linux Security Advisory : chromium (MDKSA-2006:213)

Mandrake Linux Security Advisory : clamav (MDKSA-2005:025)

Mandrake Linux Security Advisory : clamav (MDKSA-2005:113)

Mandrake Linux Security Advisory : clamav (MDKSA-2005:125)

Mandrake Linux Security Advisory : clamav (MDKSA-2005:166)

Mandrake Linux Security Advisory : clamav (MDKSA-2005:205)

Mandrake Linux Security Advisory : clamav (MDKSA-2006:016)

Mandrake Linux Security Advisory : clamav (MDKSA-2006:067)

Mandrake Linux Security Advisory : clamav (MDKSA-2006:080)

Mandrake Linux Security Advisory : clamav (MDKSA-2006:138)

Mandrake Linux Security Advisory : clamav (MDKSA-2006:184)

Mandrake Linux Security Advisory : clamav (MDKSA-2006:230)

Mandrake Linux Security Advisory : clamav (MDKSA-2007:043)

Mandrake Linux Security Advisory : clamav (MDKSA-2007:098)

Mandrake Linux Security Advisory : clamav (MDKSA-2007:115)

Mandrake Linux Security Advisory : clamav (MDKSA-2007:150)

Mandrake Linux Security Advisory : clamav (MDKSA-2007:172)

Mandrake Linux Security Advisory : cpio (MDKSA-2005:032-1)

Mandrake Linux Security Advisory : cpio (MDKSA-2005:116-1)

Mandrake Linux Security Advisory : cpio (MDKSA-2005:237)

Mandrake Linux Security Advisory : cpio (MDKSA-2007:233)

Mandrake Linux Security Advisory : cups (MDKSA-2000:070-1)

Mandrake Linux Security Advisory : cups (MDKSA-2001:020-1)

Mandrake Linux Security Advisory : cups (MDKSA-2001:023)

Mandrake Linux Security Advisory : cups (MDKSA-2001:048)

Mandrake Linux Security Advisory : cups (MDKSA-2002:015)

Mandrake Linux Security Advisory : cups (MDKSA-2003:001)

Mandrake Linux Security Advisory : cups (MDKSA-2003:062)

Mandrake Linux Security Advisory : cups (MDKSA-2003:104)

Mandrake Linux Security Advisory : cups (MDKSA-2004:097)

Mandrake Linux Security Advisory : cups (MDKSA-2004:116)

Mandrake Linux Security Advisory : cups (MDKSA-2004:164)

Mandrake Linux Security Advisory : cups (MDKSA-2005:008)

Mandrake Linux Security Advisory : cups (MDKSA-2005:018)

Mandrake Linux Security Advisory : cups (MDKSA-2005:041)

Mandrake Linux Security Advisory : cups (MDKSA-2005:138-1)

Mandrake Linux Security Advisory : cups (MDKSA-2005:165)

Mandrake Linux Security Advisory : cups (MDKSA-2006:010)

Mandrake Linux Security Advisory : cups (MDKSA-2007:086)

Mandrake Linux Security Advisory : cups (MDKSA-2007:165)

Mandrake Linux Security Advisory : cups (MDKSA-2007:204-1)

Mandrake Linux Security Advisory : cups (MDKSA-2007:228)

Mandrake Linux Security Advisory : curl (MDKSA-2005:048)

Mandrake Linux Security Advisory : curl (MDKSA-2005:182)

Mandrake Linux Security Advisory : curl (MDKSA-2005:224)

Mandrake Linux Security Advisory : cvs (MDKSA-2003:009)

Mandrake Linux Security Advisory : cvs (MDKSA-2003:112-1)

Mandrake Linux Security Advisory : cvs (MDKSA-2004:028)

Mandrake Linux Security Advisory : cvs (MDKSA-2004:048)

Mandrake Linux Security Advisory : cvs (MDKSA-2004:058)

Mandrake Linux Security Advisory : cvs (MDKSA-2004:108)

Mandrake Linux Security Advisory : cvs (MDKSA-2005:073)

Mandrake Linux Security Advisory : cvsweb (MDKSA-2000:019)

Mandrake Linux Security Advisory : cyrus-imapd (MDKSA-2004:139)

Mandrake Linux Security Advisory : cyrus-imapd (MDKSA-2005:051)

Mandrake Linux Security Advisory : cyrus-sasl (MDKSA-2002:018)

Mandrake Linux Security Advisory : cyrus-sasl (MDKSA-2004:106)

Mandrake Linux Security Advisory : cyrus-sasl (MDKSA-2005:054)

Mandrake Linux Security Advisory : dbus (MDKSA-2005:105)

Mandrake Linux Security Advisory : dbus (MDKSA-2006:233)

Mandrake Linux Security Advisory : dhcp (MDKSA-2000:013)

Mandrake Linux Security Advisory : dhcp (MDKSA-2000:022-1)

Mandrake Linux Security Advisory : dhcp (MDKSA-2002:037)

Mandrake Linux Security Advisory : dhcp (MDKSA-2003:007)

Mandrake Linux Security Advisory : dhcp (MDKSA-2004:061)

Mandrake Linux Security Advisory : dhcpcd (MDKSA-2003:003)

Mandrake Linux Security Advisory : dhcpcd (MDKSA-2005:117)

Mandrake Linux Security Advisory : dia (MDKSA-2005:187)

Mandrake Linux Security Advisory : dia (MDKSA-2006:062)

Mandrake Linux Security Advisory : dia (MDKSA-2006:093)

Mandrake Linux Security Advisory : diffutils (MDKSA-2001:008-1)

Mandrake Linux Security Advisory : doxygen (MDKSA-2006:212)

Mandrake Linux Security Advisory : dump (MDKSA-2000:007)

Mandrake Linux Security Advisory : dump (MDKSA-2000:018)

Mandrake Linux Security Advisory : e2fsprogs (MDKSA-2007:242)

Mandrake Linux Security Advisory : ed (MDKSA-2000:076)

Mandrake Linux Security Advisory : eggdrop (MDKSA-2007:175)

Mandrake Linux Security Advisory : ekiga (MDKSA-2007:044)

Mandrake Linux Security Advisory : ekiga (MDKSA-2007:058)

Mandrake Linux Security Advisory : elm (MDKSA-2001:067)

Mandrake Linux Security Advisory : emacs (MDKSA-2000:088)

Mandrake Linux Security Advisory : emacs (MDKSA-2005:038)

Mandrake Linux Security Advisory : emacs (MDKSA-2007:133)

Mandrake Linux Security Advisory : enscript (MDKSA-2002:010)

Mandrake Linux Security Advisory : enscript (MDKSA-2005:033)

Mandrake Linux Security Advisory : eog (MDKSA-2003:048)

Mandrake Linux Security Advisory : eperl (MDKSA-2001:027)

Mandrake Linux Security Advisory : eroaster (MDKSA-2003:083)

Mandrake Linux Security Advisory : esound (MDKSA-2000:051)

Mandrake Linux Security Advisory : Eterm (MDKSA-2003:040)

Mandrake Linux Security Advisory : ethereal (MDKSA-2003:051)

Mandrake Linux Security Advisory : ethereal (MDKSA-2003:067)

Mandrake Linux Security Advisory : ethereal (MDKSA-2003:070)

Mandrake Linux Security Advisory : ethereal (MDKSA-2003:114)

Mandrake Linux Security Advisory : ethereal (MDKSA-2004:002)

Mandrake Linux Security Advisory : ethereal (MDKSA-2004:024)

Mandrake Linux Security Advisory : ethereal (MDKSA-2004:067)

Mandrake Linux Security Advisory : ethereal (MDKSA-2004:152)

Mandrake Linux Security Advisory : ethereal (MDKSA-2005:013)

Mandrake Linux Security Advisory : ethereal (MDKSA-2005:053)

Mandrake Linux Security Advisory : ethereal (MDKSA-2005:083)

Mandrake Linux Security Advisory : ethereal (MDKSA-2005:131)

Mandrake Linux Security Advisory : ethereal (MDKSA-2005:193-2)

Mandrake Linux Security Advisory : ethereal (MDKSA-2005:227)

Mandrake Linux Security Advisory : ethereal (MDKSA-2006:002)

Mandrake Linux Security Advisory : ethereal (MDKSA-2006:077)

Mandrake Linux Security Advisory : evince (MDKSA-2006:229)

Mandrake Linux Security Advisory : evolution (MDKSA-2003:045)

Mandrake Linux Security Advisory : evolution (MDKSA-2005:024)

Mandrake Linux Security Advisory : evolution (MDKSA-2005:059)

Mandrake Linux Security Advisory : evolution (MDKSA-2005:141)

Mandrake Linux Security Advisory : evolution (MDKSA-2006:094)

Mandrake Linux Security Advisory : evolution (MDKSA-2007:070)

Mandrake Linux Security Advisory : evolution (MDKSA-2007:107)

Mandrake Linux Security Advisory : evolution (MDKSA-2007:136)

Mandrake Linux Security Advisory : exmh (MDKSA-2001:015)

Mandrake Linux Security Advisory : expect (MDKSA-2001:087)

Mandrake Linux Security Advisory : ez-ipupdate (MDKSA-2004:129)

Mandrake Linux Security Advisory : fdutils (MDKSA-2000:005)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2001:063)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2001:072)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2002:036)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2002:063)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2003:011)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2003:101)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2005:126)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2005:209)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2005:236)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2007:016)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2007:105)

Mandrake Linux Security Advisory : fetchmail (MDKSA-2007:179)

Mandrake Linux Security Advisory : ffmpeg (MDKSA-2005:231)

Mandrake Linux Security Advisory : ffmpeg (MDKSA-2006:173)

Mandrake Linux Security Advisory : file (MDKSA-2003:030-1)

Mandrake Linux Security Advisory : file (MDKSA-2007:067)

Mandrake Linux Security Advisory : file (MDKSA-2007:114)

Mandrake Linux Security Advisory : fileutils (MDKSA-2002:031)

Mandrake Linux Security Advisory : fileutils/coreutils (MDKSA-2003:106)

Mandrake Linux Security Advisory : flac (MDKSA-2007:214)

Mandrake Linux Security Advisory : freeciv (MDKSA-2006:053)

Mandrake Linux Security Advisory : freeciv (MDKSA-2006:135)

Mandrake Linux Security Advisory : freeradius (MDKSA-2006:060)

Mandrake Linux Security Advisory : freeradius (MDKSA-2006:066)

Mandrake Linux Security Advisory : freeradius (MDKSA-2007:085)

Mandrake Linux Security Advisory : freetype2 (MDKSA-2006:099-1)

Mandrake Linux Security Advisory : freetype2 (MDKSA-2006:129)

Mandrake Linux Security Advisory : freetype2 (MDKSA-2007:081-1)

Mandrake Linux Security Advisory : freetype2 (MDKSA-2007:121)

Mandrake Linux Security Advisory : fuse (MDKSA-2005:216)

Mandrake Linux Security Advisory : gaim (MDKSA-2002:054-1)

Mandrake Linux Security Advisory : gaim (MDKSA-2004:006-1)

Mandrake Linux Security Advisory : gaim (MDKSA-2004:081)

Mandrake Linux Security Advisory : gaim (MDKSA-2004:110)

Mandrake Linux Security Advisory : gaim (MDKSA-2004:117)

Mandrake Linux Security Advisory : gaim (MDKSA-2005:049)

Mandrake Linux Security Advisory : gaim (MDKSA-2005:071)

Mandrake Linux Security Advisory : gaim (MDKSA-2005:086)

Mandrake Linux Security Advisory : gaim (MDKSA-2005:099)

Mandrake Linux Security Advisory : gaim (MDKSA-2005:139)

Mandrake Linux Security Advisory : gd (MDKSA-2004:132)

Mandrake Linux Security Advisory : gd (MDKSA-2006:112)

Mandrake Linux Security Advisory : gd (MDKSA-2007:035)

Mandrake Linux Security Advisory : gd (MDKSA-2007:122)

Mandrake Linux Security Advisory : gd (MDKSA-2007:153)

Mandrake Linux Security Advisory : gda2.0 (MDKSA-2005:203)

Mandrake Linux Security Advisory : gdb (MDKSA-2005:095)

Mandrake Linux Security Advisory : gdk-pixbuf (MDKSA-2005:069)

Mandrake Linux Security Advisory : gdk-pixbuf (MDKSA-2005:214)

Mandrake Linux Security Advisory : gdk-pixbuf/gtk+2 (MDKSA-2004:095-1)

Mandrake Linux Security Advisory : gdm (MDKSA-2001:070)

Mandrake Linux Security Advisory : gdm (MDKSA-2003:085)

Mandrake Linux Security Advisory : gdm (MDKSA-2003:100)

Mandrake Linux Security Advisory : gdm (MDKSA-2006:083)

Mandrake Linux Security Advisory : gdm (MDKSA-2006:100)

Mandrake Linux Security Advisory : gdm (MDKSA-2006:231)

Mandrake Linux Security Advisory : gdm (MDKSA-2007:169)

Mandrake Linux Security Advisory : gedit (MDKSA-2005:102)

Mandrake Linux Security Advisory : getty\_ps (MDKSA-2001:004)

Mandrake Linux Security Advisory : gftp (MDKSA-2001:044)

Mandrake Linux Security Advisory : gftp (MDKSA-2005:050)

Mandrake Linux Security Advisory : ghostscript (MDKSA-2000:074)

Mandrake Linux Security Advisory : ghostscript (MDKSA-2003:065)

Mandrake Linux Security Advisory : ghostscript (MDKSA-2007:208)

Mandrake Linux Security Advisory : gimp (MDKSA-2006:127)

Mandrake Linux Security Advisory : gimp (MDKSA-2007:108)

Mandrake Linux Security Advisory : gimp (MDKSA-2007:170)

Mandrake Linux Security Advisory : gkrellm (MDKSA-2003:087)

Mandrake Linux Security Advisory : glibc (MDKSA-2000:040)

Mandrake Linux Security Advisory : glibc (MDKSA-2000:045-1)

Mandrake Linux Security Advisory : glibc (MDKSA-2001:012)

Mandrake Linux Security Advisory : glibc (MDKSA-2001:095)

Mandrake Linux Security Advisory : glibc (MDKSA-2002:050)

Mandrake Linux Security Advisory : glibc (MDKSA-2002:061)

Mandrake Linux Security Advisory : glibc (MDKSA-2003:037)

Mandrake Linux Security Advisory : glibc (MDKSA-2003:107)

Mandrake Linux Security Advisory : glibc (MDKSA-2004:009)

Mandrake Linux Security Advisory : glibc (MDKSA-2004:159)

Mandrake Linux Security Advisory : gnome-vfs2 (MDKSA-2005:074)

Mandrake Linux Security Advisory : gnorpm (MDKSA-2000:055)

Mandrake Linux Security Advisory : gnucash (MDKSA-2007:046)

Mandrake Linux Security Advisory : gnumeric (MDKSA-2005:153)

Mandrake Linux Security Advisory : gnupg (MDKSA-2000:063-1)

Mandrake Linux Security Advisory : gnupg (MDKSA-2000:087)

Mandrake Linux Security Advisory : gnupg (MDKSA-2001:045)

Mandrake Linux Security Advisory : gnupg (MDKSA-2001:053-1)

Mandrake Linux Security Advisory : gnupg (MDKSA-2003:061)

Mandrake Linux Security Advisory : gnupg (MDKSA-2003:109)

Mandrake Linux Security Advisory : gnupg (MDKSA-2005:057)

Mandrake Linux Security Advisory : gnupg (MDKSA-2006:043)

Mandrake Linux Security Advisory : gnupg (MDKSA-2006:055)

Mandrake Linux Security Advisory : gnupg (MDKSA-2006:110)

Mandrake Linux Security Advisory : gnupg (MDKSA-2006:141)

Mandrake Linux Security Advisory : gnupg (MDKSA-2006:221)

Mandrake Linux Security Advisory : gnupg (MDKSA-2006:228)

Mandrake Linux Security Advisory : gnupg (MDKSA-2007:059)

Mandrake Linux Security Advisory : gnutls (MDKSA-2005:084)

Mandrake Linux Security Advisory : gnutls (MDKSA-2006:039)

Mandrake Linux Security Advisory : gnutls (MDKSA-2006:166)

Mandrake Linux Security Advisory : gpdf (MDKSA-2004:114)

Mandrake Linux Security Advisory : gpdf (MDKSA-2004:162)

Mandrake Linux Security Advisory : gpdf (MDKSA-2005:016)

Mandrake Linux Security Advisory : gpdf (MDKSA-2005:042)

Mandrake Linux Security Advisory : gpm (MDKSA-2000:002)

Mandrake Linux Security Advisory : gpm (MDKSA-2000:025)

Mandrake Linux Security Advisory : gpm (MDKSA-2001:006)

Mandrake Linux Security Advisory : graphviz (MDKSA-2005:188)

Mandrake Linux Security Advisory : grip (MDKSA-2005:066)

Mandrake Linux Security Advisory : groff (MDKSA-2002:012)

Mandrake Linux Security Advisory : groff (MDKSA-2006:038)

Mandrake Linux Security Advisory : gstreamer-ffmpeg (MDKSA-2005:232)

Mandrake Linux Security Advisory : gstreamer-ffmpeg (MDKSA-2006:174)

Mandrake Linux Security Advisory : gtk+ (MDKSA-2001:061-1)

Mandrake Linux Security Advisory : gtk+2.0 (MDKSA-2005:068)

Mandrake Linux Security Advisory : gtk+2.0 (MDKSA-2007:039)

Mandrake Linux Security Advisory : gtkhtml (MDKSA-2003:046)

Mandrake Linux Security Advisory : gtkhtml (MDKSA-2003:093)

Mandrake Linux Security Advisory : gv (MDKSA-2002:069)

Mandrake Linux Security Advisory : gv (MDKSA-2006:214-1)

Mandrake Linux Security Advisory : gzip (MDKSA-2002:011)

Mandrake Linux Security Advisory : gzip (MDKSA-2003:068)

Mandrake Linux Security Advisory : gzip (MDKSA-2004:142)

Mandrake Linux Security Advisory : gzip (MDKSA-2005:092)

Mandrake Linux Security Advisory : gzip (MDKSA-2006:027)

Mandrake Linux Security Advisory : gzip (MDKSA-2006:167)

Mandrake Linux Security Advisory : heartbeat (MDKSA-2006:142)

Mandrake Linux Security Advisory : hostapd (MDKSA-2006:088)

Mandrake Linux Security Advisory : hplip (MDKSA-2007:201)

Mandrake Linux Security Advisory : htdig (MDKSA-2001:083)

Mandrake Linux Security Advisory : htdig (MDKSA-2005:063)

Mandrake Linux Security Advisory : hylafax (MDKSA-2001:041)

Mandrake Linux Security Advisory : hylafax (MDKSA-2002:055)

Mandrake Linux Security Advisory : hylafax (MDKSA-2003:105)

Mandrake Linux Security Advisory : hylafax (MDKSA-2005:006)

Mandrake Linux Security Advisory : hylafax (MDKSA-2005:177)

Mandrake Linux Security Advisory : hylafax (MDKSA-2006:015)

Mandrake Linux Security Advisory : id3lib (MDKSA-2007:180)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2004:102)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2004:143)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2005:065)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2005:107)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2006:024)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2006:155)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2006:193)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2006:223)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2007:041)

Mandrake Linux Security Advisory : ImageMagick (MDKSA-2007:147)

Mandrake Linux Security Advisory : imap (MDKSA-2001:054)

Mandrake Linux Security Advisory : imap (MDKSA-2002:034)

Mandrake Linux Security Advisory : imap (MDKSA-2005:026)

Mandrake Linux Security Advisory : imap (MDKSA-2005:189)

Mandrake Linux Security Advisory : imlib (MDKSA-2002:029)

Mandrake Linux Security Advisory : imlib (MDKSA-2005:007)

Mandrake Linux Security Advisory : imlib2 (MDKSA-2004:089)

Mandrake Linux Security Advisory : imlib2 (MDKSA-2006:198-1)

Mandrake Linux Security Advisory : imlib2 (MDKSA-2007:156)

Mandrake Linux Security Advisory : imwheel (MDKSA-2000:001)

Mandrake Linux Security Advisory : inkscape (MDKSA-2007:069)

Mandrake Linux Security Advisory : inn (MDKSA-2000:016)

Mandrake Linux Security Advisory : inn (MDKSA-2000:023)

Mandrake Linux Security Advisory : inn (MDKSA-2001:010)

Mandrake Linux Security Advisory : iproute2 (MDKSA-2004:148)

Mandrake Linux Security Advisory : ipsec-tools (MDKSA-2004:027)

Mandrake Linux Security Advisory : ipsec-tools (MDKSA-2004:069)

Mandrake Linux Security Advisory : ipsec-tools (MDKSA-2005:062)

Mandrake Linux Security Advisory : ipsec-tools (MDKSA-2006:020)

Mandrake Linux Security Advisory : ipsec-tools (MDKSA-2007:084)

Mandrake Linux Security Advisory : iptables (MDKSA-2004:125)

Mandrake Linux Security Advisory : irssi (MDKSA-2003:117)

Mandrake Linux Security Advisory : ispell (MDKSA-2001:058)

Mandrake Linux Security Advisory : jabber (MDKSA-2004:005)

Mandrake Linux Security Advisory : jasper (MDKSA-2007:129)

Mandrake Linux Security Advisory : jmcce (MDKSA-2002:008)

Mandrake Linux Security Advisory : joe (MDKSA-2000:072)

Mandrake Linux Security Advisory : joe (MDKSA-2001:026)

Mandrake Linux Security Advisory : jpilot (MDKSA-2000:081)

Mandrake Linux Security Advisory : kaffeine (MDKSA-2006:065)

Mandrake Linux Security Advisory : kde (MDKSA-2003:004-1)

Mandrake Linux Security Advisory : kde3 (MDKSA-2003:049-1)

Mandrake Linux Security Advisory : kdebase (MDKSA-2003:091)

Mandrake Linux Security Advisory : kdebase (MDKSA-2005:160)

Mandrake Linux Security Advisory : kdebase (MDKSA-2006:105)

Mandrake Linux Security Advisory : kdebase (MDKSA-2007:138)

Mandrake Linux Security Advisory : kdebase (MDKSA-2007:190)

Mandrake Linux Security Advisory : kdeedu (MDKSA-2005:159)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2002:071)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2004:115)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2004:163)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2005:020)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2005:052)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2005:143)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2006:012)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2006:031)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2006:054)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2006:227)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2007:024)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2007:162)

Mandrake Linux Security Advisory : kdegraphics (MDKSA-2007:221)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2001:046-3)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2002:058)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2002:064)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2002:079)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2003:079)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2004:022)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2004:047)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2004:150)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2004:154)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2004:160)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2005:045)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2005:058)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2005:085)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2005:122)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2006:019)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2006:130)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2006:186)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2007:031)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2007:054)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2007:072)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2007:076)

Mandrake Linux Security Advisory : kdelibs (MDKSA-2007:157)

Mandrake Linux Security Advisory : kdelibs/kdebase (MDKSA-2004:086)

Mandrake Linux Security Advisory : kdenetwork (MDKSA-2002:080)

Mandrake Linux Security Advisory : kdenetwork (MDKSA-2007:009)

Mandrake Linux Security Advisory : kdepim (MDKSA-2004:003)

Mandrake Linux Security Advisory : kdesu (MDKSA-2000:008)

Mandrake Linux Security Advisory : kdesu (MDKSA-2001:018)

Mandrake Linux Security Advisory : kernel (MDKSA-2000:012)

Mandrake Linux Security Advisory : kernel (MDKSA-2001:037)

Mandrake Linux Security Advisory : kernel (MDKSA-2001:071)

Mandrake Linux Security Advisory : kernel (MDKSA-2001:079-2)

Mandrake Linux Security Advisory : kernel (MDKSA-2001:082-1)

Mandrake Linux Security Advisory : kernel (MDKSA-2002:041)

Mandrake Linux Security Advisory : kernel (MDKSA-2003:014)

Mandrake Linux Security Advisory : kernel (MDKSA-2003:038-1)

Mandrake Linux Security Advisory : kernel (MDKSA-2003:066-2)

Mandrake Linux Security Advisory : kernel (MDKSA-2003:074)

Mandrake Linux Security Advisory : kernel (MDKSA-2003:110)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:001)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:015)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:029)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:037)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:050)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:062)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:066)

Mandrake Linux Security Advisory : kernel (MDKSA-2004:087)

Mandrake Linux Security Advisory : kernel (MDKSA-2005:022)

Mandrake Linux Security Advisory : kernel (MDKSA-2005:110)

Mandrake Linux Security Advisory : kernel (MDKSA-2005:219)

Mandrake Linux Security Advisory : kernel (MDKSA-2005:235)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:018)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:040)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:059)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:086)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:087)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:123)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:124)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:151)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:182)

Mandrake Linux Security Advisory : kernel (MDKSA-2006:197)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:002)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:012)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:040)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:047)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:060)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:078)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:171)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:195)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:226)

Mandrake Linux Security Advisory : kernel (MDKSA-2007:232)

Mandrake Linux Security Advisory : kernel-2.4 (MDKSA-2005:111)

Mandrake Linux Security Advisory : kernel22 (MDKSA-2003:039)

Mandrake Linux Security Advisory : koffice (MDKSA-2004:165)

Mandrake Linux Security Advisory : koffice (MDKSA-2005:019)

Mandrake Linux Security Advisory : koffice (MDKSA-2005:056)

Mandrake Linux Security Advisory : koffice (MDKSA-2005:185)

Mandrake Linux Security Advisory : koffice (MDKSA-2006:008)

Mandrake Linux Security Advisory : koffice (MDKSA-2006:222)

Mandrake Linux Security Advisory : koffice (MDKSA-2007:018)

Mandrake Linux Security Advisory : koffice (MDKSA-2007:163)

Mandrake Linux Security Advisory : koffice (MDKSA-2007:222)

Mandrake Linux Security Advisory : kolab-resource-handlers (MDKSA-2006:013)

Mandrake Linux Security Advisory : kolab-server (MDKSA-2004:052)

Mandrake Linux Security Advisory : kon2 (MDKSA-2000:028)

Mandrake Linux Security Advisory : kon2 (MDKSA-2003:064)

Mandrake Linux Security Advisory : konqueror (MDKSA-2007:176)

Mandrake Linux Security Advisory : kopete (MDKSA-2003:055)

Mandrake Linux Security Advisory : kphone (MDKSA-2006:089)

Mandrake Linux Security Advisory : krb5 (MDKSA-2001:093)

Mandrake Linux Security Advisory : krb5 (MDKSA-2002:057)

Mandrake Linux Security Advisory : krb5 (MDKSA-2002:073-1)

Mandrake Linux Security Advisory : krb5 (MDKSA-2003:021)

Mandrake Linux Security Advisory : krb5 (MDKSA-2003:043-1)

Mandrake Linux Security Advisory : krb5 (MDKSA-2004:056-1)

Mandrake Linux Security Advisory : krb5 (MDKSA-2004:088)

Mandrake Linux Security Advisory : krb5 (MDKSA-2004:156)

Mandrake Linux Security Advisory : krb5 (MDKSA-2005:061)

Mandrake Linux Security Advisory : krb5 (MDKSA-2005:119)

Mandrake Linux Security Advisory : krb5 (MDKSA-2006:139)

Mandrake Linux Security Advisory : krb5 (MDKSA-2007:008)

Mandrake Linux Security Advisory : krb5 (MDKSA-2007:077-1)

Mandrake Linux Security Advisory : krb5 (MDKSA-2007:137)

Mandrake Linux Security Advisory : krb5 (MDKSA-2007:174-1)

Mandrake Linux Security Advisory : ksymoops (MDKSA-2004:060)

Mandrake Linux Security Advisory : ktorrent (MDKSA-2007:095)

Mandrake Linux Security Advisory : leafnode (MDKSA-2003:005)

Mandrake Linux Security Advisory : leafnode (MDKSA-2005:114)

Mandrake Linux Security Advisory : lftp (MDKSA-2003:116)

Mandrake Linux Security Advisory : lha (MDKSA-2007:117)

Mandrake Linux Security Advisory : libast (MDKSA-2006:029)

Mandrake Linux Security Advisory : libcdaudio1 (MDKSA-2005:075)

Mandrake Linux Security Advisory : libexif (MDKSA-2005:064)

Mandrake Linux Security Advisory : libexif (MDKSA-2007:118)

Mandrake Linux Security Advisory : libexif (MDKSA-2007:128)

Mandrake Linux Security Advisory : libgsf (MDKSA-2006:220)

Mandrake Linux Security Advisory : libgtop (MDKSA-2001:094)

Mandrake Linux Security Advisory : libgtop2 (MDKSA-2007:023)

Mandrake Linux Security Advisory : libksba (MDKSA-2006:183)

Mandrake Linux Security Advisory : libmms (MDKSA-2006:117-1)

Mandrake Linux Security Advisory : libmodplug (MDKSA-2007:001)

Mandrake Linux Security Advisory : libneon (MDKSA-2004:032)

Mandrake Linux Security Advisory : libneon (MDKSA-2004:049)

Mandrake Linux Security Advisory : libneon0.26 (MDKSA-2007:013)

Mandrake Linux Security Advisory : libnfsidmap (MDKSA-2007:240)

Mandrake Linux Security Advisory : libpng (MDKSA-2002:049)

Mandrake Linux Security Advisory : libpng (MDKSA-2003:008)

Mandrake Linux Security Advisory : libpng (MDKSA-2004:040)

Mandrake Linux Security Advisory : libpng (MDKSA-2004:063)

Mandrake Linux Security Advisory : libpng (MDKSA-2004:079)

Mandrake Linux Security Advisory : libpng (MDKSA-2006:209)

Mandrake Linux Security Advisory : libpng (MDKSA-2007:116)

Mandrake Linux Security Advisory : libpng (MDKSA-2007:217)

Mandrake Linux Security Advisory : librpcsecgss (MDKSA-2007:181)

Mandrake Linux Security Advisory : libsafe (MDKSA-2002:026)

Mandrake Linux Security Advisory : libsndfile (MDKSA-2007:191)

Mandrake Linux Security Advisory : libsoup (MDKSA-2007:029)

Mandrake Linux Security Advisory : libtiff (MDKSA-2004:109)

Mandrake Linux Security Advisory : libtiff (MDKSA-2005:001)

Mandrake Linux Security Advisory : libtiff (MDKSA-2005:142)

Mandrake Linux Security Advisory : libtiff (MDKSA-2006:042)

Mandrake Linux Security Advisory : libtiff (MDKSA-2006:082)

Mandrake Linux Security Advisory : libtiff (MDKSA-2006:095)

Mandrake Linux Security Advisory : libtiff (MDKSA-2006:102)

Mandrake Linux Security Advisory : libtiff (MDKSA-2006:137)

Mandrake Linux Security Advisory : libtunepimp (MDKSA-2006:126)

Mandrake Linux Security Advisory : libungif (MDKSA-2005:207)

Mandrake Linux Security Advisory : libuser (MDKSA-2004:044)

Mandrake Linux Security Advisory : libvorbis (MDKSA-2007:167-1)

Mandrake Linux Security Advisory : libvorbis (MDKSA-2007:194)

Mandrake Linux Security Advisory : libwmf (MDKSA-2006:114-1)

Mandrake Linux Security Advisory : libwmf (MDKSA-2006:132)

Mandrake Linux Security Advisory : libwmf (MDKSA-2007:036)

Mandrake Linux Security Advisory : libwmf (MDKSA-2007:123)

Mandrake Linux Security Advisory : libwpd (MDKSA-2007:063)

Mandrake Linux Security Advisory : libx11 (MDKSA-2006:199)

Mandrake Linux Security Advisory : libxml/libxml2 (MDKSA-2004:127)

Mandrake Linux Security Advisory : libxml2 (MDKSA-2004:018)

Mandrake Linux Security Advisory : libxpm4 (MDKSA-2004:098)

Mandrake Linux Security Advisory : libxpm4 (MDKSA-2004:137-1)

Mandrake Linux Security Advisory : licq (MDKSA-2001:032-1)

Mandrake Linux Security Advisory : links (MDKSA-2006:216)

Mandrake Linux Security Advisory : linuxconf (MDKSA-2001:011)

Mandrake Linux Security Advisory : lm\_sensors (MDKSA-2005:149)

Mandrake Linux Security Advisory : logcheck (MDKSA-2004:155)

Mandrake Linux Security Advisory : lpr (MDKSA-2000:054)

Mandrake Linux Security Advisory : lpr (MDKSA-2003:059)

Mandrake Linux Security Advisory : LPRng (MDKSA-2002:042)

Mandrake Linux Security Advisory : LPRng (MDKSA-2003:060)

Mandrake Linux Security Advisory : lvm (MDKSA-2004:144)

Mandrake Linux Security Advisory : lynx (MDKSA-2003:023)

Mandrake Linux Security Advisory : lynx (MDKSA-2005:186-1)

Mandrake Linux Security Advisory : lynx (MDKSA-2005:211)

Mandrake Linux Security Advisory : madwifi-source (MDKSA-2007:082)

Mandrake Linux Security Advisory : madwifi-source (MDKSA-2007:132)

Mandrake Linux Security Advisory : mailman (MDKSA-2004:013)

Mandrake Linux Security Advisory : mailman (MDKSA-2004:051)

Mandrake Linux Security Advisory : mailman (MDKSA-2005:015)

Mandrake Linux Security Advisory : mailman (MDKSA-2005:037)

Mandrake Linux Security Advisory : mailman (MDKSA-2005:222)

Mandrake Linux Security Advisory : mailman (MDKSA-2006:165)

Mandrake Linux Security Advisory : man (MDKSA-2000:015)

Mandrake Linux Security Advisory : man (MDKSA-2003:054)

Mandrake Linux Security Advisory : MandrakeUpdate (MDKSA-2000:034)

Mandrake Linux Security Advisory : mc (MDKSA-2000:078)

Mandrake Linux Security Advisory : mc (MDKSA-2004:007)

Mandrake Linux Security Advisory : mc (MDKSA-2004:039)

Mandrake Linux Security Advisory : Mesa (MDKSA-2001:029)

Mandrake Linux Security Advisory : metamail (MDKSA-2004:014)

Mandrake Linux Security Advisory : metamail (MDKSA-2006:047)

Mandrake Linux Security Advisory : mgetty (MDKSA-2000:042)

Mandrake Linux Security Advisory : mgetty (MDKSA-2001:009)

Mandrake Linux Security Advisory : mgetty (MDKSA-2003:053-1)

Mandrake Linux Security Advisory : minicom (MDKSA-2001:051)

Mandrake Linux Security Advisory : mm (MDKSA-2002:045)

Mandrake Linux Security Advisory : mod\_frontpage (MDKSA-2002:021)

Mandrake Linux Security Advisory : mod\_perl (MDKSA-2000:046)

Mandrake Linux Security Advisory : mod\_php3 (MDKSA-2000:048)

Mandrake Linux Security Advisory : mod\_php3 (MDKSA-2000:062)

Mandrake Linux Security Advisory : mod\_ssl (MDKSA-2002:020)

Mandrake Linux Security Advisory : mod\_ssl (MDKSA-2002:048)

Mandrake Linux Security Advisory : mod\_ssl (MDKSA-2002:072)

Mandrake Linux Security Advisory : mod\_ssl (MDKSA-2004:054)

Mandrake Linux Security Advisory : mod\_ssl (MDKSA-2004:075)

Mandrake Linux Security Advisory : mod\_ssl/apache2-mod\_ssl (MDKSA-2004:122)

Mandrake Linux Security Advisory : modutils (MDKSA-2000:071-2)

Mandrake Linux Security Advisory : mono (MDKSA-2006:188)

Mandrake Linux Security Advisory : mono (MDKSA-2006:234)

Mandrake Linux Security Advisory : mono (MDKSA-2007:218)

Mandrake Linux Security Advisory : mozilla (MDKSA-2002:074)

Mandrake Linux Security Advisory : mozilla (MDKSA-2004:021)

Mandrake Linux Security Advisory : mozilla (MDKSA-2004:082)

Mandrake Linux Security Advisory : mozilla (MDKSA-2004:107)

Mandrake Linux Security Advisory : mozilla (MDKSA-2005:088)

Mandrake Linux Security Advisory : mozilla (MDKSA-2005:128)

Mandrake Linux Security Advisory : mozilla (MDKSA-2005:170)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2005:173)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2006:037)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2006:075)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2006:143-1)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2006:168)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2006:205)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2007:010)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2007:050-1)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2007:120)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2007:126-1)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2007:152)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2007:202)

Mandrake Linux Security Advisory : mozilla-firefox (MDKSA-2007:246)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2005:174)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2005:226)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2006:021)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2006:052)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2006:078)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2006:146)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2006:169)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2006:206)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2007:011)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2007:052)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2007:119)

Mandrake Linux Security Advisory : mozilla-thunderbird (MDKSA-2007:131)

Mandrake Linux Security Advisory : mpg123 (MDKSA-2003:078)

Mandrake Linux Security Advisory : mpg123 (MDKSA-2004:100)

Mandrake Linux Security Advisory : mpg123 (MDKSA-2004:120)

Mandrake Linux Security Advisory : mpg123 (MDKSA-2005:009)

Mandrake Linux Security Advisory : mpg123 (MDKSA-2006:092)

Mandrake Linux Security Advisory : mpg123 (MDKSA-2007:032)

Mandrake Linux Security Advisory : mplayer (MDKSA-2003:097)

Mandrake Linux Security Advisory : mplayer (MDKSA-2004:026)

Mandrake Linux Security Advisory : mplayer (MDKSA-2004:157)

Mandrake Linux Security Advisory : mplayer (MDKSA-2005:115)

Mandrake Linux Security Advisory : mplayer (MDKSA-2005:158)

Mandrake Linux Security Advisory : mplayer (MDKSA-2005:230)

Mandrake Linux Security Advisory : mplayer (MDKSA-2006:048)

Mandrake Linux Security Advisory : mplayer (MDKSA-2006:068)

Mandrake Linux Security Advisory : mplayer (MDKSA-2006:175)

Mandrake Linux Security Advisory : mplayer (MDKSA-2007:055)

Mandrake Linux Security Advisory : mplayer (MDKSA-2007:061)

Mandrake Linux Security Advisory : mplayer (MDKSA-2007:112)

Mandrake Linux Security Advisory : mplayer (MDKSA-2007:143)

Mandrake Linux Security Advisory : mplayer (MDKSA-2007:192)

Mandrake Linux Security Advisory : mtools (MDKSA-2004:016)

Mandrake Linux Security Advisory : musicbrainz (MDKSA-2006:157-1)

Mandrake Linux Security Advisory : mutt (MDKSA-2001:031)

Mandrake Linux Security Advisory : mutt (MDKSA-2002:002-1)

Mandrake Linux Security Advisory : mutt (MDKSA-2003:041-1)

Mandrake Linux Security Advisory : mutt (MDKSA-2004:010)

Mandrake Linux Security Advisory : mutt (MDKSA-2006:115)

Mandrake Linux Security Advisory : mutt (MDKSA-2006:190)

Mandrake Linux Security Advisory : mutt (MDKSA-2007:113)

Mandrake Linux Security Advisory : MySQL (MDKSA-2001:014-1)

Mandrake Linux Security Advisory : MySQL (MDKSA-2002:087)

Mandrake Linux Security Advisory : MYSQL (MDKSA-2003:013)

Mandrake Linux Security Advisory : MySQL (MDKSA-2003:057)

Mandrake Linux Security Advisory : MySQL (MDKSA-2003:094)

Mandrake Linux Security Advisory : MySQL (MDKSA-2004:034)

Mandrake Linux Security Advisory : MySQL (MDKSA-2004:119)

Mandrake Linux Security Advisory : MySQL (MDKSA-2005:036)

Mandrake Linux Security Advisory : MySQL (MDKSA-2005:060)

Mandrake Linux Security Advisory : MySQL (MDKSA-2005:070)

Mandrake Linux Security Advisory : MySQL (MDKSA-2005:163)

Mandrake Linux Security Advisory : MySQL (MDKSA-2006:064)

Mandrake Linux Security Advisory : MySQL (MDKSA-2006:084)

Mandrake Linux Security Advisory : MySQL (MDKSA-2006:097)

Mandrake Linux Security Advisory : MySQL (MDKSA-2006:111)

Mandrake Linux Security Advisory : MySQL (MDKSA-2006:149)

Mandrake Linux Security Advisory : MySQL (MDKSA-2006:158)

Mandrake Linux Security Advisory : MySQL (MDKSA-2006:177)

Mandrake Linux Security Advisory : MySQL (MDKSA-2007:139)

Mandrake Linux Security Advisory : MySQL (MDKSA-2007:177)

Mandrake Linux Security Advisory : MySQL (MDKSA-2007:243)

Mandrake Linux Security Advisory : nas (MDKSA-2007:065)

Mandrake Linux Security Advisory : nasm (MDKSA-2005:004)

Mandrake Linux Security Advisory : nasm (MDKSA-2005:090)

Mandrake Linux Security Advisory : ncompress (MDKSA-2006:140)

Mandrake Linux Security Advisory : ncpfs (MDKSA-2005:028)

Mandrake Linux Security Advisory : ncurses (MDKSA-2001:052)

Mandrake Linux Security Advisory : nedit (MDKSA-2001:042)

Mandrake Linux Security Advisory : net-snmp (MDKSA-2003:115)

Mandrake Linux Security Advisory : net-snmp (MDKSA-2006:025)

Mandrake Linux Security Advisory : net-snmp (MDKSA-2007:225)

Mandrake Linux Security Advisory : netatalk (MDKSA-2004:121)

Mandrake Linux Security Advisory : netpbm (MDKSA-2003:036)

Mandrake Linux Security Advisory : netpbm (MDKSA-2004:011-1)

Mandrake Linux Security Advisory : netpbm (MDKSA-2005:133)

Mandrake Linux Security Advisory : netpbm (MDKSA-2005:199)

Mandrake Linux Security Advisory : netpbm (MDKSA-2005:217)

Mandrake Linux Security Advisory : netpbm (MDKSA-2007:209)

Mandrake Linux Security Advisory : netscape (MDKSA-2000:027-1)

Mandrake Linux Security Advisory : netscape (MDKSA-2000:036)

Mandrake Linux Security Advisory : netscape (MDKSA-2000:080)

Mandrake Linux Security Advisory : netscape (MDKSA-2001:038)

Mandrake Linux Security Advisory : nfs-utils (MDKSA-2000:021)

Mandrake Linux Security Advisory : nfs-utils (MDKSA-2003:076)

Mandrake Linux Security Advisory : nfs-utils (MDKSA-2004:146)

Mandrake Linux Security Advisory : nfs-utils (MDKSA-2005:005)

Mandrake Linux Security Advisory : nmh (MDKSA-2000:000)

Mandrake Linux Security Advisory : nss\_ldap (MDKSA-2000:066-1)

Mandrake Linux Security Advisory : nss\_ldap (MDKSA-2002:075)

Mandrake Linux Security Advisory : nss\_ldap (MDKSA-2005:121)

Mandrake Linux Security Advisory : nss\_ldap (MDKSA-2005:190)

Mandrake Linux Security Advisory : ntp (MDKSA-2001:036)

Mandrake Linux Security Advisory : ntp (MDKSA-2006:178)

Mandrake Linux Security Advisory : nvidia (MDKSA-2007:007)

Mandrake Linux Security Advisory : opal (MDKSA-2007:205)

Mandrake Linux Security Advisory : openafs (MDKSA-2007:066)

Mandrake Linux Security Advisory : openldap (MDKSA-2000:003)

Mandrake Linux Security Advisory : openldap (MDKSA-2001:069)

Mandrake Linux Security Advisory : openldap (MDKSA-2002:013)

Mandrake Linux Security Advisory : openldap (MDKSA-2003:006)

Mandrake Linux Security Advisory : openldap (MDKSA-2006:096)

Mandrake Linux Security Advisory : openldap (MDKSA-2006:171)

Mandrake Linux Security Advisory : openldap (MDKSA-2006:208)

Mandrake Linux Security Advisory : openldap (MDKSA-2007:215)

Mandrake Linux Security Advisory : OpenOffice.org (MDKSA-2004:078)

Mandrake Linux Security Advisory : OpenOffice.org (MDKSA-2004:103)

Mandrake Linux Security Advisory : OpenOffice.org (MDKSA-2005:082)

Mandrake Linux Security Advisory : OpenOffice.org (MDKSA-2006:033)

Mandrake Linux Security Advisory : OpenOffice.org (MDKSA-2006:118)

Mandrake Linux Security Advisory : openoffice.org (MDKSA-2007:006)

Mandrake Linux Security Advisory : openoffice.org (MDKSA-2007:064)

Mandrake Linux Security Advisory : openoffice.org (MDKSA-2007:073)

Mandrake Linux Security Advisory : openoffice.org (MDKSA-2007:144)

Mandrake Linux Security Advisory : openoffice.org (MDKSA-2007:186)

Mandrake Linux Security Advisory : openslp (MDKSA-2005:055)

Mandrake Linux Security Advisory : openssh (MDKSA-2000:068-1)

Mandrake Linux Security Advisory : openssh (MDKSA-2001:033-2)

Mandrake Linux Security Advisory : openssh (MDKSA-2001:081)

Mandrake Linux Security Advisory : openssh (MDKSA-2001:092)

Mandrake Linux Security Advisory : openssh (MDKSA-2002:019)

Mandrake Linux Security Advisory : openssh (MDKSA-2002:040-1)

Mandrake Linux Security Advisory : openssh (MDKSA-2003:090-1)

Mandrake Linux Security Advisory : openssh (MDKSA-2006:034)

Mandrake Linux Security Advisory : openssh (MDKSA-2006:179)

Mandrake Linux Security Advisory : openssh (MDKSA-2006:204)

Mandrake Linux Security Advisory : openssh (MDKSA-2007:236)

Mandrake Linux Security Advisory : openssl (MDKSA-2001:065)

Mandrake Linux Security Advisory : openssl (MDKSA-2002:046-1)

Mandrake Linux Security Advisory : openssl (MDKSA-2003:020)

Mandrake Linux Security Advisory : openssl (MDKSA-2003:035)

Mandrake Linux Security Advisory : openssl (MDKSA-2003:098)

Mandrake Linux Security Advisory : openssl (MDKSA-2004:023)

Mandrake Linux Security Advisory : openssl (MDKSA-2004:147)

Mandrake Linux Security Advisory : openssl (MDKSA-2005:096)

Mandrake Linux Security Advisory : openssl (MDKSA-2005:179)

Mandrake Linux Security Advisory : openssl (MDKSA-2006:161)

Mandrake Linux Security Advisory : openssl (MDKSA-2006:172-1)

Mandrake Linux Security Advisory : openssl (MDKSA-2007:193)

Mandrake Linux Security Advisory : openssl (MDKSA-2007:237)

Mandrake Linux Security Advisory : openvpn (MDKSA-2005:206-1)

Mandrake Linux Security Advisory : openvpn (MDKSA-2006:069)

Mandrake Linux Security Advisory : pam (MDKSA-2000:029)

Mandrake Linux Security Advisory : pam (MDKSA-2000:082-1)

Mandrake Linux Security Advisory : pam (MDKSA-2003:017-1)

Mandrake Linux Security Advisory : pam\_ldap (MDKSA-2003:088)

Mandrake Linux Security Advisory : pam\_ldap (MDKSA-2006:201)

Mandrake Linux Security Advisory : passwd (MDKSA-2001:091)

Mandrake Linux Security Advisory : passwd (MDKSA-2004:045)

Mandrake Linux Security Advisory : pcre (MDKSA-2005:151)

Mandrake Linux Security Advisory : pcre (MDKSA-2007:211)

Mandrake Linux Security Advisory : pcre (MDKSA-2007:212)

Mandrake Linux Security Advisory : pdftohtml (MDKSA-2007:019)

Mandrake Linux Security Advisory : pdftohtml (MDKSA-2007:160)

Mandrake Linux Security Advisory : pdftohtml (MDKSA-2007:223)

Mandrake Linux Security Advisory : perl (MDKSA-2000:031)

Mandrake Linux Security Advisory : perl (MDKSA-2005:031)

Mandrake Linux Security Advisory : perl (MDKSA-2005:079)

Mandrake Linux Security Advisory : perl (MDKSA-2005:225)

Mandrake Linux Security Advisory : perl (MDKSA-2007:207)

Mandrake Linux Security Advisory : perl-Archive-Zip (MDKSA-2004:118)

Mandrake Linux Security Advisory : perl-CGI (MDKSA-2003:084)

Mandrake Linux Security Advisory : perl-Compress-Zlib (MDKSA-2005:196)

Mandrake Linux Security Advisory : perl-DBI (MDKSA-2005:030)

Mandrake Linux Security Advisory : perl-Digest-MD5 (MDKSA-2002:035)

Mandrake Linux Security Advisory : perl-MailTools (MDKSA-2002:076)

Mandrake Linux Security Advisory : perl-MIME-tools (MDKSA-2004:123)

Mandrake Linux Security Advisory : perl-Net-DNS (MDKSA-2007:146)

Mandrake Linux Security Advisory : perl-Net\_SSLeay (MDKSA-2006:023)

Mandrake Linux Security Advisory : php (MDKSA-2001:013)

Mandrake Linux Security Advisory : php (MDKSA-2002:017)

Mandrake Linux Security Advisory : php (MDKSA-2002:059)

Mandrake Linux Security Advisory : php (MDKSA-2003:019)

Mandrake Linux Security Advisory : php (MDKSA-2003:082-1)

Mandrake Linux Security Advisory : php (MDKSA-2004:068)

Mandrake Linux Security Advisory : php (MDKSA-2004:151)

Mandrake Linux Security Advisory : php (MDKSA-2005:072)

Mandrake Linux Security Advisory : php (MDKSA-2005:152)

Mandrake Linux Security Advisory : php (MDKSA-2005:213)

Mandrake Linux Security Advisory : php (MDKSA-2005:238)

Mandrake Linux Security Advisory : php (MDKSA-2006:028)

Mandrake Linux Security Advisory : php (MDKSA-2006:035)

Mandrake Linux Security Advisory : php (MDKSA-2006:063)

Mandrake Linux Security Advisory : php (MDKSA-2006:074)

Mandrake Linux Security Advisory : php (MDKSA-2006:091)

Mandrake Linux Security Advisory : php (MDKSA-2006:122)

Mandrake Linux Security Advisory : php (MDKSA-2006:144)

Mandrake Linux Security Advisory : php (MDKSA-2006:162)

Mandrake Linux Security Advisory : php (MDKSA-2006:185)

Mandrake Linux Security Advisory : php (MDKSA-2006:196)

Mandrake Linux Security Advisory : php (MDKSA-2007:038)

Mandrake Linux Security Advisory : php (MDKSA-2007:048)

Mandrake Linux Security Advisory : php (MDKSA-2007:089)

Mandrake Linux Security Advisory : php (MDKSA-2007:090)

Mandrake Linux Security Advisory : php (MDKSA-2007:102)

Mandrake Linux Security Advisory : php (MDKSA-2007:187)

Mandrake Linux Security Advisory : php-imap (MDKSA-2005:194)

Mandrake Linux Security Advisory : php-pear (MDKSA-2005:109)

Mandrake Linux Security Advisory : php-pear (MDKSA-2005:146)

Mandrake Linux Security Advisory : php-pear (MDKSA-2007:110)

Mandrake Linux Security Advisory : phpgroupware (MDKSA-2003:077)

Mandrake Linux Security Advisory : pine (MDKSA-2000:073-1)

Mandrake Linux Security Advisory : pine (MDKSA-2001:047-1)

Mandrake Linux Security Advisory : pine (MDKSA-2002:084)

Mandrake Linux Security Advisory : playmidi (MDKSA-2005:010)

Mandrake Linux Security Advisory : poppler (MDKSA-2006:030)

Mandrake Linux Security Advisory : poppler (MDKSA-2007:020)

Mandrake Linux Security Advisory : poppler (MDKSA-2007:161)

Mandrake Linux Security Advisory : poppler (MDKSA-2007:227)

Mandrake Linux Security Advisory : postfix (MDKSA-2001:089)

Mandrake Linux Security Advisory : postfix (MDKSA-2003:081)

Mandrake Linux Security Advisory : postgresql (MDKSA-2002:062-1)

Mandrake Linux Security Advisory : postgresql (MDKSA-2003:102)

Mandrake Linux Security Advisory : postgresql (MDKSA-2004:149)

Mandrake Linux Security Advisory : postgresql (MDKSA-2005:040)

Mandrake Linux Security Advisory : postgresql (MDKSA-2005:093)

Mandrake Linux Security Advisory : postgresql (MDKSA-2006:098)

Mandrake Linux Security Advisory : postgresql (MDKSA-2006:194)

Mandrake Linux Security Advisory : postgresql (MDKSA-2007:037-1)

Mandrake Linux Security Advisory : postgresql (MDKSA-2007:094)

Mandrake Linux Security Advisory : postgresql (MDKSA-2007:188)

Mandrake Linux Security Advisory : ppp (MDKSA-2006:119)

Mandrake Linux Security Advisory : printer-drivers (MDKSA-2003:010)

Mandrake Linux Security Advisory : printer-drivers (MDKSA-2004:094)

Mandrake Linux Security Advisory : printer-filters-utils (MDKSA-2005:239)

Mandrake Linux Security Advisory : procmail (MDKSA-2001:085)

Mandrake Linux Security Advisory : proftpd (MDKSA-2001:021)

Mandrake Linux Security Advisory : proftpd (MDKSA-2002:005)

Mandrake Linux Security Advisory : proftpd (MDKSA-2003:095-1)

Mandrake Linux Security Advisory : proftpd (MDKSA-2004:041)

Mandrake Linux Security Advisory : proftpd (MDKSA-2005:140)

Mandrake Linux Security Advisory : proftpd (MDKSA-2006:217-1)

Mandrake Linux Security Advisory : proftpd (MDKSA-2006:232)

Mandrake Linux Security Advisory : proftpd (MDKSA-2007:130)

Mandrake Linux Security Advisory : pwlib (MDKSA-2004:017)

Mandrake Linux Security Advisory : pwlib (MDKSA-2007:206)

Mandrake Linux Security Advisory : pxelinux (MDKSA-2006:211)

Mandrake Linux Security Advisory : python (MDKSA-2002:082-1)

Mandrake Linux Security Advisory : python (MDKSA-2004:019)

Mandrake Linux Security Advisory : python (MDKSA-2005:035)

Mandrake Linux Security Advisory : python (MDKSA-2005:154)

Mandrake Linux Security Advisory : python (MDKSA-2006:181)

Mandrake Linux Security Advisory : python (MDKSA-2007:099)

Mandrake Linux Security Advisory : qt (MDKSA-2006:187)

Mandrake Linux Security Advisory : qt (MDKSA-2007:183)

Mandrake Linux Security Advisory : qt3 (MDKSA-2004:085)

Mandrake Linux Security Advisory : qt3 (MDKSA-2007:074)

Mandrake Linux Security Advisory : qt3 (MDKSA-2007:151)

Mandrake Linux Security Advisory : qt4 (MDKSA-2007:075-1)

Mandrake Linux Security Advisory : rdist (MDKSA-2001:005)

Mandrake Linux Security Advisory : rp-pppoe (MDKSA-2000:084)

Mandrake Linux Security Advisory : rp-pppoe (MDKSA-2004:145)

Mandrake Linux Security Advisory : rpm (MDKSA-2006:200)

Mandrake Linux Security Advisory : rpmdrake (MDKSA-2001:043)

Mandrake Linux Security Advisory : rsh (MDKSA-2005:100)

Mandrake Linux Security Advisory : rsync (MDKSA-2002:009)

Mandrake Linux Security Advisory : rsync (MDKSA-2002:024)

Mandrake Linux Security Advisory : rsync (MDKSA-2003:111)

Mandrake Linux Security Advisory : rsync (MDKSA-2004:042)

Mandrake Linux Security Advisory : rsync (MDKSA-2004:083)

Mandrake Linux Security Advisory : ruby (MDKSA-2004:128)

Mandrake Linux Security Advisory : ruby (MDKSA-2005:118)

Mandrake Linux Security Advisory : ruby (MDKSA-2005:191)

Mandrake Linux Security Advisory : ruby (MDKSA-2006:079)

Mandrake Linux Security Advisory : ruby (MDKSA-2006:134)

Mandrake Linux Security Advisory : ruby (MDKSA-2006:192)

Mandrake Linux Security Advisory : ruby (MDKSA-2006:225)

Mandrake Linux Security Advisory : rwho (MDKSA-2005:039)

Mandrake Linux Security Advisory : rxvt (MDKSA-2003:034)

Mandrake Linux Security Advisory : samba (MDKSA-2001:040-1)

Mandrake Linux Security Advisory : samba (MDKSA-2001:062)

Mandrake Linux Security Advisory : samba (MDKSA-2002:081)

Mandrake Linux Security Advisory : samba (MDKSA-2003:032)

Mandrake Linux Security Advisory : samba (MDKSA-2003:044)

Mandrake Linux Security Advisory : samba (MDKSA-2004:035)

Mandrake Linux Security Advisory : samba (MDKSA-2004:071)

Mandrake Linux Security Advisory : samba (MDKSA-2004:092)

Mandrake Linux Security Advisory : samba (MDKSA-2004:104)

Mandrake Linux Security Advisory : samba (MDKSA-2004:131)

Mandrake Linux Security Advisory : samba (MDKSA-2004:136)

Mandrake Linux Security Advisory : samba (MDKSA-2004:158)

Mandrake Linux Security Advisory : samba (MDKSA-2006:120)

Mandrake Linux Security Advisory : samba (MDKSA-2007:034)

Mandrake Linux Security Advisory : samba (MDKSA-2007:104-1)

Mandrake Linux Security Advisory : samba (MDKSA-2007:224-3)

Mandrake Linux Security Advisory : samba (MDKSA-2007:244)

Mandrake Linux Security Advisory : sane (MDKSA-2003:099)

Mandrake Linux Security Advisory : sash (MDKSA-2006:070)

Mandrake Linux Security Advisory : screen (MDKSA-2003:113)

Mandrake Linux Security Advisory : screen (MDKSA-2006:191)

Mandrake Linux Security Advisory : sendmail (MDKSA-2001:075)

Mandrake Linux Security Advisory : sendmail (MDKSA-2002:083)

Mandrake Linux Security Advisory : sendmail (MDKSA-2003:028)

Mandrake Linux Security Advisory : sendmail (MDKSA-2003:042-1)

Mandrake Linux Security Advisory : sendmail (MDKSA-2003:086)

Mandrake Linux Security Advisory : sendmail (MDKSA-2003:092)

Mandrake Linux Security Advisory : sendmail (MDKSA-2006:058)

Mandrake Linux Security Advisory : sendmail (MDKSA-2006:104)

Mandrake Linux Security Advisory : sendmail (MDKSA-2006:156)

Mandrake Linux Security Advisory : sgml-tools (MDKSA-2001:030-1)

Mandrake Linux Security Advisory : shadow-utils (MDKSA-2001:007)

Mandrake Linux Security Advisory : shadow-utils (MDKSA-2003:026)

Mandrake Linux Security Advisory : shadow-utils (MDKSA-2004:126)

Mandrake Linux Security Advisory : sharutils (MDKSA-2002:052)

Mandrake Linux Security Advisory : sharutils (MDKSA-2005:067)

Mandrake Linux Security Advisory : shorewall (MDKSA-2004:080)

Mandrake Linux Security Advisory : shorewall (MDKSA-2005:123)

Mandrake Linux Security Advisory : slocate (MDKSA-2000:085)

Mandrake Linux Security Advisory : slocate (MDKSA-2003:015)

Mandrake Linux Security Advisory : slocate (MDKSA-2004:004)

Mandrake Linux Security Advisory : slocate (MDKSA-2005:147)

Mandrake Linux Security Advisory : slrn (MDKSA-2001:028)

Mandrake Linux Security Advisory : smb4k (MDKSA-2005:157)

Mandrake Linux Security Advisory : smb4k (MDKSA-2007:042)

Mandrake Linux Security Advisory : snort (MDKSA-2003:029)

Mandrake Linux Security Advisory : snort (MDKSA-2003:052)

Mandrake Linux Security Advisory : snort (MDKSA-2007:051)

Mandrake Linux Security Advisory : sox (MDKSA-2004:076)

Mandrake Linux Security Advisory : spamassassin (MDKSA-2004:084)

Mandrake Linux Security Advisory : spamassassin (MDKSA-2005:106)

Mandrake Linux Security Advisory : spamassassin (MDKSA-2005:221)

Mandrake Linux Security Advisory : spamassassin (MDKSA-2006:103)

Mandrake Linux Security Advisory : spamassassin (MDKSA-2007:049)

Mandrake Linux Security Advisory : spamassassin (MDKSA-2007:125)

Mandrake Linux Security Advisory : speedtouch (MDKSA-2004:130)

Mandrake Linux Security Advisory : sqlite (MDKSA-2007:091)

Mandrake Linux Security Advisory : squid (MDKSA-2001:003)

Mandrake Linux Security Advisory : squid (MDKSA-2001:066)

Mandrake Linux Security Advisory : squid (MDKSA-2001:088)

Mandrake Linux Security Advisory : squid (MDKSA-2002:016-1)

Mandrake Linux Security Advisory : squid (MDKSA-2002:027)

Mandrake Linux Security Advisory : squid (MDKSA-2002:044)

Mandrake Linux Security Advisory : squid (MDKSA-2004:025)

Mandrake Linux Security Advisory : squid (MDKSA-2004:059)

Mandrake Linux Security Advisory : squid (MDKSA-2004:093)

Mandrake Linux Security Advisory : squid (MDKSA-2004:112)

Mandrake Linux Security Advisory : squid (MDKSA-2005:014)

Mandrake Linux Security Advisory : squid (MDKSA-2005:034)

Mandrake Linux Security Advisory : squid (MDKSA-2005:047)

Mandrake Linux Security Advisory : squid (MDKSA-2005:078)

Mandrake Linux Security Advisory : squid (MDKSA-2005:104)

Mandrake Linux Security Advisory : squid (MDKSA-2005:162)

Mandrake Linux Security Advisory : squid (MDKSA-2005:181)

Mandrake Linux Security Advisory : squid (MDKSA-2005:195)

Mandrake Linux Security Advisory : squid (MDKSA-2007:026)

Mandrake Linux Security Advisory : squid (MDKSA-2007:068)

Mandrake Linux Security Advisory : stunnel (MDKSA-2002:004)

Mandrake Linux Security Advisory : stunnel (MDKSA-2003:108)

Mandrake Linux Security Advisory : sudo (MDKSA-2001:024-1)

Mandrake Linux Security Advisory : sudo (MDKSA-2002:003)

Mandrake Linux Security Advisory : sudo (MDKSA-2002:028)

Mandrake Linux Security Advisory : sudo (MDKSA-2004:133)

Mandrake Linux Security Advisory : sudo (MDKSA-2005:103)

Mandrake Linux Security Advisory : sudo (MDKSA-2005:201)

Mandrake Linux Security Advisory : sudo (MDKSA-2005:234)

Mandrake Linux Security Advisory : sudo (MDKSA-2006:159)

Mandrake Linux Security Advisory : super-freeswan (MDKSA-2004:070-1)

Mandrake Linux Security Advisory : sysklogd (MDKSA-2000:050-1)

Mandrake Linux Security Advisory : sysklogd (MDKSA-2004:038)

Mandrake Linux Security Advisory : syslinux (MDKSA-2006:210)

Mandrake Linux Security Advisory : t1lib (MDKSA-2007:189)

Mandrake Linux Security Advisory : tar (MDKSA-2002:066)

Mandrake Linux Security Advisory : tar (MDKSA-2006:046)

Mandrake Linux Security Advisory : tar (MDKSA-2006:219)

Mandrake Linux Security Advisory : tar (MDKSA-2007:173)

Mandrake Linux Security Advisory : tar (MDKSA-2007:197)

Mandrake Linux Security Advisory : tcltk (MDKSA-2002:060)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2001:056)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2002:032)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2003:027)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2004:008)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2004:030)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2005:087)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2005:101)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2007:056)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2007:148)

Mandrake Linux Security Advisory : tcpdump (MDKSA-2007:155)

Mandrake Linux Security Advisory : tcsh (MDKSA-2000:069)

Mandrake Linux Security Advisory : teetx (MDKSA-2002:070)

Mandrake Linux Security Advisory : telnet (MDKSA-2001:068)

Mandrake Linux Security Advisory : tetex (MDKSA-2001:086)

Mandrake Linux Security Advisory : tetex (MDKSA-2004:166)

Mandrake Linux Security Advisory : tetex (MDKSA-2005:021)

Mandrake Linux Security Advisory : tetex (MDKSA-2005:044)

Mandrake Linux Security Advisory : tetex (MDKSA-2006:011)

Mandrake Linux Security Advisory : tetex (MDKSA-2006:113)

Mandrake Linux Security Advisory : tetex (MDKSA-2007:022)

Mandrake Linux Security Advisory : tetex (MDKSA-2007:109)

Mandrake Linux Security Advisory : tetex (MDKSA-2007:124)

Mandrake Linux Security Advisory : tetex (MDKSA-2007:164)

Mandrake Linux Security Advisory : tetex (MDKSA-2007:230)

Mandrake Linux Security Advisory : texinfo (MDKSA-2005:175)

Mandrake Linux Security Advisory : texinfo (MDKSA-2006:203)

Mandrake Linux Security Advisory : tightvnc (MDKSA-2007:080-1)

Mandrake Linux Security Advisory : timed (MDKSA-2001:034)

Mandrake Linux Security Advisory : tk (MDKSA-2007:200)

Mandrake Linux Security Advisory : tkcvs (MDKSA-2006:001)

Mandrake Linux Security Advisory : tmpwatch (MDKSA-2000:056)

Mandrake Linux Security Advisory : tomcat5 (MDKSA-2007:241)

Mandrake Linux Security Advisory : traceroute (MDKSA-2000:053)

Mandrake Linux Security Advisory : tripwire (MDKSA-2001:064)

Mandrake Linux Security Advisory : tripwire (MDKSA-2004:057-1)

Mandrake Linux Security Advisory : ucd-snmp (MDKSA-2002:014)

Mandrake Linux Security Advisory : ucd-snmp (MDKSA-2005:137)

Mandrake Linux Security Advisory : uim (MDKSA-2005:046)

Mandrake Linux Security Advisory : uim (MDKSA-2005:198)

Mandrake Linux Security Advisory : unzip (MDKSA-2002:065)

Mandrake Linux Security Advisory : unzip (MDKSA-2003:073-1)

Mandrake Linux Security Advisory : unzip (MDKSA-2005:197)

Mandrake Linux Security Advisory : unzip (MDKSA-2006:050)

Mandrake Linux Security Advisory : usermode (MDKSA-2000:020)

Mandrake Linux Security Advisory : usermode (MDKSA-2003:031-1)

Mandrake Linux Security Advisory : utempter (MDKSA-2004:031-1)

Mandrake Linux Security Advisory : util-linux (MDKSA-2001:084)

Mandrake Linux Security Advisory : util-linux (MDKSA-2002:047)

Mandrake Linux Security Advisory : util-linux (MDKSA-2003:016)

Mandrake Linux Security Advisory : util-linux (MDKSA-2005:167)

Mandrake Linux Security Advisory : util-linux (MDKSA-2007:053)

Mandrake Linux Security Advisory : util-linux (MDKSA-2007:111)

Mandrake Linux Security Advisory : util-linux (MDKSA-2007:198)

Mandrake Linux Security Advisory : uucp (MDKSA-2001:078)

Mandrake Linux Security Advisory : vim (MDKSA-2001:035)

Mandrake Linux Security Advisory : vim (MDKSA-2003:012)

Mandrake Linux Security Advisory : vim (MDKSA-2005:003)

Mandrake Linux Security Advisory : vim (MDKSA-2005:029)

Mandrake Linux Security Advisory : vim (MDKSA-2005:148)

Mandrake Linux Security Advisory : vim (MDKSA-2007:101)

Mandrake Linux Security Advisory : vim (MDKSA-2007:168)

Mandrake Linux Security Advisory : vixie-cron (MDKSA-2001:022)

Mandrake Linux Security Advisory : vixie-cron (MDKSA-2001:050)

Mandrake Linux Security Advisory : vixie-cron (MDKSA-2007:234)

Mandrake Linux Security Advisory : vnc (MDKSA-2003:022)

Mandrake Linux Security Advisory : w3c-libwww (MDKSA-2005:210)

Mandrake Linux Security Advisory : webmin (MDKSA-2001:016)

Mandrake Linux Security Advisory : webmin (MDKSA-2001:059)

Mandrake Linux Security Advisory : webmin (MDKSA-2002:033)

Mandrake Linux Security Advisory : webmin (MDKSA-2003:025)

Mandrake Linux Security Advisory : webmin (MDKSA-2004:074)

Mandrake Linux Security Advisory : webmin (MDKSA-2004:101)

Mandrake Linux Security Advisory : webmin (MDKSA-2005:176)

Mandrake Linux Security Advisory : webmin (MDKSA-2005:223)

Mandrake Linux Security Advisory : webmin (MDKSA-2006:125)

Mandrake Linux Security Advisory : webmin (MDKSA-2006:170-1)

Mandrake Linux Security Advisory : webmin (MDKSA-2007:135)

Mandrake Linux Security Advisory : wget (MDKSA-2002:086)

Mandrake Linux Security Advisory : wget (MDKSA-2005:098)

Mandrake Linux Security Advisory : wget (MDKSA-2005:183)

Mandrake Linux Security Advisory : wget (MDKSA-2005:204)

Mandrake Linux Security Advisory : wget (MDKSA-2007:017)

Mandrake Linux Security Advisory : WindowMaker (MDKSA-2001:074)

Mandrake Linux Security Advisory : WindowMaker (MDKSA-2002:085)

Mandrake Linux Security Advisory : wine (MDKSA-2006:014)

Mandrake Linux Security Advisory : wireshark (MDKSA-2006:128)

Mandrake Linux Security Advisory : wireshark (MDKSA-2006:152)

Mandrake Linux Security Advisory : wireshark (MDKSA-2006:195)

Mandrake Linux Security Advisory : wireshark (MDKSA-2007:033)

Mandrake Linux Security Advisory : wireshark (MDKSA-2007:145)

Mandrake Linux Security Advisory : wpa\_supplicant (MDKSA-2007:245)

Mandrake Linux Security Advisory : wu-ftpd (MDKSA-2000:014)

Mandrake Linux Security Advisory : wu-ftpd (MDKSA-2001:001-2)

Mandrake Linux Security Advisory : wu-ftpd (MDKSA-2001:090)

Mandrake Linux Security Advisory : wu-ftpd (MDKSA-2003:080)

Mandrake Linux Security Advisory : wv (MDKSA-2004:077)

Mandrake Linux Security Advisory : wv (MDKSA-2006:202)

Mandrake Linux Security Advisory : wv2 (MDKSA-2006:109)

Mandrake Linux Security Advisory : wxGTK2 (MDKSA-2004:111)

Mandrake Linux Security Advisory : wxGTK2 (MDKSA-2005:002)

Mandrake Linux Security Advisory : wxPythonGTK (MDKSA-2005:144)

Mandrake Linux Security Advisory : x11-server (MDKSA-2007:178)

Mandrake Linux Security Advisory : xchat (MDKSA-2000:039-1)

Mandrake Linux Security Advisory : xchat (MDKSA-2002:006)

Mandrake Linux Security Advisory : xchat (MDKSA-2002:051)

Mandrake Linux Security Advisory : xchat (MDKSA-2004:036)

Mandrake Linux Security Advisory : xemacs (MDKSA-2000:006)

Mandrake Linux Security Advisory : xemacs (MDKSA-2001:019)

Mandrake Linux Security Advisory : xen (MDKSA-2007:203)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2003:089)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2003:118)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2004:012)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2004:073)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2004:099)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2004:138)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2005:081)

Mandrake Linux Security Advisory : XFree86 (MDKSA-2005:164)

Mandrake Linux Security Advisory : xfs (MDKSA-2007:210)

Mandrake Linux Security Advisory : xfsdump (MDKSA-2003:047)

Mandrake Linux Security Advisory : xfsdump (MDKSA-2007:134)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2004:105)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2005:011)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2005:094)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2005:180)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2005:228)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2006:108)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2006:121)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2006:176)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2006:224)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2007:057)

Mandrake Linux Security Advisory : xine-lib (MDKSA-2007:062)

Mandrake Linux Security Advisory : xine-ui (MDKSA-2004:033)

Mandrake Linux Security Advisory : xine-ui (MDKSA-2006:085)

Mandrake Linux Security Advisory : xine-ui (MDKSA-2007:027)

Mandrake Linux Security Advisory : xine-ui (MDKSA-2007:154)

Mandrake Linux Security Advisory : xinetd (MDKSA-2001:055-1)

Mandrake Linux Security Advisory : xinetd (MDKSA-2001:076)

Mandrake Linux Security Advisory : xinetd (MDKSA-2002:053)

Mandrake Linux Security Advisory : xinetd (MDKSA-2003:056)

Mandrake Linux Security Advisory : xinitrc (MDKSA-2000:052)

Mandrake Linux Security Advisory : xli (MDKSA-2005:076)

Mandrake Linux Security Advisory : xli (MDKSA-2005:192)

Mandrake Linux Security Advisory : xloadimage (MDKSA-2001:073-1)

Mandrake Linux Security Advisory : xlockmore (MDKSA-2000:011)

Mandrake Linux Security Advisory : xlockmore (MDKSA-2000:038)

Mandrake Linux Security Advisory : xmovie (MDKSA-2005:229)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2004:124)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2006:056)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2006:081-1)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2006:148)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2006:160)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2006:164-1)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2007:005)

Mandrake Linux Security Advisory : xorg-x11 (MDKSA-2007:079-1)

Mandrake Linux Security Advisory : xpcd (MDKSA-2004:053)

Mandrake Linux Security Advisory : xpdf (MDKSA-2000:041-1)

Mandrake Linux Security Advisory : xpdf (MDKSA-2003:002)

Mandrake Linux Security Advisory : xpdf (MDKSA-2003:071-1)

Mandrake Linux Security Advisory : xpdf (MDKSA-2004:113)

Mandrake Linux Security Advisory : xpdf (MDKSA-2004:161)

Mandrake Linux Security Advisory : xpdf (MDKSA-2005:017)

Mandrake Linux Security Advisory : xpdf (MDKSA-2005:043)

Mandrake Linux Security Advisory : xpdf (MDKSA-2005:134)

Mandrake Linux Security Advisory : xpdf (MDKSA-2006:032)

Mandrake Linux Security Advisory : xpdf (MDKSA-2007:021)

Mandrake Linux Security Advisory : xpdf (MDKSA-2007:158)

Mandrake Linux Security Advisory : xpdf (MDKSA-2007:219)

Mandrake Linux Security Advisory : xpm (MDKSA-2005:080)

Mandrake Linux Security Advisory : xscreensaver (MDKSA-2007:097)

Mandrake Linux Security Advisory : xsoldier (MDKSA-2000:004)

Mandrake Linux Security Advisory : xsupplicant (MDKSA-2006:189)

Mandrake Linux Security Advisory : ypserv (MDKSA-2000:064)

Mandrake Linux Security Advisory : ypserv (MDKSA-2002:078)

Mandrake Linux Security Advisory : ypserv (MDKSA-2003:072)

Mandrake Linux Security Advisory : zhcon (MDKSA-2005:012)

Mandrake Linux Security Advisory : zip (MDKSA-2004:141)

Mandrake Linux Security Advisory : zlib (MDKSA-2002:022)

Mandrake Linux Security Advisory : zlib (MDKSA-2003:033)

Mandrake Linux Security Advisory : zlib (MDKSA-2004:090)

Mandrake Linux Security Advisory : zlib (MDKSA-2005:112)

Mandrake Linux Security Advisory : zlib (MDKSA-2005:124)

Mandrake Linux Security Advisory : zlib-pkgs (MDKSA-2002:023-1)

Mandrake Linux Security Advisory : Zope (MDKSA-2000:026)

Mandrake Linux Security Advisory : Zope (MDKSA-2000:035)

Mandrake Linux Security Advisory : Zope (MDKSA-2000:043)

Mandrake Linux Security Advisory : Zope (MDKSA-2000:083)

Mandrake Linux Security Advisory : Zope (MDKSA-2000:086)

Mandrake Linux Security Advisory : Zope (MDKSA-2001:025)

Mandrake Linux Security Advisory : Zope (MDKSA-2001:049)

Mandrake Linux Security Advisory : Zope (MDKSA-2001:080)

Mandriva Linux Security Advisory : a2ps (MDVSA-2014:076)

Mandriva Linux Security Advisory : accountsservice (MDVSA-2013:060)

Mandriva Linux Security Advisory : acl (MDVSA-2009:345)

Mandriva Linux Security Advisory : acpid (MDVSA-2009:107-1)

Mandriva Linux Security Advisory : acpid (MDVSA-2009:343)

Mandriva Linux Security Advisory : acpid (MDVSA-2012:086)

Mandriva Linux Security Advisory : acpid (MDVSA-2012:137)

Mandriva Linux Security Advisory : aircrack-ng (MDVSA-2013:251)

Mandriva Linux Security Advisory : aircrack-ng (MDVSA-2015:028)

Mandriva Linux Security Advisory : amarok (MDVSA-2008:172)

Mandriva Linux Security Advisory : amarok (MDVSA-2009:030-1)

Mandriva Linux Security Advisory : apache (MDVSA-2008:016)

Mandriva Linux Security Advisory : apache (MDVSA-2008:195)

Mandriva Linux Security Advisory : apache (MDVSA-2009:102)

Mandriva Linux Security Advisory : apache (MDVSA-2009:124-1)

Mandriva Linux Security Advisory : apache (MDVSA-2009:149)

Mandriva Linux Security Advisory : apache (MDVSA-2009:240)

Mandriva Linux Security Advisory : apache (MDVSA-2009:295)

Mandriva Linux Security Advisory : apache (MDVSA-2009:323)

Mandriva Linux Security Advisory : apache (MDVSA-2010:053)

Mandriva Linux Security Advisory : apache (MDVSA-2010:057)

Mandriva Linux Security Advisory : apache (MDVSA-2010:152)

Mandriva Linux Security Advisory : apache (MDVSA-2010:153)

Mandriva Linux Security Advisory : apache (MDVSA-2011:057)

Mandriva Linux Security Advisory : apache (MDVSA-2011:130-1)

Mandriva Linux Security Advisory : apache (MDVSA-2011:144)

Mandriva Linux Security Advisory : apache (MDVSA-2011:168)

Mandriva Linux Security Advisory : apache (MDVSA-2012:003)

Mandriva Linux Security Advisory : apache (MDVSA-2012:012)

Mandriva Linux Security Advisory : apache (MDVSA-2012:154-1)

Mandriva Linux Security Advisory : apache (MDVSA-2013:015-1)

Mandriva Linux Security Advisory : apache (MDVSA-2013:174)

Mandriva Linux Security Advisory : apache (MDVSA-2013:193)

Mandriva Linux Security Advisory : apache (MDVSA-2014:065)

Mandriva Linux Security Advisory : apache (MDVSA-2014:142)

Mandriva Linux Security Advisory : apache (MDVSA-2014:174)

Mandriva Linux Security Advisory : apache (MDVSA-2015:093)

Mandriva Linux Security Advisory : apache-commons-fileupload (MDVSA-2014:056)

Mandriva Linux Security Advisory : apache-conf (MDVSA-2009:300-2)

Mandriva Linux Security Advisory : apache-mod\_auth\_mysql (MDVSA-2009:189-1)

Mandriva Linux Security Advisory : apache-mod\_auth\_shadow (MDVSA-2010:081)

Mandriva Linux Security Advisory : apache-mod\_fcgid (MDVSA-2013:256)

Mandriva Linux Security Advisory : apache-mod\_security (MDVSA-2012:182)

Mandriva Linux Security Advisory : apache-mod\_security (MDVSA-2013:029)

Mandriva Linux Security Advisory : apache-mod\_security (MDVSA-2013:156)

Mandriva Linux Security Advisory : apache-mod\_security (MDVSA-2013:187)

Mandriva Linux Security Advisory : apache-mod\_security (MDVSA-2014:081)

Mandriva Linux Security Advisory : apache-mod\_security (MDVSA-2015:106)

Mandriva Linux Security Advisory : apache-mod\_wsgi (MDVSA-2014:137)

Mandriva Linux Security Advisory : apache-mod\_wsgi (MDVSA-2014:253)

Mandriva Linux Security Advisory : apache-mod\_wsgi (MDVSA-2015:180)

Mandriva Linux Security Advisory : apr (MDVSA-2009:195)

Mandriva Linux Security Advisory : apr (MDVSA-2009:314)

Mandriva Linux Security Advisory : apr (MDVSA-2011:084)

Mandriva Linux Security Advisory : apr (MDVSA-2011:095-1)

Mandriva Linux Security Advisory : apr (MDVSA-2012:019)

Mandriva Linux Security Advisory : apr-util (MDVSA-2009:131)

Mandriva Linux Security Advisory : apr-util (MDVSA-2010:192)

Mandriva Linux Security Advisory : argyllcms (MDVSA-2013:090)

Mandriva Linux Security Advisory : aria2 (MDVSA-2009:226)

Mandriva Linux Security Advisory : aria2 (MDVSA-2010:106)

Mandriva Linux Security Advisory : arj (MDVSA-2015:201)

Mandriva Linux Security Advisory : arpwatch (MDVSA-2012:113)

Mandriva Linux Security Advisory : arpwatch (MDVSA-2013:030)

Mandriva Linux Security Advisory : asterisk (MDVSA-2013:140)

Mandriva Linux Security Advisory : asterisk (MDVSA-2013:223)

Mandriva Linux Security Advisory : asterisk (MDVSA-2013:300)

Mandriva Linux Security Advisory : asterisk (MDVSA-2014:078)

Mandriva Linux Security Advisory : asterisk (MDVSA-2014:138)

Mandriva Linux Security Advisory : asterisk (MDVSA-2014:218)

Mandriva Linux Security Advisory : asterisk (MDVSA-2015:018)

Mandriva Linux Security Advisory : asterisk (MDVSA-2015:206)

Mandriva Linux Security Advisory : audacity (MDVSA-2008:074)

Mandriva Linux Security Advisory : audacity (MDVSA-2009:055)

Mandriva Linux Security Advisory : audacity (MDVSA-2009:215-1)

Mandriva Linux Security Advisory : audit (MDVSA-2008:083)

Mandriva Linux Security Advisory : augeas (MDVSA-2014:022)

Mandriva Linux Security Advisory : autofs (MDVSA-2008:009-1)

Mandriva Linux Security Advisory : automake (MDVSA-2010:203)

Mandriva Linux Security Advisory : automake (MDVSA-2012:103)

Mandriva Linux Security Advisory : automake (MDVSA-2013:031)

Mandriva Linux Security Advisory : autotrace (MDVSA-2013:190)

Mandriva Linux Security Advisory : avahi (MDVSA-2009:031)

Mandriva Linux Security Advisory : avahi (MDVSA-2009:076)

Mandriva Linux Security Advisory : avahi (MDVSA-2010:204)

Mandriva Linux Security Advisory : avahi (MDVSA-2011:037)

Mandriva Linux Security Advisory : awstats (MDVSA-2013:061)

Mandriva Linux Security Advisory : backuppc (MDVSA-2013:062)

Mandriva Linux Security Advisory : banshee (MDVSA-2011:034)

Mandriva Linux Security Advisory : bash (MDVSA-2010:004)

Mandriva Linux Security Advisory : bash (MDVSA-2012:128)

Mandriva Linux Security Advisory : bash (MDVSA-2013:032)

Mandriva Linux Security Advisory : bash (MDVSA-2014:186)

Mandriva Linux Security Advisory : bash (MDVSA-2014:190)

Mandriva Linux Security Advisory : bash (MDVSA-2015:164)

Mandriva Linux Security Advisory : batik (MDVSA-2015:203)

Mandriva Linux Security Advisory : bind (MDVSA-2008:139)

Mandriva Linux Security Advisory : bind (MDVSA-2009:002)

Mandriva Linux Security Advisory : bind (MDVSA-2009:037)

Mandriva Linux Security Advisory : bind (MDVSA-2009:181)

Mandriva Linux Security Advisory : bind (MDVSA-2009:313-1)

Mandriva Linux Security Advisory : bind (MDVSA-2010:021)

Mandriva Linux Security Advisory : bind (MDVSA-2010:253)

Mandriva Linux Security Advisory : bind (MDVSA-2011:104)

Mandriva Linux Security Advisory : bind (MDVSA-2011:115)

Mandriva Linux Security Advisory : bind (MDVSA-2011:176-2)

Mandriva Linux Security Advisory : bind (MDVSA-2012:089)

Mandriva Linux Security Advisory : bind (MDVSA-2012:119)

Mandriva Linux Security Advisory : bind (MDVSA-2012:152-1)

Mandriva Linux Security Advisory : bind (MDVSA-2012:162)

Mandriva Linux Security Advisory : bind (MDVSA-2012:177)

Mandriva Linux Security Advisory : bind (MDVSA-2013:058)

Mandriva Linux Security Advisory : bind (MDVSA-2013:202)

Mandriva Linux Security Advisory : bind (MDVSA-2014:002)

Mandriva Linux Security Advisory : bind (MDVSA-2014:238)

Mandriva Linux Security Advisory : bind (MDVSA-2015:054)

Mandriva Linux Security Advisory : bind (MDVSA-2015:165)

Mandriva Linux Security Advisory : binutils (MDVSA-2015:029-1)

Mandriva Linux Security Advisory : bip (MDVSA-2013:063)

Mandriva Linux Security Advisory : blender (MDVSA-2008:204)

Mandriva Linux Security Advisory : blender (MDVSA-2009:038-1)

Mandriva Linux Security Advisory : blender (MDVSA-2011:112)

Mandriva Linux Security Advisory : blender (MDVSA-2011:114)

Mandriva Linux Security Advisory : bluez (MDVSA-2008:145)

Mandriva Linux Security Advisory : bogofilter (MDVSA-2013:064)

Mandriva Linux Security Advisory : boost (MDVSA-2008:032)

Mandriva Linux Security Advisory : boost (MDVSA-2013:065)

Mandriva Linux Security Advisory : brltty (MDVSA-2010:080)

Mandriva Linux Security Advisory : bugzilla (MDVSA-2013:066)

Mandriva Linux Security Advisory : bugzilla (MDVSA-2013:285)

Mandriva Linux Security Advisory : bugzilla (MDVSA-2014:169)

Mandriva Linux Security Advisory : bugzilla (MDVSA-2014:200)

Mandriva Linux Security Advisory : bugzilla (MDVSA-2015:030)

Mandriva Linux Security Advisory : busybox (MDVSA-2012:129-1)

Mandriva Linux Security Advisory : busybox (MDVSA-2014:173)

Mandriva Linux Security Advisory : busybox (MDVSA-2015:031)

Mandriva Linux Security Advisory : bzip2 (MDVSA-2008:075)

Mandriva Linux Security Advisory : bzip2 (MDVSA-2010:185)

Mandriva Linux Security Advisory : bzr (MDVSA-2013:229)

Mandriva Linux Security Advisory : c-icap (MDVSA-2015:001)

Mandriva Linux Security Advisory : cabextract (MDVSA-2010:154)

Mandriva Linux Security Advisory : cabextract (MDVSA-2015:041)

Mandriva Linux Security Advisory : cabextract (MDVSA-2015:064)

Mandriva Linux Security Advisory : cairo (MDVSA-2008:019)

Mandriva Linux Security Advisory : catfish (MDVSA-2014:162)

Mandriva Linux Security Advisory : cherokee (MDVSA-2015:225)

Mandriva Linux Security Advisory : chkrootkit (MDVSA-2014:122)

Mandriva Linux Security Advisory : cifs-utils (MDVSA-2012:069)

Mandriva Linux Security Advisory : cifs-utils (MDVSA-2015:114)

Mandriva Linux Security Advisory : clamav (MDVSA-2008:003)

Mandriva Linux Security Advisory : clamav (MDVSA-2008:088)

Mandriva Linux Security Advisory : clamav (MDVSA-2008:122)

Mandriva Linux Security Advisory : clamav (MDVSA-2008:166)

Mandriva Linux Security Advisory : clamav (MDVSA-2008:189-1)

Mandriva Linux Security Advisory : clamav (MDVSA-2008:229)

Mandriva Linux Security Advisory : clamav (MDVSA-2008:239)

Mandriva Linux Security Advisory : clamav (MDVSA-2009:097)

Mandriva Linux Security Advisory : clamav (MDVSA-2009:327)

Mandriva Linux Security Advisory : clamav (MDVSA-2010:082-1)

Mandriva Linux Security Advisory : clamav (MDVSA-2010:110)

Mandriva Linux Security Advisory : clamav (MDVSA-2010:249)

Mandriva Linux Security Advisory : clamav (MDVSA-2011:122)

Mandriva Linux Security Advisory : clamav (MDVSA-2013:027-1)

Mandriva Linux Security Advisory : clamav (MDVSA-2013:159)

Mandriva Linux Security Advisory : clamav (MDVSA-2014:217)

Mandriva Linux Security Advisory : clamav (MDVSA-2015:042)

Mandriva Linux Security Advisory : clamav (MDVSA-2015:166)

Mandriva Linux Security Advisory : clamav (MDVSA-2015:221)

Mandriva Linux Security Advisory : clutter (MDVSA-2013:255)

Mandriva Linux Security Advisory : compiz-fusion-plugins-main (MDVSA-2009:278)

Mandriva Linux Security Advisory : coreutils (MDVSA-2010:024)

Mandriva Linux Security Advisory : coreutils (MDVSA-2013:023-1)

Mandriva Linux Security Advisory : coreutils (MDVSA-2015:179)

Mandriva Linux Security Advisory : couchdb (MDVSA-2013:067)

Mandriva Linux Security Advisory : couchdb (MDVSA-2014:093)

Mandriva Linux Security Advisory : courier-authlib (MDVSA-2013:068)

Mandriva Linux Security Advisory : cpio (MDVSA-2010:065)

Mandriva Linux Security Advisory : cpio (MDVSA-2014:250)

Mandriva Linux Security Advisory : cpio (MDVSA-2015:065)

Mandriva Linux Security Advisory : cpio (MDVSA-2015:066)

Mandriva Linux Security Advisory : cronie (MDVSA-2013:033)

Mandriva Linux Security Advisory : ctags (MDVSA-2014:206)

Mandriva Linux Security Advisory : ctags (MDVSA-2015:178)

Mandriva Linux Security Advisory : ctdb (MDVSA-2015:177)

Mandriva Linux Security Advisory : cups (MDVSA-2008:036)

Mandriva Linux Security Advisory : cups (MDVSA-2008:051)

Mandriva Linux Security Advisory : cups (MDVSA-2008:081)

Mandriva Linux Security Advisory : cups (MDVSA-2008:170)

Mandriva Linux Security Advisory : cups (MDVSA-2008:211)

Mandriva Linux Security Advisory : cups (MDVSA-2009:027)

Mandriva Linux Security Advisory : cups (MDVSA-2009:028)

Mandriva Linux Security Advisory : cups (MDVSA-2009:280)

Mandriva Linux Security Advisory : cups (MDVSA-2009:282-1)

Mandriva Linux Security Advisory : cups (MDVSA-2010:073-1)

Mandriva Linux Security Advisory : cups (MDVSA-2010:232)

Mandriva Linux Security Advisory : cups (MDVSA-2010:233)

Mandriva Linux Security Advisory : cups (MDVSA-2011:146)

Mandriva Linux Security Advisory : cups (MDVSA-2011:147)

Mandriva Linux Security Advisory : cups (MDVSA-2012:179)

Mandriva Linux Security Advisory : cups (MDVSA-2013:034)

Mandriva Linux Security Advisory : cups (MDVSA-2014:015)

Mandriva Linux Security Advisory : cups (MDVSA-2014:091)

Mandriva Linux Security Advisory : cups (MDVSA-2014:151)

Mandriva Linux Security Advisory : cups (MDVSA-2015:049)

Mandriva Linux Security Advisory : cups (MDVSA-2015:108)

Mandriva Linux Security Advisory : cups-filters (MDVSA-2015:100)

Mandriva Linux Security Advisory : cups-filters (MDVSA-2015:196)

Mandriva Linux Security Advisory : cups-pk-helper (MDVSA-2013:069)

Mandriva Linux Security Advisory : curl (MDVSA-2009:069)

Mandriva Linux Security Advisory : curl (MDVSA-2009:203-1)

Mandriva Linux Security Advisory : curl (MDVSA-2010:062)

Mandriva Linux Security Advisory : curl (MDVSA-2011:116)

Mandriva Linux Security Advisory : curl (MDVSA-2012:058)

Mandriva Linux Security Advisory : curl (MDVSA-2013:151)

Mandriva Linux Security Advisory : curl (MDVSA-2013:180)

Mandriva Linux Security Advisory : curl (MDVSA-2013:276)

Mandriva Linux Security Advisory : curl (MDVSA-2014:110)

Mandriva Linux Security Advisory : curl (MDVSA-2014:187)

Mandriva Linux Security Advisory : curl (MDVSA-2014:213)

Mandriva Linux Security Advisory : curl (MDVSA-2015:021)

Mandriva Linux Security Advisory : curl (MDVSA-2015:098)

Mandriva Linux Security Advisory : curl (MDVSA-2015:219)

Mandriva Linux Security Advisory : curl (MDVSA-2015:220)

Mandriva Linux Security Advisory : cvs (MDVSA-2012:044)

Mandriva Linux Security Advisory : cyrus-imapd (MDVSA-2009:229-1)

Mandriva Linux Security Advisory : cyrus-imapd (MDVSA-2011:100)

Mandriva Linux Security Advisory : cyrus-imapd (MDVSA-2011:149)

Mandriva Linux Security Advisory : cyrus-imapd (MDVSA-2012:037)

Mandriva Linux Security Advisory : cyrus-sasl (MDVSA-2009:113-1)

Mandriva Linux Security Advisory : davfs (MDVSA-2009:220-1)

Mandriva Linux Security Advisory : davfs2 (MDVSA-2013:244)

Mandriva Linux Security Advisory : dbus (MDVSA-2008:054)

Mandriva Linux Security Advisory : dbus (MDVSA-2008:213)

Mandriva Linux Security Advisory : dbus (MDVSA-2009:256-1)

Mandriva Linux Security Advisory : dbus (MDVSA-2013:070)

Mandriva Linux Security Advisory : dbus (MDVSA-2013:177)

Mandriva Linux Security Advisory : dbus (MDVSA-2014:148)

Mandriva Linux Security Advisory : dbus (MDVSA-2014:214)

Mandriva Linux Security Advisory : dbus (MDVSA-2015:176)

Mandriva Linux Security Advisory : dbus-glib (MDVSA-2013:071)

Mandriva Linux Security Advisory : dhcp (MDVSA-2009:151)

Mandriva Linux Security Advisory : dhcp (MDVSA-2009:153)

Mandriva Linux Security Advisory : dhcp (MDVSA-2009:154)

Mandriva Linux Security Advisory : dhcp (MDVSA-2009:312)

Mandriva Linux Security Advisory : dhcp (MDVSA-2010:114)

Mandriva Linux Security Advisory : dhcp (MDVSA-2010:226)

Mandriva Linux Security Advisory : dhcp (MDVSA-2011:001)

Mandriva Linux Security Advisory : dhcp (MDVSA-2011:022)

Mandriva Linux Security Advisory : dhcp (MDVSA-2011:073)

Mandriva Linux Security Advisory : dhcp (MDVSA-2011:128)

Mandriva Linux Security Advisory : dhcp (MDVSA-2011:182)

Mandriva Linux Security Advisory : dhcp (MDVSA-2012:115)

Mandriva Linux Security Advisory : dhcp (MDVSA-2012:153-1)

Mandriva Linux Security Advisory : dhcp (MDVSA-2013:059)

Mandriva Linux Security Advisory : dhcpcd (MDVSA-2014:171)

Mandriva Linux Security Advisory : dia (MDVSA-2009:040)

Mandriva Linux Security Advisory : dia (MDVSA-2009:046-1)

Mandriva Linux Security Advisory : directfb (MDVSA-2015:223)

Mandriva Linux Security Advisory : dnsmasq (MDVSA-2013:072)

Mandriva Linux Security Advisory : dokuwiki (MDVSA-2013:073)

Mandriva Linux Security Advisory : dokuwiki (MDVSA-2015:185)

Mandriva Linux Security Advisory : dovecot (MDVSA-2008:232)

Mandriva Linux Security Advisory : dovecot (MDVSA-2009:242)

Mandriva Linux Security Advisory : dovecot (MDVSA-2009:306)

Mandriva Linux Security Advisory : dovecot (MDVSA-2010:104)

Mandriva Linux Security Advisory : dovecot (MDVSA-2010:196)

Mandriva Linux Security Advisory : dovecot (MDVSA-2010:217)

Mandriva Linux Security Advisory : dovecot (MDVSA-2011:101)

Mandriva Linux Security Advisory : dovecot (MDVSA-2014:099)

Mandriva Linux Security Advisory : dovecot (MDVSA-2015:113)

Mandriva Linux Security Advisory : dropbear (MDVSA-2013:261)

Mandriva Linux Security Advisory : drupal (MDVSA-2013:074)

Mandriva Linux Security Advisory : drupal (MDVSA-2013:287-1)

Mandriva Linux Security Advisory : drupal (MDVSA-2014:031)

Mandriva Linux Security Advisory : drupal (MDVSA-2015:181)

Mandriva Linux Security Advisory : dump (MDVSA-2014:181)

Mandriva Linux Security Advisory : e2fsprogs (MDVSA-2015:045)

Mandriva Linux Security Advisory : e2fsprogs (MDVSA-2015:067)

Mandriva Linux Security Advisory : e2fsprogs (MDVSA-2015:068)

Mandriva Linux Security Advisory : eclipse (MDVSA-2011:032)

Mandriva Linux Security Advisory : ed (MDVSA-2008:200)

Mandriva Linux Security Advisory : eggdrop (MDVSA-2009:126-1)

Mandriva Linux Security Advisory : egroupware (MDVSA-2014:104)

Mandriva Linux Security Advisory : egroupware (MDVSA-2015:087)

Mandriva Linux Security Advisory : ejabberd (MDVSA-2014:005)

Mandriva Linux Security Advisory : ejabberd (MDVSA-2014:207)

Mandriva Linux Security Advisory : ejabberd (MDVSA-2015:175)

Mandriva Linux Security Advisory : elfutils (MDVSA-2015:047)

Mandriva Linux Security Advisory : elfutils (MDVSA-2015:104)

Mandriva Linux Security Advisory : elinks (MDVSA-2013:075)

Mandriva Linux Security Advisory : elinks (MDVSA-2014:019)

Mandriva Linux Security Advisory : emacs (MDVSA-2008:034)

Mandriva Linux Security Advisory : emacs (MDVSA-2008:096)

Mandriva Linux Security Advisory : emacs (MDVSA-2008:153)

Mandriva Linux Security Advisory : emacs (MDVSA-2008:216)

Mandriva Linux Security Advisory : emacs (MDVSA-2010:083)

Mandriva Linux Security Advisory : emacs (MDVSA-2013:076)

Mandriva Linux Security Advisory : emacs (MDVSA-2014:118)

Mandriva Linux Security Advisory : emacs (MDVSA-2015:117)

Mandriva Linux Security Advisory : enscript (MDVSA-2008:243)

Mandriva Linux Security Advisory : eog (MDVSA-2009:063)

Mandriva Linux Security Advisory : epiphany (MDVSA-2009:048-2)

Mandriva Linux Security Advisory : erlang (MDVSA-2015:174)

Mandriva Linux Security Advisory : ettercap (MDVSA-2013:077)

Mandriva Linux Security Advisory : evince (MDVSA-2011:005)

Mandriva Linux Security Advisory : evolution (MDVSA-2008:063)

Mandriva Linux Security Advisory : evolution (MDVSA-2008:111)

Mandriva Linux Security Advisory : evolution-data-server (MDVSA-2009:078)

Mandriva Linux Security Advisory : exif (MDVSA-2012:107)

Mandriva Linux Security Advisory : exif (MDVSA-2013:036)

Mandriva Linux Security Advisory : exiv2 (MDVSA-2008:006)

Mandriva Linux Security Advisory : exiv2 (MDVSA-2008:119)

Mandriva Linux Security Advisory : expat (MDVSA-2009:211-1)

Mandriva Linux Security Advisory : expat (MDVSA-2009:316-3)

Mandriva Linux Security Advisory : expat (MDVSA-2012:041)

Mandriva Linux Security Advisory : fail2ban (MDVSA-2013:078)

Mandriva Linux Security Advisory : fail2ban (MDVSA-2013:191)

Mandriva Linux Security Advisory : fastjar (MDVSA-2010:122)

Mandriva Linux Security Advisory : fcgi (MDVSA-2012:001)

Mandriva Linux Security Advisory : fcgi (MDVSA-2015:226)

Mandriva Linux Security Advisory : fetchmail (MDVSA-2008:117)

Mandriva Linux Security Advisory : fetchmail (MDVSA-2009:201-1)

Mandriva Linux Security Advisory : fetchmail (MDVSA-2010:037)

Mandriva Linux Security Advisory : fetchmail (MDVSA-2011:107)

Mandriva Linux Security Advisory : fetchmail (MDVSA-2012:149)

Mandriva Linux Security Advisory : fetchmail (MDVSA-2013:037)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2008:157)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2009:015)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2009:297-1)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2009:335)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2011:060)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2011:061)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2011:062)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2012:075)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2012:076)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2012:148)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2013:079)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2014:037)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2014:129)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2014:227)

Mandriva Linux Security Advisory : ffmpeg (MDVSA-2015:173)

Mandriva Linux Security Advisory : file (MDVSA-2009:129)

Mandriva Linux Security Advisory : file (MDVSA-2012:035)

Mandriva Linux Security Advisory : file (MDVSA-2014:051)

Mandriva Linux Security Advisory : file (MDVSA-2014:073)

Mandriva Linux Security Advisory : file (MDVSA-2014:116)

Mandriva Linux Security Advisory : file (MDVSA-2014:131)

Mandriva Linux Security Advisory : file (MDVSA-2014:146)

Mandriva Linux Security Advisory : file (MDVSA-2014:167)

Mandriva Linux Security Advisory : file (MDVSA-2014:236)

Mandriva Linux Security Advisory : file (MDVSA-2015:010)

Mandriva Linux Security Advisory : firebird (MDVSA-2015:172)

Mandriva Linux Security Advisory : firefox (MDVSA-2008:230)

Mandriva Linux Security Advisory : firefox (MDVSA-2008:245)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:044)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:075)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:084)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:111-1)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:134)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:182)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:198)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:236)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:290-1)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:294)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:338)

Mandriva Linux Security Advisory : firefox (MDVSA-2009:339)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:000)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:042)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:070-1)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:125)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:147)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:173)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:210)

Mandriva Linux Security Advisory : firefox (MDVSA-2010:251-2)

Mandriva Linux Security Advisory : firefox (MDVSA-2011:041)

Mandriva Linux Security Advisory : firefox (MDVSA-2011:068)

Mandriva Linux Security Advisory : firefox (MDVSA-2011:079)

Mandriva Linux Security Advisory : firefox (MDVSA-2011:139)

Mandriva Linux Security Advisory : firefox (MDVSA-2011:141)

Mandriva Linux Security Advisory : firefox (MDVSA-2012:017)

Mandriva Linux Security Advisory : firefox (MDVSA-2012:145)

Mandriva Linux Security Advisory : flac (MDVSA-2014:239)

Mandriva Linux Security Advisory : flac (MDVSA-2015:188)

Mandriva Linux Security Advisory : flite (MDVSA-2014:032)

Mandriva Linux Security Advisory : foomatic-filters (MDVSA-2011:125)

Mandriva Linux Security Advisory : freeciv (MDVSA-2010:205)

Mandriva Linux Security Advisory : freeradius (MDVSA-2009:227-1)

Mandriva Linux Security Advisory : freeradius (MDVSA-2012:047)

Mandriva Linux Security Advisory : freeradius (MDVSA-2012:159)

Mandriva Linux Security Advisory : freeradius (MDVSA-2013:038)

Mandriva Linux Security Advisory : freeradius (MDVSA-2014:058)

Mandriva Linux Security Advisory : freerdp (MDVSA-2015:171)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2008:121)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2009:243-2)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2010:137)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2010:149)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2010:156)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2010:157)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2010:201)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2010:236)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2011:120)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2011:157)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2011:177)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2012:057)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2013:006)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2013:039)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2015:055)

Mandriva Linux Security Advisory : freetype2 (MDVSA-2015:089)

Mandriva Linux Security Advisory : fuse (MDVSA-2010:047)

Mandriva Linux Security Advisory : ganglia (MDVSA-2013:080)

Mandriva Linux Security Advisory : gc (MDVSA-2012:158)

Mandriva Linux Security Advisory : gcc (MDVSA-2008:066)

Mandriva Linux Security Advisory : gcc (MDVSA-2015:170)

Mandriva Linux Security Advisory : gd (MDVSA-2008:038)

Mandriva Linux Security Advisory : gd (MDVSA-2009:284-1)

Mandriva Linux Security Advisory : gd (MDVSA-2014:133)

Mandriva Linux Security Advisory : gdm (MDVSA-2011:070)

Mandriva Linux Security Advisory : gedit (MDVSA-2009:039)

Mandriva Linux Security Advisory : gegl (MDVSA-2013:081)

Mandriva Linux Security Advisory : gftp (MDVSA-2008:018)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2008:055)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2009:095)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2009:144)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2009:311)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2010:102)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2010:134)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2010:136)

Mandriva Linux Security Advisory : ghostscript (MDVSA-2012:151-1)

Mandriva Linux Security Advisory : gif2png (MDVSA-2011:009)

Mandriva Linux Security Advisory : gimp (MDVSA-2009:296-1)

Mandriva Linux Security Advisory : gimp (MDVSA-2009:332-1)

Mandriva Linux Security Advisory : gimp (MDVSA-2011:103)

Mandriva Linux Security Advisory : gimp (MDVSA-2011:110)

Mandriva Linux Security Advisory : gimp (MDVSA-2011:167)

Mandriva Linux Security Advisory : gimp (MDVSA-2012:142)

Mandriva Linux Security Advisory : gimp (MDVSA-2013:082)

Mandriva Linux Security Advisory : gimp (MDVSA-2013:293)

Mandriva Linux Security Advisory : git (MDVSA-2009:155)

Mandriva Linux Security Advisory : git (MDVSA-2010:194)

Mandriva Linux Security Advisory : git (MDVSA-2010:256)

Mandriva Linux Security Advisory : git (MDVSA-2015:169)

Mandriva Linux Security Advisory : glib2.0 (MDVSA-2009:080)

Mandriva Linux Security Advisory : glib2.0 (MDVSA-2009:245)

Mandriva Linux Security Advisory : glib2.0 (MDVSA-2013:083)

Mandriva Linux Security Advisory : glibc (MDVSA-2010:111)

Mandriva Linux Security Advisory : glibc (MDVSA-2010:112)

Mandriva Linux Security Advisory : glibc (MDVSA-2010:207)

Mandriva Linux Security Advisory : glibc (MDVSA-2010:212)

Mandriva Linux Security Advisory : glibc (MDVSA-2011:178)

Mandriva Linux Security Advisory : glibc (MDVSA-2011:179)

Mandriva Linux Security Advisory : glibc (MDVSA-2013:163)

Mandriva Linux Security Advisory : glibc (MDVSA-2013:283)

Mandriva Linux Security Advisory : glibc (MDVSA-2014:152)

Mandriva Linux Security Advisory : glibc (MDVSA-2014:175)

Mandriva Linux Security Advisory : glibc (MDVSA-2014:232)

Mandriva Linux Security Advisory : glibc (MDVSA-2015:039)

Mandriva Linux Security Advisory : glibc (MDVSA-2015:168)

Mandriva Linux Security Advisory : glibc (MDVSA-2015:218)

Mandriva Linux Security Advisory : glpi (MDVSA-2013:240)

Mandriva Linux Security Advisory : glpi (MDVSA-2015:167)

Mandriva Linux Security Advisory : glusterfs (MDVSA-2015:211)

Mandriva Linux Security Advisory : gnome-keyring (MDVSA-2013:084)

Mandriva Linux Security Advisory : gnome-screensaver (MDVSA-2008:132)

Mandriva Linux Security Advisory : gnome-screensaver (MDVSA-2008:135)

Mandriva Linux Security Advisory : gnome-screensaver (MDVSA-2010:040)

Mandriva Linux Security Advisory : gnucash (MDVSA-2010:241)

Mandriva Linux Security Advisory : gnumeric (MDVSA-2008:056)

Mandriva Linux Security Advisory : gnumeric (MDVSA-2009:043)

Mandriva Linux Security Advisory : gnupg (MDVSA-2013:001-1)

Mandriva Linux Security Advisory : gnupg (MDVSA-2013:205)

Mandriva Linux Security Advisory : gnupg (MDVSA-2013:247)

Mandriva Linux Security Advisory : gnupg (MDVSA-2013:295)

Mandriva Linux Security Advisory : gnupg (MDVSA-2014:127)

Mandriva Linux Security Advisory : gnupg (MDVSA-2014:180)

Mandriva Linux Security Advisory : gnupg (MDVSA-2015:154)

Mandriva Linux Security Advisory : gnupg (MDVSA-2015:155)

Mandriva Linux Security Advisory : gnupg2 (MDVSA-2010:143)

Mandriva Linux Security Advisory : gnutls (MDVSA-2008:106)

Mandriva Linux Security Advisory : gnutls (MDVSA-2008:227-1)

Mandriva Linux Security Advisory : gnutls (MDVSA-2009:116)

Mandriva Linux Security Advisory : gnutls (MDVSA-2009:210)

Mandriva Linux Security Advisory : gnutls (MDVSA-2009:308)

Mandriva Linux Security Advisory : gnutls (MDVSA-2012:040)

Mandriva Linux Security Advisory : gnutls (MDVSA-2012:045)

Mandriva Linux Security Advisory : gnutls (MDVSA-2013:040)

Mandriva Linux Security Advisory : gnutls (MDVSA-2014:043)

Mandriva Linux Security Advisory : gnutls (MDVSA-2014:048)

Mandriva Linux Security Advisory : gnutls (MDVSA-2014:108)

Mandriva Linux Security Advisory : gnutls (MDVSA-2014:215)

Mandriva Linux Security Advisory : gnutls (MDVSA-2015:072)

Mandriva Linux Security Advisory : gpgme (MDVSA-2014:160)

Mandriva Linux Security Advisory : graphicsmagick (MDVSA-2009:261)

Mandriva Linux Security Advisory : graphicsmagick (MDVSA-2012:165)

Mandriva Linux Security Advisory : graphite2 (MDVSA-2011:174)

Mandriva Linux Security Advisory : graphviz (MDVSA-2009:254-1)

Mandriva Linux Security Advisory : graphviz (MDVSA-2014:024)

Mandriva Linux Security Advisory : graphviz (MDVSA-2014:248)

Mandriva Linux Security Advisory : graphviz (MDVSA-2015:187)

Mandriva Linux Security Advisory : groff (MDVSA-2013:086)

Mandriva Linux Security Advisory : grub2 (MDVSA-2015:163)

Mandriva Linux Security Advisory : gstreamer-plugins-good (MDVSA-2008:092)

Mandriva Linux Security Advisory : gstreamer0.10-plugins-base (MDVSA-2009:085)

Mandriva Linux Security Advisory : gstreamer0.10-plugins-good (MDVSA-2009:035)

Mandriva Linux Security Advisory : gstreamer0.10-plugins-good (MDVSA-2009:130-1)

Mandriva Linux Security Advisory : gtk+2.0 (MDVSA-2010:109)

Mandriva Linux Security Advisory : gtk+3.0 (MDVSA-2015:162)

Mandriva Linux Security Advisory : gv (MDVSA-2010:159)

Mandriva Linux Security Advisory : gwenhywfar (MDVSA-2011:072)

Mandriva Linux Security Advisory : gzip (MDVSA-2010:020)

Mandriva Linux Security Advisory : hostapd (MDVSA-2012:168)

Mandriva Linux Security Advisory : hplip (MDVSA-2008:169)

Mandriva Linux Security Advisory : hplip (MDVSA-2011:013)

Mandriva Linux Security Advisory : hplip (MDVSA-2013:088)

Mandriva Linux Security Advisory : hplip (MDVSA-2014:023)

Mandriva Linux Security Advisory : html2ps (MDVSA-2012:161)

Mandriva Linux Security Advisory : html2ps (MDVSA-2013:041)

Mandriva Linux Security Advisory : htmldoc (MDVSA-2009:231-1)

Mandriva Linux Security Advisory : icclib (MDVSA-2013:089)

Mandriva Linux Security Advisory : icecast (MDVSA-2013:091)

Mandriva Linux Security Advisory : icecast (MDVSA-2014:231)

Mandriva Linux Security Advisory : icedtea-web (MDVSA-2012:122)

Mandriva Linux Security Advisory : icu (MDVSA-2008:026)

Mandriva Linux Security Advisory : icu (MDVSA-2011:194)

Mandriva Linux Security Advisory : icu (MDVSA-2013:258)

Mandriva Linux Security Advisory : icu (MDVSA-2015:161-1)

Mandriva Linux Security Advisory : ImageMagick (MDVSA-2008:035)

Mandriva Linux Security Advisory : ImageMagick (MDVSA-2008:099)

Mandriva Linux Security Advisory : imagemagick (MDVSA-2009:260-1)

Mandriva Linux Security Advisory : imagemagick (MDVSA-2012:077)

Mandriva Linux Security Advisory : imagemagick (MDVSA-2012:078)

Mandriva Linux Security Advisory : imagemagick (MDVSA-2012:160)

Mandriva Linux Security Advisory : imagemagick (MDVSA-2013:092)

Mandriva Linux Security Advisory : imagemagick (MDVSA-2014:226)

Mandriva Linux Security Advisory : imagemagick (MDVSA-2015:105)

Mandriva Linux Security Advisory : imap (MDVSA-2009:146-1)

Mandriva Linux Security Advisory : imapsync (MDVSA-2014:060)

Mandriva Linux Security Advisory : imlib2 (MDVSA-2008:123)

Mandriva Linux Security Advisory : imlib2 (MDVSA-2009:019)

Mandriva Linux Security Advisory : imlib2 (MDVSA-2010:127)

Mandriva Linux Security Advisory : initscripts (MDVSA-2009:170)

Mandriva Linux Security Advisory : inn (MDVSA-2012:156)

Mandriva Linux Security Advisory : iodine (MDVSA-2014:128)

Mandriva Linux Security Advisory : ipmitool (MDVSA-2011:196)

Mandriva Linux Security Advisory : iproute2 (MDVSA-2011:135)

Mandriva Linux Security Advisory : ipsec-tools (MDVSA-2008:181)

Mandriva Linux Security Advisory : ipsec-tools (MDVSA-2009:112-1)

Mandriva Linux Security Advisory : iputils (MDVSA-2010:138)

Mandriva Linux Security Advisory : ipython (MDVSA-2014:157)

Mandriva Linux Security Advisory : ipython (MDVSA-2015:160)

Mandriva Linux Security Advisory : ircd-hybrid (MDVSA-2013:093)

Mandriva Linux Security Advisory : irssi (MDVSA-2009:133-1)

Mandriva Linux Security Advisory : irssi (MDVSA-2010:079)

Mandriva Linux Security Advisory : jakarta-commons-httpclient (MDVSA-2014:170)

Mandriva Linux Security Advisory : jakarta-poi (MDVSA-2013:094)

Mandriva Linux Security Advisory : jasper (MDVSA-2009:142-1)

Mandriva Linux Security Advisory : jasper (MDVSA-2011:189)

Mandriva Linux Security Advisory : jasper (MDVSA-2014:247)

Mandriva Linux Security Advisory : jasper (MDVSA-2015:012)

Mandriva Linux Security Advisory : jasper (MDVSA-2015:034)

Mandriva Linux Security Advisory : jasper (MDVSA-2015:159)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2009:137)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2009:209)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2010:084)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2011:054)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2011:126)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2011:170)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2012:021)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2012:095)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2012:150-1)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2012:169)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2013:010)

Mandriva Linux Security Advisory : java-1.6.0-openjdk (MDVSA-2013:014)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2013:095)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2013:161)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2013:183)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2013:267)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2014:011)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2014:100)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2014:141)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2014:209)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2015:033)

Mandriva Linux Security Advisory : java-1.7.0-openjdk (MDVSA-2015:212)

Mandriva Linux Security Advisory : java-1.8.0-openjdk (MDVSA-2015:198)

Mandriva Linux Security Advisory : jbigkit (MDVSA-2014:077)

Mandriva Linux Security Advisory : jbigkit (MDVSA-2015:101)

Mandriva Linux Security Advisory : jetty5 (MDVSA-2009:291)

Mandriva Linux Security Advisory : jhead (MDVSA-2009:041)

Mandriva Linux Security Advisory : joomla (MDVSA-2008:060)

Mandriva Linux Security Advisory : json-c (MDVSA-2014:079)

Mandriva Linux Security Advisory : json-c (MDVSA-2015:102)

Mandriva Linux Security Advisory : jython (MDVSA-2015:158)

Mandriva Linux Security Advisory : kde (MDVSA-2009:346)

Mandriva Linux Security Advisory : kdebase (MDVSA-2010:074)

Mandriva Linux Security Advisory : kdegraphics (MDVSA-2010:182)

Mandriva Linux Security Advisory : kdegraphics4 (MDVSA-2010:162)

Mandriva Linux Security Advisory : kdelibs (MDVSA-2008:097)

Mandriva Linux Security Advisory : kdelibs4 (MDVSA-2010:027)

Mandriva Linux Security Advisory : kdelibs4 (MDVSA-2010:028)

Mandriva Linux Security Advisory : kdelibs4 (MDVSA-2011:071)

Mandriva Linux Security Advisory : kdelibs4 (MDVSA-2011:075)

Mandriva Linux Security Advisory : kdelibs4 (MDVSA-2011:162)

Mandriva Linux Security Advisory : kdenetwork4 (MDVSA-2010:098)

Mandriva Linux Security Advisory : kdenetwork4 (MDVSA-2011:081)

Mandriva Linux Security Advisory : keepalived (MDVSA-2013:096)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:043)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:044)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:104)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:105)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:109)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:112)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:113)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:167)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:223)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:224-1)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:234)

Mandriva Linux Security Advisory : kernel (MDVSA-2008:246)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:032)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:071)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:118)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:119)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:135)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:148)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:205)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:233)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:289)

Mandriva Linux Security Advisory : kernel (MDVSA-2009:329)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:030)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:034)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:066)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:067)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:088)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:172)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:188)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:198)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:247)

Mandriva Linux Security Advisory : kernel (MDVSA-2010:257)

Mandriva Linux Security Advisory : kernel (MDVSA-2013:176)

Mandriva Linux Security Advisory : kernel (MDVSA-2013:194)

Mandriva Linux Security Advisory : kernel (MDVSA-2013:242)

Mandriva Linux Security Advisory : kernel (MDVSA-2013:265)

Mandriva Linux Security Advisory : kernel (MDVSA-2013:291)

Mandriva Linux Security Advisory : kernel (MDVSA-2014:001)

Mandriva Linux Security Advisory : kernel (MDVSA-2014:038)

Mandriva Linux Security Advisory : kernel (MDVSA-2014:124)

Mandriva Linux Security Advisory : kernel (MDVSA-2014:155)

Mandriva Linux Security Advisory : kernel (MDVSA-2014:201)

Mandriva Linux Security Advisory : kernel (MDVSA-2014:230)

Mandriva Linux Security Advisory : kernel (MDVSA-2015:027)

Mandriva Linux Security Advisory : kernel (MDVSA-2015:057)

Mandriva Linux Security Advisory : kernel (MDVSA-2015:058)

Mandriva Linux Security Advisory : koffice (MDVSA-2008:197-1)

Mandriva Linux Security Advisory : koffice (MDVSA-2009:336)

Mandriva Linux Security Advisory : kolab-horde-framework (MDVSA-2010:108)

Mandriva Linux Security Advisory : kompozer (MDVSA-2009:219-1)

Mandriva Linux Security Advisory : krb5 (MDVSA-2008:069)

Mandriva Linux Security Advisory : krb5 (MDVSA-2008:070)

Mandriva Linux Security Advisory : krb5 (MDVSA-2009:082)

Mandriva Linux Security Advisory : krb5 (MDVSA-2009:098-1)

Mandriva Linux Security Advisory : krb5 (MDVSA-2010:006)

Mandriva Linux Security Advisory : krb5 (MDVSA-2010:100)

Mandriva Linux Security Advisory : krb5 (MDVSA-2010:202)

Mandriva Linux Security Advisory : krb5 (MDVSA-2010:245)

Mandriva Linux Security Advisory : krb5 (MDVSA-2010:246)

Mandriva Linux Security Advisory : krb5 (MDVSA-2011:024)

Mandriva Linux Security Advisory : krb5 (MDVSA-2011:025)

Mandriva Linux Security Advisory : krb5 (MDVSA-2011:048)

Mandriva Linux Security Advisory : krb5 (MDVSA-2011:077)

Mandriva Linux Security Advisory : krb5 (MDVSA-2011:159)

Mandriva Linux Security Advisory : krb5 (MDVSA-2011:160)

Mandriva Linux Security Advisory : krb5 (MDVSA-2011:184)

Mandriva Linux Security Advisory : krb5 (MDVSA-2012:102)

Mandriva Linux Security Advisory : krb5 (MDVSA-2012:120)

Mandriva Linux Security Advisory : krb5 (MDVSA-2013:042)

Mandriva Linux Security Advisory : krb5 (MDVSA-2013:158)

Mandriva Linux Security Advisory : krb5 (MDVSA-2013:166)

Mandriva Linux Security Advisory : krb5 (MDVSA-2013:275)

Mandriva Linux Security Advisory : krb5 (MDVSA-2014:165)

Mandriva Linux Security Advisory : krb5 (MDVSA-2014:224)

Mandriva Linux Security Advisory : krb5 (MDVSA-2015:009)

Mandriva Linux Security Advisory : krb5 (MDVSA-2015:069)

Mandriva Linux Security Advisory : krb5-appl (MDVSA-2011:117)

Mandriva Linux Security Advisory : krb5-appl (MDVSA-2011:195)

Mandriva Linux Security Advisory : kvm (MDVSA-2009:009)

Mandriva Linux Security Advisory : lcms (MDVSA-2009:121-1)

Mandriva Linux Security Advisory : lcms (MDVSA-2013:220)

Mandriva Linux Security Advisory : lcms2 (MDVSA-2013:211)

Mandriva Linux Security Advisory : lcms2 (MDVSA-2015:107)

Mandriva Linux Security Advisory : ldns (MDVSA-2014:085)

Mandriva Linux Security Advisory : less (MDVSA-2015:199)

Mandriva Linux Security Advisory : lftp (MDVSA-2010:128)

Mandriva Linux Security Advisory : lftp (MDVSA-2015:213)

Mandriva Linux Security Advisory : libarchive (MDVSA-2011:190)

Mandriva Linux Security Advisory : libarchive (MDVSA-2013:147)

Mandriva Linux Security Advisory : libarchive (MDVSA-2015:157)

Mandriva Linux Security Advisory : libcap (MDVSA-2011:185)

Mandriva Linux Security Advisory : libcap-ng (MDVSA-2014:117)

Mandriva Linux Security Advisory : libcap-ng (MDVSA-2015:156)

Mandriva Linux Security Advisory : libcdaudio (MDVSA-2008:233-1)

Mandriva Linux Security Advisory : libcdio (MDVSA-2008:037)

Mandriva Linux Security Advisory : libdigidoc (MDVSA-2013:225)

Mandriva Linux Security Advisory : libesmtp (MDVSA-2010:195)

Mandriva Linux Security Advisory : libevent (MDVSA-2015:017-1)

Mandriva Linux Security Advisory : libexif (MDVSA-2008:005)

Mandriva Linux Security Advisory : libexif (MDVSA-2012:106)

Mandriva Linux Security Advisory : libexif (MDVSA-2013:035)

Mandriva Linux Security Advisory : libgadu (MDVSA-2009:208-1)

Mandriva Linux Security Advisory : libgadu (MDVSA-2014:039)

Mandriva Linux Security Advisory : libgadu (MDVSA-2014:121)

Mandriva Linux Security Advisory : libgadu (MDVSA-2014:185)

Mandriva Linux Security Advisory : libgcrypt (MDVSA-2014:176)

Mandriva Linux Security Advisory : libgd (MDVSA-2015:153)

Mandriva Linux Security Advisory : libgdata (MDVSA-2012:111)

Mandriva Linux Security Advisory : libgdiplus (MDVSA-2010:166)

Mandriva Linux Security Advisory : libglpng (MDVSA-2010:179)

Mandriva Linux Security Advisory : libgssglue (MDVSA-2013:043)

Mandriva Linux Security Advisory : libHX (MDVSA-2010:165)

Mandriva Linux Security Advisory : libid3tag (MDVSA-2008:103)

Mandriva Linux Security Advisory : libjpeg (MDVSA-2013:044)

Mandriva Linux Security Advisory : libjpeg (MDVSA-2013:273)

Mandriva Linux Security Advisory : libjpeg (MDVSA-2015:014)

Mandriva Linux Security Advisory : libjpeg (MDVSA-2015:152)

Mandriva Linux Security Advisory : libjpeg-turbo (MDVSA-2012:121)

Mandriva Linux Security Advisory : libksba (MDVSA-2014:234)

Mandriva Linux Security Advisory : libksba (MDVSA-2015:151)

Mandriva Linux Security Advisory : libksba (MDVSA-2015:214)

Mandriva Linux Security Advisory : liblzo (MDVSA-2014:134)

Mandriva Linux Security Advisory : liblzo (MDVSA-2015:150)

Mandriva Linux Security Advisory : libmbfl (MDVSA-2010:225-1)

Mandriva Linux Security Advisory : libmikmod (MDVSA-2009:272-1)

Mandriva Linux Security Advisory : libmikmod (MDVSA-2010:151)

Mandriva Linux Security Advisory : libmodplug (MDVSA-2009:128-1)

Mandriva Linux Security Advisory : libmodplug (MDVSA-2011:085)

Mandriva Linux Security Advisory : libmodplug (MDVSA-2013:232)

Mandriva Linux Security Advisory : libneon (MDVSA-2009:315)

Mandriva Linux Security Advisory : libneon0.27 (MDVSA-2009:074)

Mandriva Linux Security Advisory : libneon0.27 (MDVSA-2009:221)

Mandriva Linux Security Advisory : libneon0.27 (MDVSA-2010:123)

Mandriva Linux Security Advisory : libotr (MDVSA-2012:131)

Mandriva Linux Security Advisory : libotr (MDVSA-2013:097)

Mandriva Linux Security Advisory : libpng (MDVSA-2008:156)

Mandriva Linux Security Advisory : libpng (MDVSA-2009:051)

Mandriva Linux Security Advisory : libpng (MDVSA-2010:063)

Mandriva Linux Security Advisory : libpng (MDVSA-2010:064)

Mandriva Linux Security Advisory : libpng (MDVSA-2010:133)

Mandriva Linux Security Advisory : libpng (MDVSA-2011:151)

Mandriva Linux Security Advisory : libpng (MDVSA-2012:033)

Mandriva Linux Security Advisory : libpng (MDVSA-2012:046)

Mandriva Linux Security Advisory : libpng (MDVSA-2014:035)

Mandriva Linux Security Advisory : libpng (MDVSA-2014:084)

Mandriva Linux Security Advisory : libpng (MDVSA-2015:090)

Mandriva Linux Security Advisory : libpng12 (MDVSA-2015:071)

Mandriva Linux Security Advisory : libproxy (MDVSA-2012:172)

Mandriva Linux Security Advisory : libraw (MDVSA-2013:249)

Mandriva Linux Security Advisory : libreoffice (MDVSA-2011:172)

Mandriva Linux Security Advisory : libreoffice (MDVSA-2012:063)

Mandriva Linux Security Advisory : libreoffice (MDVSA-2012:091)

Mandriva Linux Security Advisory : libreoffice (MDVSA-2012:123)

Mandriva Linux Security Advisory : librsvg (MDVSA-2014:009)

Mandriva Linux Security Advisory : librsync (MDVSA-2015:204)

Mandriva Linux Security Advisory : libsamplerate (MDVSA-2008:238)

Mandriva Linux Security Advisory : libsamplerate (MDVSA-2009:232-1)

Mandriva Linux Security Advisory : libsmi (MDVSA-2010:209)

Mandriva Linux Security Advisory : libsndfile (MDVSA-2009:067)

Mandriva Linux Security Advisory : libsndfile (MDVSA-2009:132-1)

Mandriva Linux Security Advisory : libsndfile (MDVSA-2010:150)

Mandriva Linux Security Advisory : libsndfile (MDVSA-2011:119)

Mandriva Linux Security Advisory : libsndfile (MDVSA-2015:024)

Mandriva Linux Security Advisory : libsndfile (MDVSA-2015:149)

Mandriva Linux Security Advisory : libsoup (MDVSA-2009:081)

Mandriva Linux Security Advisory : libsoup (MDVSA-2012:036)

Mandriva Linux Security Advisory : libssh (MDVSA-2012:175)

Mandriva Linux Security Advisory : libssh (MDVSA-2013:009)

Mandriva Linux Security Advisory : libssh (MDVSA-2013:045)

Mandriva Linux Security Advisory : libssh (MDVSA-2014:053)

Mandriva Linux Security Advisory : libssh (MDVSA-2015:020)

Mandriva Linux Security Advisory : libssh (MDVSA-2015:086)

Mandriva Linux Security Advisory : libssh2 (MDVSA-2015:148-1)

Mandriva Linux Security Advisory : libtar (MDVSA-2013:253)

Mandriva Linux Security Advisory : libtar (MDVSA-2014:045)

Mandriva Linux Security Advisory : libtasn1 (MDVSA-2012:039)

Mandriva Linux Security Advisory : libtasn1 (MDVSA-2014:107)

Mandriva Linux Security Advisory : libtasn1 (MDVSA-2015:116)

Mandriva Linux Security Advisory : libtasn1 (MDVSA-2015:193)

Mandriva Linux Security Advisory : libtasn1 (MDVSA-2015:232)

Mandriva Linux Security Advisory : libthai (MDVSA-2010:010)

Mandriva Linux Security Advisory : libtheora (MDVSA-2010:043)

Mandriva Linux Security Advisory : libtiff (MDVSA-2008:184)

Mandriva Linux Security Advisory : libtiff (MDVSA-2009:150)

Mandriva Linux Security Advisory : libtiff (MDVSA-2009:169-1)

Mandriva Linux Security Advisory : libtiff (MDVSA-2010:145)

Mandriva Linux Security Advisory : libtiff (MDVSA-2010:146)

Mandriva Linux Security Advisory : libtiff (MDVSA-2010:190)

Mandriva Linux Security Advisory : libtiff (MDVSA-2011:043)

Mandriva Linux Security Advisory : libtiff (MDVSA-2011:064)

Mandriva Linux Security Advisory : libtiff (MDVSA-2011:078)

Mandriva Linux Security Advisory : libtiff (MDVSA-2012:054)

Mandriva Linux Security Advisory : libtiff (MDVSA-2012:101)

Mandriva Linux Security Advisory : libtiff (MDVSA-2012:127)

Mandriva Linux Security Advisory : libtiff (MDVSA-2012:174)

Mandriva Linux Security Advisory : libtiff (MDVSA-2012:184)

Mandriva Linux Security Advisory : libtiff (MDVSA-2013:046)

Mandriva Linux Security Advisory : libtiff (MDVSA-2013:208)

Mandriva Linux Security Advisory : libtiff (MDVSA-2013:219)

Mandriva Linux Security Advisory : libtiff (MDVSA-2013:224)

Mandriva Linux Security Advisory : libtiff (MDVSA-2015:147-1)

Mandriva Linux Security Advisory : libtool (MDVSA-2009:307-1)

Mandriva Linux Security Advisory : libtorrent-rasterbar (MDVSA-2009:139)

Mandriva Linux Security Advisory : libupnp (MDVSA-2013:098)

Mandriva Linux Security Advisory : libuser (MDVSA-2011:019)

Mandriva Linux Security Advisory : libvirt (MDVSA-2014:097)

Mandriva Linux Security Advisory : libvirt (MDVSA-2014:195)

Mandriva Linux Security Advisory : libvirt (MDVSA-2014:222)

Mandriva Linux Security Advisory : libvirt (MDVSA-2015:023)

Mandriva Linux Security Advisory : libvirt (MDVSA-2015:035)

Mandriva Linux Security Advisory : libvirt (MDVSA-2015:070)

Mandriva Linux Security Advisory : libvirt (MDVSA-2015:115)

Mandriva Linux Security Advisory : libvncserver (MDVSA-2014:168)

Mandriva Linux Security Advisory : libvncserver (MDVSA-2014:229)

Mandriva Linux Security Advisory : libvncserver (MDVSA-2015:146)

Mandriva Linux Security Advisory : libvorbis (MDVSA-2008:102)

Mandriva Linux Security Advisory : libvorbis (MDVSA-2012:052)

Mandriva Linux Security Advisory : libvpx (MDVSA-2012:023-1)

Mandriva Linux Security Advisory : libwmf (MDVSA-2009:106-1)

Mandriva Linux Security Advisory : libxext (MDVSA-2010:095)

Mandriva Linux Security Advisory : libxfont (MDVSA-2008:024)

Mandriva Linux Security Advisory : libxfont (MDVSA-2011:153)

Mandriva Linux Security Advisory : libxfont (MDVSA-2014:013)

Mandriva Linux Security Advisory : libxfont (MDVSA-2014:132)

Mandriva Linux Security Advisory : libxfont (MDVSA-2015:145-1)

Mandriva Linux Security Advisory : libxml (MDVSA-2009:200-1)

Mandriva Linux Security Advisory : libxml (MDVSA-2011:131-1)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2008:010)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2008:180-1)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2008:192)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2008:212)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2008:231)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2010:243)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2010:260)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2011:145)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2011:188)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2012:005)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2012:098)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2012:126)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2012:176)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2013:056)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2013:198)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2014:086)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2014:204)

Mandriva Linux Security Advisory : libxml2 (MDVSA-2015:111)

Mandriva Linux Security Advisory : libxslt (MDVSA-2008:151)

Mandriva Linux Security Advisory : libxslt (MDVSA-2008:160)

Mandriva Linux Security Advisory : libxslt (MDVSA-2012:028)

Mandriva Linux Security Advisory : libxslt (MDVSA-2012:109)

Mandriva Linux Security Advisory : libxslt (MDVSA-2012:164)

Mandriva Linux Security Advisory : libxslt (MDVSA-2013:047)

Mandriva Linux Security Advisory : libxslt (MDVSA-2013:141)

Mandriva Linux Security Advisory : libytnef (MDVSA-2013:099)

Mandriva Linux Security Advisory : libzip (MDVSA-2011:099)

Mandriva Linux Security Advisory : libzip (MDVSA-2012:034)

Mandriva Linux Security Advisory : lighttpd (MDVSA-2013:100)

Mandriva Linux Security Advisory : lighttpd (MDVSA-2013:277)

Mandriva Linux Security Advisory : live (MDVSA-2014:144)

Mandriva Linux Security Advisory : logrotate (MDVSA-2011:065)

Mandriva Linux Security Advisory : lua (MDVSA-2014:205)

Mandriva Linux Security Advisory : lua (MDVSA-2015:144)

Mandriva Linux Security Advisory : lvm2 (MDVSA-2010:171)

Mandriva Linux Security Advisory : lynx (MDVSA-2008:218)

Mandriva Linux Security Advisory : lynx (MDVSA-2013:101)

Mandriva Linux Security Advisory : madwifi-source (MDVSA-2008:007)

Mandriva Linux Security Advisory : mailman (MDVSA-2008:061)

Mandriva Linux Security Advisory : mailman (MDVSA-2010:191)

Mandriva Linux Security Advisory : mailman (MDVSA-2011:036)

Mandriva Linux Security Advisory : mariadb (MDVSA-2013:102)

Mandriva Linux Security Advisory : mariadb (MDVSA-2014:028)

Mandriva Linux Security Advisory : mariadb (MDVSA-2014:102)

Mandriva Linux Security Advisory : mariadb (MDVSA-2014:210)

Mandriva Linux Security Advisory : mariadb (MDVSA-2015:091)

Mandriva Linux Security Advisory : mariadb (MDVSA-2015:227)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2013:235)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2013:290)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2014:057)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2014:083)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2014:119)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2014:153)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2014:198)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2014:241)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2015:006)

Mandriva Linux Security Advisory : mediawiki (MDVSA-2015:200)

Mandriva Linux Security Advisory : memcached (MDVSA-2009:105)

Mandriva Linux Security Advisory : memcached (MDVSA-2009:202)

Mandriva Linux Security Advisory : memcached (MDVSA-2013:280)

Mandriva Linux Security Advisory : memcached (MDVSA-2014:010)

Mandriva Linux Security Advisory : mesa (MDVSA-2013:103)

Mandriva Linux Security Advisory : mesa (MDVSA-2013:164)

Mandriva Linux Security Advisory : mesa (MDVSA-2013:182)

Mandriva Linux Security Advisory : metisse (MDVSA-2008:179)

Mandriva Linux Security Advisory : MHonArc (MDVSA-2011:003)

Mandriva Linux Security Advisory : miniupnpc (MDVSA-2014:120)

Mandriva Linux Security Advisory : mod\_perl (MDVSA-2009:091-1)

Mandriva Linux Security Advisory : mono (MDVSA-2008:210-1)

Mandriva Linux Security Advisory : mono (MDVSA-2009:268)

Mandriva Linux Security Advisory : mono (MDVSA-2009:269)

Mandriva Linux Security Advisory : mono (MDVSA-2009:322)

Mandriva Linux Security Advisory : mono (MDVSA-2010:240)

Mandriva Linux Security Advisory : mono (MDVSA-2012:140)

Mandriva Linux Security Advisory : mosh (MDVSA-2013:104)

Mandriva Linux Security Advisory : mozilla (MDVSA-2011:111)

Mandriva Linux Security Advisory : mozilla (MDVSA-2011:127)

Mandriva Linux Security Advisory : mozilla (MDVSA-2011:129)

Mandriva Linux Security Advisory : mozilla (MDVSA-2011:133-1)

Mandriva Linux Security Advisory : mozilla (MDVSA-2011:169)

Mandriva Linux Security Advisory : mozilla (MDVSA-2011:192)

Mandriva Linux Security Advisory : mozilla (MDVSA-2012:013)

Mandriva Linux Security Advisory : mozilla (MDVSA-2012:022-1)

Mandriva Linux Security Advisory : mozilla (MDVSA-2012:032-1)

Mandriva Linux Security Advisory : mozilla (MDVSA-2012:066)

Mandriva Linux Security Advisory : mozilla (MDVSA-2012:088-1)

Mandriva Linux Security Advisory : mozilla (MDVSA-2012:110-1)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:048)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:080)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:110)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:136)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:148)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:205)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:228)

Mandriva Linux Security Advisory : mozilla-firefox (MDVSA-2008:244)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2008:047)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2008:062)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2008:155-1)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2008:206)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2008:235)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2009:012)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2009:083)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2009:141)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2009:217-3)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2010:051)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2010:071)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2010:126)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2010:169)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2010:211)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2010:219)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2010:258)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2011:042)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2011:080)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2011:140)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2011:142)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2012:018)

Mandriva Linux Security Advisory : mozilla-thunderbird (MDVSA-2012:147)

Mandriva Linux Security Advisory : mpfr (MDVSA-2015:025)

Mandriva Linux Security Advisory : mpfr (MDVSA-2015:143)

Mandriva Linux Security Advisory : mpg123 (MDVSA-2009:093-1)

Mandriva Linux Security Advisory : mplayer (MDVSA-2008:045)

Mandriva Linux Security Advisory : mplayer (MDVSA-2008:196)

Mandriva Linux Security Advisory : mplayer (MDVSA-2008:219)

Mandriva Linux Security Advisory : mplayer (MDVSA-2009:013)

Mandriva Linux Security Advisory : mplayer (MDVSA-2009:014)

Mandriva Linux Security Advisory : mplayer (MDVSA-2011:088)

Mandriva Linux Security Advisory : mplayer (MDVSA-2011:089)

Mandriva Linux Security Advisory : munin (MDVSA-2013:105)

Mandriva Linux Security Advisory : munin (MDVSA-2013:297)

Mandriva Linux Security Advisory : mutt (MDVSA-2012:048)

Mandriva Linux Security Advisory : mutt (MDVSA-2014:245)

Mandriva Linux Security Advisory : mutt (MDVSA-2015:078)

Mandriva Linux Security Advisory : mysql (MDVSA-2008:017)

Mandriva Linux Security Advisory : mysql (MDVSA-2008:028)

Mandriva Linux Security Advisory : mysql (MDVSA-2008:149)

Mandriva Linux Security Advisory : mysql (MDVSA-2008:150)

Mandriva Linux Security Advisory : mysql (MDVSA-2009:094)

Mandriva Linux Security Advisory : mysql (MDVSA-2009:159)

Mandriva Linux Security Advisory : mysql (MDVSA-2009:326)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:011)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:012)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:044)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:093)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:101)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:107)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:155-1)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:222)

Mandriva Linux Security Advisory : mysql (MDVSA-2010:223)

Mandriva Linux Security Advisory : mysql (MDVSA-2011:012)

Mandriva Linux Security Advisory : mysql (MDVSA-2012:178)

Mandriva Linux Security Advisory : mysql (MDVSA-2013:007)

Mandriva Linux Security Advisory : nagios (MDVSA-2014:004)

Mandriva Linux Security Advisory : nagios (MDVSA-2014:089)

Mandriva Linux Security Advisory : nail (MDVSA-2015:011)

Mandriva Linux Security Advisory : nasm (MDVSA-2008:120)

Mandriva Linux Security Advisory : ncompress (MDVSA-2011:152)

Mandriva Linux Security Advisory : ncpfs (MDVSA-2010:046)

Mandriva Linux Security Advisory : ncpfs (MDVSA-2010:061)

Mandriva Linux Security Advisory : ncpfs (MDVSA-2012:084)

Mandriva Linux Security Advisory : ncpfs (MDVSA-2013:048)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2008:118)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2008:225)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2009:056)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2012:099)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2013:049)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2014:017)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2014:052)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2014:184)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2015:092)

Mandriva Linux Security Advisory : net-snmp (MDVSA-2015:229)

Mandriva Linux Security Advisory : netpbm (MDVSA-2009:262)

Mandriva Linux Security Advisory : netpbm (MDVSA-2009:317)

Mandriva Linux Security Advisory : netpbm (MDVSA-2010:039)

Mandriva Linux Security Advisory : networkmanager (MDVSA-2011:171)

Mandriva Linux Security Advisory : newt (MDVSA-2009:249-1)

Mandriva Linux Security Advisory : nfs-utils (MDVSA-2009:060)

Mandriva Linux Security Advisory : nfs-utils (MDVSA-2011:186)

Mandriva Linux Security Advisory : nfs-utils (MDVSA-2013:178)

Mandriva Linux Security Advisory : nginx (MDVSA-2012:043)

Mandriva Linux Security Advisory : nginx (MDVSA-2013:281)

Mandriva Linux Security Advisory : nginx (MDVSA-2015:094)

Mandriva Linux Security Advisory : nodejs (MDVSA-2015:142)

Mandriva Linux Security Advisory : nodejs (MDVSA-2015:228)

Mandriva Linux Security Advisory : not-yet-commons-ssl (MDVSA-2015:141)

Mandriva Linux Security Advisory : nspr (MDVSA-2014:125)

Mandriva Linux Security Advisory : nss (MDVSA-2009:197-3)

Mandriva Linux Security Advisory : nss (MDVSA-2010:069)

Mandriva Linux Security Advisory : nss (MDVSA-2013:050)

Mandriva Linux Security Advisory : nss (MDVSA-2013:257)

Mandriva Linux Security Advisory : nss (MDVSA-2013:270)

Mandriva Linux Security Advisory : nss (MDVSA-2013:301)

Mandriva Linux Security Advisory : nss (MDVSA-2014:012)

Mandriva Linux Security Advisory : nss (MDVSA-2014:139)

Mandriva Linux Security Advisory : nss (MDVSA-2014:189)

Mandriva Linux Security Advisory : nss (MDVSA-2014:252)

Mandriva Linux Security Advisory : nss (MDVSA-2015:059)

Mandriva Linux Security Advisory : nss-pam-ldapd (MDVSA-2013:106)

Mandriva Linux Security Advisory : nss\_db (MDVSA-2010:077)

Mandriva Linux Security Advisory : nss\_ldap (MDVSA-2008:049)

Mandriva Linux Security Advisory : ntop (MDVSA-2015:216)

Mandriva Linux Security Advisory : ntp (MDVSA-2009:007)

Mandriva Linux Security Advisory : ntp (MDVSA-2009:092)

Mandriva Linux Security Advisory : ntp (MDVSA-2009:117)

Mandriva Linux Security Advisory : ntp (MDVSA-2009:309)

Mandriva Linux Security Advisory : ntp (MDVSA-2009:328)

Mandriva Linux Security Advisory : ntp (MDVSA-2015:003)

Mandriva Linux Security Advisory : ntp (MDVSA-2015:046)

Mandriva Linux Security Advisory : ntp (MDVSA-2015:140)

Mandriva Linux Security Advisory : ntp (MDVSA-2015:202)

Mandriva Linux Security Advisory : nut (MDVSA-2012:087)

Mandriva Linux Security Advisory : oath-toolkit (MDVSA-2014:061)

Mandriva Linux Security Advisory : ocaml-xml-light (MDVSA-2013:107)

Mandriva Linux Security Advisory : ocsinventory (MDVSA-2014:156)

Mandriva Linux Security Advisory : open-iscsi (MDVSA-2013:109)

Mandriva Linux Security Advisory : openafs (MDVSA-2008:207)

Mandriva Linux Security Advisory : openafs (MDVSA-2009:099-1)

Mandriva Linux Security Advisory : openafs (MDVSA-2014:244)

Mandriva Linux Security Advisory : openconnect (MDVSA-2013:108)

Mandriva Linux Security Advisory : OpenEXR (MDVSA-2009:190)

Mandriva Linux Security Advisory : OpenEXR (MDVSA-2009:191-1)

Mandriva Linux Security Advisory : openjpa (MDVSA-2013:246)

Mandriva Linux Security Advisory : openjpeg (MDVSA-2012:104)

Mandriva Linux Security Advisory : openjpeg (MDVSA-2012:157)

Mandriva Linux Security Advisory : openjpeg (MDVSA-2013:110)

Mandriva Linux Security Advisory : openjpeg (MDVSA-2014:008)

Mandriva Linux Security Advisory : openldap (MDVSA-2008:058)

Mandriva Linux Security Advisory : openldap (MDVSA-2008:144)

Mandriva Linux Security Advisory : openldap (MDVSA-2010:026)

Mandriva Linux Security Advisory : openldap (MDVSA-2010:142)

Mandriva Linux Security Advisory : openldap (MDVSA-2011:055)

Mandriva Linux Security Advisory : openldap (MDVSA-2011:056)

Mandriva Linux Security Advisory : openldap (MDVSA-2012:130)

Mandriva Linux Security Advisory : openldap (MDVSA-2014:026)

Mandriva Linux Security Advisory : openldap (MDVSA-2015:073)

Mandriva Linux Security Advisory : openldap (MDVSA-2015:074)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2008:095)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2008:137)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2008:138)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2009:006)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2009:070)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2010:035)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2010:056)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2010:075)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2010:105)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2010:221)

Mandriva Linux Security Advisory : openoffice.org (MDVSA-2011:027)

Mandriva Linux Security Advisory : opensc (MDVSA-2008:183)

Mandriva Linux Security Advisory : opensc (MDVSA-2009:089)

Mandriva Linux Security Advisory : opensc (MDVSA-2009:123)

Mandriva Linux Security Advisory : opensc (MDVSA-2011:011)

Mandriva Linux Security Advisory : openslp (MDVSA-2012:141)

Mandriva Linux Security Advisory : openslp (MDVSA-2013:111)

Mandriva Linux Security Advisory : openssh (MDVSA-2008:078)

Mandriva Linux Security Advisory : openssh (MDVSA-2008:098)

Mandriva Linux Security Advisory : openssh (MDVSA-2013:051)

Mandriva Linux Security Advisory : openssh (MDVSA-2014:068)

Mandriva Linux Security Advisory : openssh (MDVSA-2015:095)

Mandriva Linux Security Advisory : openssl (MDVSA-2008:107)

Mandriva Linux Security Advisory : openssl (MDVSA-2009:001)

Mandriva Linux Security Advisory : openssl (MDVSA-2009:087)

Mandriva Linux Security Advisory : openssl (MDVSA-2009:120)

Mandriva Linux Security Advisory : openssl (MDVSA-2009:238)

Mandriva Linux Security Advisory : openssl (MDVSA-2009:239)

Mandriva Linux Security Advisory : openssl (MDVSA-2009:258)

Mandriva Linux Security Advisory : openssl (MDVSA-2009:310)

Mandriva Linux Security Advisory : openssl (MDVSA-2010:022)

Mandriva Linux Security Advisory : openssl (MDVSA-2010:076-1)

Mandriva Linux Security Advisory : openssl (MDVSA-2010:168)

Mandriva Linux Security Advisory : openssl (MDVSA-2010:238)

Mandriva Linux Security Advisory : openssl (MDVSA-2010:248)

Mandriva Linux Security Advisory : openssl (MDVSA-2011:028)

Mandriva Linux Security Advisory : openssl (MDVSA-2011:136)

Mandriva Linux Security Advisory : openssl (MDVSA-2011:137)

Mandriva Linux Security Advisory : openssl (MDVSA-2012:006)

Mandriva Linux Security Advisory : openssl (MDVSA-2012:007)

Mandriva Linux Security Advisory : openssl (MDVSA-2012:011)

Mandriva Linux Security Advisory : openssl (MDVSA-2012:038)

Mandriva Linux Security Advisory : openssl (MDVSA-2012:060)

Mandriva Linux Security Advisory : openssl (MDVSA-2012:073)

Mandriva Linux Security Advisory : openssl (MDVSA-2013:052)

Mandriva Linux Security Advisory : openssl (MDVSA-2014:007)

Mandriva Linux Security Advisory : openssl (MDVSA-2014:067)

Mandriva Linux Security Advisory : openssl (MDVSA-2014:080)

Mandriva Linux Security Advisory : openssl (MDVSA-2014:090)

Mandriva Linux Security Advisory : openssl (MDVSA-2014:106)

Mandriva Linux Security Advisory : openssl (MDVSA-2014:158)

Mandriva Linux Security Advisory : openssl (MDVSA-2014:203)

Mandriva Linux Security Advisory : openssl (MDVSA-2015:019)

Mandriva Linux Security Advisory : openssl (MDVSA-2015:062)

Mandriva Linux Security Advisory : openssl (MDVSA-2015:063)

Mandriva Linux Security Advisory : openssl0.9.8 (MDVSA-2011:173)

Mandriva Linux Security Advisory : openssl0.9.8 (MDVSA-2012:064)

Mandriva Linux Security Advisory : openvpn (MDVSA-2013:167)

Mandriva Linux Security Advisory : openvpn (MDVSA-2014:246)

Mandriva Linux Security Advisory : openvpn (MDVSA-2015:139)

Mandriva Linux Security Advisory : otrs (MDVSA-2013:112)

Mandriva Linux Security Advisory : otrs (MDVSA-2013:188)

Mandriva Linux Security Advisory : otrs (MDVSA-2013:212)

Mandriva Linux Security Advisory : otrs (MDVSA-2014:054)

Mandriva Linux Security Advisory : otrs (MDVSA-2014:111)

Mandriva Linux Security Advisory : otrs (MDVSA-2015:043)

Mandriva Linux Security Advisory : owncloud (MDVSA-2013:175)

Mandriva Linux Security Advisory : owncloud (MDVSA-2013:206)

Mandriva Linux Security Advisory : owncloud (MDVSA-2013:289)

Mandriva Linux Security Advisory : owncloud (MDVSA-2014:055)

Mandriva Linux Security Advisory : owncloud (MDVSA-2014:101)

Mandriva Linux Security Advisory : owncloud (MDVSA-2014:140)

Mandriva Linux Security Advisory : owncloud (MDVSA-2015:190)

Mandriva Linux Security Advisory : owncloud (MDVSA-2015:191)

Mandriva Linux Security Advisory : pam (MDVSA-2009:077)

Mandriva Linux Security Advisory : pam (MDVSA-2010:220)

Mandriva Linux Security Advisory : pam\_krb5 (MDVSA-2008:209-1)

Mandriva Linux Security Advisory : pam\_krb5 (MDVSA-2010:054)

Mandriva Linux Security Advisory : pam\_mount (MDVSA-2008:208-1)

Mandriva Linux Security Advisory : pam\_mount (MDVSA-2009:004)

Mandriva Linux Security Advisory : pan (MDVSA-2008:201)

Mandriva Linux Security Advisory : pango (MDVSA-2009:158-3)

Mandriva Linux Security Advisory : pango (MDVSA-2010:121)

Mandriva Linux Security Advisory : pango (MDVSA-2011:020)

Mandriva Linux Security Advisory : pango (MDVSA-2011:040)

Mandriva Linux Security Advisory : patch (MDVSA-2015:050)

Mandriva Linux Security Advisory : patch (MDVSA-2015:138)

Mandriva Linux Security Advisory : pcre (MDVSA-2008:053)

Mandriva Linux Security Advisory : pcre (MDVSA-2008:147)

Mandriva Linux Security Advisory : pcre (MDVSA-2015:002)

Mandriva Linux Security Advisory : pcre (MDVSA-2015:137)

Mandriva Linux Security Advisory : pcsc-lite (MDVSA-2010:189)

Mandriva Linux Security Advisory : pcsc-lite (MDVSA-2011:015)

Mandriva Linux Security Advisory : perl (MDVSA-2008:100)

Mandriva Linux Security Advisory : perl (MDVSA-2008:165)

Mandriva Linux Security Advisory : perl (MDVSA-2010:115)

Mandriva Linux Security Advisory : perl (MDVSA-2010:116)

Mandriva Linux Security Advisory : perl (MDVSA-2011:091)

Mandriva Linux Security Advisory : perl (MDVSA-2012:008)

Mandriva Linux Security Advisory : perl (MDVSA-2013:005)

Mandriva Linux Security Advisory : perl (MDVSA-2013:113)

Mandriva Linux Security Advisory : perl (MDVSA-2014:199)

Mandriva Linux Security Advisory : perl (MDVSA-2015:136)

Mandriva Linux Security Advisory : perl-CGI (MDVSA-2010:237)

Mandriva Linux Security Advisory : perl-CGI (MDVSA-2011:008)

Mandriva Linux Security Advisory : perl-CGI (MDVSA-2012:180)

Mandriva Linux Security Advisory : perl-Compress-Raw-Bzip2 (MDVSA-2009:207)

Mandriva Linux Security Advisory : perl-Compress-Raw-Zlib (MDVSA-2009:157-1)

Mandriva Linux Security Advisory : perl-Crypt-DSA (MDVSA-2013:241)

Mandriva Linux Security Advisory : perl-Dancer (MDVSA-2013:184)

Mandriva Linux Security Advisory : perl-DBD-Pg (MDVSA-2009:344)

Mandriva Linux Security Advisory : perl-DBD-Pg (MDVSA-2012:112)

Mandriva Linux Security Advisory : perl-Email-Address (MDVSA-2014:192)

Mandriva Linux Security Advisory : perl-Gtk2 (MDVSA-2015:044)

Mandriva Linux Security Advisory : perl-HTTP-Body (MDVSA-2013:282)

Mandriva Linux Security Advisory : perl-IO-Socket-SSL (MDVSA-2009:252-1)

Mandriva Linux Security Advisory : perl-IO-Socket-SSL (MDVSA-2011:092)

Mandriva Linux Security Advisory : perl-libwww-perl (MDVSA-2010:167)

Mandriva Linux Security Advisory : perl-MDK-Common (MDVSA-2009:072)

Mandriva Linux Security Advisory : perl-Module-Signature (MDVSA-2013:185)

Mandriva Linux Security Advisory : perl-Module-Signature (MDVSA-2015:207)

Mandriva Linux Security Advisory : perl-Mojolicious (MDVSA-2014:237)

Mandriva Linux Security Advisory : perl-Net-DNS (MDVSA-2008:073)

Mandriva Linux Security Advisory : perl-Plack (MDVSA-2014:235)

Mandriva Linux Security Advisory : perl-Proc-Daemon (MDVSA-2014:021)

Mandriva Linux Security Advisory : perl-Proc-ProcessTable (MDVSA-2013:216)

Mandriva Linux Security Advisory : perl-Tk (MDVSA-2008:077)

Mandriva Linux Security Advisory : perl-XML-DT (MDVSA-2014:191)

Mandriva Linux Security Advisory : perl-XML-LibXML (MDVSA-2015:231)

Mandriva Linux Security Advisory : perl-YAML-LibYAML (MDVSA-2014:069)

Mandriva Linux Security Advisory : php (MDVSA-2008:126)

Mandriva Linux Security Advisory : php (MDVSA-2008:127)

Mandriva Linux Security Advisory : php (MDVSA-2008:128)

Mandriva Linux Security Advisory : php (MDVSA-2009:021)

Mandriva Linux Security Advisory : php (MDVSA-2009:022)

Mandriva Linux Security Advisory : php (MDVSA-2009:045)

Mandriva Linux Security Advisory : php (MDVSA-2009:066)

Mandriva Linux Security Advisory : php (MDVSA-2009:090)

Mandriva Linux Security Advisory : php (MDVSA-2009:145)

Mandriva Linux Security Advisory : php (MDVSA-2009:247)

Mandriva Linux Security Advisory : php (MDVSA-2009:248)

Mandriva Linux Security Advisory : php (MDVSA-2009:285)

Mandriva Linux Security Advisory : php (MDVSA-2009:302)

Mandriva Linux Security Advisory : php (MDVSA-2009:303)

Mandriva Linux Security Advisory : php (MDVSA-2009:304)

Mandriva Linux Security Advisory : php (MDVSA-2009:324)

Mandriva Linux Security Advisory : php (MDVSA-2010:008)

Mandriva Linux Security Advisory : php (MDVSA-2010:009)

Mandriva Linux Security Advisory : php (MDVSA-2010:045)

Mandriva Linux Security Advisory : php (MDVSA-2010:058)

Mandriva Linux Security Advisory : php (MDVSA-2010:068)

Mandriva Linux Security Advisory : php (MDVSA-2010:139)

Mandriva Linux Security Advisory : php (MDVSA-2010:140)

Mandriva Linux Security Advisory : php (MDVSA-2010:218)

Mandriva Linux Security Advisory : php (MDVSA-2010:224)

Mandriva Linux Security Advisory : php (MDVSA-2010:239)

Mandriva Linux Security Advisory : php (MDVSA-2010:254)

Mandriva Linux Security Advisory : php (MDVSA-2011:052)

Mandriva Linux Security Advisory : php (MDVSA-2011:053)

Mandriva Linux Security Advisory : php (MDVSA-2011:069)

Mandriva Linux Security Advisory : php (MDVSA-2011:165)

Mandriva Linux Security Advisory : php (MDVSA-2011:166)

Mandriva Linux Security Advisory : php (MDVSA-2011:197)

Mandriva Linux Security Advisory : php (MDVSA-2012:065)

Mandriva Linux Security Advisory : php (MDVSA-2012:068-1)

Mandriva Linux Security Advisory : php (MDVSA-2012:093)

Mandriva Linux Security Advisory : php (MDVSA-2012:108)

Mandriva Linux Security Advisory : php (MDVSA-2013:016)

Mandriva Linux Security Advisory : php (MDVSA-2013:114)

Mandriva Linux Security Advisory : php (MDVSA-2013:195)

Mandriva Linux Security Advisory : php (MDVSA-2013:221)

Mandriva Linux Security Advisory : php (MDVSA-2014:014)

Mandriva Linux Security Advisory : php (MDVSA-2014:027)

Mandriva Linux Security Advisory : php (MDVSA-2014:059)

Mandriva Linux Security Advisory : php (MDVSA-2014:075)

Mandriva Linux Security Advisory : php (MDVSA-2014:087)

Mandriva Linux Security Advisory : php (MDVSA-2014:115)

Mandriva Linux Security Advisory : php (MDVSA-2014:130)

Mandriva Linux Security Advisory : php (MDVSA-2014:149)

Mandriva Linux Security Advisory : php (MDVSA-2014:172)

Mandriva Linux Security Advisory : php (MDVSA-2014:202)

Mandriva Linux Security Advisory : php (MDVSA-2015:004)

Mandriva Linux Security Advisory : php (MDVSA-2015:032)

Mandriva Linux Security Advisory : php (MDVSA-2015:079)

Mandriva Linux Security Advisory : php (MDVSA-2015:080)

Mandriva Linux Security Advisory : php (MDVSA-2015:209)

Mandriva Linux Security Advisory : php-pear (MDVSA-2011:187)

Mandriva Linux Security Advisory : php-pear-Mail (MDVSA-2010:025)

Mandriva Linux Security Advisory : php-radius (MDVSA-2013:192)

Mandriva Linux Security Advisory : php-smarty (MDVSA-2009:052)

Mandriva Linux Security Advisory : php-smarty (MDVSA-2014:221)

Mandriva Linux Security Advisory : php-suhosin (MDVSA-2011:180)

Mandriva Linux Security Advisory : php-ZendFramework (MDVSA-2013:115)

Mandriva Linux Security Advisory : php-ZendFramework (MDVSA-2014:072)

Mandriva Linux Security Advisory : php-ZendFramework (MDVSA-2014:145)

Mandriva Linux Security Advisory : php-ZendFramework (MDVSA-2014:216)

Mandriva Linux Security Advisory : php-ZendFramework (MDVSA-2015:097)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2013:144)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2013:160)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2013:203)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:046)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:126)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:143)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:164)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:183)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:194)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:208)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:228)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2014:243)

Mandriva Linux Security Advisory : phpmyadmin (MDVSA-2015:186)

Mandriva Linux Security Advisory : pidgin (MDVSA-2008:143)

Mandriva Linux Security Advisory : pidgin (MDVSA-2009:025)

Mandriva Linux Security Advisory : pidgin (MDVSA-2009:147)

Mandriva Linux Security Advisory : pidgin (MDVSA-2009:230)

Mandriva Linux Security Advisory : pidgin (MDVSA-2009:321)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:001)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:002)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:041)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:085)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:097)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:148)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:208)

Mandriva Linux Security Advisory : pidgin (MDVSA-2010:259)

Mandriva Linux Security Advisory : pidgin (MDVSA-2011:050)

Mandriva Linux Security Advisory : pidgin (MDVSA-2011:132-1)

Mandriva Linux Security Advisory : pidgin (MDVSA-2011:183)

Mandriva Linux Security Advisory : pidgin (MDVSA-2012:029)

Mandriva Linux Security Advisory : pidgin (MDVSA-2012:082)

Mandriva Linux Security Advisory : pidgin (MDVSA-2012:105)

Mandriva Linux Security Advisory : pixman (MDVSA-2013:116)

Mandriva Linux Security Advisory : pixman (MDVSA-2013:302)

Mandriva Linux Security Advisory : pmake (MDVSA-2013:271)

Mandriva Linux Security Advisory : policykit (MDVSA-2008:087)

Mandriva Linux Security Advisory : polkit (MDVSA-2011:086)

Mandriva Linux Security Advisory : polkit (MDVSA-2013:243)

Mandriva Linux Security Advisory : poppler (MDVSA-2008:146)

Mandriva Linux Security Advisory : poppler (MDVSA-2009:068-1)

Mandriva Linux Security Advisory : poppler (MDVSA-2010:055)

Mandriva Linux Security Advisory : poppler (MDVSA-2010:230)

Mandriva Linux Security Advisory : poppler (MDVSA-2010:231)

Mandriva Linux Security Advisory : poppler (MDVSA-2013:143)

Mandriva Linux Security Advisory : poppler (MDVSA-2013:272)

Mandriva Linux Security Advisory : postfix (MDVSA-2008:171)

Mandriva Linux Security Advisory : postfix (MDVSA-2008:190)

Mandriva Linux Security Advisory : postfix (MDVSA-2009:224-1)

Mandriva Linux Security Advisory : postfix (MDVSA-2011:045)

Mandriva Linux Security Advisory : postfix (MDVSA-2011:090)

Mandriva Linux Security Advisory : postgresql (MDVSA-2008:004)

Mandriva Linux Security Advisory : postgresql (MDVSA-2009:079)

Mandriva Linux Security Advisory : postgresql (MDVSA-2009:333)

Mandriva Linux Security Advisory : postgresql (MDVSA-2010:103)

Mandriva Linux Security Advisory : postgresql (MDVSA-2010:197)

Mandriva Linux Security Advisory : postgresql (MDVSA-2011:021)

Mandriva Linux Security Advisory : postgresql (MDVSA-2011:161)

Mandriva Linux Security Advisory : postgresql (MDVSA-2012:026)

Mandriva Linux Security Advisory : postgresql (MDVSA-2012:092)

Mandriva Linux Security Advisory : postgresql (MDVSA-2012:139)

Mandriva Linux Security Advisory : postgresql (MDVSA-2013:012)

Mandriva Linux Security Advisory : postgresql (MDVSA-2013:142)

Mandriva Linux Security Advisory : postgresql (MDVSA-2014:047)

Mandriva Linux Security Advisory : postgresql (MDVSA-2015:048)

Mandriva Linux Security Advisory : postgresql (MDVSA-2015:110)

Mandriva Linux Security Advisory : postgresql8.2 (MDVSA-2009:251-1)

Mandriva Linux Security Advisory : ppp (MDVSA-2014:178)

Mandriva Linux Security Advisory : ppp (MDVSA-2015:135)

Mandriva Linux Security Advisory : ppp (MDVSA-2015:222)

Mandriva Linux Security Advisory : proftpd (MDVSA-2009:061)

Mandriva Linux Security Advisory : proftpd (MDVSA-2009:288)

Mandriva Linux Security Advisory : proftpd (MDVSA-2009:337)

Mandriva Linux Security Advisory : proftpd (MDVSA-2010:227)

Mandriva Linux Security Advisory : proftpd (MDVSA-2011:023)

Mandriva Linux Security Advisory : proftpd (MDVSA-2011:047)

Mandriva Linux Security Advisory : proftpd (MDVSA-2011:181)

Mandriva Linux Security Advisory : proftpd (MDVSA-2013:053)

Mandriva Linux Security Advisory : proftpd (MDVSA-2013:245)

Mandriva Linux Security Advisory : pulseaudio (MDVSA-2008:027)

Mandriva Linux Security Advisory : pulseaudio (MDVSA-2008:065)

Mandriva Linux Security Advisory : pulseaudio (MDVSA-2009:152)

Mandriva Linux Security Advisory : pulseaudio (MDVSA-2010:124)

Mandriva Linux Security Advisory : pulseaudio (MDVSA-2015:134)

Mandriva Linux Security Advisory : puppet (MDVSA-2013:186)

Mandriva Linux Security Advisory : puppet (MDVSA-2013:222)

Mandriva Linux Security Advisory : puppet (MDVSA-2014:040)

Mandriva Linux Security Advisory : pure-ftpd (MDVSA-2011:046)

Mandriva Linux Security Advisory : pure-ftpd (MDVSA-2011:094)

Mandriva Linux Security Advisory : pwgen (MDVSA-2015:008)

Mandriva Linux Security Advisory : pycrypto (MDVSA-2009:049-1)

Mandriva Linux Security Advisory : python (MDVSA-2008:013)

Mandriva Linux Security Advisory : python (MDVSA-2008:085)

Mandriva Linux Security Advisory : python (MDVSA-2008:163)

Mandriva Linux Security Advisory : python (MDVSA-2009:003)

Mandriva Linux Security Advisory : python (MDVSA-2009:212-1)

Mandriva Linux Security Advisory : python (MDVSA-2010:132)

Mandriva Linux Security Advisory : python (MDVSA-2010:215)

Mandriva Linux Security Advisory : python (MDVSA-2010:216)

Mandriva Linux Security Advisory : python (MDVSA-2011:096)

Mandriva Linux Security Advisory : python (MDVSA-2012:096)

Mandriva Linux Security Advisory : python (MDVSA-2012:097)

Mandriva Linux Security Advisory : python (MDVSA-2013:117)

Mandriva Linux Security Advisory : python (MDVSA-2013:214)

Mandriva Linux Security Advisory : python (MDVSA-2014:041)

Mandriva Linux Security Advisory : python (MDVSA-2014:074)

Mandriva Linux Security Advisory : python (MDVSA-2014:135)

Mandriva Linux Security Advisory : python (MDVSA-2014:197)

Mandriva Linux Security Advisory : python (MDVSA-2015:075)

Mandriva Linux Security Advisory : python-celementtree (MDVSA-2009:214)

Mandriva Linux Security Advisory : python-django (MDVSA-2008:185)

Mandriva Linux Security Advisory : python-django (MDVSA-2009:275)

Mandriva Linux Security Advisory : python-django (MDVSA-2009:276-1)

Mandriva Linux Security Advisory : python-django (MDVSA-2011:031)

Mandriva Linux Security Advisory : python-django (MDVSA-2012:143)

Mandriva Linux Security Advisory : python-django (MDVSA-2012:181)

Mandriva Linux Security Advisory : python-django (MDVSA-2013:234)

Mandriva Linux Security Advisory : python-django (MDVSA-2014:113)

Mandriva Linux Security Advisory : python-django (MDVSA-2014:179)

Mandriva Linux Security Advisory : python-django (MDVSA-2015:036)

Mandriva Linux Security Advisory : python-django (MDVSA-2015:109)

Mandriva Linux Security Advisory : python-django (MDVSA-2015:195)

Mandriva Linux Security Advisory : python-feedparser (MDVSA-2011:082)

Mandriva Linux Security Advisory : python-feedparser (MDVSA-2013:118)

Mandriva Linux Security Advisory : python-httplib2 (MDVSA-2013:119)

Mandriva Linux Security Advisory : python-httplib2 (MDVSA-2013:168)

Mandriva Linux Security Advisory : python-imaging (MDVSA-2014:082)

Mandriva Linux Security Advisory : python-imaging (MDVSA-2014:163)

Mandriva Linux Security Advisory : python-jinja2 (MDVSA-2014:096)

Mandriva Linux Security Advisory : python-lxml (MDVSA-2014:088)

Mandriva Linux Security Advisory : python-lxml (MDVSA-2015:112)

Mandriva Linux Security Advisory : python-numpy (MDVSA-2015:077)

Mandriva Linux Security Advisory : python-OpenSSL (MDVSA-2013:233)

Mandriva Linux Security Advisory : python-pillow (MDVSA-2015:099)

Mandriva Linux Security Advisory : python-pycrypto (MDVSA-2009:050-1)

Mandriva Linux Security Advisory : python-pycrypto (MDVSA-2012:117)

Mandriva Linux Security Advisory : python-pycrypto (MDVSA-2013:120)

Mandriva Linux Security Advisory : python-pycrypto (MDVSA-2013:262)

Mandriva Linux Security Advisory : python-requests (MDVSA-2015:133)

Mandriva Linux Security Advisory : python-setuptools (MDVSA-2013:227)

Mandriva Linux Security Advisory : python-sqlalchemy (MDVSA-2012:059)

Mandriva Linux Security Advisory : python3 (MDVSA-2015:076)

Mandriva Linux Security Advisory : qemu (MDVSA-2008:162)

Mandriva Linux Security Advisory : qemu (MDVSA-2009:008)

Mandriva Linux Security Advisory : qemu (MDVSA-2009:010)

Mandriva Linux Security Advisory : qemu (MDVSA-2009:257)

Mandriva Linux Security Advisory : qemu (MDVSA-2013:121)

Mandriva Linux Security Advisory : qemu (MDVSA-2014:220)

Mandriva Linux Security Advisory : qemu (MDVSA-2014:249)

Mandriva Linux Security Advisory : qemu (MDVSA-2015:061)

Mandriva Linux Security Advisory : qemu (MDVSA-2015:210)

Mandriva Linux Security Advisory : qt-creator (MDVSA-2010:193)

Mandriva Linux Security Advisory : qt4 (MDVSA-2008:042)

Mandriva Linux Security Advisory : qt4 (MDVSA-2009:225)

Mandriva Linux Security Advisory : qt4 (MDVSA-2011:074)

Mandriva Linux Security Advisory : quagga (MDVSA-2013:122)

Mandriva Linux Security Advisory : quagga (MDVSA-2013:254)

Mandriva Linux Security Advisory : R-base (MDVSA-2008:198)

Mandriva Linux Security Advisory : raptor (MDVSA-2012:061)

Mandriva Linux Security Advisory : rawtherapee (MDVSA-2014:098)

Mandriva Linux Security Advisory : rdesktop (MDVSA-2008:101)

Mandriva Linux Security Advisory : rdesktop (MDVSA-2011:102)

Mandriva Linux Security Advisory : readline (MDVSA-2014:154)

Mandriva Linux Security Advisory : readline (MDVSA-2015:132)

Mandriva Linux Security Advisory : rootcerts (MDVSA-2010:029)

Mandriva Linux Security Advisory : rootcerts (MDVSA-2010:032)

Mandriva Linux Security Advisory : rootcerts (MDVSA-2013:003)

Mandriva Linux Security Advisory : roundcubemail (MDVSA-2013:149)

Mandriva Linux Security Advisory : roundcubemail (MDVSA-2013:226)

Mandriva Linux Security Advisory : roundcubemail (MDVSA-2013:263)

Mandriva Linux Security Advisory : rpm (MDVSA-2010:180)

Mandriva Linux Security Advisory : rpm (MDVSA-2011:143)

Mandriva Linux Security Advisory : rpm (MDVSA-2012:056)

Mandriva Linux Security Advisory : rpm (MDVSA-2014:251)

Mandriva Linux Security Advisory : rpm (MDVSA-2015:056)

Mandriva Linux Security Advisory : rpmdevtools (MDVSA-2013:123)

Mandriva Linux Security Advisory : rsh (MDVSA-2008:191)

Mandriva Linux Security Advisory : rsync (MDVSA-2008:011)

Mandriva Linux Security Advisory : rsync (MDVSA-2008:084)

Mandriva Linux Security Advisory : rsync (MDVSA-2011:066)

Mandriva Linux Security Advisory : rsync (MDVSA-2015:131)

Mandriva Linux Security Advisory : rsyslog (MDVSA-2011:134-1)

Mandriva Linux Security Advisory : rsyslog (MDVSA-2012:100)

Mandriva Linux Security Advisory : rsyslog (MDVSA-2014:196)

Mandriva Linux Security Advisory : rsyslog (MDVSA-2015:130)

Mandriva Linux Security Advisory : ruby (MDVSA-2008:029)

Mandriva Linux Security Advisory : ruby (MDVSA-2008:140)

Mandriva Linux Security Advisory : ruby (MDVSA-2008:141)

Mandriva Linux Security Advisory : ruby (MDVSA-2008:226)

Mandriva Linux Security Advisory : ruby (MDVSA-2009:160)

Mandriva Linux Security Advisory : ruby (MDVSA-2009:193)

Mandriva Linux Security Advisory : ruby (MDVSA-2009:325)

Mandriva Linux Security Advisory : ruby (MDVSA-2010:017)

Mandriva Linux Security Advisory : ruby (MDVSA-2011:097)

Mandriva Linux Security Advisory : ruby (MDVSA-2012:024)

Mandriva Linux Security Advisory : ruby (MDVSA-2013:124)

Mandriva Linux Security Advisory : ruby (MDVSA-2013:201)

Mandriva Linux Security Advisory : ruby (MDVSA-2013:286)

Mandriva Linux Security Advisory : ruby (MDVSA-2014:225)

Mandriva Linux Security Advisory : ruby (MDVSA-2015:129)

Mandriva Linux Security Advisory : ruby (MDVSA-2015:224)

Mandriva Linux Security Advisory : ruby-gnome2 (MDVSA-2008:033)

Mandriva Linux Security Advisory : rxvt (MDVSA-2008:161)

Mandriva Linux Security Advisory : rxvt-unicode (MDVSA-2014:094)

Mandriva Linux Security Advisory : samba (MDVSA-2008:108)

Mandriva Linux Security Advisory : samba (MDVSA-2009:042)

Mandriva Linux Security Advisory : samba (MDVSA-2009:196)

Mandriva Linux Security Advisory : samba (MDVSA-2009:277)

Mandriva Linux Security Advisory : samba (MDVSA-2009:320)

Mandriva Linux Security Advisory : samba (MDVSA-2010:090-1)

Mandriva Linux Security Advisory : samba (MDVSA-2010:119)

Mandriva Linux Security Advisory : samba (MDVSA-2010:141)

Mandriva Linux Security Advisory : samba (MDVSA-2010:184)

Mandriva Linux Security Advisory : samba (MDVSA-2011:038)

Mandriva Linux Security Advisory : samba (MDVSA-2011:121)

Mandriva Linux Security Advisory : samba (MDVSA-2011:148)

Mandriva Linux Security Advisory : samba (MDVSA-2012:055)

Mandriva Linux Security Advisory : samba (MDVSA-2012:067)

Mandriva Linux Security Advisory : samba (MDVSA-2012:070)

Mandriva Linux Security Advisory : samba (MDVSA-2013:011)

Mandriva Linux Security Advisory : samba (MDVSA-2013:207)

Mandriva Linux Security Advisory : samba (MDVSA-2013:278)

Mandriva Linux Security Advisory : samba (MDVSA-2013:299)

Mandriva Linux Security Advisory : samba (MDVSA-2014:136)

Mandriva Linux Security Advisory : samba (MDVSA-2015:081)

Mandriva Linux Security Advisory : samba (MDVSA-2015:082)

Mandriva Linux Security Advisory : samba4 (MDVSA-2015:083)

Mandriva Linux Security Advisory : sarg (MDVSA-2008:079)

Mandriva Linux Security Advisory : sarg (MDVSA-2009:073)

Mandriva Linux Security Advisory : SDL\_image (MDVSA-2008:040)

Mandriva Linux Security Advisory : sendmail (MDVSA-2010:003)

Mandriva Linux Security Advisory : sendmail (MDVSA-2014:147)

Mandriva Linux Security Advisory : sendmail (MDVSA-2015:128)

Mandriva Linux Security Advisory : serf (MDVSA-2014:166)

Mandriva Linux Security Advisory : serf (MDVSA-2015:127)

Mandriva Linux Security Advisory : setup (MDVSA-2015:184)

Mandriva Linux Security Advisory : setup (MDVSA-2015:208)

Mandriva Linux Security Advisory : shadow-utils (MDVSA-2009:062)

Mandriva Linux Security Advisory : silc-toolkit (MDVSA-2008:158)

Mandriva Linux Security Advisory : silc-toolkit (MDVSA-2009:234-2)

Mandriva Linux Security Advisory : silc-toolkit (MDVSA-2009:235)

Mandriva Linux Security Advisory : sleuthkit (MDVSA-2013:125)

Mandriva Linux Security Advisory : snack (MDVSA-2013:126)

Mandriva Linux Security Advisory : snort (MDVSA-2009:259-1)

Mandriva Linux Security Advisory : socat (MDVSA-2013:127)

Mandriva Linux Security Advisory : socat (MDVSA-2013:170)

Mandriva Linux Security Advisory : socat (MDVSA-2014:033)

Mandriva Linux Security Advisory : sox (MDVSA-2015:015)

Mandriva Linux Security Advisory : speex (MDVSA-2008:094)

Mandriva Linux Security Advisory : spice (MDVSA-2013:217)

Mandriva Linux Security Advisory : spice (MDVSA-2014:016)

Mandriva Linux Security Advisory : sqlite3 (MDVSA-2015:217)

Mandriva Linux Security Advisory : squashfs-tools (MDVSA-2013:128)

Mandriva Linux Security Advisory : squid (MDVSA-2008:002)

Mandriva Linux Security Advisory : squid (MDVSA-2008:134)

Mandriva Linux Security Advisory : squid (MDVSA-2009:034)

Mandriva Linux Security Advisory : squid (MDVSA-2009:161-1)

Mandriva Linux Security Advisory : squid (MDVSA-2009:241-1)

Mandriva Linux Security Advisory : squid (MDVSA-2010:033)

Mandriva Linux Security Advisory : squid (MDVSA-2010:060)

Mandriva Linux Security Advisory : squid (MDVSA-2010:187)

Mandriva Linux Security Advisory : squid (MDVSA-2011:150)

Mandriva Linux Security Advisory : squid (MDVSA-2011:193)

Mandriva Linux Security Advisory : squid (MDVSA-2013:013)

Mandriva Linux Security Advisory : squid (MDVSA-2013:129)

Mandriva Linux Security Advisory : squid (MDVSA-2013:199)

Mandriva Linux Security Advisory : squid (MDVSA-2014:114)

Mandriva Linux Security Advisory : squid (MDVSA-2014:177)

Mandriva Linux Security Advisory : squid (MDVSA-2015:103)

Mandriva Linux Security Advisory : squid (MDVSA-2015:230)

Mandriva Linux Security Advisory : squidGuard (MDVSA-2009:293-1)

Mandriva Linux Security Advisory : srtp (MDVSA-2014:219)

Mandriva Linux Security Advisory : struts (MDVSA-2014:095)

Mandriva Linux Security Advisory : stunnel (MDVSA-2008:168)

Mandriva Linux Security Advisory : stunnel (MDVSA-2013:130)

Mandriva Linux Security Advisory : stunnel (MDVSA-2015:096)

Mandriva Linux Security Advisory : subversion (MDVSA-2009:199-1)

Mandriva Linux Security Advisory : subversion (MDVSA-2010:199)

Mandriva Linux Security Advisory : subversion (MDVSA-2011:006)

Mandriva Linux Security Advisory : subversion (MDVSA-2011:067)

Mandriva Linux Security Advisory : subversion (MDVSA-2011:106)

Mandriva Linux Security Advisory : subversion (MDVSA-2013:153)

Mandriva Linux Security Advisory : subversion (MDVSA-2013:173)

Mandriva Linux Security Advisory : subversion (MDVSA-2013:209)

Mandriva Linux Security Advisory : subversion (MDVSA-2013:236)

Mandriva Linux Security Advisory : subversion (MDVSA-2013:288)

Mandriva Linux Security Advisory : subversion (MDVSA-2014:049)

Mandriva Linux Security Advisory : subversion (MDVSA-2014:161)

Mandriva Linux Security Advisory : subversion (MDVSA-2015:005)

Mandriva Linux Security Advisory : subversion (MDVSA-2015:085)

Mandriva Linux Security Advisory : subversion (MDVSA-2015:192)

Mandriva Linux Security Advisory : sudo (MDVSA-2009:033)

Mandriva Linux Security Advisory : sudo (MDVSA-2010:049)

Mandriva Linux Security Advisory : sudo (MDVSA-2010:052)

Mandriva Linux Security Advisory : sudo (MDVSA-2010:078-1)

Mandriva Linux Security Advisory : sudo (MDVSA-2010:118)

Mandriva Linux Security Advisory : sudo (MDVSA-2010:175)

Mandriva Linux Security Advisory : sudo (MDVSA-2011:018)

Mandriva Linux Security Advisory : sudo (MDVSA-2012:079)

Mandriva Linux Security Advisory : sudo (MDVSA-2013:054)

Mandriva Linux Security Advisory : sudo (MDVSA-2015:126)

Mandriva Linux Security Advisory : sympa (MDVSA-2009:263)

Mandriva Linux Security Advisory : sympa (MDVSA-2015:051)

Mandriva Linux Security Advisory : systemd (MDVSA-2012:030)

Mandriva Linux Security Advisory : systemtap (MDVSA-2011:154)

Mandriva Linux Security Advisory : systemtap (MDVSA-2011:155)

Mandriva Linux Security Advisory : t1lib (MDVSA-2011:016)

Mandriva Linux Security Advisory : t1lib (MDVSA-2012:002)

Mandriva Linux Security Advisory : t1lib (MDVSA-2012:004)

Mandriva Linux Security Advisory : t1utils (MDVSA-2015:215)

Mandriva Linux Security Advisory : taglib (MDVSA-2013:131)

Mandriva Linux Security Advisory : tcl (MDVSA-2008:059)

Mandriva Linux Security Advisory : tcpdump (MDVSA-2014:240)

Mandriva Linux Security Advisory : tcpdump (MDVSA-2015:125)

Mandriva Linux Security Advisory : tcpdump (MDVSA-2015:182)

Mandriva Linux Security Advisory : tetex (MDVSA-2010:094)

Mandriva Linux Security Advisory : tetex (MDVSA-2011:017)

Mandriva Linux Security Advisory : tk (MDVSA-2008:041)

Mandriva Linux Security Advisory : tomboy (MDVSA-2008:064)

Mandriva Linux Security Advisory : tomboy (MDVSA-2011:035)

Mandriva Linux Security Advisory : tomcat (MDVSA-2015:052)

Mandriva Linux Security Advisory : tomcat (MDVSA-2015:084)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2008:188)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2009:018)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2009:136)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2009:138)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2010:176)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2010:177)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2011:030)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2011:156)

Mandriva Linux Security Advisory : tomcat5 (MDVSA-2012:085)

Mandriva Linux Security Advisory : tomcat6 (MDVSA-2014:042)

Mandriva Linux Security Advisory : tomcat6 (MDVSA-2015:053)

Mandriva Linux Security Advisory : tor (MDVSA-2013:132)

Mandriva Linux Security Advisory : tor (MDVSA-2014:123)

Mandriva Linux Security Advisory : tor (MDVSA-2014:150)

Mandriva Linux Security Advisory : tor (MDVSA-2015:189)

Mandriva Linux Security Advisory : tor (MDVSA-2015:205)

Mandriva Linux Security Advisory : torque (MDVSA-2013:252)

Mandriva Linux Security Advisory : torque (MDVSA-2013:268)

Mandriva Linux Security Advisory : torque (MDVSA-2015:124)

Mandriva Linux Security Advisory : transmission (MDVSA-2010:013)

Mandriva Linux Security Advisory : transmission (MDVSA-2010:014)

Mandriva Linux Security Advisory : udev (MDVSA-2009:103-1)

Mandriva Linux Security Advisory : udisks (MDVSA-2014:064)

Mandriva Linux Security Advisory : udisks2 (MDVSA-2015:088)

Mandriva Linux Security Advisory : unrtf (MDVSA-2015:007)

Mandriva Linux Security Advisory : untrf (MDVSA-2015:026)

Mandriva Linux Security Advisory : unzip (MDVSA-2008:068)

Mandriva Linux Security Advisory : unzip (MDVSA-2015:016)

Mandriva Linux Security Advisory : unzip (MDVSA-2015:123)

Mandriva Linux Security Advisory : usbmuxd (MDVSA-2012:133)

Mandriva Linux Security Advisory : usbmuxd (MDVSA-2013:133)

Mandriva Linux Security Advisory : util-linux (MDVSA-2012:083)

Mandriva Linux Security Advisory : util-linux (MDVSA-2013:154)

Mandriva Linux Security Advisory : util-linux (MDVSA-2015:122)

Mandriva Linux Security Advisory : util-linux-ng (MDVSA-2008:114)

Mandriva Linux Security Advisory : valgrind (MDVSA-2009:057)

Mandriva Linux Security Advisory : varnish (MDVSA-2014:036)

Mandriva Linux Security Advisory : viewvc (MDVSA-2013:134)

Mandriva Linux Security Advisory : vim (MDVSA-2008:236-1)

Mandriva Linux Security Advisory : vim (MDVSA-2009:047-1)

Mandriva Linux Security Advisory : vinagre (MDVSA-2008:240)

Mandriva Linux Security Advisory : vino (MDVSA-2011:087)

Mandriva Linux Security Advisory : virtualbox (MDVSA-2009:011)

Mandriva Linux Security Advisory : virtualbox (MDVSA-2010:059)

Mandriva Linux Security Advisory : vorbis-tools (MDVSA-2008:093)

Mandriva Linux Security Advisory : vorbis-tools (MDVSA-2015:037)

Mandriva Linux Security Advisory : vsftpd (MDVSA-2011:049)

Mandriva Linux Security Advisory : vte (MDVSA-2010:161)

Mandriva Linux Security Advisory : vte (MDVSA-2013:135)

Mandriva Linux Security Advisory : w3c-libwww (MDVSA-2009:218-1)

Mandriva Linux Security Advisory : webkit (MDVSA-2011:039)

Mandriva Linux Security Advisory : webmin (MDVSA-2010:036)

Mandriva Linux Security Advisory : webmin (MDVSA-2011:109)

Mandriva Linux Security Advisory : webmin (MDVSA-2014:062)

Mandriva Linux Security Advisory : weechat (MDVSA-2013:136)

Mandriva Linux Security Advisory : wget (MDVSA-2009:206-1)

Mandriva Linux Security Advisory : wget (MDVSA-2010:170)

Mandriva Linux Security Advisory : wget (MDVSA-2014:212)

Mandriva Linux Security Advisory : wget (MDVSA-2015:121)

Mandriva Linux Security Advisory : wireshark (MDVSA-2008:001-1)

Mandriva Linux Security Advisory : wireshark (MDVSA-2008:057)

Mandriva Linux Security Advisory : wireshark (MDVSA-2008:091)

Mandriva Linux Security Advisory : wireshark (MDVSA-2008:152)

Mandriva Linux Security Advisory : wireshark (MDVSA-2008:199)

Mandriva Linux Security Advisory : wireshark (MDVSA-2008:215)

Mandriva Linux Security Advisory : wireshark (MDVSA-2008:242)

Mandriva Linux Security Advisory : wireshark (MDVSA-2009:058)

Mandriva Linux Security Advisory : wireshark (MDVSA-2009:088)

Mandriva Linux Security Advisory : wireshark (MDVSA-2009:125)

Mandriva Linux Security Advisory : wireshark (MDVSA-2009:194)

Mandriva Linux Security Advisory : wireshark (MDVSA-2009:270)

Mandriva Linux Security Advisory : wireshark (MDVSA-2009:292-1)

Mandriva Linux Security Advisory : wireshark (MDVSA-2010:016)

Mandriva Linux Security Advisory : wireshark (MDVSA-2010:031)

Mandriva Linux Security Advisory : wireshark (MDVSA-2010:099)

Mandriva Linux Security Advisory : wireshark (MDVSA-2010:113)

Mandriva Linux Security Advisory : wireshark (MDVSA-2010:144)

Mandriva Linux Security Advisory : wireshark (MDVSA-2010:200)

Mandriva Linux Security Advisory : wireshark (MDVSA-2010:242)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:002)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:007)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:044)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:083)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:105)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:118)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:138)

Mandriva Linux Security Advisory : wireshark (MDVSA-2011:164)

Mandriva Linux Security Advisory : wireshark (MDVSA-2012:015)

Mandriva Linux Security Advisory : wireshark (MDVSA-2012:042)

Mandriva Linux Security Advisory : wireshark (MDVSA-2012:080)

Mandriva Linux Security Advisory : wireshark (MDVSA-2012:125)

Mandriva Linux Security Advisory : wireshark (MDVSA-2012:134)

Mandriva Linux Security Advisory : wireshark (MDVSA-2013:055)

Mandriva Linux Security Advisory : wireshark (MDVSA-2013:172)

Mandriva Linux Security Advisory : wireshark (MDVSA-2013:204)

Mandriva Linux Security Advisory : wireshark (MDVSA-2013:238)

Mandriva Linux Security Advisory : wireshark (MDVSA-2013:279)

Mandriva Linux Security Advisory : wireshark (MDVSA-2013:296)

Mandriva Linux Security Advisory : wireshark (MDVSA-2014:050)

Mandriva Linux Security Advisory : wireshark (MDVSA-2014:159)

Mandriva Linux Security Advisory : wireshark (MDVSA-2014:188)

Mandriva Linux Security Advisory : wireshark (MDVSA-2014:223)

Mandriva Linux Security Advisory : wireshark (MDVSA-2015:022)

Mandriva Linux Security Advisory : wireshark (MDVSA-2015:183)

Mandriva Linux Security Advisory : wml (MDVSA-2008:076)

Mandriva Linux Security Advisory : wordnet (MDVSA-2008:182-1)

Mandriva Linux Security Advisory : wordpress (MDVSA-2013:137)

Mandriva Linux Security Advisory : wordpress (MDVSA-2013:189)

Mandriva Linux Security Advisory : wordpress (MDVSA-2013:239)

Mandriva Linux Security Advisory : wordpress (MDVSA-2014:103)

Mandriva Linux Security Advisory : wordpress (MDVSA-2014:233)

Mandriva Linux Security Advisory : wpa\_supplicant (MDVSA-2014:211)

Mandriva Linux Security Advisory : wpa\_supplicant (MDVSA-2015:120)

Mandriva Linux Security Advisory : wxgtk (MDVSA-2009:204)

Mandriva Linux Security Advisory : wxgtk (MDVSA-2009:213-1)

Mandriva Linux Security Advisory : x11-driver-video-qxl (MDVSA-2013:138)

Mandriva Linux Security Advisory : x11-server (MDVSA-2008:023)

Mandriva Linux Security Advisory : x11-server (MDVSA-2008:116)

Mandriva Linux Security Advisory : x11-server (MDVSA-2013:139)

Mandriva Linux Security Advisory : x11-server (MDVSA-2013:259)

Mandriva Linux Security Advisory : x11-server (MDVSA-2014:020)

Mandriva Linux Security Advisory : x11-server (MDVSA-2015:119)

Mandriva Linux Security Advisory : x11-server-xgl (MDVSA-2008:025)

Mandriva Linux Security Advisory : x2goserver (MDVSA-2014:063)

Mandriva Linux Security Advisory : xchat (MDVSA-2009:059-1)

Mandriva Linux Security Advisory : xdg-utils (MDVSA-2008:031)

Mandriva Linux Security Advisory : xerces-c (MDVSA-2009:223-1)

Mandriva Linux Security Advisory : xerces-j2 (MDVSA-2011:108)

Mandriva Linux Security Advisory : xerces-j2 (MDVSA-2014:193)

Mandriva Linux Security Advisory : xfig (MDVSA-2009:244-1)

Mandriva Linux Security Advisory : xfig (MDVSA-2011:010)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2008:020)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2008:046-1)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2008:124)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2008:177)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2008:178)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2009:020)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2009:299)

Mandriva Linux Security Advisory : xine-lib (MDVSA-2009:319)

Mandriva Linux Security Advisory : xinetd (MDVSA-2012:155-1)

Mandriva Linux Security Advisory : xinetd (MDVSA-2013:057)

Mandriva Linux Security Advisory : xinetd (MDVSA-2013:248)

Mandriva Linux Security Advisory : xlockmore (MDVSA-2015:118)

Mandriva Linux Security Advisory : xmlsec1 (MDVSA-2009:267)

Mandriva Linux Security Advisory : xmlsec1 (MDVSA-2009:318)

Mandriva Linux Security Advisory : xmlsec1 (MDVSA-2011:063)

Mandriva Linux Security Advisory : xpdf (MDVSA-2009:101)

Mandriva Linux Security Advisory : xpdf (MDVSA-2009:287-1)

Mandriva Linux Security Advisory : xpdf (MDVSA-2010:228)

Mandriva Linux Security Advisory : xrdb (MDVSA-2011:076)

Mandriva Linux Security Advisory : xterm (MDVSA-2009:005)

Mandriva Linux Security Advisory : xulrunner (MDVSA-2010:213)

Mandriva Linux Security Advisory : xymon (MDVSA-2013:213)

Mandriva Linux Security Advisory : yaml (MDVSA-2014:034)

Mandriva Linux Security Advisory : yaml (MDVSA-2014:071)

Mandriva Linux Security Advisory : yaml (MDVSA-2014:242)

Mandriva Linux Security Advisory : yaml (MDVSA-2015:060)

Mandriva Linux Security Advisory : yelp (MDVSA-2008:175)

Mandriva Linux Security Advisory : zarafa (MDVSA-2014:044)

Mandriva Linux Security Advisory : zarafa (MDVSA-2014:182)

Mandriva Linux Security Advisory : zarafa (MDVSA-2015:040)

Mandriva Linux Security Advisory : znc (MDVSA-2015:013)

Mandriva Linux Security Advisory : zsh (MDVSA-2009:108-1)

MDVA-2008:001 : urpmi

MDVA-2008:002 : drakx-net

MDVA-2008:003 : dosfstools

MDVA-2008:004 : timezone

MDVA-2008:006 : openafs

MDVA-2008:006-1 : openafs

MDVA-2008:007 : e2fsprogs

MDVA-2008:007-1 : e2fsprogs

MDVA-2008:008 : kdetoys

MDVA-2008:009 : rpmdrake

MDVA-2008:010 : vorbis-tools

MDVA-2008:011 : kdelibs

MDVA-2008:012 : lzma

MDVA-2008:013 : skencil

MDVA-2008:014 : isdn4k-utils

MDVA-2008:015 : kdelibs

MDVA-2008:016 : kdebase

MDVA-2008:017 : php-timezonedb

MDVA-2008:018 : mysql

MDVA-2008:020 : drakbt

MDVA-2008:021 : gcc

MDVA-2008:022 : x11-data-xkbdata

MDVA-2008:023 : x11-driver-video-via

MDVA-2008:024 : rpmdrake

MDVA-2008:025 : drakxtools

MDVA-2008:026 : desktop-common-data

MDVA-2008:027 : mandriva-kde-config

MDVA-2008:028 : psad

MDVA-2008:029 : evolution

MDVA-2008:030 : kdelibs

MDVA-2008:031 : x11-driver-video-openchrome

MDVA-2008:032 : fluxbox

MDVA-2008:032-1 : fluxbox

MDVA-2008:033 : rpmdrake

MDVA-2008:035 : drakconf

MDVA-2008:036 : timezone

MDVA-2008:037 : pdksh

MDVA-2008:038 : kdepim

MDVA-2008:039 : kdeutils

MDVA-2008:040 : monitor-edid

MDVA-2008:041 : webmin

MDVA-2008:042 : rpmdrake

MDVA-2008:043 : timezone

MDVA-2008:044 : giftrans

MDVA-2008:045 : drakbt

MDVA-2008:046 : kdeutils

MDVA-2008:047 : laptop-mode-tools

MDVA-2008:048 : x11-driver-video

MDVA-2008:049 : drakxtools

MDVA-2008:050 : x11-driver-video-mga

MDVA-2008:051 : silc-toolkit

MDVA-2008:052 : mesa

MDVA-2008:053 : notification-daemon

MDVA-2008:054 : freeradius

MDVA-2008:055 : xkeyboard-config

MDVA-2008:056 : rhythmbox

MDVA-2008:057 : wine

MDVA-2008:058 : drakx-net

MDVA-2008:059 : drakx-kbd-mouse-x11

MDVA-2008:060 : hal-info

MDVA-2008:061 : rpmdrake

MDVA-2008:062 : drakxtools

MDVA-2008:063 : rpmdrake

MDVA-2008:064 : draksnapshot

MDVA-2008:065 : iproute2

MDVA-2008:066 : xinitrc

MDVA-2008:067 : ksplash-engine-moodin

MDVA-2008:068 : mandriva-kde-config

MDVA-2008:069 : initscripts

MDVA-2008:070 : dkms

MDVA-2008:071 : nfs-utils

MDVA-2008:072 : x11-server

MDVA-2008:073 : hal-info

MDVA-2008:074 : drakxtools

MDVA-2008:075 : drakconf

MDVA-2008:076 : krandr

MDVA-2008:077 : gnome-settings-daemon

MDVA-2008:078 : kdebase

MDVA-2008:079 : kdegraphics

MDVA-2008:080 : gnome-themes-extras

MDVA-2008:081 : mandriva-kde-config

MDVA-2008:082 : timezone

MDVA-2008:082-1 : timezone

MDVA-2008:083 : GConf2

MDVA-2008:084 : udev

MDVA-2008:085 : initscripts

MDVA-2008:086 : drakxtools

MDVA-2008:087 : ppp

MDVA-2008:088 : drakx-net

MDVA-2008:089 : wireshark

MDVA-2008:090 : nautilus

MDVA-2008:091 : gnome-panel

MDVA-2008:091-1 : gnome-applets

MDVA-2008:092 : python-sip

MDVA-2008:093 : kdesdk

MDVA-2008:093-1 : kdesdk

MDVA-2008:094 : cairo

MDVA-2008:095 : rsh

MDVA-2008:096 : ntfs-3g

MDVA-2008:097 : beagle

MDVA-2008:098 : gnome-session

MDVA-2008:099 : swi-prolog

MDVA-2008:100 : libgnomeui2

MDVA-2008:101 : evince

MDVA-2008:102 : mkinitrd

MDVA-2008:103 : pidgin

MDVA-2008:104 : x11-driver-input-evdev

MDVA-2008:105 : locales

MDVA-2008:106 : openoffice.org-voikko

MDVA-2008:106-1 : openoffice.org-voikko

MDVA-2008:107 : myspell-dictionaries

MDVA-2008:108 : x11-server

MDVA-2008:109 : timezone

MDVA-2008:110 : pulseaudio

MDVA-2008:111 : dbus

MDVA-2008:112 : kino

MDVA-2008:113 : beagle

MDVA-2008:114 : audacity

MDVA-2008:115 : drakxtools

MDVA-2008:116 : initscripts

MDVA-2008:117 : x11-server

MDVA-2008:118 : shared-mime-info

MDVA-2008:119 : timezone

MDVA-2008:120 : draksnapshot

MDVA-2008:121 : blt

MDVA-2008:122 : vpnc

MDVA-2008:123 : rpmdrake

MDVA-2008:123-1 : rpmdrake

MDVA-2008:124 : rpmdrake

MDVA-2008:125 : bash-completion

MDVA-2008:126 : x11-server

MDVA-2008:127 : x11-driver-video-ati

MDVA-2008:128 : xdm

MDVA-2008:129 : apache-conf

MDVA-2008:130 : drakxtools

MDVA-2008:131 : rpmdrake

MDVA-2008:132 : mandriva-release

MDVA-2008:133 : timezone

MDVA-2008:134 : rpm

MDVA-2008:135 : draksnapshot

MDVA-2008:135-1 : draksnapshot

MDVA-2008:136 : urpmi

MDVA-2008:137 : drakxtools

MDVA-2008:138 : mdkonline

MDVA-2008:139 : lirc

MDVA-2008:140 : symlinks

MDVA-2008:141 : mdkonline

MDVA-2008:142 : gdb

MDVA-2008:143 : x11-driver-video-intel

MDVA-2008:145 : opensc

MDVA-2008:146 : kdegames4

MDVA-2008:147 : rhythmbox

MDVA-2008:148 : pulseaudio

MDVA-2008:149 : drakx-net

MDVA-2008:150 : banshee

MDVA-2008:151 : timezone

MDVA-2008:152 : totem-pl-parser

MDVA-2008:153 : phonon

MDVA-2008:154 : util-linux-ng

MDVA-2008:155 : kdebase4-runtime

MDVA-2008:156 : kdebase4-workspace

MDVA-2008:156-1 : kdebase4-workspace

MDVA-2008:157 : hplip

MDVA-2008:159 : curl

MDVA-2008:160 : mandriva-doc

MDVA-2008:161 : beagle

MDVA-2008:162 : openoffice.org

MDVA-2008:163 : mdkonline

MDVA-2008:164 : rpm

MDVA-2008:165 : gnome-power-manager

MDVA-2008:166 : openafs

MDVA-2008:167 : libtool

MDVA-2008:168 : sound-scripts

MDVA-2008:169 : f-spot

MDVA-2008:170 : alsa-plugins

MDVA-2008:171 : gdm

MDVA-2008:172 : kdebase

MDVA-2008:173 : imwheel

MDVA-2008:174 : kbd

MDVA-2008:175 : urpmi

MDVA-2008:176 : mdadm

MDVA-2008:177 : lirc

MDVA-2008:178 : openvpn

MDVA-2008:179 : graphviz

MDVA-2008:180 : cracklib

MDVA-2008:181 : gstreamer0.10-plugins-ugly

MDVA-2008:182 : evince

MDVA-2008:183 : live

MDVA-2008:184 : kdevelop

MDVA-2008:185 : kde4

MDVA-2008:186 : evolution

MDVA-2008:186-1 : evolution

MDVA-2008:187 : evolution

MDVA-2008:188 : kdewebdev4

MDVA-2008:189 : bluez-utils

MDVA-2008:190 : drakx-net

MDVA-2008:191 : enchant

MDVA-2008:192 : mandriva-release

MDVA-2008:193 : kernel-headers

MDVA-2008:194 : metisse

MDVA-2008:195 : timezone

MDVA-2008:196 : nasm

MDVA-2008:197 : mandriva-kde-config

MDVA-2008:198 : openoffice.org

MDVA-2008:199 : kde4-splash-mdv

MDVA-2008:200 : jackit

MDVA-2008:201 : mdkonline

MDVA-2008:202 : drakx-net

MDVA-2009:001 : dos2unix

MDVA-2009:001-1 : dos2unix

MDVA-2009:002 : msec

MDVA-2009:003 : draksnapshot

MDVA-2009:004 : rpmdrake

MDVA-2009:005 : x11-server

MDVA-2009:006 : xen

MDVA-2009:008 : amarok

MDVA-2009:009 : kdemultimedia

MDVA-2009:010 : bind

MDVA-2009:011 : kdegraphics4

MDVA-2009:012 : kphotoalbum

MDVA-2009:013 : phonon

MDVA-2009:014 : drak3d

MDVA-2009:015 : openct

MDVA-2009:016 : at

MDVA-2009:017 : glibc

MDVA-2009:018 : clamav

MDVA-2009:018-1 : clamav

MDVA-2009:019 : glibc

MDVA-2009:020 : rhythmbox

MDVA-2009:021 : drakxtools

MDVA-2009:022 : xkeyboard-config

MDVA-2009:023 : db46

MDVA-2009:024 : totem

MDVA-2009:025 : keyutils

MDVA-2009:025-1 : keyutils

MDVA-2009:026 : samba

MDVA-2009:026-1 : samba

MDVA-2009:027 : kernel

MDVA-2009:031 : drakx-net

MDVA-2009:032 : eclipse

MDVA-2009:032-1 : eclipse

MDVA-2009:033 : tomboy

MDVA-2009:034 : alsa

MDVA-2009:036 : postfix

MDVA-2009:037 : php-ssh2

MDVA-2009:038 : nspluginwrapper

MDVA-2009:039 : coreutils

MDVA-2009:040 : libdvdread

MDVA-2009:041 : php

MDVA-2009:042 : rpmdrake

MDVA-2009:043 : module-init-tools

MDVA-2009:044 : module-init-tools

MDVA-2009:045 : dhcp

MDVA-2009:046 : pidgin

MDVA-2009:047 : drakconf

MDVA-2009:048 : evolution

MDVA-2009:049 : mdkonline

MDVA-2009:050 : libtommath

MDVA-2009:051 : perl-Crypt-SSLeay

MDVA-2009:053 : ldetect

MDVA-2009:054 : iproute2

MDVA-2009:055 : webmin

MDVA-2009:056 : x11-driver-video-intel

MDVA-2009:057 : usermode

MDVA-2009:058 : SDL12

MDVA-2009:059 : drakx-net

MDVA-2009:060 : initscripts

MDVA-2009:061 : portreserve

MDVA-2009:062 : bash

MDVA-2009:063 : mdkonline

MDVA-2009:064 : openoffice.org-voikko

MDVA-2009:065 : nasm

MDVA-2009:066 : perl-URPM

MDVA-2009:067 : drakxtools

MDVA-2009:068 : x11-driver-video-sisimedia

MDVA-2009:069 : x11-server

MDVA-2009:070 : x11-driver-video-ati

MDVA-2009:071 : podsleuth

MDVA-2009:072 : shared-mime-info

MDVA-2009:073 : amarok

MDVA-2009:074 : x11-server

MDVA-2009:075 : pidgin

MDVA-2009:076 : kdelibs

MDVA-2009:076-1 : kdelibs

MDVA-2009:077 : kdevelop

MDVA-2009:078 : rpmdrake

MDVA-2009:079 : drakguard

MDVA-2009:080 : strace

MDVA-2009:081 : x11-server

MDVA-2009:082 : quassel

MDVA-2009:083 : armagetron

MDVA-2009:084 : x11-driver-video-intel

MDVA-2009:085 : mesa

MDVA-2009:086 : sudo

MDVA-2009:087 : mandriva-kde4-config

MDVA-2009:088 : rpmdrake

MDVA-2009:090 : mkinitrd

MDVA-2009:091 : gedit-plugins

MDVA-2009:092 : codeina

MDVA-2009:093 : ipset

MDVA-2009:094 : dansguardian

MDVA-2009:095 : apache

MDVA-2009:096 : perl-MDK-Common

MDVA-2009:097 : drakx-net

MDVA-2009:098 : drakx-net

MDVA-2009:099 : ntp

MDVA-2009:100 : clamav

MDVA-2009:101 : urpmi

MDVA-2009:102 : grep

MDVA-2009:104 : fuse

MDVA-2009:105 : fuse

MDVA-2009:106 : mysql

MDVA-2009:107 : udev

MDVA-2009:108 : libx11

MDVA-2009:109 : mysql

MDVA-2009:110 : qt3

MDVA-2009:111 : sqlite3

MDVA-2009:112 : drakx-net

MDVA-2009:113 : rpm

MDVA-2009:114 : logcheck

MDVA-2009:115 : webkit

MDVA-2009:116 : glibc

MDVA-2009:117 : ruby-RubyGems

MDVA-2009:118 : kde4

MDVA-2009:118-1 : kde4

MDVA-2009:119 : yelp

MDVA-2009:119-1 : yelp

MDVA-2009:120 : aspell-nb

MDVA-2009:121 : pulseaudio

MDVA-2009:122 : timezone

MDVA-2009:123 : kde4

MDVA-2009:124 : msec

MDVA-2009:125 : kde4-style-iaora

MDVA-2009:126 : initscripts

MDVA-2009:127 : digikam

MDVA-2009:128 : gnokii

MDVA-2009:129 : x11-driver-video-sisimedia

MDVA-2009:130 : evolution

MDVA-2009:131 : bluez

MDVA-2009:132 : gnome-power-manager

MDVA-2009:137 : rpm

MDVA-2009:140 : x11-driver-video-openchrome

MDVA-2009:141 : urpmi

MDVA-2009:144 : libv4l

MDVA-2009:145 : x11-driver-input-synaptics

MDVA-2009:146 : coreutils

MDVA-2009:147 : indilib

MDVA-2009:149 : gtkmm2.4

MDVA-2009:151 : samba

MDVA-2009:152 : iptables

MDVA-2009:153 : kde4-style-iaora

MDVA-2009:154 : timezone

MDVA-2009:155 : beagle

MDVA-2009:156 : kde4

MDVA-2009:157 : kdebase4-workspace

MDVA-2009:158 : xmlrpc-c

MDVA-2009:159 : hplip

MDVA-2009:161 : silc-toolkit

MDVA-2009:162 : qca

MDVA-2009:163 : libxcb

MDVA-2009:164 : qt4

MDVA-2009:165 : cfengine

MDVA-2009:166 : setup

MDVA-2009:168 : rrdtool

MDVA-2009:169 : drakxtools

MDVA-2009:169-1 : drakxtools

MDVA-2009:170 : ldetect

MDVA-2009:171 : ldetect-lst

MDVA-2009:172 : drakxtools

MDVA-2009:173 : ldetect-lst

MDVA-2009:174 : aria2

MDVA-2009:175 : kdepim4

MDVA-2009:176 : mdadm

MDVA-2009:177 : x11-server

MDVA-2009:178 : xkeyboard-config

MDVA-2009:179 : mesa

MDVA-2009:180 : x11-driver-video-openchrome

MDVA-2009:182 : gnucash

MDVA-2009:183 : nvidia

MDVA-2009:184 : mdkonline

MDVA-2009:185 : msec

MDVA-2009:186 : firefox

MDVA-2009:187 : desktop-common-data

MDVA-2009:188 : indexhtml

MDVA-2009:189 : qt4

MDVA-2009:190 : netprofile

MDVA-2009:191 : mc

MDVA-2009:193 : php

MDVA-2009:194 : mdkonline

MDVA-2009:195 : urlview

MDVA-2009:196 : libsndfile

MDVA-2009:197 : glibc

MDVA-2009:198 : apache

MDVA-2009:199 : squid

MDVA-2009:200 : mmc-agent

MDVA-2009:201 : samba

MDVA-2009:202 : java-1.6.0-openjdk

MDVA-2009:203 : php

MDVA-2009:204 : kompozer

MDVA-2009:206 : phonon

MDVA-2009:207 : tcsh

MDVA-2009:208 : alsa-oss

MDVA-2009:209 : drakx-net

MDVA-2009:210 : kino

MDVA-2009:211 : pango

MDVA-2009:212 : SDL\_image

MDVA-2009:213 : perl-URPM

MDVA-2009:215 : fuse

MDVA-2009:217 : qemu

MDVA-2009:218 : kdebase4-workspace

MDVA-2009:219 : libxcb

MDVA-2009:220 : libxt

MDVA-2009:221 : perl

MDVA-2009:222 : eclipse

MDVA-2009:223 : mplayer

MDVA-2009:224 : mandriva-kde4-config

MDVA-2009:226 : apache

MDVA-2009:227 : mandriva-doc

MDVA-2009:228 : kdebase4-workspace

MDVA-2009:229 : mandriva-kde4-config

MDVA-2009:229-1 : mandriva-kde4-config

MDVA-2009:230 : kdelibs4

MDVA-2009:231 : kdebase4

MDVA-2009:232 : drakx-net

MDVA-2009:233 : msec

MDVA-2009:234 : msec

MDVA-2009:235 : freeradius

MDVA-2009:236 : kdemultimedia4

MDVA-2009:237 : xdpyinfo

MDVA-2009:238 : netpbm

MDVA-2009:239 : imagemagick

MDVA-2009:240 : doxygen

MDVA-2009:241 : shorewall

MDVA-2009:242 : python-qt

MDVA-2009:243 : kdemultimedia4

MDVA-2009:244 : kdelibs4

MDVA-2009:245 : espeak

MDVA-2009:246 : hal-cups-utils

MDVA-2009:247 : mdkonline

MDVA-2009:248 : mdkonline

MDVA-2009:249 : mdkonline

MDVA-2009:250 : wireless-regdb

MDVA-2009:251 : mdkonline

MDVA-2009:252 : webkitgtk

MDVA-2009:253 : mpg123

MDVA-2009:254 : graphviz

MDVA-2009:255 : fontconfig

MDVA-2009:256 : kdepim4

MDVA-2009:257 : mandriva-kde4-config

MDVA-2009:258 : webkit

MDVA-2009:259 : webkit

MDVA-2009:260 : gnome-desktop

MDVA-2009:261 : kdepim4

MDVA-2009:262 : kde4-splash-mdv

MDVA-2009:263 : drakx-net

MDVA-2009:264 : kdenetwork4

MDVA-2009:265 : beagle

MDVA-2009:266 : pcsc-lite

MDVA-2009:267 : tcb

MDVA-2009:268 : dansguardian

MDVA-2009:269 : gvfs

MDVA-2009:270 : kdebase4

MDVA-2009:271 : k3b

MDVA-2009:272 : kdebase4-runtime

MDVA-2009:273 : kdegraphics4

MDVA-2009:274 : digikam

MDVA-2010:001 : a2ps

MDVA-2010:002 : rpmstats

MDVA-2010:003 : phonon

MDVA-2010:004 : kdebase4

MDVA-2010:005 : msec

MDVA-2010:006 : timezone

MDVA-2010:006-1 : timezone

MDVA-2010:007 : kdelibs4

MDVA-2010:010 : kde4-style-iaora

MDVA-2010:011 : apache-conf

MDVA-2010:012 : kdebase4

MDVA-2010:013 : kdepim4

MDVA-2010:014 : spamassassin

MDVA-2010:015 : firefox

MDVA-2010:016 : firefox

MDVA-2010:017 : consolekit

MDVA-2010:018 : fetchmail

MDVA-2010:019 : polkit-gnome

MDVA-2010:022 : python-gobject

MDVA-2010:023 : kde4-style-iaora

MDVA-2010:024 : kdelibs4

MDVA-2010:027 : net-snmp

MDVA-2010:030 : msec

MDVA-2010:031 : freeradius

MDVA-2010:032 : mkinitrd

MDVA-2010:033 : gnupg2

MDVA-2010:034 : phonon-gstreamer

MDVA-2010:035 : drakxtools

MDVA-2010:035-1 : drakxtools

MDVA-2010:036 : initscripts

MDVA-2010:037 : xinit

MDVA-2010:038 : libxrender

MDVA-2010:039 : dbus-glib

MDVA-2010:041 : mjpegtools

MDVA-2010:042 : urpmi

MDVA-2010:043 : pciutils

MDVA-2010:045 : urpmi

MDVA-2010:046 : webkit

MDVA-2010:047 : evolution

MDVA-2010:048 : gtk

MDVA-2010:049 : mailcap

MDVA-2010:056 : samba

MDVA-2010:059 : msec

MDVA-2010:060 : openoffice.org-voikko

MDVA-2010:061 : xfig

MDVA-2010:062 : drakxtools

MDVA-2010:062-1 : drakxtools

MDVA-2010:063 : totem

MDVA-2010:064 : pptp-linux

MDVA-2010:065 : mandriva-release

MDVA-2010:066 : drakxtools

MDVA-2010:067 : mdkonline

MDVA-2010:067-1 : mdkonline

MDVA-2010:068 : drakconf

MDVA-2010:069 : mandriva-release

MDVA-2010:070 : blogtk

MDVA-2010:070-1 : blogtk

MDVA-2010:071 : eject

MDVA-2010:073 : dhcp

MDVA-2010:074 : xdg-utils

MDVA-2010:076 : rsh

MDVA-2010:077 : aria2

MDVA-2010:078 : msec

MDVA-2010:080 : python-qt4

MDVA-2010:081 : glibc

MDVA-2010:082 : drakxtools

MDVA-2010:083 : initscripts

MDVA-2010:084 : x11-driver-video-ati

MDVA-2010:085 : dhcp

MDVA-2010:086 : irqbalance

MDVA-2010:088 : rsnapshot

MDVA-2010:090 : openssh

MDVA-2010:091 : slib

MDVA-2010:098 : urpmi

MDVA-2010:100 : rootcerts

MDVA-2010:101 : timezone

MDVA-2010:103 : poppler

MDVA-2010:104 : iptables

MDVA-2010:105 : lvm2

MDVA-2010:106 : system-config-printer

MDVA-2010:107 : pulseaudio

MDVA-2010:108 : kde4

MDVA-2010:108-1 : kde4

MDVA-2010:110 : dbus

MDVA-2010:111 : initscripts

MDVA-2010:112 : kdebase4-workspace

MDVA-2010:113 : rpmdrake

MDVA-2010:114 : rpmdrake

MDVA-2010:115 : tkcvs

MDVA-2010:116 : timezone

MDVA-2010:117 : flashplayer

MDVA-2010:118 : firefox-ext-plasmanotify

MDVA-2010:120 : openoffice.org-voikko

MDVA-2010:121 : firefox

MDVA-2010:122 : k3b

MDVA-2010:123 : tcsh

MDVA-2010:124 : mandriva-release

MDVA-2010:125 : ldetect-lst

MDVA-2010:126 : totem

MDVA-2010:127 : kde4-style-iaora

MDVA-2010:128 : epiphany

MDVA-2010:128-1 : epiphany

MDVA-2010:129 : netcdf

MDVA-2010:130 : rpm

MDVA-2010:131 : yelp

MDVA-2010:132 : plymouth

MDVA-2010:133 : gdm

MDVA-2010:134 : sane

MDVA-2010:135 : desktop-common-data

MDVA-2010:138 : timezone

MDVA-2010:139 : php-timezonedb

MDVA-2010:140 : gtkspell

MDVA-2010:141 : kdevelop4

MDVA-2010:143 : xine-ui

MDVA-2010:144 : mdkonline

MDVA-2010:145 : lirc

MDVA-2010:146 : mysql

MDVA-2010:147 : x11-server

MDVA-2010:148 : msec

MDVA-2010:149 : SDL12

MDVA-2010:150 : k3b

MDVA-2010:152 : openbox

MDVA-2010:153 : kdelibs4

MDVA-2010:155 : mono

MDVA-2010:156 : digikam

MDVA-2010:157 : gtk+2.0

MDVA-2010:158 : gdcm

MDVA-2010:160 : heartbeat

MDVA-2010:160-1 : heartbeat

MDVA-2010:161 : findutils

MDVA-2010:162 : openssh

MDVA-2010:163 : php

MDVA-2010:164 : pidgin

MDVA-2010:166 : php-eaccelerator

MDVA-2010:166-1 : php-eaccelerator

MDVA-2010:168 : espeak

MDVA-2010:169 : php-xdebug

MDVA-2010:171 : libgdata

MDVA-2010:172 : libneon0.27

MDVA-2010:173 : gnupg2

MDVA-2010:174 : mkinitrd

MDVA-2010:175 : firefox

MDVA-2010:176 : x11-driver-input-evdev

MDVA-2010:178 : mdkonline

MDVA-2010:179 : bind

MDVA-2010:181 : php-xdebug

MDVA-2010:181-1 : php-xdebug

MDVA-2010:182 : rpmdrake

MDVA-2010:183 : paprefs

MDVA-2010:184 : net-snmp

MDVA-2010:185 : nfs-utils

MDVA-2010:186 : rsh

MDVA-2010:187 : rpmstats

MDVA-2010:188 : slib

MDVA-2010:189 : cairo

MDVA-2010:190 : gthumb

MDVA-2010:191 : xdg-utils

MDVA-2010:192 : pcmanfm

MDVA-2010:193 : openssl

MDVA-2010:194 : boost

MDVA-2010:195 : openssl

MDVA-2010:196 : firefox

MDVA-2010:198 : beagle

MDVA-2010:199 : clamav

MDVA-2010:200 : rpmdrake

MDVA-2010:201 : evolution

MDVA-2010:202 : mdkonline

MDVA-2010:204 : gnupg2

MDVA-2010:205 : xdg-user-dirs

MDVA-2010:207 : urpmi

MDVA-2010:208 : cyrus-imapd

MDVA-2010:210 : mysql

MDVA-2010:211 : wine

MDVA-2010:212 : mailman

MDVA-2010:213 : clamav

MDVA-2010:214 : perl-URPM

MDVA-2010:215 : libgpod

MDVA-2010:216 : gkrellm

MDVA-2010:217 : gjs

MDVA-2010:218 : sudo

MDVA-2010:219 : kdeplasma-addons

MDVA-2010:220 : kipi-plugins

MDVA-2010:221 : postgresql

MDVA-2010:222 : tomboy

MDVA-2010:223 : nss\_updatedb

MDVA-2010:224 : snort

MDVA-2010:225 : commoncpp

MDVA-2010:226 : perl-URPM

MDVA-2010:227 : libalsa2

MDVA-2010:228 : firefox

MDVA-2010:230 : kolab-webadmin

MDVA-2010:231 : x11-driver-input-evtouch

MDVA-2010:232 : pidgin

MDVA-2010:233 : nautilus-sendto

MDVA-2010:235 : keychain

MDVA-2010:237 : libxt

MDVA-2010:238 : php

MDVA-2010:239 : mandriva-release

MDVA-2010:240 : mysql

MDVA-2010:241 : nss

MDVA-2010:242 : xulrunner

MDVA-2011:000 : openoffice.org

MDVA-2011:001 : openoffice.org-voikko

MDVA-2011:002 : cyrus-sasl

MDVA-2011:003 : lsb-release

MDVA-2011:004 : lsb-release

MDVA-2011:005 : mysql

MDVA-2011:006 : php

MDVA-2011:007 : clamav

MDVA-2011:008 : firefox

MDVA-2011:010 : djvulibre

MDVA-2011:011 : mono-tools

MDVA-2011:014 : kde4

MDVA-2011:018 : perl-URPM

MDVA-2011:019 : tcl-sqlite3

MDVA-2011:020 : ffmpeg

MDVA-2011:025 : mysql

MDVA-2011:027 : bind

MDVA-2011:029 : hplip

MDVA-2011:032 : kdepim4

MDVA-2011:040 : null

MDVA-2011:045 : nspluginwrapper

MDVA-2011:046 : drakx-net

MDVA-2011:049 : hostapd

MDVA-2011:055 : hplip

MDVA-2011:057 : rpm

MDVA-2011:058 : timezone

MDVA-2011:068 : php-apc

MDVA-2011:072 : timezone

MDVA-2011:081-1 : libmsn

MDVA-2011:083 : bind

MDVA-2011:093-1 : psmisc

MDVA-2011:094 : python

MDVA-2011:099 : mysql

MDVA-2012:002 : util-linux

MDVA-2012:004 : php

MDVA-2012:005 : mysql

MDVA-2012:006 : firefox

MDVA-2012:007 : firefox

MDVA-2012:014 : firefox

MDVA-2012:019 : mozilla-thunderbird

MDVA-2012:024 : rpm-mandriva-setup

MDVA-2012:025 : kdegraphics4

MDVA-2012:026 : kdeedu4

MDVA-2012:031 : mysql

MDVA-2012:034 : bind

MDVA-2012:035 : libarchive

MDVA-2012:042 : libdc1394

MDVA-2012:044 : timezone

MDVA-2012:045 : mysql

MDVA-2012:046 : initscripts

MDVSA-2009:177 : postgresql

MDVSA-2009:178 : perl-IO-Socket-SSL

# MacOS X Local Security Checks

Adobe Acrobat < 10.1.10 / 11.0.07 Multiple Vulnerabilities (APSB14-15) (Mac OS X)

Adobe Acrobat < 10.1.13 / 11.0.10 Multiple Vulnerabilities (APSB14-28) (Mac OS X)

Adobe Acrobat < 10.1.14 / 11.0.11 Multiple Vulnerabilities (APSB15-10)

Adobe Acrobat < 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-15) (Mac OS X)

Adobe Acrobat < 10.1.9 / 11.0.6 Multiple Vulnerabilities (APSB14-01) (Mac OS X)

Adobe Acrobat < 11.0.14 / 15.006.30119 / 15.010.20056 Multiple Vulnerabilities (APSB16-02) (Mac OS X)

Adobe Acrobat < 11.0.15 / 15.006.30121 / 15.010.20060 Multiple Vulnerabilities (APSB16-09) (Mac OS X)

Adobe Acrobat < 11.0.16 / 15.006.30172 / 15.016.20039 Multiple Vulnerabilities (APSB16-14) (Mac OS X)

Adobe Acrobat < 11.0.17 / 15.006.30198 / 15.017.20050 Multiple Vulnerabilities (APSB16-26) (Mac OS X)

Adobe Acrobat < 11.0.18 / 15.006.30243 / 15.020.20039 Multiple Vulnerabilities (APSB16-33) (macOS)

Adobe Acrobat < 11.0.19 / 15.006.30279 / 15.023.20053 Multiple Vulnerabilities (APSB17-01) (macOS)

Adobe Acrobat < 11.0.20 / 2015.006.30306 / 2017.009.20044 Multiple Vulnerabilities (APSB17-11) (macOS)

Adobe Acrobat < 11.0.21 / 2015.006.30355 / 2017.011.30066 / 2017.012.20098 Multiple Vulnerabilities (APSB17-24) (macOS)

Adobe Acrobat < 11.0.23 / 2015.006.30392 / 2017.011.30068 / 2018.009.20044 Multiple Vulnerabilities (APSB17-36) (macOS)

Adobe Acrobat < 15.006.30434 / 17.011.30096 / 18.011.20055 Multiple Vulnerabilities (APSB18-21) (macOS)

Adobe Acrobat < 2015.006.30416 / 2017.011.30078 / 2018.011.20035 Multiple Vulnerabilities (APSB18-02) (macOS)

Adobe Acrobat < 2015.006.30418 / 2017.011.30080 / 2018.011.20040 Multiple Vulnerabilities (APSB18-09) (macOS)

Adobe Acrobat < 2019.010.20091 / 2017.011.30120 / 2015.006.30475 Multiple Vulnerabilities (APSB19-07) (macOS)

Adobe Acrobat <= 10.1.10 / 11.0.07 Multiple Vulnerabilities (APSB14-20) (Mac OS X)

Adobe Acrobat <= 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-24) (Mac OS X)

Adobe Acrobat <= 15.006.30434 / 17.011.30096 / 18.011.20055 Multiple Vulnerabilities (APSB18-29) (macOS)

Adobe Acrobat <= 15.006.30448 / 17.011.30099 / 18.011.20058 Multiple Vulnerabilities (APSB18-34) (macOS)

Adobe Acrobat <= 15.006.30452 / 17.011.30102 / 18.011.20063 Multiple Vulnerabilities (APSB18-30) (macOS)

Adobe Acrobat <= 15.006.30456 / 17.011.30105 / 19.008.20080 Multiple Vulnerabilities (APSB18-41) (macOS)

Adobe Acrobat <= 2015.006.30461 / 2017.011.30110 / 2019.010.20064 Multiple Vulnerabilities (APSB19-02) (macOS)

Adobe Acrobat <= 2015.006.30482 / 2017.011.30127 / 2019.010.20098 Multiple Vulnerabilities (APSB19-17) (macOS)

Adobe Acrobat <= 2015.006.30495 / 2017.011.30140 / 2019.010.20100 Multiple Vulnerabilities (APSB19-18) (macOS)

Adobe Acrobat <= 2015.006.30497 / 2017.011.30142 / 2019.012.20034 Multiple Vulnerabilities (APSB19-41) (macOS)

Adobe Acrobat <= 2015.006.30503 / 2017.011.30148 / 2019.012.20040 Multiple Vulnerabilities (APSB19-49) (macOS)

Adobe Acrobat <= 2015.006.30505 / 2017.011.30155 / 2019.021.20056 Multiple Vulnerabilities (APSB19-55) (macOS)

Adobe Acrobat <= 2015.006.30508 / 2019.021.20061 Multiple Vulnerabilities (APSB20-05) (macOS)

Adobe Acrobat <= 2015.006.30510 / 2017.011.30158 / 2020.006.20034 Multiple Vulnerabilities (APSB20-13) (macOS)

Adobe Acrobat <= 2019.010.20091 Vulnerability (APSB19-13) (macOS)

Adobe Acrobat Help Page XSS (Mac OS X)

Adobe Acrobat Installed (Mac OS X)

Adobe Acrobat Unsupported Version Detection (Mac OS X)

Adobe AIR for Mac 3.x <= 3.1.0.4880 Multiple Memory Corruption Vulnerabilities (APSB12-07)

Adobe AIR for Mac 3.x <= 3.2.0.2070 Multiple Vulnerabilities (APSB12-14)

Adobe AIR for Mac 3.x <= 3.3.0.3670 Multiple Vulnerabilities (APSB12-19)

Adobe AIR for Mac 3.x <= 3.4.0.2540 Multiple Vulnerabilities (APSB12-22)

Adobe AIR for Mac 3.x <= 3.4.0.2710 Multiple Vulnerabilities (APSB12-24)

Adobe AIR for Mac 3.x <= 3.5.0.1060 Multiple Vulnerabilities (APSB13-05)

Adobe AIR for Mac 3.x <= 3.5.0.600 Multiple Vulnerabilities (APSB12-27)

Adobe AIR for Mac 3.x <= 3.5.0.890 Buffer Overflow (APSB13-01)

Adobe AIR for Mac 3.x <= 3.6.0.597 Multiple Vulnerabilities (APSB13-09)

Adobe AIR for Mac 3.x <= 3.6.0.6090 Multiple Vulnerabilities (APSB13-11)

Adobe AIR for Mac <= 13.0.0.111 Multiple Vulnerabilities (APSB14-16)

Adobe AIR for Mac <= 13.0.0.83 Multiple Vulnerabilities (APSB14-14)

Adobe AIR for Mac <= 14.0.0.110 Multiple Vulnerabilities (APSB14-18)

Adobe AIR for Mac <= 14.0.0.178 Multiple Vulnerabilities (APSB14-21)

Adobe AIR for Mac <= 15.0.0.249 Multiple Vulnerabilities (APSB14-21)

Adobe AIR for Mac <= 15.0.0.293 Multiple Vulnerabilities (APSB14-24)

Adobe AIR for Mac <= 15.0.0.356 Multiple Vulnerabilities (APSB15-01)

Adobe AIR for Mac <= 17.0.0.124 Multiple Vulnerabilities (APSB15-05)

Adobe AIR for Mac <= 17.0.0.144 Multiple Vulnerabilities (APSB15-06)

Adobe AIR for Mac <= 17.0.0.144 Multiple Vulnerabilities (APSB15-09)

Adobe AIR for Mac <= 17.0.0.172 Multiple Vulnerabilities (APSB15-11)

Adobe AIR for Mac <= 18.0.0.144 Multiple Vulnerabilities (APSB15-16)

Adobe AIR for Mac <= 18.0.0.180 Multiple Vulnerabilities (APSB15-16)

Adobe AIR for Mac <= 18.0.0.199 Multiple Vulnerabilities (APSB15-23)

Adobe AIR for Mac <= 19.0.0.190 Multiple Vulnerabilities (APSB15-25)

Adobe AIR for Mac <= 19.0.0.213 Multiple Vulnerabilities (APSB15-28)

Adobe AIR for Mac <= 19.0.0.241 Multiple Vulnerabilities (APSB15-32)

Adobe AIR for Mac <= 20.0.0.204 Multiple Vulnerabilities (APSB16-01)

Adobe AIR for Mac <= 20.0.0.233 Multiple Vulnerabilities (APSB16-04)

Adobe AIR for Mac <= 20.0.0.260 Multiple Vulnerabilities (APSB16-08)

Adobe AIR for Mac <= 21.0.0.198 Multiple Vulnerabilities (APSB16-15)

Adobe AIR for Mac <= 22.0.0.153 Android Applications Runtime Analytics MitM (APSB16-31)

Adobe AIR for Mac <= 3.0 Multiple Vulnerabilities (APSB11-28)

Adobe AIR for Mac <= 3.7.0.1530 Multiple Vulnerabilities (APSB13-14)

Adobe AIR for Mac <= 3.7.0.1860 Memory Corruption (APSB13-16)

Adobe AIR for Mac <= 3.7.0.2100 Multiple Vulnerabilities (APSB13-17)

Adobe AIR for Mac <= 3.8.0.910 Memory Corruptions (APSB13-21)

Adobe AIR for Mac <= 3.9.0.1030 Memory Corruptions (APSB13-26)

Adobe AIR for Mac <= 3.9.0.1210 Multiple Vulnerabilities (APSB13-28)

Adobe AIR for Mac <= 3.9.0.1380 Multiple Vulnerabilities (APSB14-02)

Adobe AIR for Mac <= 4.0.0.1628 Multiple Vulnerabilities (APSB14-09)

Adobe AIR for Mac Installed

Adobe AIR Unsupported Version Detection (Mac OS X)

Adobe Bridge CC 9.0.2 Multiple Vulnerabilities (APSB19-04) (Mac OS X)

Adobe Bridge CC < 6.2 Multiple Memory Corruption Vulnerabilities (APSB16-03) (Mac OS X)

Adobe Bridge for Mac Installed

Adobe Camera Raw Plugin Multiple Vulnerabilities (Mac OS X)

Adobe Creative Cloud <= 3.5.1.209 Arbitrary File Read/Write Vulnerability (Mac OS X)

Adobe Creative Cloud Desktop <= 4.6.1.393 Multiple Vulnerabilities (APSB19-39) (macOS)

Adobe Creative Cloud for Mac Installed

Adobe Digital Editions 2.0.0 Memory Corruption (Mac OS X)

Adobe Digital Editions 2.0.1 Memory Corruption (Mac OS X)

Adobe Digital Editions < 4.0.1 Information Disclosure (APSB14-25) (Mac OS X)

Adobe Digital Editions < 4.5.1 RCE (APSB16-06) (Mac OS X)

Adobe Digital Editions < 4.5.10 Out-Of-Bounds Read Vulnerability (APSB19-04) (Mac OS X)

Adobe Digital Editions < 4.5.2 Multiple Vulnerabilities (APSB16-28) (Mac OS X)

Adobe Digital Editions < 4.5.3 Multiple Information Disclosure Vulnerabilities (APSB16-45) (macOS)

Adobe Digital Editions < 4.5.4 Multiple Vulnerabilities (APSB17-05) (macOS)

Adobe Digital Editions < 4.5.5 Multiple Vulnerabilities (APSB17-20) (macOS)

Adobe Digital Editions < 4.5.6 Multiple Vulnerabilities (APSB17-27) (macOS)

Adobe Digital Editions < 4.5.8 Multiple Vulnerabilities (APSB18-13) (macOS)

Adobe Digital Editions < 4.5.9 Multiple Vulnerabilities (APSB18-27) (macOS)

Adobe Digital Editions Installed (Mac OS X)

Adobe Flash Player <= 17.0.0.134 Multiple Vulnerabilities (APSB15-06)

Adobe Flash Player <= 17.0.0.169 Multiple Vulnerabilities (APSB15-09) (Mac OS X)

Adobe Flash Player <= 17.0.0.188 Multiple Vulnerabilities (APSB15-11) (Mac OS X)

Adobe Flash Player <= 18.0.0.161 RCE (APSB15-14) (Mac OS X)

Adobe Flash Player <= 18.0.0.194 Multiple Vulnerabilities (APSB15-16) (Mac OS X)

Adobe Flash Player <= 18.0.0.203 Multiple RCE Vulnerabilities (APSB15-18) (Mac OS X)

Adobe Flash Player <= 18.0.0.209 Multiple Vulnerabilities (APSB15-19) (Mac OS X)

Adobe Flash Player for Mac <= 18.0.0.232 Multiple Vulnerabilities (APSB15-23)

Adobe Flash Player for Mac <= 19.0.0.185 Multiple Vulnerabilities (APSB15-25)

Adobe Flash Player for Mac <= 19.0.0.207 Vulnerability (APSB15-27)

Adobe Flash Player for Mac <= 19.0.0.226 Multiple Vulnerabilities (APSB15-28)

Adobe Flash Player for Mac <= 19.0.0.245 Multiple Vulnerabilities (APSB15-32)

Adobe Flash Player for Mac <= 20.0.0.235 Multiple Vulnerabilities (APSB16-01)

Adobe Flash Player for Mac <= 20.0.0.286 Multiple Vulnerabilities (APSB16-04)

Adobe Flash Player for Mac <= 20.0.0.306 Multiple Vulnerabilities (APSB16-08)

Adobe Flash Player for Mac <= 21.0.0.197 Multiple Vulnerabilities (APSB16-10)

Adobe Flash Player for Mac <= 21.0.0.226 Multiple Vulnerabilities (APSB16-15)

Adobe Flash Player for Mac <= 21.0.0.242 Multiple Vulnerabilities (APSB16-18)

Adobe Flash Player for Mac <= 22.0.0.192 Multiple Vulnerabilities (APSB16-25)

Adobe Flash Player for Mac <= 22.0.0.211 Multiple Vulnerabilities (APSB16-29)

Adobe Flash Player for Mac <= 23.0.0.162 Multiple Vulnerabilities (APSB16-32)

Adobe Flash Player for Mac <= 23.0.0.185 Arbitrary Code Execution (APSB16-36)

Adobe Flash Player for Mac <= 23.0.0.205 Multiple Vulnerabilities (APSB16-37)

Adobe Flash Player for Mac <= 23.0.0.207 Multiple Vulnerabilities (APSB16-39)

Adobe Flash Player for Mac <= 24.0.0.186 Multiple Vulnerabilities (APSB17-02)

Adobe Flash Player for Mac <= 24.0.0.194 Multiple Vulnerabilities (APSB17-04)

Adobe Flash Player for Mac <= 24.0.0.221 Multiple Vulnerabilities (APSB17-07)

Adobe Flash Player for Mac <= 25.0.0.127 Multiple Vulnerabilities (APSB17-10)

Adobe Flash Player for Mac <= 25.0.0.163 Multiple Vulnerabilities (APSB17-15)

Adobe Flash Player for Mac <= 25.0.0.171 Multiple Vulnerabilities (APSB17-17)

Adobe Flash Player for Mac <= 26.0.0.131 Multiple Vulnerabilities (APSB17-21)

Adobe Flash Player for Mac <= 26.0.0.137 Multiple Vulnerabilities (APSB17-23)

Adobe Flash Player for Mac <= 26.0.0.151 Multiple Vulnerabilities (APSB17-23)

Adobe Flash Player for Mac <= 27.0.0.159 Multiple Vulnerabilities (APSB17-32)

Adobe Flash Player for Mac <= 27.0.0.183 (APSB17-33)

Adobe Flash Player for Mac <= 27.0.0.187 (APSB17-42)

Adobe Flash Player for Mac <= 28.0.0.126 (APSB18-01)

Adobe Flash Player for Mac <= 28.0.0.137 Use-after-free Remote Code Execution (APSA18-01) (APSB18-03)

Adobe Flash Player for Mac <= 28.0.0.161 (APSB18-05)

Adobe Flash Player for Mac <= 29.0.0.113 (APSB18-08)

Adobe Flash Player for Mac <= 29.0.0.140 (APSB18-16)

Adobe Flash Player for Mac <= 29.0.0.171 (APSB18-19)

Adobe Flash Player for Mac <= 30.0.0.113 (APSB18-24)

Adobe Flash Player for Mac <= 30.0.0.134 (APSB18-25)

Adobe Flash Player for Mac <= 30.0.0.154 (APSB18-31)

Adobe Flash Player for Mac <= 31.0.0.122 (APSB18-39)

Adobe Flash Player for Mac <= 31.0.0.148 (APSB18-44)

Adobe Flash Player for Mac <= 31.0.0.153 (APSB18-42)

Adobe Flash Player for Mac <= 32.0.0.114 (APSB19-06)

Adobe Flash Player for Mac <= 32.0.0.156 (APSB19-19)

Adobe Flash Player for Mac <= 32.0.0.171 (APSB19-26)

Adobe Flash Player for Mac <= 32.0.0.192 (APSB19-30)

Adobe Flash Player for Mac <= 32.0.0.238 (APSB19-46)

Adobe Flash Player for Mac <= 32.0.0.321 (APSB20-06)

Adobe Flash Player for Mac Installed

Adobe Flash Player Unsupported Version Detection (Mac OS X)

Adobe Flash Professional for Mac <= 11.5.1.349 JPG Object Dimension Memory Allocation FLA File Handling Remote Overflow (APSB12-12)

Adobe Flash Professional for Mac Installed

Adobe InDesign CC < 13.1 Multiple Vulnerabilities (APSB18-11) (macOS)

Adobe InDesign CC < 14.0.2 Arbitrary Code Execution Vulnerability (APSB19-23) (macOS)

Adobe InDesign for macOS Installed

Adobe Media Encoder Installed (macOS)

Adobe Photoshop 21.x <= 21.1.1 / CC 20.x <= 20.0.8 Multiple Vulnerabilities (APSB20-14)

Adobe Photoshop CC 17.x < 17.0.2 / 18.x < 18.1 PCX File Handling Arbitrary Code Execution (APSB17-12) (macOS)

Adobe Photoshop CC 18.x < 18.1.2 Multiple Vulnerabilities (APSB17-34) (macOS)

Adobe Photoshop CC 18.x < 18.1.4 / 19.x < 19.1.4 Remote Code Execution Vulnerability (APSB18-17) (macOS)

Adobe Photoshop CC 18.x < 18.1.6 / 19.x < 19.1.6 Multiple Vulnerabilities (APSB18-28) (macOS)

Adobe Photoshop CC 19.x < 19.1.7 Information Disclosure Vulnerability (APSB18-43) (macOS)

Adobe Photoshop CC 19.x <= 19.1.7 / 20.x <= 20.0.2 Vulnerability (APSB19-15)

Adobe Photoshop CC 19.x <= 19.1.8 / 20.x <= 20.0.5 Vulnerability (APSB19-15)

Adobe Photoshop CC 20.x <= 20.0.7 / 21.x <= 21.0.1 Multiple Vulnerabilities (APSB19-56)

Adobe Photoshop CC < 15.2.4 / 16.1.2 Multiple Memory Corruption Vulnerabilities (APSB16-03) (Mac OS X)

Adobe Photoshop CC Multiple Vulnerabilities (APSB15-12) (Mac OS X)

Adobe Photoshop CS6 for Mac Multiple RCE Vulnerabilities (APSB12-20) (Mac OS X)

Adobe Photoshop for Mac Installed

Adobe Photoshop for Mac Unsupported Version Detection

Adobe Reader < 10.1 / 9.4.5 / 8.3 Multiple Vulnerabilities (APSB11-12, APSB11-12, APSB11-16) (Mac OS X)

Adobe Reader < 10.1.1 / 9.4.6 / 8.3.1 Multiple Vulnerabilities (APSB11-21, APSB11-24, APSB11-26) (Mac OS X)

Adobe Reader < 10.1.10 / 11.0.07 Multiple Vulnerabilities (APSB14-15) (Mac OS X)

Adobe Reader < 10.1.13 / 11.0.10 Multiple Vulnerabilities (APSB14-28) (Mac OS X)

Adobe Reader < 10.1.14 / 11.0.11 Multiple Vulnerabilities (APSB15-10)

Adobe Reader < 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-15) (Mac OS X)

Adobe Reader < 10.1.3 / 9.5.1 Multiple Vulnerabilities (APSB12-03, APSB12-05, APSB12-07, APSB12-08) (Mac OS X)

Adobe Reader < 10.1.4 / 9.5.2 Multiple Vulnerabilities (APSB12-16) (Mac OS X)

Adobe Reader < 10.1.9 / 11.0.6 Multiple Vulnerabilities (APSB14-01) (Mac OS X)

Adobe Reader < 11.0.1 / 10.1.5 / 9.5.3 Multiple Vulnerabilities (APSB13-02) (Mac OS X)

Adobe Reader < 11.0.14 / 15.006.30119 / 15.010.20056 Multiple Vulnerabilities (APSB16-02) (Mac OS X)

Adobe Reader < 11.0.15 / 15.006.30121 / 15.010.20060 Multiple Vulnerabilities (APSB16-09) (Mac OS X)

Adobe Reader < 11.0.16 / 15.006.30172 / 15.016.20039 Multiple Vulnerabilities (APSB16-14) (Mac OS X)

Adobe Reader < 11.0.17 / 15.006.30198 / 15.017.20050 Multiple Vulnerabilities (APSB16-26) (Mac OS X)

Adobe Reader < 11.0.18 / 15.006.30243 / 15.020.20039 Multiple Vulnerabilities (APSB16-33) (macOS)

Adobe Reader < 11.0.19 / 15.006.30279 / 15.023.20053 Multiple Vulnerabilities (APSB17-01) (macOS)

Adobe Reader < 11.0.2 / 10.1.6 / 9.5.4 Multiple Vulnerabilities (APSA13-02, APSB13-07) (Mac OS X)

Adobe Reader < 11.0.20 / 2015.006.30306 / 2017.009.20044 Multiple Vulnerabilities (APSB17-11) (macOS)

Adobe Reader < 11.0.21 / 2015.006.30355 / 2017.011.30066 / 2017.012.20098 Multiple Vulnerabilities (APSB17-24) (macOS)

Adobe Reader < 11.0.23 / 2015.006.30392 / 2017.011.30068 / 2018.009.20044 Multiple Vulnerabilities (APSB17-36) (macOS)

Adobe Reader < 11.0.3 / 10.1.7 / 9.5.5 Multiple Vulnerabilities (APSB13-15) (Mac OS X)

Adobe Reader < 11.0.4 / 10.1.8 Multiple Vulnerabilities (APSB13-22) (Mac OS X)

Adobe Reader < 15.006.30434 / 17.011.30096 / 18.011.20055 Multiple Vulnerabilities (APSB18-21) (macOS)

Adobe Reader < 2015.006.30416 / 2017.011.30078 / 2018.011.20035 Multiple Vulnerabilities (APSB18-02) (macOS)

Adobe Reader < 2015.006.30418 / 2017.011.30080 / 2018.011.20040 Multiple Vulnerabilities (APSB18-09) (macOS)

Adobe Reader < 2019.010.20091 / 2017.011.30120 / 2015.006.30475 Multiple Vulnerabilities (APSB19-07) (macOS)

Adobe Reader <= 10.1.1 / 9.4.6 U3D Memory Corruption (APSA11-04, APSB11-28, APSB11-30, APSB12-01) (Mac OS X)

Adobe Reader <= 10.1.10 / 11.0.07 Multiple Vulnerabilities (APSB14-20) (Mac OS X)

Adobe Reader <= 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-24) (Mac OS X)

Adobe Reader <= 15.006.30434 / 17.011.30096 / 18.011.20055 Multiple Vulnerabilities (APSB18-29) (macOS)

Adobe Reader <= 15.006.30448 / 17.011.30099 / 18.011.20058 Multiple Vulnerabilities (APSB18-34) (macOS)

Adobe Reader <= 15.006.30452 / 17.011.30102 / 18.011.20063 Multiple Vulnerabilities (APSB18-30) (macOS)

Adobe Reader <= 15.006.30456 / 17.011.30105 / 19.008.20080 Multiple Vulnerabilities (APSB18-41) (macOS)

Adobe Reader <= 2015.006.30461 / 2017.011.30110 / 2019.010.20064 Multiple Vulnerabilities (APSB19-02) (macOS)

Adobe Reader <= 2015.006.30482 / 2017.011.30127 / 2019.010.20098 Multiple Vulnerabilities (APSB19-17) (macOS)

Adobe Reader <= 2015.006.30493 / 2017.011.30138 / 2019.010.20099 Multiple Vulnerabilities (APSB19-18) (macOS)

Adobe Reader <= 2015.006.30497 / 2017.011.30142 / 2019.012.20034 Multiple Vulnerabilities (APSB19-41) (macOS)

Adobe Reader <= 2015.006.30503 / 2017.011.30148 / 2019.012.20040 Multiple Vulnerabilities (APSB19-49) (macOS)

Adobe Reader <= 2015.006.30505 / 2017.011.30152 / 2019.021.20056 Multiple Vulnerabilities (APSB19-55) (macOS)

Adobe Reader <= 2015.006.30508 / 2017.011.30156 / 2019.021.20061 Multiple Vulnerabilities (APSB20-05) (macOS)

Adobe Reader <= 2015.006.30510 / 2017.011.30158 / 2020.006.20034 Multiple Vulnerabilities (APSB20-13) (macOS)

Adobe Reader <= 2019.010.20091 Vulnerability (APSB19-13) (macOS)

Adobe Reader Installed (Mac OS X)

Adobe Reader Unsupported Version Detection (Mac OS X)

Adobe Shockwave Player <= 11.5.1.601 Multiple Vulnerabilities (APSB09-16) (Mac OS X)

Adobe Shockwave Player <= 11.5.2.602 Multiple Vulnerabilities (APSB10-03) (Mac OS X)

Adobe Shockwave Player <= 11.5.6.606 Multiple Vulnerabilities (APSB10-12) (Mac OS X)

Adobe Shockwave Player <= 11.5.7.609 (APSB10-20) (Mac OS X)

Adobe Shockwave Player <= 11.5.8.612 (APSB10-25) (Mac OS X)

Adobe Shockwave Player <= 11.5.9.615 (APSB11-01) (Mac OS X)

Adobe Shockwave Player <= 11.5.9.620 (APSB11-17) (Mac OS X)

Adobe Shockwave Player <= 11.6.0.626 Multiple Memory Corruption Vulnerabilities (APSB11-19) (Mac OS X)

Adobe Shockwave Player <= 11.6.1.629 Multiple Memory Corruption Vulnerabilities (APSB11-27) (Mac OS X)

Adobe Shockwave Player <= 11.6.3.633 Multiple Code Execution Vulnerabilities (APSB12-02) (Mac OS X)

Adobe Shockwave Player <= 11.6.4.634 Multiple Memory Corruption Vulnerabilities (APSB12-13) (Mac OS X)

Adobe Shockwave Player <= 11.6.5.635 Multiple Memory Corruption Vulnerabilities (APSB12-17) (Mac OS X)

Adobe Shockwave Player <= 11.6.7.637 Multiple Vulnerabilities (APSB12-23) (Mac OS X)

Adobe Shockwave Player <= 11.6.8.638 Multiple Vulnerabilities (APSB13-06) (Mac OS X)

Adobe Shockwave Player <= 12.0.0.112 Multiple Vulnerabilities (APSB13-12) (Mac OS X)

Adobe Shockwave Player <= 12.0.2.122 Memory Corruption (APSB13-18) (Mac OS X)

Adobe Shockwave Player <= 12.0.3.133 Memory Corruption Vulnerabilities (APSB13-23) (Mac OS X)

Adobe Shockwave Player <= 12.0.6.147 Memory Corruptions (APSB13-29) (Mac OS X)

Adobe Shockwave Player <= 12.0.7.148 Multiple Memory Corruption Vulnerabilities (APSB14-06) (Mac OS X)

Adobe Shockwave Player <= 12.0.9.149 Unspecified Memory Corruption Vulnerabilities (APSB14-10) (Mac OS X)

Adobe Shockwave Player <= 12.1.8.158 Multiple RCE Vulnerabilities (APSB15-17) (Mac OS X)

Adobe Shockwave Player <= 12.1.9.160 Multiple RCE (APSB15-22) (Mac OS X)

Adobe Shockwave Player <= 12.2.0.162 RCE (APSB15-26) (Mac OS X)

Adobe Shockwave Player <= 12.3.4.204 Multiple memory corruption vulnerabilities (APSB19-20) (Mac OS X)

Adobe Shockwave Player Installed (Mac OS X)

AgileBits 1Password 6.3.3 Multiple Vulnerabilities (macOS)

AgileBits 1Password Installed (macOS)

Airport < 4.2

AirPort Update 2006-001 / Security Update 2006-005

Apple iTunes < 12.6 Multiple Vulnerabilities (macOS) (credentialed check)

Apple iTunes < 12.6.2 Multiple Vulnerabilities (macOS) (credentialed check)

Apple Keynote < 6.0 Presentation Mode Lock Engagement Screen Lock Bypass

Apple Keynote Detection (Mac OS X)

Apple Keynote Presentation < 2.0.2 keynote: URI Handler Arbitrary File Access

Apple Mac OS X USB Keyboard Ctrl Key Root Access (Apple SA 2003-12-19)

Apple Motion < 5.1 OZDocument::parseElement() Function MOTN File Subview Attribute Handling Integer Overflow

Apple Motion Installed (Mac OS X)

Apple Pages < 2.1 / 5.1 Microsoft Word Document Handling Double Free Arbitrary Code Execution

Apple Pages Installed (Mac OS X)

Apple Remote Desktop < 3.5.3 / 3.6.1 Information Disclosure (Mac OS X)

Apple Remote Desktop < 3.5.4 / 3.7 Multiple Vulnerabilities (Mac OS X)

Apple Remote Desktop Admin Detection (Mac OS X)

Apple Safari Installed (macOS)

Apple Xcode < 10.2 Code Execution (macOS)

Apple Xcode < 11.3 Code Execution (macOS)

Apple Xcode < 4.4 Multiple Vulnerabilities (Mac OS X) (BEAST)

Apple Xcode < 5.0 (Mac OS X)

Apple Xcode < 6.0.1 (Mac OS X)

Apple Xcode < 6.2 (Mac OS X)

Apple Xcode < 6.3 (Mac OS X)

Apple Xcode < 7.0 (Mac OS X) (POODLE)

Apple Xcode < 7.1 (Mac OS X)

Apple Xcode < 7.2 Multiple Vulnerabilities (Mac OS X)

Apple Xcode < 7.3 Multiple Vulnerabilities (Mac OS X)

Apple Xcode < 7.3.1 Multiple RCE (Mac OS X)

Apple Xcode < 8.0 otool RCE (Mac OS X)

Apple Xcode < 8.1 Node.js Multiple RCE (macOS)

Apple Xcode < 9.0 Multiple RCE (macOS)

Apple Xcode IDE Detection (Mac OS X)

APPLE-SA-2014-12-22-1 OS X NTP Security Update (Mac OS X)

Atlassian SourceTree 1.0b2 < 2.7.6 Remote Code Execution Vulnerabilities (Mac OSX)

Atlassian SourceTree 1.2 < 3.1.1 Multiple remote code execution vulnerabilities

Autodesk SketchBook Pro < 6.2.5 / SketchBook Copic Edition < 2.0.2 Heap Buffer Overflow

Autodesk SketchBook Pro < 6.2.6 Multiple Overflow Vulnerabilities

Autodesk SketchBook Pro Detection

Bitcoin Installed (Mac OS X)

BlackBerry Link Detection (Mac OS X)

BlackBerry Link Multiple Vulnerabilities (Mac OS X)

Blue Coat ProxyClient < 3.3.3.3 / 3.4.x < 3.4.4.10 Certificate Validation MitM

Blue Coat ProxyClient Installed (Mac OS X)

CylancePROTECT 2.0.x < 2.0.1480 SSL Validation (Cy2008-002) (macOS)

CylancePROTECT Detection (Mac OS X)

Dropbox Installed (Mac OS X)

Evernote Installed (Mac OS X)

EvoCam 3.6.6 / 3.6.7 Web Server GET Request Overflow

F-Secure Key Detection (Mac OS X)

F-Secure Key Plaintext Information Disclosure (Mac OS X)

Facebook OSQuery Code Signing Bypass (macOS)

Facebook OSQuery Installed (macOS)

FileVault Detection (Mac OS X)

FileZilla Client Detection (Mac OS X)

Firefox 18.x Multiple Vulnerabilities (Mac OS X)

Firefox 3.6 < 3.6.18 Multiple Vulnerabilities (Mac OS X)

Firefox 3.6 < 3.6.23 Multiple Vulnerabilities (Mac OS X)

Firefox 3.6 < 3.6.24 Multiple Vulnerabilities (Mac OS X)

Firefox 3.6 < 3.6.25 Jar File Enter Key Dialog Bypass (Mac OS X)

Firefox 3.6 < 3.6.26 Multiple Vulnerabilities (Mac OS X)

Firefox 3.6.x < 3.6.27 png\_decompress\_chunk Integer Overflow (Mac OS X)

Firefox 3.6.x < 3.6.28 Multiple Vulnerabilities (Mac OS X)

Firefox 8.x Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.1 Memory Corruption (Mac OS X)

Firefox < 10.0.10 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.11 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.12 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.2 png\_decompress\_chunk Integer Overflow (Mac OS X)

Firefox < 10.0.3 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.4 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.5 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.6 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.7 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.8 Multiple Vulnerabilities (Mac OS X)

Firefox < 10.0.9 Multiple Vulnerabilities (Mac OS X)

Firefox < 12.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 13.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 14.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 15.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 16.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 16.0.1 Multiple Vulnerabilities (Mac OS X)

Firefox < 16.0.2 Multiple Vulnerabilities (Mac OS X)

Firefox < 17.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 17.0.1 Multiple Vulnerabilities (Mac OS X)

Firefox < 18.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 19.0.2 nsHTMLEditor Use-After-Free (Mac OS X)

Firefox < 20 Multiple Vulnerabilities (Mac OS X)

Firefox < 21.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 22.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 23.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 24.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 25.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 25.0.1 NSS and NSPR Multiple Vulnerabilities (Mac OS X)

Firefox < 26.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 27.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 28.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 29.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 30.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 31.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 32.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 32.0.3 NSS Signature Verification Vulnerability (Mac OS X)

Firefox < 33.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 34.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 35.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 36.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 36.0.3 JIT Code Execution (Mac OS X)

Firefox < 36.0.4 SVG Bypass Privilege Escalation (Mac OS X)

Firefox < 37.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 37.0.1 HTTP/2 Alt-Svc Header Certificate Verification Bypass (Mac OS X)

Firefox < 37.0.2 Failed Plugin Memory Corruption (Mac OS X)

Firefox < 38.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 39.0 Multiple Vulnerabilities (Mac OS X) (Logjam)

Firefox < 39.0.3 PDF Reader Arbitrary File Access (Mac OS X)

Firefox < 40 Multiple Vulnerabilities (Mac OS X)

Firefox < 40.0.3 Multiple Vulnerabilities (Mac OS X)

Firefox < 41 Multiple Vulnerabilities (Mac OS X)

Firefox < 41.0.2 'fetch' API Cross-Origin Bypass (Mac OS X)

Firefox < 42 Multiple Vulnerabilities (Mac OS X)

Firefox < 43 Multiple Vulnerabilities (Mac OS X)

Firefox < 44 Multiple Vulnerabilities (Mac OS X)

Firefox < 44.0.2 Service Workers Security Bypass (Mac OS X)

Firefox < 45 Multiple Vulnerabilities (Mac OS X)

Firefox < 46 Multiple Vulnerabilities (Mac OS X)

Firefox < 47 Multiple Vulnerabilities (Mac OS X)

Firefox < 48 Multiple Vulnerabilities (Mac OS X)

Firefox < 5.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 7.0 Multiple Vulnerabilities (Mac OS X)

Firefox < 8.0 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 17.x < 17.0.3 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 17.x < 17.0.4 nsHTMLEditor Use-After-Free (Mac OS X)

Firefox ESR 17.x < 17.0.5 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 17.x < 17.0.6 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 17.x < 17.0.7 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 17.x < 17.0.8 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 17.x < 17.0.9 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.1 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.1.1 NSS and NSPR Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.2 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.3 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.4 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.5 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.6 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.8 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 24.x < 24.8.1 NSS Signature Verification Vulnerability (Mac OS X)

Firefox ESR 24.x< 24.7 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 31.x < 31.1 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 31.x < 31.1.1 NSS Signature Verification Vulnerability (Mac OS X)

Firefox ESR 31.x < 31.2 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 31.x < 31.3 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 31.x < 31.4 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 31.x < 31.5 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 31.x < 31.5.2 JIT Code Execution (Mac OS X)

Firefox ESR 31.x < 31.5.3 SVG Bypass Privilege Escalation (Mac OS X)

Firefox ESR 31.x < 31.6 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 31.x < 31.7 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 45.x < 45.1 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 45.x < 45.2 Multiple Vulnerabilities (Mac OS X)

Firefox ESR 45.x < 45.3 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 17.0.10 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 17.0.11 Null\_Cipher Code Execution (Mac OS X)

Firefox ESR < 17.0.2 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 31.8 Multiple Vulnerabilities (Mac OS X) (Logjam)

Firefox ESR < 38.1 Multiple Vulnerabilities (Mac OS X) (Logjam)

Firefox ESR < 38.1.1 PDF Reader Arbitrary File Access (Mac OS X)

Firefox ESR < 38.2 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 38.2.1 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 38.3 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 38.4 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 38.5 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 38.6 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 38.6.1 Multiple Graphite 2 Library RCE (Mac OS X)

Firefox ESR < 38.7 Multiple Vulnerabilities (Mac OS X)

Firefox ESR < 38.8 Multiple Vulnerabilities (Mac OS X)

Firefox Installed (Mac OS X)

Flash Player for Mac < 10.3.181.14 Remote Code Execution (APSB11-12)

Flash Player for Mac < 10.3.181.22 XSS (APSB11-13)

Flash Player for Mac < 10.3.181.26 Remote Memory Corruption (APSB11-18)

Flash Player for Mac <= 10.3.181.36 Multiple Vulnerabilities (APSB11-21)

Flash Player for Mac <= 10.3.183.10 / 11.0.1.152 Multiple Vulnerabilities (APSB11-28)

Flash Player for Mac <= 10.3.183.14 / 11.1.102.62 Multiple Vulnerabilities (APSB12-03)

Flash Player for Mac <= 10.3.183.15 / 11.1.102.62 Multiple Vulnerabilities (APSB12-05)

Flash Player for Mac <= 10.3.183.16 / 11.1.102.63 Multiple Memory Corruption Vulnerabilities (APSB12-07)

Flash Player for Mac <= 10.3.183.18 / 11.2.202.233 Object Confusion Vulnerability (APSB12-09)

Flash Player for Mac <= 10.3.183.19 / 11.3.300.256 Multiple Vulnerabilities (APSB12-14)

Flash Player for Mac <= 10.3.183.22 / 11.4.402.264 Code Execution (APSB12-19)

Flash Player for Mac <= 10.3.183.23 / 11.4.402.265 Multiple Vulnerabilities (APSB12-22)

Flash Player for Mac <= 10.3.183.29 / 11.4.402.287 Multiple Vulnerabilities (APSB12-24)

Flash Player for Mac <= 10.3.183.43 / 11.5.502.110 Multiple Vulnerabilities (APSB12-27)

Flash Player for Mac <= 10.3.183.48 / 11.5.502.136 Buffer Overflow (APSB13-01)

Flash Player for Mac <= 10.3.183.50 / 11.5.502.146 Multiple Vulnerabilities (APSB13-04)

Flash Player for Mac <= 10.3.183.51 / 11.5.502.149 Multiple Vulnerabilities (APSB13-05)

Flash Player for Mac <= 10.3.183.61 / 11.6.602.167 Multiple Vulnerabilities (APSB13-08)

Flash Player for Mac <= 10.3.183.67 / 11.6.602.171 Multiple Vulnerabilities (APSB13-09)

Flash Player for Mac <= 10.3.183.68 / 11.6.602.180 Multiple Vulnerabilities (APSB13-11)

Flash Player for Mac <= 10.3.183.7 Multiple Vulnerabilities (APSB11-26)

Flash Player for Mac <= 10.3.183.75 / 11.7.700.169 Multiple Vulnerabilities (APSB13-14)

Flash Player for Mac <= 10.3.183.86 / 11.7.700.203 Memory Corruption (APSB13-16)

Flash Player for Mac <= 10.3.183.90 / 11.7.700.225 Memory Corruption (APSB13-17)

Flash Player for Mac <= 11.3.300.270 Code Execution (APSB12-18)

Flash Player for Mac <= 11.7.700.232 / 11.8.800.94 Memory Corruptions (APSB13-21)

Flash Player for Mac <= 11.7.700.242 / 11.9.900.117 Memory Corruptions (APSB13-26)

Flash Player for Mac <= 11.7.700.252 / 11.9.900.152 Multiple Vulnerabilities (APSB13-28)

Flash Player for Mac <= 11.7.700.257 / 11.9.900.170 Multiple Vulnerabilities (APSB14-02)

Flash Player for Mac <= 11.7.700.260 / 12.0.0.43 Unspecified Remote Code Execution (APSB14-04)

Flash Player for Mac <= 11.7.700.261 / 12.0.0.44 Multiple Vulnerabilities (APSB14-07) (Mac OS X)

Flash Player for Mac <= 11.7.700.269 / 12.0.0.70 Multiple Vulnerabilities (APSB14-08) (Mac OS X)

Flash Player for Mac <= 11.7.700.272 / 12.0.0.77 Multiple Vulnerabilities (APSB14-09) (Mac OS X)

Flash Player for Mac <= 11.7.700.275 / 13.0.0.201 Pixel Bender Component Buffer Overflow (APSB14-13)

Flash Player for Mac <= 13.0.0.206 Multiple Vulnerabilities (APSB14-14)

Flash Player for Mac <= 13.0.0.214 Multiple Vulnerabilities (APSB14-16)

Flash Player for Mac <= 14.0.0.125 Multiple Vulnerabilities (APSB14-17)

Flash Player for Mac <= 14.0.0.145 Multiple Vulnerabilities (APSB14-18)

Flash Player for Mac <= 14.0.0.179 Multiple Vulnerabilities (APSB14-21)

Flash Player for Mac <= 15.0.0.167 Multiple Vulnerabilities (APSB14-22)

Flash Player For Mac <= 15.0.0.189 Multiple Vulnerabilities (APSB14-24)

Flash Player For Mac <= 15.0.0.223 Dereferenced Memory Pointer RCE (APSB14-26)

Flash Player For Mac <= 15.0.0.239 Multiple Vulnerabilities (APSB14-27)

Flash Player For Mac <= 16.0.0.235 Multiple Vulnerabilities (APSB15-01)

Flash Player For Mac <= 16.0.0.257 Information Disclosure (APSB15-02)

Flash Player For Mac <= 16.0.0.287 Unspecified Code Execution (APSA15-01)

Flash Player For Mac <= 16.0.0.296 Unspecified Code Execution (APSA15-02 / APSB15-04)

Flash Player For Mac <= 16.0.0.305 Multiple Vulnerabilities (APSB15-05)

Fortinet FortiClient 6.0.1 < 6.0.5 Local DoS (macOS)

Fortinet FortiClient 6.2.x < 6.2.1 Missing Encryption Of Sensitive Data Vulnerability (macOS)

Fortinet FortiClient < 6.2.2 Information Disclosure MitM (FG-IR-18-100) (macOS)

Fortinet FortiClient Detection (macOS)

Fortinet FortiClient Unsupported Version Detection (macOS)

Fortinet FortiOS (Mac OS X) 5.4.1 < 5.4.11 / 5.6.x < 5.6.9 / 6.0.x < 6.0.5 SSL VPN Security Bypass (FG-IR-18-389)

Fortinet FortiOS (Mac OS X) 5.4.6 <= 5.4.12 / 5.6.3 < 5.6.8 / 6.0.x < 6.0.5 SSL VPN Directory Traversal (FG-IR-18-384)

Fortinet FortiOS (Mac OS X) 5.6.0 < 5.6.8 / 6.0.x < 6.0.5 multiple pre-auth XSS vulnerabilities on SSL VPN (FG-IR-18-383)

Fortinet FortiOS (Mac OS X) < 5.2.15, 5.4.0 < 6.0.5 SSL VPN Web Portal Host Header Redirection (FG-IR-19-002)

Fortinet FortiOS (Mac OS X) < 5.6.11, 6.0.x < 6.0.5 SSL VPN Heap Buffer Overflow (FG-IR-18-388)

Fortinet FortiOS (Mac OS X) <= 5.4 / 5.6.x < 5.6.8 / 6.0.x < 6.0.5 SSL VPN Web Portal login redir XSS (FG-IR-17-242)

Fortinet FortiOS (Mac OS X) <= 5.4, 5.6.x < 5.6.8, 6.0.x < 6.0.5 SSL VPN Buffer Overflow (FG-IR-18-387)

GitHub < 1.9.4 .git/config Command Execution (Mac OS X)

GitHub Installed (Mac OS X)

GNU Bash Local Environment Variable Handling Command Injection (Mac OS X) (Shellshock)

GNU Image Manipulation Program (GIMP) Installed (Mac OS X)

Google Chrome < 29.0.1547.57 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 30.0.1599.101 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 30.0.1599.66 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 31.0.1650.48 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 31.0.1650.57 Multiple Memory Corruptions (Mac OS X)

Google Chrome < 31.0.1650.63 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 32.0.1700.102 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 32.0.1700.77 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 33.0.1750.117 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 33.0.1750.146 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 33.0.1750.149 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 33.0.1750.152 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 34.0.1847.116 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 34.0.1847.131 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 34.0.1847.137 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 35.0.1916.114 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 35.0.1916.153 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 36.0.1985.125 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 36.0.1985.143 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 37.0.2062.120 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 37.0.2062.124 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 37.0.2062.94 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 38.0.2125.101 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 38.0.2125.104 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 38.0.2125.122 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 39.0.2171.65 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 39.0.2171.71 Flash Player Remote Code Execution (Mac OS X)

Google Chrome < 39.0.2171.95 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 39.0.2171.99 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 40.0.2214.111 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 40.0.2214.91 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 40.0.2214.93 Flash Player Multiple Remote Code Execution (Mac OS X)

Google Chrome < 41.0.2272.118 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 41.0.2272.76 Multiple Vulnerabilities (Mac OS X) (FREAK)

Google Chrome < 42.0.2311.135 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 42.0.2311.152 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 42.0.2311.90 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 43.0.2357.124 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 43.0.2357.130 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 43.0.2357.132 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 43.0.2357.134 RCE Multiple Vulnerabilities (Mac OS X)

Google Chrome < 43.0.2357.65 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 44.0.2403.155 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 44.0.2403.89 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 45.0.2454.101 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 45.0.2454.85 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 45.0.2454.99 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 46.0.2490.71 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 46.0.2490.80 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 46.0.2490.86 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 47.0.2526.106 Multiple RCE (Mac OS X)

Google Chrome < 47.0.2526.73 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 47.0.2526.80 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 48.0.2564.109 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 48.0.2564.116 Blink Same-Origin Policy Bypass (Mac OS X)

Google Chrome < 48.0.2564.82 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 49.0.2623.108 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 49.0.2623.75 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 49.0.2623.87 Multiple RCE

Google Chrome < 50.0.2661.102 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 50.0.2661.75 Multiple Vulnerabilities

Google Chrome < 50.0.2661.94 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 51.0.2704.103 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 51.0.2704.63 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 51.0.2704.79 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 52.0.2743.116 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 52.0.2743.82 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 53.0.2785.113 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 53.0.2785.143 Multiple Vulnerabilities (Mac OS X)

Google Chrome < 53.0.2785.89 Multiple Vulnerabilities (Mac OS X

Google Chrome < 54.0.2840.59 Multiple Vulnerabilities (macOS)

Google Chrome < 54.0.2840.87 V8 Globals Stable Map Assumption Handling RCE (macOS)

Google Chrome < 54.0.2840.98 Multiple Vulnerabilities (macOS)

Google Chrome < 55.0.2883.75 Multiple Vulnerabilities (macOS)

Google Chrome < 56.0.2924.76 Multiple Vulnerabilities (macOS)

Google Chrome < 57.0.2987.133 Multiple Vulnerabilities (macOS)

Google Chrome < 57.0.2987.98 Multiple Vulnerabilities (macOS)

Google Chrome < 58.0.3029.81 Multiple Vulnerabilities (macOS)

Google Chrome < 58.0.3029.96 WebRTC Frame Order Handling Race Condition (macOS)

Google Chrome < 59.0.3071.104 Multiple Vulnerabilities (macOS)

Google Chrome < 59.0.3071.86 Multiple Vulnerabilities (macOS)

Google Chrome < 60.0.3112.78 Multiple Vulnerabilities (macOS)

Google Chrome < 61.0.3163.100 Multiple Vulnerabilities (macOS)

Google Chrome < 61.0.3163.110 Multiple Vulnerabilities (macOS)

Google Chrome < 61.0.3163.79 Multiple Vulnerabilities (macOS)

Google Chrome < 62.0.3202.62 Multiple Vulnerabilities (macOS)

Google Chrome < 62.0.3202.89 Multiple Vulnerabilities (macOS)

Google Chrome < 62.0.3202.94 Out of bounds read flaw in V8 (macOS)

Google Chrome < 63.0.3239.108 Multiple Vulnerabilities (macOS)

Google Chrome < 63.0.3239.84 Multiple Vulnerabilities (macOS)

Google Chrome < 64.0.3282.119 Multiple Vulnerabilities (macOS)

Google Chrome < 64.0.3282.140 V8 Factory::NewFunction() RCE (macOS)

Google Chrome < 64.0.3282.167 V8 JSFunction::CalculateInstanceSizeForDerivedClass() RCE (macOS)

Google Chrome < 65.0.3325.146 Multiple Vulnerabilities (macOS)

Google Chrome < 66.0.3359.117 Multiple Vulnerabilities (macOS)

Google Chrome < 66.0.3359.170 Multiple Vulnerabilities (macOS)

Google Chrome < 67.0.3396.62 Multiple Vulnerabilities (macOS)

Google Chrome < 68.0.3440.75 Multiple Vulnerabilities

Google Chrome < 69.0.3497.100 Vulnerability

Google Chrome < 69.0.3497.81 Multiple Vulnerabilities

Google Chrome < 69.0.3497.92 Vulnerability

Google Chrome < 70.0.3538.102 Vulnerability

Google Chrome < 70.0.3538.110 Vulnerability

Google Chrome < 70.0.3538.67 Multiple Vulnerabilities

Google Chrome < 71.0.3578.80 Multiple Vulnerabilities

Google Chrome < 71.0.3578.98

Google Chrome < 72.0.3626.121 Vulnerability

Google Chrome < 72.0.3626.81 Multiple Vulnerabilities

Google Chrome < 72.0.3626.96 Vulnerability

Google Chrome < 73.0.3683.103 Heap Corruption

Google Chrome < 73.0.3683.75 Multiple Vulnerabilities

Google Chrome < 74.0.3729.108 Multiple Vulnerabilities

Google Chrome < 74.0.3729.131 Multiple Vulnerabilities

Google Chrome < 74.0.3729.157 Vulnerability

Google Chrome < 75.0.3770.142 Multiple Vulnerabilities

Google Chrome < 75.0.3770.80 Multiple Vulnerabilities

Google Chrome < 75.0.3770.90 Vulnerability

Google Chrome < 76.0.3809.100 Multiple Vulnerabilities

Google Chrome < 76.0.3809.132 Use-After-Free Vulnerability

Google Chrome < 76.0.3809.87 Multiple Vulnerabilities

Google Chrome < 77.0.3865.120 Multiple Vulnerabilities

Google Chrome < 77.0.3865.75 Multiple Vulnerabilities

Google Chrome < 77.0.3865.90 Multiple Vulnerabilities

Google Chrome < 78.0.3904.108 Multiple Vulnerabilities

Google Chrome < 78.0.3904.70 Multiple Vulnerabilities

Google Chrome < 78.0.3904.87 Multiple Vulnerabilities

Google Chrome < 78.0.3904.97 Vulnerability

Google Chrome < 79.0.3945.117 Multiple Vulnerabilities

Google Chrome < 79.0.3945.130 Multiple Vulnerabilities

Google Chrome < 79.0.3945.79 Multiple Vulnerabilities

Google Chrome < 79.0.3945.88 Vulnerability

Google Chrome < 80.0.3987.116 Multiple Vulnerabilities

Google Chrome < 80.0.3987.122 Multiple Vulnerabilities

Google Chrome < 80.0.3987.132 Multiple Vulnerabilities

Google Chrome < 80.0.3987.149 Multiple Vulnerabilities

Google Chrome < 80.0.3987.162 Multiple Vulnerabilities

Google Chrome < 80.0.3987.87 Multiple Vulnerabilities

Google Chrome < 81.0.4044.113 Vulnerability

Google Chrome < 81.0.4044.92 Multiple Vulnerabilities

Google Chrome Browser Extension Enumeration (macOS)

Google Chrome Installed (Mac OS X)

Google Picasa < 3.9 Build 137.119 Multiple Vulnerabilities (Mac OS X)

Google Picasa < 3.9 Build 3.9.14.34 Multiple Vulnerabilities (Mac OS X)

Google Picasa Installed (Mac OS X)

Google Santa Code Signing Bypass (macOS)

Google Santa Installed (macOS)

HandBrake Installed (macOS)

HandBrake OSX/Proton.B Trojan Backdoor (macOS)

iCal < 1.5.4

iPhoto < 6.0.6

iPhoto < 7.1.2 Format String Vulnerability

iTunes < 10.5.1 Update Authenticity Verification Weakness (Mac OS X)

iTunes < 10.6.3 m3u Multiple Buffer Overflow Vulnerabilities (Mac OS X)

iTunes < 11.0.3 Certificate Validation Vulnerability (Mac OS X)

iTunes < 11.1.4 Tutorials Content Injection (Mac OS X)

iTunes < 11.2.1 User Directory Insecure Permissions Vulnerability (Mac OS X)

iTunes < 12.7 Data Sync Vulnerability (Mac OS)

iTunes < 4.7.1

iTunes < 4.8.0 MPEG-4 Parsing Overflow (Mac OS X)

iTunes < 6.0.5 AAC File Integer Overflow (Mac OS X)

iTunes < 7.4 Malformed Music File Heap Overflow (Mac OS X)

iTunes < 8.1 Malicious Podcast Information Disclosure (Mac OS X)

iTunes < 8.2 itms: URL Stack Overflow (Mac OS X)

iTunes < 9.0.1 PLS File Buffer Overflow (Mac OS X)

iTunes < 9.1 Multiple Vulnerabilities (Mac OS X)

iTunes < 9.2.1 'itpc:' Buffer Overflow (Mac OS X)

iTunes Mobile iOS Device Backup Enumeration (Mac OS X)

iTunes Version Detection (macOS)

Jamf Installed (macOS)

Jenkins Installed (macOS)

KB4019460: Security Update for the libjpeg Information Disclosure Vulnerability for Mono Framework (macOS)

LibreOffice 4.2.x < 4.2.3 OpenSSL Multiple Vulnerabilities (Mac OS X) (Heartbleed)

LibreOffice 6.1.x < 6.1.3.2 Arbitrary Code Execution (macOS)

LibreOffice < 3.3.3 / 3.4.0 LWP File Handling Overflow (Mac OS X)

LibreOffice < 3.4.6 / 3.5.1 XML External Entity RDF Document Handling Information Disclosure (Mac OS X)

LibreOffice < 3.5.3 RTF File Handling Remote Memory Corruption (Mac OS X)

LibreOffice < 3.5.5 Multiple Heap-Based Buffer Overflows (Mac OS X)

LibreOffice < 3.5.7 / 3.6.1 Multiple Denial of Service Vulnerabilities (Mac OS X)

LibreOffice < 3.6.7 / 4.0.4 / 4.1.0 .docm Import DoS (Mac OS X)

LibreOffice < 4.1.5 / 4.2.0 Python Multiple Vulnerabilities (Mac OS X)

LibreOffice < 4.2.5 Unspecified Macro Code Execution (Mac OS X)

LibreOffice < 4.2.8 / 4.3.5 RTF File Handling Code Execution (Mac OS X)

LibreOffice < 4.4.5 Multiple Vulnerabilities (Mac OS X)

LibreOffice < 4.4.6 / 5.x < 5.0.1 Document Bookmark Arbitrary Code Execution (Mac OS X)

LibreOffice < 5.0.5 Multiple RCE (Mac OS X)

LibreOffice < 5.1.4 RTF Character Style Index RCE (macOS)

LibreOffice < 5.1.6 / 5.2.5 / 5.3.0 Multiple Vulnerabilities (macOS)

LibreOffice < 5.4.5 or 6.x < 6.0.1 Multiple Vulnerabilities (macOS)

LibreOffice < 5.4.6 or 6.x < 6.0.2 Heap Buffer Overflow (macOS)

LibreOffice < 5.4.7 or 6.x < 6.0.4 Information Disclosure (macOS)

LibreOffice < 6.2.5 Multiple Vulnerabilities (macOS)

LibreOffice < 6.2.7 / 6.3.x < 6.3.1 Directory Traversal (macOS)

LibreOffice Detection (Mac OS X)

LibreOffice Unsupported (Mac OS X)

List Installed Mac OS X Software

Mac OS X 10.10.5 / 10.11.6 Multiple Vulnerabilities (Security Update 2016-002 / 2016-006)

Mac OS X 10.10.x < 10.10.1 Multiple Vulnerabilities

Mac OS X 10.10.x < 10.10.2 Multiple Vulnerabilities (POODLE)

Mac OS X 10.10.x < 10.10.3 Multiple Vulnerabilities (FREAK)

Mac OS X 10.10.x < 10.10.4 Multiple Vulnerabilities (GHOST) (Logjam)

Mac OS X 10.10.x < 10.10.5 Multiple Vulnerabilities

Mac OS X 10.11.x < 10.11.2 Multiple Vulnerabilities

Mac OS X 10.11.x < 10.11.3 Multiple Vulnerabilities

Mac OS X 10.11.x < 10.11.4 Multiple Vulnerabilities

Mac OS X 10.11.x < 10.11.5 Multiple Vulnerabilities

Mac OS X 10.11.x < 10.11.6 Multiple Vulnerabilities

Mac OS X 10.3.x < 10.3.9 Multiple Vulnerabilities

Mac OS X 10.4.x < 10.4.1 Multiple Vulnerabilities

Mac OS X 10.4.x < 10.4.10 IPv6 Type 0 Route Headers DoS

Mac OS X 10.4.x < 10.4.2 Multiple Vulnerabilities

Mac OS X 10.4.x < 10.4.3 Multiple Vulnerabilities

Mac OS X 10.4.x < 10.4.5 Kernel Undocumented System Call Local DoS

Mac OS X 10.4.x < 10.4.6 Firmware Unspecified Password Bypass

Mac OS X 10.4.x < 10.4.7 Multiple Vulnerabilities

Mac OS X 10.4.x < 10.4.8 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.1 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.2 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.3 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.4 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.5 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.6 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.7 Multiple Vulnerabilities

Mac OS X 10.5.x < 10.5.8 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.1 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.2 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.3 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.4 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.5 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.6 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.7 Multiple Vulnerabilities

Mac OS X 10.6.x < 10.6.8 Multiple Vulnerabilities

Mac OS X 10.7.x < 10.7.2 Multiple Vulnerabilities

Mac OS X 10.7.x < 10.7.3 Multiple Vulnerabilities (BEAST)

Mac OS X 10.7.x < 10.7.4 Multiple Vulnerabilities (BEAST)

Mac OS X 10.7.x < 10.7.5 Multiple Vulnerabilities (BEAST)

Mac OS X 10.8 < 10.8.5 Supplemental Update

Mac OS X 10.8.x < 10.8.2 Multiple Vulnerabilities

Mac OS X 10.8.x < 10.8.3 Multiple Vulnerabilities

Mac OS X 10.8.x < 10.8.4 Multiple Vulnerabilities

Mac OS X 10.8.x < 10.8.5 Multiple Vulnerabilities

Mac OS X 10.9.5 / 10.10.5 Multiple Vulnerabilities (Security Update 2016-002)

Mac OS X 10.9.5 / 10.10.5 Multiple Vulnerabilities (Security Update 2016-003)

Mac OS X 10.9.5 and 10.10.5 Multiple Vulnerabilities (Security Update 2016-004)

Mac OS X 10.9.x < 10.9.2 Multiple Vulnerabilities

Mac OS X 10.9.x < 10.9.4 Multiple Vulnerabilities

Mac OS X 10.9.x < 10.9.5 Multiple Vulnerabilities

Mac OS X 10.x < 10.9 Multiple Vulnerabilities (BEAST)

Mac OS X : Apple Safari < 10.0 Multiple Vulnerabilities

Mac OS X : Apple Safari < 3.1

Mac OS X : Apple Safari < 3.1.1

Mac OS X : Apple Safari < 3.1.2

Mac OS X : Apple Safari < 3.2

Mac OS X : Apple Safari < 4.0

Mac OS X : Apple Safari < 4.0.2

Mac OS X : Apple Safari < 4.0.3

Mac OS X : Apple Safari < 4.0.4

Mac OS X : Apple Safari < 4.0.5

Mac OS X : Apple Safari < 5.0 / 4.1

Mac OS X : Apple Safari < 5.0.1 / 4.1.1

Mac OS X : Apple Safari < 5.0.2 / 4.1.2

Mac OS X : Apple Safari < 5.0.3 / 4.1.3

Mac OS X : Apple Safari < 5.0.4

Mac OS X : Apple Safari < 5.0.5

Mac OS X : Apple Safari < 5.1 / 5.0.6

Mac OS X : Apple Safari < 5.1.1

Mac OS X : Apple Safari < 5.1.10 Memory Corruptions

Mac OS X : Apple Safari < 5.1.4 Multiple Vulnerabilities

Mac OS X : Apple Safari < 5.1.7 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.0 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.0.1 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.0.2 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.0.3 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.0.4 SVG File Handling Arbitrary Code Execution

Mac OS X : Apple Safari < 6.0.5 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.1 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.1.1 / 7.0.1 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.1.2 / 7.0.2 Multiple Memory Corruption Vulnerabilities

Mac OS X : Apple Safari < 6.1.3 / 7.0.3 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.1.4 / 7.0.4 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.1.5 / 7.0.5 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.1.6 / 7.0.6 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2 / 7.1 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2.2 / 7.1.2 / 8.0.2 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2.3 / 7.1.3 / 8.0.3 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2.4 / 7.1.4 / 8.0.4 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2.5 / 7.1.5 / 8.0.5 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2.6 / 7.1.6 / 8.0.6 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2.7 / 7.1.7 / 8.0.7 Multiple Vulnerabilities

Mac OS X : Apple Safari < 6.2.8 / 7.1.8 / 8.0.8 Multiple Vulnerabilities

Mac OS X : Apple Safari < 9.0 Multiple Vulnerabilities

Mac OS X : Apple Safari < 9.0.1 Multiple RCE

Mac OS X : Apple Safari < 9.0.2 Multiple RCE

Mac OS X : Apple Safari < 9.0.3 Multiple Vulnerabilities

Mac OS X : Apple Safari < 9.1.1 Multiple Vulnerabilities

Mac OS X : Apple Safari < 9.1.2 Multiple Vulnerabilities

Mac OS X : Apple Safari < 9.1.3 WebKit Memory Corruption RCE

Mac OS X : Cisco AnyConnect Secure Mobility Client 2.x / 3.x < 3.0(629) Multiple Vulnerabilities

Mac OS X : Cisco AnyConnect Secure Mobility Client 2.x / 3.x < 3.1(5170) Multiple OpenSSL Vulnerabilities

Mac OS X : Cisco AnyConnect Secure Mobility Client 3.0.x / 3.1.x Local Privilege Escalation

Mac OS X : Cisco AnyConnect Secure Mobility Client 3.1 < 3.1(495) MiTM

Mac OS X : Cisco AnyConnect Secure Mobility Client 3.x < 3.1.10010.0 / 4.x < 4.1.4011.0 Arbitrary File Write

Mac OS X : Cisco AnyConnect Secure Mobility Client < 3.1(5187) (POODLE)

Mac OS X : Cisco AnyConnect Secure Mobility Client < 3.1(6042) Host Validation Vulnerability

Mac OS X : Cisco AnyConnect Secure Mobility Client < 3.1(7021) <= 4.0(48) Multiple Vulnerabilities (FREAK)

Mac OS X : Cisco AnyConnect Secure Mobility Client < 3.1.10010.0 / 4.0.x < 4.0.4013.0 / 4.1.x < 4.1.4011.0 IPC File Write Vulnerability

Mac OS X : Cisco AnyConnect Secure Mobility Client < 3.1.10010.0 / 4.0.x < 4.0.4014.0 / 4.1.x < 4.1.4011.0 Code Execution Vulnerability

Mac OS X : Cisco AnyConnect Secure Mobility Client < 3.1.13015.0 / 4.2.x < 4.2.1035.0 Multiple OpenSSL Vulnerabilities

Mac OS X : Cisco AnyConnect Secure Mobility Client < 3.1.8009.0 / 4.0.x < 4.0.2052.0 / 4.1.x < 4.1.28.0 Multiple Vulnerabilities

Mac OS X : Flip4Mac < 2.2.1 Unspecified Vulnerability

Mac OS X : GarageBand < 5.1

Mac OS X : iWork 9.x < 9.1 Multiple Vulnerabilities

Mac OS X : Java for Mac OS X 1.3.1 and 1.4.2 Release 2 Multiple Vulnerabilities

Mac OS X : Java for Mac OS X 10.4 Release 6

Mac OS X : Java for Mac OS X 10.4 Release 7

Mac OS X : Java for Mac OS X 10.4 Release 8

Mac OS X : Java for Mac OS X 10.4 Release 9

Mac OS X : Java for Mac OS X 10.5 Update 10

Mac OS X : Java for Mac OS X 10.5 Update 2

Mac OS X : Java for Mac OS X 10.5 Update 3

Mac OS X : Java for Mac OS X 10.5 Update 4

Mac OS X : Java for Mac OS X 10.5 Update 5

Mac OS X : Java for Mac OS X 10.5 Update 6

Mac OS X : Java for Mac OS X 10.5 Update 7

Mac OS X : Java for Mac OS X 10.5 Update 8

Mac OS X : Java for Mac OS X 10.5 Update 9

Mac OS X : Java for Mac OS X 10.6 Update 1

Mac OS X : Java for Mac OS X 10.6 Update 10

Mac OS X : Java for Mac OS X 10.6 Update 11

Mac OS X : Java for Mac OS X 10.6 Update 12

Mac OS X : Java for Mac OS X 10.6 Update 13

Mac OS X : Java for Mac OS X 10.6 Update 14

Mac OS X : Java for Mac OS X 10.6 Update 15

Mac OS X : Java for Mac OS X 10.6 Update 16

Mac OS X : Java for Mac OS X 10.6 Update 17

Mac OS X : Java for Mac OS X 10.6 Update 2

Mac OS X : Java for Mac OS X 10.6 Update 3

Mac OS X : Java for Mac OS X 10.6 Update 4

Mac OS X : Java for Mac OS X 10.6 Update 5

Mac OS X : Java for Mac OS X 10.6 Update 6 (BEAST)

Mac OS X : Java for Mac OS X 10.6 Update 7

Mac OS X : Java for Mac OS X 10.6 Update 9

Mac OS X : Java for Mac OS X 10.7 Update 1 (BEAST)

Mac OS X : Java for OS X 2012-004

Mac OS X : Java for OS X 2012-005

Mac OS X : Java for OS X 2012-006

Mac OS X : Java for OS X 2013-001

Mac OS X : Java for OS X 2013-002

Mac OS X : Java for OS X 2013-003

Mac OS X : Java for OS X 2013-004

Mac OS X : Java for OS X 2013-005

Mac OS X : Java for OS X 2014-001

Mac OS X : Java for OS X Lion 2012-001

Mac OS X : OS X Server < 2.1.1 Multiple Vulnerabilities

Mac OS X : OS X Server < 2.2.1 Multiple Vulnerabilities

Mac OS X : OS X Server < 2.2.2 Multiple Vulnerabilities

Mac OS X : OS X Server < 2.2.3 Wiki SQL Injection

Mac OS X : OS X Server < 2.2.5 SSLv3 Information Disclosure (POODLE)

Mac OS X : OS X Server < 3.0 Multiple Vulnerabilities

Mac OS X : OS X Server < 3.1.2 Heap-Based Buffer Overflow

Mac OS X : OS X Server < 3.2.1 Multiple Vulnerabilities

Mac OS X : OS X Server < 3.2.2 SSLv3 Information Disclosure (POODLE)

Mac OS X : OS X Server < 4.0 Multiple Vulnerabilities (POODLE)

Mac OS X : OS X Server < 4.1 Multiple Vulnerabilities (POODLE)

Mac OS X : OS X Server < 4.1.5 BIND DoS

Mac OS X : OS X Server < 5.0.15 Multiple Vulnerabilities

Mac OS X : OS X Server < 5.0.3 Multiple Vulnerabilities

Mac OS X < 10.10 Multiple Vulnerabilities (POODLE) (Shellshock)

Mac OS X < 10.11 Multiple Vulnerabilities (GHOST)

Mac OS X < 10.11.1 Multiple Vulnerabilities

Mac OS X < 10.3.4 Multiple Vulnerabilities

Mac OS X < 10.4 pty Permission Weakness

Mac OS X < 10.4.11 Multiple Vulnerabilities (Security Update 2007-008)

Mac OS X < 10.4.9 Multiple Vulnerabilities (Security Update 2007-003)

Mac OS X Admin Group User List

Mac OS X AFP Shared Folders Unauthenticated Access (Security Update 2010-006)

Mac OS X Airport Update 2007-001

Mac OS X BIND Dynamic Update Message Handling Remote DoS (Security Update 2009-004)

Mac OS X DNS Server Enumeration

Mac OS X EFI Function Execution Vulnerability (EFI Security Update 2015-002)

Mac OS X FileVault Plaintext Password Logging

Mac OS X Fraudulent DigiNotar Digital Certificates (Security Update 2011-005)

Mac OS X Fraudulent Digital Certificates (Security Update 2011-002)

Mac OS X Gatekeeper Disabled

Mac OS X iChat Link Handling Arbitrary Command Execution (Security Update 2004-09-16)

Mac OS X Java JRE Plug-in Capability Arbitrary Package Access (Security Update 2005-002)

Mac OS X Libxslt Function Type Confusion RCE (Security Update 2016-001)

Mac OS X Mac Defender Malware Detection

Mac OS X Multiple EFI Vulnerabilities (EFI Security Update 2015-001)

Mac OS X Multiple Vulnerabilities (Security Update 2003-12-19)

Mac OS X Multiple Vulnerabilities (Security Update 2004-01-26)

Mac OS X Multiple Vulnerabilities (Security Update 2004-05-03)

Mac OS X Multiple Vulnerabilities (Security Update 2004-05-24)

Mac OS X Multiple Vulnerabilities (Security Update 2004-06-07)

Mac OS X Multiple Vulnerabilities (Security Update 2004-08-09)

Mac OS X Multiple Vulnerabilities (Security Update 2004-09-07)

Mac OS X Multiple Vulnerabilities (Security Update 2004-09-30)

Mac OS X Multiple Vulnerabilities (Security Update 2004-12-02)

Mac OS X Multiple Vulnerabilities (Security Update 2005-001)

Mac OS X Multiple Vulnerabilities (Security Update 2005-003)

Mac OS X Multiple Vulnerabilities (Security Update 2005-005)

Mac OS X Multiple Vulnerabilities (Security Update 2005-006)

Mac OS X Multiple Vulnerabilities (Security Update 2005-007)

Mac OS X Multiple Vulnerabilities (Security Update 2005-008)

Mac OS X Multiple Vulnerabilities (Security Update 2005-009)

Mac OS X Multiple Vulnerabilities (Security Update 2006-001)

Mac OS X Multiple Vulnerabilities (Security Update 2006-002)

Mac OS X Multiple Vulnerabilities (Security Update 2006-003)

Mac OS X Multiple Vulnerabilities (Security Update 2006-004)

Mac OS X Multiple Vulnerabilities (Security Update 2006-006)

Mac OS X Multiple Vulnerabilities (Security Update 2006-007)

Mac OS X Multiple Vulnerabilities (Security Update 2007-002)

Mac OS X Multiple Vulnerabilities (Security Update 2007-004)

Mac OS X Multiple Vulnerabilities (Security Update 2007-005)

Mac OS X Multiple Vulnerabilities (Security Update 2007-006)

Mac OS X Multiple Vulnerabilities (Security Update 2007-007)

Mac OS X Multiple Vulnerabilities (Security Update 2007-009)

Mac OS X Multiple Vulnerabilities (Security Update 2008-001)

Mac OS X Multiple Vulnerabilities (Security Update 2008-002)

Mac OS X Multiple Vulnerabilities (Security Update 2008-003)

Mac OS X Multiple Vulnerabilities (Security Update 2008-004)

Mac OS X Multiple Vulnerabilities (Security Update 2008-005)

Mac OS X Multiple Vulnerabilities (Security Update 2008-006)

Mac OS X Multiple Vulnerabilities (Security Update 2008-007)

Mac OS X Multiple Vulnerabilities (Security Update 2008-008)

Mac OS X Multiple Vulnerabilities (Security Update 2009-001)

Mac OS X Multiple Vulnerabilities (Security Update 2009-002)

Mac OS X Multiple Vulnerabilities (Security Update 2009-003)

Mac OS X Multiple Vulnerabilities (Security Update 2009-005)

Mac OS X Multiple Vulnerabilities (Security Update 2009-006)

Mac OS X Multiple Vulnerabilities (Security Update 2010-001)

Mac OS X Multiple Vulnerabilities (Security Update 2010-002)

Mac OS X Multiple Vulnerabilities (Security Update 2010-003)

Mac OS X Multiple Vulnerabilities (Security Update 2010-004)

Mac OS X Multiple Vulnerabilities (Security Update 2010-005)

Mac OS X Multiple Vulnerabilities (Security Update 2010-007)

Mac OS X Multiple Vulnerabilities (Security Update 2011-001)

Mac OS X Multiple Vulnerabilities (Security Update 2011-003)

Mac OS X Multiple Vulnerabilities (Security Update 2011-004)

Mac OS X Multiple Vulnerabilities (Security Update 2011-006)

Mac OS X Multiple Vulnerabilities (Security Update 2012-001) (BEAST)

Mac OS X Multiple Vulnerabilities (Security Update 2012-002) (BEAST)

Mac OS X Multiple Vulnerabilities (Security Update 2012-004) (BEAST)

Mac OS X Multiple Vulnerabilities (Security Update 2013-001)

Mac OS X Multiple Vulnerabilities (Security Update 2013-002)

Mac OS X Multiple Vulnerabilities (Security Update 2013-003)

Mac OS X Multiple Vulnerabilities (Security Update 2013-004)

Mac OS X Multiple Vulnerabilities (Security Update 2014-001) (BEAST)

Mac OS X Multiple Vulnerabilities (Security Update 2014-002)

Mac OS X Multiple Vulnerabilities (Security Update 2014-003)

Mac OS X Multiple Vulnerabilities (Security Update 2014-004)

Mac OS X Multiple Vulnerabilities (Security Update 2014-005) (POODLE) (Shellshock)

Mac OS X Multiple Vulnerabilities (Security Update 2015-001) (POODLE)

Mac OS X Multiple Vulnerabilities (Security Update 2015-002)

Mac OS X Multiple Vulnerabilities (Security Update 2015-003)

Mac OS X Multiple Vulnerabilities (Security Update 2015-004) (FREAK)

Mac OS X Multiple Vulnerabilities (Security Update 2015-005) (GHOST) (Logjam)

Mac OS X Multiple Vulnerabilities (Security Update 2015-006)

Mac OS X Multiple Vulnerabilities (Security Update 2017-001

Mac OS X Multiple Vulnerabilities (Security Update 2017-002)

Mac OS X Multiple Vulnerabilities (Security Updates 2015-004 / 2015-007)

Mac OS X Multiple Vulnerabilities (Security Updates 2015-005 / 2015-008)

Mac OS X Multiple Vulnerabilities (Security Updates 2016-001 / 2016-005)

Mac OS X Multiple Vulnerabilities (Security Updates 2016-003 / 2016-007)

Mac OS X OSX/Flashback Trojan Detection

Mac OS X OSX/Sabpab Trojan Detection

Mac OS X Safari Null Character Cookie Theft (Security Update 2003-12-05)

Mac OS X Security Update 2005-004

Mac OS X Security Update 2006-008

Mac OS X Security Update 2007-001

Mac OS X Server Service List

Mac OS X Server v10.6.5 (10H575)

Mac OS X Terminal Application Unspecified Issue (Security Update 2003-11-04)

Mac OS X Wireless Networks List

Mac OS X XProtect Detection

Mac OS X XProtect Installed

macOS 10.12.x < 10.12.1 Multiple Vulnerabilities

macOS 10.12.x < 10.12.2 Multiple Vulnerabilities

macOS 10.12.x < 10.12.3 Multiple Vulnerabilities

macOS 10.12.x < 10.12.4 Multiple Vulnerabilities (httpoxy)

macOS 10.12.x < 10.12.5 Multiple Vulnerabilities

MacOS 10.13 root Authentication Bypass (Security Update 2017-001)

macOS 10.13 root Authentication Bypass Direct Check

macOS 10.13.3 Supplemental Update

macOS 10.13.6 Multiple Vulnerabilities (Security Update 2018-002)

macOS 10.13.6 Multiple Vulnerabilities (Security Update 2018-003)

macOS 10.13.6 Multiple Vulnerabilities (Security Update 2019-001)

macOS 10.13.6 Multiple Vulnerabilities (Security Update 2019-002)

macOS 10.13.x < 10.13.1 Multiple Vulnerabilities

macOS 10.13.x < 10.13.2 Multiple Vulnerabilities (Meltdown)

macOS 10.13.x < 10.13.3 Multiple Vulnerabilities

macOS 10.13.x < 10.13.4 Multiple Vulnerabilities

macOS 10.13.x < 10.13.5 Multiple Vulnerabilities

macOS 10.13.x < 10.13.6 Multiple Vulnerabilities

macOS 10.14.3 Supplemental Update

macOS 10.14.x < 10.14.1 Multiple Vulnerabilities

macOS 10.14.x < 10.14.2 Multiple Vulnerabilities

macOS 10.14.x < 10.14.3 Multiple Vulnerabilities

macOS 10.14.x < 10.14.4 Multiple Vulnerabilities

macOS 10.14.x < 10.14.5 Multiple Vulnerabilities

macOS 10.14.x < 10.14.6 Multiple Vulnerabilities

macOS 10.14.x < 10.14.6 SU2 / 10.13.x < 10.13.6 Update 2019-005 / 10.12.x < 10.12.6 Update 2019-005 Out-of-Bounds Read Vulnerability

macOS 10.15.x < 10.15.1 / 10.14.x < 10.14.6 Security Update 2019-001 / 10.13.x < 10.13.6 Security Update 2019-006

macOS 10.15.x < 10.15.2 / 10.14.x < 10.14.6 Security Update 2019-002 / 10.13.x < 10.13.6 Security Update 2019-007

macOS 10.15.x < 10.15.3 / 10.14.x < 10.14.6 / 10.13.x < 10.13.6

macOS 10.15.x < 10.15.4 / 10.14.x < 10.14.6 Security Update 2020-002 / 10.13.x < 10.13.6 Security Update 2020-002

macOS : Apple Safari 11.1 APPLE-SA-2018-04-24-3 Multiple Vulnerabilities

macOS : Apple Safari < 10.0.1 Multiple Vulnerabilities

macOS : Apple Safari < 10.0.2 Multiple Vulnerabilities

macOS : Apple Safari < 10.0.3 Multiple Vulnerabilities

macOS : Apple Safari < 10.1 Multiple Vulnerabilities

macOS : Apple Safari < 10.1.1 Multiple Vulnerabilities

macOS : Apple Safari < 10.1.2 Multiple Vulnerabilities

macOS : Apple Safari < 11.0 Multiple Vulnerabilities

macOS : Apple Safari < 11.0.1 Multiple Vulnerabilities

macOS : Apple Safari < 11.0.2 Multiple Vulnerabilities

macOS : Apple Safari < 11.0.3 Multiple Vulnerabilities

macOS : Apple Safari < 11.1 Multiple Vulnerabilities

macOS : Apple Safari < 11.1.1 Multiple Vulnerabilities

macOS : Apple Safari < 11.1.2 Multiple Vulnerabilities

macOS : Apple Safari < 12 Multiple Vulnerabilities

macOS : Apple Safari < 12.0.1 Multiple Vulnerabilities

macOS : Apple Safari < 12.0.2 Multiple Vulnerabilities

macOS : Apple Safari < 12.0.3 Multiple Vulnerabilities

macOS : Apple Safari < 12.1.1 Multiple Vulnerabilities

macOS : Apple Safari < 12.1.2 Multiple Vulnerabilities

macOS : Apple Safari <= 11.0.2 (11604.4.7.1.6 / 12604.4.7.1.6 / 13604.4.7.10.6) Information Disclosure (Spectre)

macOS : macOS Server < 5.2 Multiple Vulnerabilities (httpoxy)

macOS : macOS Server < 5.3 Multiple Vulnerabilities

macOS : macOS Server < 5.4 Multiple Vulnerabilities

macOS < 10.12 Multiple Vulnerabilities

macOS < 10.13 Multiple Vulnerabilities

macOS < 10.14 Multiple Vulnerabilities

macOS < 10.15 Multiple Vulnerabilities

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2017-001 and 2017-004)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2017-002 and 2017-005)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2017-003)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2018-001) (Meltdown)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2018-002)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2018-003)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2018-004)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2018-005)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2018-006)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2019-001)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2019-002)

macOS and Mac OS X Multiple Vulnerabilities (Security Update 2019-003)

macOS and Mac OS X User List Enumeration

macOS Multiple Vulnerabilities (Security Update 2018-001)

macOS Remote Listeners Enumeration

macOS Sierra / High Sierra Multiple Vulnerabilities (Security Update 2019-004)

MacOSX Cisco AnyConnect Secure Mobility Client Detection

MacOSX Cisco AnyConnect Secure Mobility Client Multiple Vulnerabilities

Microsoft .NET Core Installed (macOS)

Microsoft Office Installed (Mac OS X)

Microsoft Office Unsupported Version Detection (Mac OS X)

Microsoft Silverlight < 5.1.40416.00 Multiple Vulnerabilities (MS15-044 / MS15-049) (Mac OS X)

Microsoft Silverlight < 5.1.40728.0 Multiple Vulnerabilities (MS15-080) (Mac OS X)

Microsoft Silverlight < 5.1.41105.0 Multiple Vulnerabilities (MS15-128) (Mac OS X)

Microsoft Silverlight Installed (Mac OS X)

Microsoft Silverlight Unsupported Version Detection (Mac OS X)

Microsoft Visual Studio Code Installed (Mac OS X)

Mono Installed (macOS)

Mozilla Firefox 48.x / 49.x < 49.0.2 Multiple Vulnerabilities (macOS)

Mozilla Firefox 49.x < 50.0.1 HTTP Redirect Handling Same-origin Policy Bypass

Mozilla Firefox < 49 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 49.0 Multiple Vulnerabilities (Mac OS X)

Mozilla Firefox < 50.0 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 50.0.2 nsSMILTimeContainer.cpp SVG Animation RCE (macOS)

Mozilla Firefox < 50.1 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 51 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 52.0 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 52.0.1 CreateImageBitmap RCE (macOS)

Mozilla Firefox < 53 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 54 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 55 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 56 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 57 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 57.0.1 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 57.0.4 Speculative Execution Side-Channel Attack Vulnerability (Spectre) (macOS)

Mozilla Firefox < 58 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 58.0.1 Arbitrary Code Execution (macOS)

Mozilla Firefox < 59 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities (macOS)

Mozilla Firefox < 59.0.2 Denial of Service Vulnerability (macOS)

Mozilla Firefox < 60 Multiple Critical Vulnerabilities (macOS)

Mozilla Firefox < 61 Multiple Critical Vulnerabilities (macOS)

Mozilla Firefox < 62 Multiple Critical Vulnerabilities (macOS)

Mozilla Firefox < 62 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 62.0.2 Vulnerability (macOS)

Mozilla Firefox < 62.0.3 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 63 Multiple Vulnerabilities (macOS)

Mozilla Firefox < 64.0

Mozilla Firefox < 64.0 Multiple Vulnerabilities (macOS) (deprecated)

Mozilla Firefox < 65.0

Mozilla Firefox < 65.0.1

Mozilla Firefox < 66.0

Mozilla Firefox < 66.0.1

Mozilla Firefox < 67.0

Mozilla Firefox < 67.0.3

Mozilla Firefox < 67.0.4

Mozilla Firefox < 68.0

Mozilla Firefox < 68.0.2

Mozilla Firefox < 69.0

Mozilla Firefox < 69.0.1

Mozilla Firefox < 70.0 Multiple Vulnerabilities

Mozilla Firefox < 71.0

Mozilla Firefox < 72.0 Multiple Vulnerabilities

Mozilla Firefox < 72.0.1

Mozilla Firefox < 73.0

Mozilla Firefox < 74.0 Multiple Vulnerabilities

Mozilla Firefox < 74.0.1

Mozilla Firefox < 75.0 Multiple Vulnerabilities (mfsa2020-12)

Mozilla Firefox ESR 45.x < 45.4 Multiple Vulnerabilities (Mac OS X)

Mozilla Firefox ESR 45.x < 45.5 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR 45.x < 45.5.1 nsSMILTimeContainer.cpp SVG Animation RCE (macOS)

Mozilla Firefox ESR 45.x < 45.6 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR 45.x < 45.7 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR 45.x < 45.9 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR 68.x < 68.2 Multiple Vulnerabilities

Mozilla Firefox ESR 68.x < 68.3 Multiple Vulnerabilities

Mozilla Firefox ESR < 52.8 Multiple Critical Vulnerabilities (macOS)

Mozilla Firefox ESR < 45.8 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.0.1 CreateImageBitmap RCE (macOS)

Mozilla Firefox ESR < 52.1 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.2 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.3 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.4 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.5 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.5.2 Private Mode Fingerprinting Vulnerability (macOS)

Mozilla Firefox ESR < 52.6 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.7 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.7.2 Multiple Code Execution Vulnerabilities (macOS)

Mozilla Firefox ESR < 52.7.3 Denial of Service Vulnerability (macOS)

Mozilla Firefox ESR < 52.9 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 60.1 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 60.2 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 60.2.1 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 60.2.2 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 60.3 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 60.4

Mozilla Firefox ESR < 60.4 Multiple Vulnerabilities (macOS)

Mozilla Firefox ESR < 60.5

Mozilla Firefox ESR < 60.5.1

Mozilla Firefox ESR < 60.6

Mozilla Firefox ESR < 60.6.1

Mozilla Firefox ESR < 60.7

Mozilla Firefox ESR < 60.7.1

Mozilla Firefox ESR < 60.7.2

Mozilla Firefox ESR < 60.8

Mozilla Firefox ESR < 60.9

Mozilla Firefox ESR < 68.0.2

Mozilla Firefox ESR < 68.1

Mozilla Firefox ESR < 68.4 Multiple Vulnerabilities

Mozilla Firefox ESR < 68.4.1

Mozilla Firefox ESR < 68.5 Multiple Vulnerabilities

Mozilla Firefox ESR < 68.6 Multiple Vulnerabilities

Mozilla Firefox ESR < 68.6.1

Mozilla Firefox ESR < 68.7 Multiple Vulnerabilities (mfsa2020-13)

Mozilla Foundation Unsupported Application Detection (macOS)

Mozilla Thunderbird 10.0.x < 10.0.8 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird 24.x < 24.7 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird 24.x < 24.8 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird 24.x < 24.8.1 NSS Signature Verification Vulnerability (Mac OS X)

Mozilla Thunderbird < 16.0 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.0 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.1 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.1.2 NSS Signature Verification Vulnerability (Mac OS X)

Mozilla Thunderbird < 31.2 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.3 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.4 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.5 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.6 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 31.7 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 38.1 Multiple Vulnerabilities (Mac OS X) (Logjam)

Mozilla Thunderbird < 38.4 Multiple Vulnerabilities (Mac OS X)

Mozilla Thunderbird < 45.5.1 nsSMILTimeContainer.cpp SVG Animation RCE (macOS)

Mozilla Thunderbird < 45.6 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 45.7 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 45.8 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 52.1 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 52.2 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 52.5 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 52.6 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 52.9 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 60.0 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 60.2.1

Mozilla Thunderbird < 60.2.1 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 60.3 Multiple Vulnerabilities (macOS)

Mozilla Thunderbird < 60.5

Mozilla Thunderbird < 60.5.1

Mozilla Thunderbird < 60.6

Mozilla Thunderbird < 60.6.1

Mozilla Thunderbird < 60.7

Mozilla Thunderbird < 60.7.1

Mozilla Thunderbird < 60.7.2

Mozilla Thunderbird < 60.8

Mozilla Thunderbird < 60.9 Multiple Vulnerabilities

Mozilla Thunderbird < 68.0

Mozilla Thunderbird < 68.1 Multiple Vulnerabilities

Mozilla Thunderbird < 68.1.1

Mozilla Thunderbird < 68.2

Mozilla Thunderbird < 68.3

Mozilla Thunderbird < 68.4.1

Mozilla Thunderbird < 68.5

Mozilla Thunderbird < 68.7.0

MS06-028: Vulnerability in Microsoft PowerPoint Could Allow Remote Code Execution (916768) (Mac OS X)

MS06-037 / MS06-038: Vulnerabilities in Microsoft Excel and Office Could Allow Remote Code Execution (917284 / 917285) (Mac OS X)

MS06-058 / MS06-059 / MS06-0060 / MS06-062: Vulnerabilities in Microsoft Office Allow Remote Code Execution (924163 / 924164 / 924554 / 922581) (Mac OS X)

MS07-014 / MS07-015: Vulnerabilities in Microsoft Word and Office Could Allow Remote Code Execution (929434 / 932554) (Mac OS X)

MS07-023 / MS07-024 / MS07-025: Vulnerabilities in Microsoft Office Allow Remote Code Execution (934233 / 934232 / 934873) (Mac OS X)

MS07-036: Vulnerability in Microsoft Excel Could Allow Remote Code Execution (936542) (Mac OS X)

MS07-043 / MS07-044: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (921503 / 940965) (Mac OS X)

MS07-060: Vulnerability in Microsoft Word Could Allow Remote Code Execution (942695) (Mac OS X)

MS08-008 / MS08-013: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (947890 / 947108) (Mac OS X)

MS08-014 / MS08-016: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (949029 / 949030) (Mac OS X)

MS08-026: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (951207) (Mac OS X)

MS08-043 / MS08-051: Vulnerabilities in Microsoft Could Allow Remote Code Execution (954066 / 949785) (Mac OS X)

MS08-057: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (956416) (Mac OS X)

MS08-072 / MS08-074: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (957173 / 959070) (Mac OS X)

MS09-009: Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557) (Mac OS X)

MS09-017 / MS09-021 / MS09-027: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (967340 / 969462 / 969514) (Mac OS X)

MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (Mac OS X)

MS09-067 / MS09-068: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (972652 / 976307) (Mac OS X)

MS10-003 / MS10-004: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (978214 / 975416) (Mac OS X)

MS10-017: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150) (Mac OS X)

MS10-038: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2027452) (Mac OS X)

MS10-056 / MS10-057: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2269638 / 2269707) (Mac OS X)

MS10-079 / MS10-080 : Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2293194 / 2293211) (Mac OS X)

MS10-087: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930) (Mac OS X)

MS11-021 / MS11-022 / MS11-023: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2489279 / 2489283 / 2489293) (Mac OS X)

MS11-036 / MS11-045: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2545814 / 2537146) (Mac OS X)

MS11-072: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2587505) (Mac OS X)

MS11-078: Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (2514842) (Mac OS X)

MS11-078: Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (2604930) (Mac OS X)

MS11-089 / MS11-094 / MS11-096 : Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2590602 / 2639142 / 2640241) (Mac OS X)

MS12-016: Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (2651026) (Mac OS X)

MS12-029 / MS12-030: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2680352 / 2663830) (Mac OS X)

MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578) (Mac OS X)

MS12-051: Vulnerability in Microsoft Office for Mac Could Allow Elevation of Privilege (2721015) (Mac OS X)

MS12-076: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2720184) (Mac OS X)

MS13-022: Vulnerability in Silverlight Could Allow Remote Code Execution (2814124) (Mac OS X)

MS13-026: Vulnerability in Office Outlook for Mac Could Allow Information Disclosure (2813682) (Mac OS X)

MS13-051: Vulnerability in Microsoft Office Could Allow Remote Code Execution (2839571) (Mac OS X)

MS13-052: Vulnerability in Silverlight Could Allow Remote Code Execution (2861561) (Mac OS X)

MS13-073: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2858300) (Mac OS X)

MS13-085: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080) (Mac OS X)

MS13-087: Vulnerability in Silverlight Could Allow Information Disclosure (2890788) (Mac OS X)

MS14-014: Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677) (Mac OS X)

MS14-017: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2949660) (Mac OS X)

MS14-061: Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

MS14-081: Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (3017301) (Mac OS X)

MS15-033: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)

MS15-033: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)

MS15-046: Vulnerability in Microsoft Office Could Allow Remote Code Execution (3057181)

MS15-070: Vulnerability in Microsoft Office Could Allow Remote Code Execution (3072620)

MS15-081: Vulnerability in Microsoft Office Could Allow Remote Code Execution (3072620) (Mac OS X)

MS15-099: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664) (Mac OS X)

MS15-110: Security Updates for Microsoft Office to Address Remote Code Execution (3096440) (Mac OS X)

MS15-116: Security Updates for Microsoft Office to Address Remote Code Execution (3104540) (Mac OS X)

MS15-129: Security Update for Silverlight to Address Remote Code Execution (3106614) (Mac OS X)

MS15-131: Security Update for Microsoft Office to Address Remote Code Execution (3116111) (Mac OS X)

MS16-004: Security Update for Microsoft Office to Address Remote Code Execution (3124585) (Mac OS X)

MS16-006: Security Update for Silverlight to Address Remote Code Execution (3126036) (Mac OS X)

MS16-015: Security Update for Microsoft Office to Address Remote Code Execution (3134226) (Mac OS X)

MS16-029: Security Update for Microsoft Office to Address Remote Code Execution (3141806) (Mac OS X)

MS16-042: Security Update for Microsoft Office (3148775) (Mac OS X)

MS16-054: Security Update for Microsoft Office (3155544) (Mac OS X)

MS16-070: Security Update for Microsoft Office (3163610) (Mac OS X)

MS16-088: Security Update for Microsoft Office (3170008) (Mac OS X)

MS16-107: Security Update for Microsoft Office (3185852) (Mac OS X)

MS16-109: Security Update for Silverlight (3182373) (Mac OS X)

MS16-120: Security Update for Microsoft Graphics Component (3192884) (macOS)

MS16-121: Security Update for Microsoft Office (3194063) (Mac OS X)

MS16-133: Security Update for Microsoft Office (3199168) (macOS)

MS16-148: Security Update for Microsoft Office (3204068) (macOS)

MS17-014: Security Update for Microsoft Office (4013241) (macOS)

Novell Messenger Client Detection (Mac OS X)

Opera < 28.0.1750.40 SSL/TLS EXPORT\_RSA Ciphers Downgrade MitM (Mac OS X) (FREAK)

Opera Installed (Mac OS X)

Oracle VirtualBox Unsupported Version Detection (Mac OS X)

Oracle VM VirtualBox 5.2.x < 5.2.34 / 6.0.x < 6.0.14 (Oct 2019 CPU) (MacOSX)

Oracle VM VirtualBox Installed (Mac OS X)

Quicktime < 6.5.2

Quicktime < 7.0.1 Quartz Composer Information Disclosure (Mac OS X)

Quicktime < 7.0.3 Multiple Vulnerabilities (Mac OS X)

Quicktime < 7.1 Multiple Vulnerabilities (Mac OS X)

Quicktime < 7.1.3 Multiple Vulnerabilities (Mac OS X)

Quicktime < 7.1.5 Multiple Vulnerabilities (Mac OS X)

Quicktime < 7.1.6 quicktime.util.QTHandleRef toQTPointer Method Arbitrary Code Execution (Mac OS X)

QuickTime < 7.2 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.3 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.3.1 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.4 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.4.1 RTSP Response Long Reason-Phrase Arbitrary Remote Code Execution (Mac OS X)

QuickTime < 7.4.5 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.5 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.5.5 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.6 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.6.2 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.6.4 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.6.6 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.6.9 Multiple Vulnerabilities (Mac OS X)

QuickTime < 7.7 Multiple Vulnerabilities (Mac OS X)

Quicktime Multiple Vulnerabilities (Mac OS X 7.1.6 Security Update)

Security Update for .NET Core (January 2018) (macOS)

Security Update for .NET Core (November 2017) (macOS)

Security Update for Microsoft Office (Apr 2019) (macOS)

Security Update for Microsoft Office (April 2017) (macOS)

Security Update for Microsoft Office (April 2018) (macOS)

Security Update for Microsoft Office (Auguest 2018) (macOS)

Security Update for Microsoft Office (August 2019) (macOS)

Security Update for Microsoft Office (December 2017) (macOS)

Security Update for Microsoft Office (December 2018) (macOS)

Security Update for Microsoft Office (Feb 2019) (macOS)

Security Update for Microsoft Office (Jan 2019) (macOS)

Security Update for Microsoft Office (January 2018) (macOS)

Security Update for Microsoft Office (July 2017) (macOS)

Security Update for Microsoft Office (July 2018) (macOS)

Security Update for Microsoft Office (June 2017) (macOS)

Security Update for Microsoft Office (June 2019) (macOS)

Security Update for Microsoft Office (March 2018) (macOS)

Security Update for Microsoft Office (May 2017) (macOS)

Security Update for Microsoft Office (May 2018) (macOS)

Security Update for Microsoft Office (May 2019) (macOS)

Security Update for Microsoft Office (November 2017) (macOS)

Security Update for Microsoft Office (November 2018) (macOS)

Security Update for Microsoft Office (October 2017) (macOS)

Security Update for Microsoft Office (October 2018) (macOS)

Security Update for Microsoft Office (September 2017) (macOS)

Security Update for Microsoft Office (September 2018) (macOS)

Security Update for Microsoft Office (September 2019) (macOS)

Security Updates for Microsoft Office (July 2019) (macOS)

Security Updates for Microsoft Office Products (April 2020) (macOS)

Security Updates for Microsoft Office Products (February 2020) (macOS)

Security Updates for Microsoft Office Products (January 2020) (macOS)

Security Updates for Microsoft Office Products (March 2020) (macOS)

Security Updates for Microsoft Office Products (November 2019) (macOS)

Security Updates for Microsoft Office Products (November 2019) (macOS)

Serial Number Identification (macOS)

Skype for Mac 5.x < 5.1.0.922 Unspecified Remote Code Execution (credentialed check)

Skype for Mac Installed (credentialed check)

Sophos Anti-Virus Detection and Status (Mac OS X)

Sophos Anti-Virus for Mac Multiple Vulnerabilities

Sophos Anti-Virus for Mac OS X Detection

SourceTree by Atlassian Detection on Mac OSX

Symantec Encryption Desktop 10.x < 10.3.2 MP3 DoS

Symantec Encryption Desktop 10.x < 10.4.1 MP2 DoS

Symantec Encryption Desktop 10.x =< 10.4.1 MP2HF1 (SYM17-010)

Symantec Encryption Desktop Installed

TeamViewer Installed (macOS)

TeamViewer Permissions Vulnerability (macOS)

Tenable Log Correlation Engine (LCE) Client Installed (Mac OS X) (credentialed check)

Tenable Log Correlation Engine Client Unsupported Version Detection (Mac OS X)

Tenable Nessus Agent Installed (macOS)

Tenable Passive Vulnerability Scanner Installed (Mac OS X) (credentialed check)

Thunderbird 10.0.x < 10.0.3 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.0.x < 10.0.4 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.0.x < 10.0.5 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.0.x < 10.0.6 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.0.x < 10.0.7 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.x < 10.0.1 Memory Corruption (Mac OS X)

Thunderbird 10.x < 10.0.10 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.x < 10.0.11 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.x < 10.0.12 Multiple Vulnerabilities (Mac OS X)

Thunderbird 10.x < 10.0.2 png\_decompress\_chunk Integer Overflow (Mac OS X)

Thunderbird 10.x < 10.0.9 Multiple Vulnerabilities (Mac OS X)

Thunderbird 16.x Multiple Vulnerabilities (Mac OS X)

Thunderbird 17.x < 17.0.4 nsHTMLEditor Use-After-Free (Mac OS X)

Thunderbird 17.x < 17.0.6 Multiple Vulnerabilities (Mac OS X)

Thunderbird 17.x through 23.x Multiple Vulnerabilities (Mac OS X)

Thunderbird 3.1 < 3.1.16 Multiple Vulnerabilities (Mac OS X)

Thunderbird 3.1 < 3.1.17 Jar File Enter Key Dialog Bypass (Mac OS X)

Thunderbird 3.1 < 3.1.18 Multiple Vulnerabilities (Mac OS X)

Thunderbird 3.1.x < 3.1.19 png\_decompress\_chunk Integer Overflow (Mac OS X)

Thunderbird 3.1.x < 3.1.20 Multiple Vulnerabilities (Mac OS X)

Thunderbird 7.x Multiple Vulnerabilities (Mac OS X)

Thunderbird 8.x Multiple Vulnerabilities (Mac OS X)

Thunderbird 9.x Multiple Vulnerabilities (Mac OS X)

Thunderbird < 12.0 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 13.0 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 14.0 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 15.0 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 16.0.1 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 16.0.2 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 17.0.2 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 17.0.3 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 17.0.5 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 17.0.7 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 17.0.8 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 24.1 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 24.1 NSS and NSPR Multiple Vulnerabilities (Mac OS X)

Thunderbird < 24.2 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 24.3 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 24.4 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 24.5 Multiple Vulnerabilities (Mac OS X)

Thunderbird < 24.6 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR 17.x < 17.0.3 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR 17.x < 17.0.4 nsHTMLEditor Use-After-Free (Mac OS X)

Thunderbird ESR 17.x < 17.0.5 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR 17.x < 17.0.6 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR 17.x < 17.0.7 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR 17.x < 17.0.8 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR 17.x < 17.0.9 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR < 17.0.10 Multiple Vulnerabilities (Mac OS X)

Thunderbird ESR < 17.0.11 Null\_Cipher Code Execution (Mac OS X)

Thunderbird Installed (Mac OS X)

VideoLAN VLC for OS X Web Plugin Installed (Mac OS X)

VideoLAN VLC Media Player Installed (Mac OS X)

Viscosity ViscosityHelper Symlink Attack Local Privilege Escalation

Viscosity VPN Client Detection (Mac OS X)

VMware Carbon Black Cloud Endpoint Standard Installed (macOS)

VMware Fusion 10.0.x < 10.1.6 / 11.0.x < 11.0.3 Pixel Shader out-of-bounds read/write vulnerabilities (VMSA-2019-0012)

VMware Fusion 10.x < 10.1.1 Denial of Service Vulnerability (VMSA-2018-0008) (macOS)

VMware Fusion 10.x < 10.1.2 Multiple Vulnerabilities (VMSA-2018-0013) (macOS)

VMware Fusion 10.x < 10.1.3 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (macOS)

VMware Fusion 10.x < 10.1.3 Out-of-Bounds Write Vulnerabilities (VMSA-2018-0022) (macOS)

VMware Fusion 10.x < 10.1.3 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (macOS)

VMware Fusion 10.x < 10.1.4 / 11.x < 11.0.1 vmxnet3 Guest-to-Host Code Execution Vulnerability (VMSA-2018-0027) (macOS)

VMware Fusion 10.x < 10.1.5 / 11.x < 11.0.2 Virtual Network Integer Overflow Vulnerability (VMSA-2018-0030) (macOS)

VMware Fusion 10.x < 10.1.6 / 11.x < 11.0.3 Multiple Vulnerabilities (VMSA-2019-0005) (macOS)

VMware Fusion 10.x < 10.1.6 / 11.x < 11.0.3 Multiple Vulnerabilities (VMSA-2019-0005) (macOS)

VMware Fusion 11.0.x < 11.5.0 Multiple Vulnerabilities (VMSA-2019-0014)

VMware Fusion 11.0.x < 11.5.1 Multiple Vulnerabilities (VMSA-2019-0020, VMSA-2019-0021)

VMware Fusion 11.0.x < 11.5.2 Multiple Vulnerabilities (VMSA-2020-0005)

VMware Fusion 11.x < 11.5.2 Multiple Vulnerabilities (VMSA-2020-0004)

VMware Fusion 4.1 < 4.1.4 / 5.0 < 5.0.2 VMCI Privilege Escalation (VMSA-2013-0002)

VMware Fusion 4.x < 4.1.2 (VMSA-2012-0007)

VMware Fusion 4.x < 4.1.3 (VMSA-2012-0009, VMSA-2012-0011)

VMware Fusion 5.x < 5.0.1 VMX Process DoS (VMSA-2014-0001)

VMware Fusion 5.x < 5.0.4 LGTOSYNC.SYS Privilege Escalation (VMSA-2013-0014)

VMware Fusion 6.x < 6.0.3 OpenSSL Library Multiple Vulnerabilities (VMSA-2014-0004) (Heartbleed)

VMware Fusion 6.x < 6.0.3 Windows 8.1 Guest Privilege Escalation (VMSA-2014-0005)

VMware Fusion 6.x < 6.0.5 / 7.x < 7.0.1 Multiple Vulnerabilities (VMSA-2015-0001)

VMware Fusion 6.x < 6.0.6 / 7.x < 7.0.1 RPC Command DoS

VMware Fusion 7.x < 7.1.2 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001)

VMware Fusion 8.1.x < 8.1.1 Shared Folders (HGFS) Guest DLL Hijacking Arbitrary Code Execution (VMSA-2016-0010)

VMware Fusion 8.x < 8.5.0 Kernel Memory Address Disclosure (VMSA-2016-0017) (Mac OS X)

VMware Fusion 8.x < 8.5.0 Multiple Privilege Escalations (VMSA-2016-0014) (Mac OS X)

VMware Fusion 8.x < 8.5.10 / 10.x < 10.1.1 Multiple Vulnerabilities (VMSA-2018-0004) (VMSA-2018-0005) (Spectre) (macOS)

VMware Fusion 8.x < 8.5.2 Drag-and-Drop Feature Arbitrary Code Execution (VMSA-2016-0019)

VMware Fusion 8.x < 8.5.4 DoS Vulnerability (VMSA-2017-0015) (macOS)

VMware Fusion 8.x < 8.5.5 Drag-and-Drop Feature Guest-to-Host Code Execution (VMSA-2017-0005) (macOS)

VMware Fusion 8.x < 8.5.6 Multiple Vulnerabilities (VMSA-2017-0006) (macOS)

VMware Fusion 8.x < 8.5.8 SVGA Code Execution Vulnerability (VMSA-2017-0015) (macOS)

VMware Fusion 8.x < 8.5.9 Multiple Vulnerabilities (VMSA-2017-0018) (macOS)

VMware Fusion 8.x < 8.5.9 Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (macOS)

VMware Fusion < 11.5.0 Vulnerability (VMSA-2019-0019)

VMware Fusion < 2.0.6 (VMSA-2009-0013)

VMware Fusion < 2.0.8 (VMSA-2010-0018)

VMware Fusion < 3.1.2 (VMSA-2010-0018)

VMware Fusion < 3.1.3 (VMSA-2011-0009 / VMSA-2011-0011)

VMware Fusion < 5.0.5 / 6.0.4 OpenSSL Library Multiple Vulnerabilities

VMware Fusion Unsupported Version Detection

VMware Fusion Version Detection (Mac OS X)

VMware Horizon View Client 2.x / 3.x / 4.x < 4.5.0 Startup Script Command Injection (VMSA-2017-0011) (macOS)

VMware Horizon View Client < 3.0.0 Multiple SSL Vulnerabilities (VMSA-2014-0006) (Mac OS X)

VMware Horizon View Client Detection (Mac OS X)

VMware OVF Tool 3.x < 3.5.2 Multiple OpenSSL Vulnerabilities (VMSA-2014-0006) (Mac OS X)

VMware OVF Tool Detection (Mac OS X)

VMware Tools 9.x / 10.x < 10.0.9 Multiple Privilege Escalations (VMSA-2016-0014) (Mac OS X)

VMware Tools 9.x / 10.x < 10.1.0 Kernel Memory Address Disclosure (VMSA-2016-0017) (Mac OS X)

VMware Tools < 10.2.0 Program Execution Vulnerability (VMSA-2018-0003) (macOS)

VMware Tools Detection (Mac OS X)

VMware Tools Detection (macOS)

WinZip Installed (Mac OS X)

WinZip Unsupported (Mac OS X)

Wireshark 1.12.x < 1.12.10 Multiple Vulnerabilities (Mac OS X)

Wireshark 1.12.x < 1.12.11 Multiple DoS (Mac OS X)

Wireshark 1.12.x < 1.12.7 Multiple DoS (Mac OS X)

Wireshark 2.0.x < 2.0.10 / 2.2.x < 2.2.4 Multiple DoS (macOS)

Wireshark 2.0.x < 2.0.11 / 2.2.x < 2.2.5 Multiple DoS (macOS)

Wireshark 2.0.x < 2.0.12 / 2.2.x < 2.2.6 Multiple DoS (macOS)

Wireshark 2.0.x < 2.0.13 / 2.2.x < 2.2.7 Multiple DoS (macOS)

Wireshark 2.0.x < 2.0.14 / 2.2.x < 2.2.8 Multiple DoS (macOS)

Wireshark 2.0.x < 2.0.16 DMP dissector DoS (MacOS)

Wireshark 2.0.x < 2.0.2 Multiple Vulnerabilities (Mac OS X)

Wireshark 2.0.x < 2.0.3 Multiple DoS (Mac OS X)

Wireshark 2.0.x < 2.0.6 Multiple DoS (Mac OS X)

Wireshark 2.2.x < 2.2.10 Multiple DoS (MacOS)

Wireshark 2.2.x < 2.2.11 / 2.4.x < 2.4.3 DoS Vulnerabilities (MacOS)

Wireshark 2.2.x < 2.2.12 / 2.4.x < 2.4.4 DoS Vulnerabilities (MacOS)

Wireshark 2.2.x < 2.2.13 / 2.4.x < 2.4.5 Multiple DoS Vulnerabilities (MacOS)

Wireshark 2.2.x < 2.2.14 / 2.4.x < 2.4.6 Multiple Vulnerabilities (MacOS)

Wireshark 2.2.x < 2.2.15 / 2.4.x < 2.4.7 / 2.6.x < 2.6.1 Multiple Vulnerabilities (MacOS)

Wireshark 2.2.x < 2.2.16 / 2.4.x < 2.4.8 / 2.6.x < 2.6.2 Multiple Vulnerabilities (macOS)

Wireshark 2.2.x < 2.2.17 / 2.4.x < 2.4.9 / 2.6.x < 2.6.3 Multiple Vulnerabilities (macOS)

Wireshark 2.4.x < 2.4.10 / 2.6.x < 2.6.4 Multiple Vulnerabilities (macOS)

Wireshark 2.4.x < 2.4.11 Multiple Vulnerabilities (MacOS)

Wireshark 2.4.x < 2.4.12 Multiple Vulnerabilities (macOS)

Wireshark 2.4.x < 2.4.13 Multiple Vulnerabilities (macOS)

Wireshark 2.4.x < 2.4.14 Multiple Vulnerabilities (macOS)

Wireshark 2.4.x < 2.4.15 A Vulnerability (macOS)

Wireshark 2.4.x < 2.4.16 DoS Vulnerability (macOS)

Wireshark 2.4.x < 2.4.2 Multiple DoS (MacOS)

Wireshark 2.6.x < 2.6.10 DoS Vulnerability (macOS)

Wireshark 2.6.x < 2.6.11 Gryphon Dissector DoS Vulnerability (macOS)

Wireshark 2.6.x < 2.6.13 A Vulnerability (macOS)

Wireshark 2.6.x < 2.6.15 Multiple Vulnerabilities (macOS)

Wireshark 2.6.x < 2.6.5 Multiple Vulnerabilities (MacOS)

Wireshark 2.6.x < 2.6.6 Multiple Vulnerabilities (macOS)

Wireshark 2.6.x < 2.6.7 Multiple Vulnerabilities (macOS)

Wireshark 2.6.x < 2.6.8 Multiple Vulnerabilities (macOS)

Wireshark 2.6.x < 2.6.9 A Vulnerability (macOS)

Wireshark 3.0.x < 3.0.1 Multiple Vulnerabilities (macOS)

Wireshark 3.0.x < 3.0.2 A Vulnerability (macOS)

Wireshark 3.0.x < 3.0.3 DoS Vulnerability (macOS)

Wireshark 3.0.x < 3.0.4 Gryphon Dissector DoS Vulnerability (macOS)

Wireshark 3.0.x < 3.0.7 A Vulnerability (macOS)

Wireshark 3.0.x < 3.0.8 Denial of Service (DoS) Vulnerability (macOS)

Wireshark 3.0.x < 3.0.9 Multiple Vulnerabilities (macOS)

Wireshark 3.2.x < 3.2.1 Denial of Service (DoS) Vulnerability (macOS)

Wireshark 3.2.x < 3.2.2 Multiple Vulnerabilities (macOS)

Wireshark Installed (Mac OS X)

Zoom Client for Meetings 4.x < 4.1.34801.1116 Message Spoofing Vulnerability (macOS)

Zoom Client for Meetings 4.x < 4.4.53932.0709 Webcam Hijacking Vulnerability (macOS)

Zoom Client for Meetings < 4.6.9.19273.0402 Multiple Issues (macOS)

Zoom.us Installed (macOS)

# Junos Local Security Checks

Juniper Embedthis GoAhead Denial Of Service Vulnerabilities (JSA10948)

Juniper JSA10879

Juniper JSA10889

Juniper JSA10904

Juniper JSA10922

Juniper JSA10924

Juniper JSA10925

Juniper JSA10928

Juniper JSA10929

Juniper JSA10930

Juniper JSA10931 BGP Tracing DoS

Juniper JSA10932

Juniper JSA10933

Juniper JSA10935

Juniper JSA10936

Juniper JSA10938

Juniper JSA10940

Juniper JSA10943

Juniper JSA10946

Juniper JSA10947

Juniper JSA10949

Juniper JSA10956

Juniper JSA10960

Juniper JSA10962

Juniper JSA10970

Juniper JSA10975

Juniper JSA10979

Juniper Junos 'em' Interface Fragmentation Remote DoS (JSA10655)

Juniper Junos ALG Fragmented Traffic Handling MS-MPC / MS-MIC Service PIC DoS (JSA10794)

Juniper Junos bfdd RCE (JSA10690)

Juniper Junos BGP FlowSpec rpd DoS (JSA10670)

Juniper Junos BGP Multiple Remote DoS (PSN-2012-01-475)

Juniper Junos BGP PDU Vulnerability (JSA10810)

Juniper Junos BGP UPDATE 'rpd' Remote DoS (JSA10653)

Juniper Junos BGP UPDATE DoS (PSN-2012-10-733)

Juniper Junos BGP UPDATE Malformed ATTR\_SET Attribute Remote DoS (PSN-2012-01-472)

Juniper Junos BGP Update Vulnerability (JSA10820)

Juniper Junos BGP-VPLS Advertisements RPD DoS (JSA10687)

Juniper Junos Certificate Validation Bypass (JSA10755)

Juniper Junos CLI libc recomp() rpd DoS (JSA10612)

Juniper Junos CLI Local Privilege Escalation (JSA10803)

Juniper Junos CLI Multiple Privilege Escalation Vulnerabilities (JSA10608)

Juniper Junos CLI Privilege Escalation (JSA10634)

Juniper Junos CLI XML Privilege Escalation (JSA10805)

Juniper Junos Commit Script Handling Local Console Port Access Weakness Vulnerability (JSA10835)

Juniper Junos Connectionless Network Protocol (CLNP) Packet Handling Unspecified Remote Code Execution / DoS (JSA10844)

Juniper Junos Corrupt pam.conf Security Bypass (JSA10707)

Juniper Junos Crafted ICMP Packet DoS (JSA10752)

Juniper Junos Crafted UDP Packet Handling DoS (JSA10758)

Juniper Junos Custom Application UUID Rule Handling Remote Firewall Bypass Vulnerability (JSA10836)

Juniper Junos debug.php J-Web Component Unauthenticated Debug Access (PSN-2011-02-158)

Juniper Junos DNSSEC Validation DoS (PSN-2013-04-918)

Juniper Junos DoS Telnet Vulnerability (JSA10817)

Juniper Junos DoS Vulnerability (JSA10821)

Juniper Junos Extended DHCP Relay Agent Traffic Redirection (PSN-2011-07-300)

Juniper Junos Firewall Bypass DoS (PSN-2013-04-912)

Juniper Junos Flowd TCP/IP Response Packet Handling Remote DoS (JSA10829)

Juniper Junos for EX Series Switches IPv6 Neighbor Discovery DoS (JSA10781)

Juniper Junos for M/MX Series Routers IPv6 Neighbor Discovery DoS (JSA10786)

Juniper Junos FPC Crash Vulnerability (JSA10814)

Juniper Junos Fragmented ICMP Packet Handling Remote DoS (PSN-2011-07-298)

Juniper Junos Fragmented OSPFv3 Packet DoS (JSA10668)

Juniper Junos Fragmented TCP Packet Sequence Handling DoS (JSA10696)

Juniper Junos FreeBSD libc db Information Disclosure (JSA10756)

Juniper Junos GNU libc glob Remote DoS (JSA10598)

Juniper Junos GRE DoS (PSN-2013-04-917)

Juniper Junos host-inbound-traffic Implicit Allow (PSN-2012-07-653)

Juniper Junos HTTP Request Handling J-Web DoS (JSA10720)

Juniper Junos HTTP/HTTPS Firewall User Authentication Remote Information Disclosure (JSA10858)

Juniper Junos HTTPS Server Certificate AV Vulnerability (JSA10822)

Juniper Junos ICMP Ping 'composite next-hop' Remote DoS (PSN-2011-07-297)

Juniper Junos ICMPv6 DoS (PSN-2012-07-644)

Juniper Junos ICMPv6 PTB Atomic Fragment DoS (JSA10780)

Juniper Junos IDP Policy Compilation Packet Handling Firewall Rule Bypass Remote Information Disclosure (JSA10846)

Juniper Junos IGMPv3 Protocol Multicast DoS (JSA10714)

Juniper Junos Invalid Ether-type DoS (PSN-2013-04-916)

Juniper Junos Invalid PIM DoS (JSA10637)

Juniper Junos IPv6 Egress Filter DoS (PSN-2013-04-915)

Juniper Junos IPv6 Neighbor Discovery (ND) Traffic Handling Multiple Vulnerabilities (JSA10749)

Juniper Junos IPv6 over IPv4 Security Policy Bypass (PSN-2011-07-299)

Juniper Junos IPv6 Packet Handling mbuf Chain Corruption DoS (JSA10699)

Juniper Junos IPv6 Packet Handling Remote DoS (JSA10762)

Juniper Junos IPv6 sendd DoS (JSA10688)

Juniper Junos IS-IS hello DoS (PSN-2012-07-647)

Juniper Junos J-Web Administrator Logs XSS (PSN-2011-10-392)

Juniper Junos J-Web Component Unspecified CSRF (PSN-2012-01-474)

Juniper Junos J-Web CPU Utilization DoS (PSN-2012-04-547)

Juniper Junos J-Web CSRF Protection Bypass (JSA10597)

Juniper Junos J-Web Hash Collision DoS (PSN-2012-07-650)

Juniper Junos J-Web Interface PHP URL Handling Use-after-free RCE (JSA10828)

Juniper Junos J-Web Multiple Vulnerabilities (JSA10682)

Juniper Junos J-Web Persistent XSS (JSA10619)

Juniper Junos J-Web Reflected XSS (JSA10764)

Juniper Junos J-Web Remote Code Execution (PSN-2013-04-914)

Juniper Junos J-Web Sajax Remote Code Execution (JSA10560)

Juniper Junos J-Web Service Multiple Vulnerabilities (JSA10723)

Juniper Junos J-Web Service Privilege Escalation (JSA10754)

Juniper Junos J-Web URL Encoding Heap-Based Buffer Overflow (PSN-2013-01-807)

Juniper Junos J-Web Weak SSL Ciphers (PSN-2011-01-147)

Juniper Junos J-Web XSS (PSN-2012-07-649)

Juniper Junos jdhcpd crash denial of service (JSA10926)

Juniper Junos jdhcpd DHCPv6 DoS (JSA10769)

Juniper Junos jdhcpd IPv6 UDP DoS (JSA10800)

Juniper Junos Kernel IGMP Flood DoS (JSA10618)

Juniper Junos Kernel Register and Schedule Software Interrupt Handler Subsystem CPU Consumption Remote DoS (JSA10832)

Juniper Junos Kernel Vulnerability (JSA10816)

Juniper Junos Key Exchange Initialization Handling Memory Exhaustion Remote DoS (JSA10837)

Juniper Junos Key Generation Weakness (PSN-2012-04-549)

Juniper Junos LAST\_ACK State DoS (JSA10686)

Juniper Junos libgd Compressed GD2 Data RCE (JSA10798)

Juniper Junos libxml2 Library Multiple Vulnerabilities (JSA10669)

Juniper Junos LLDP Packet Handling Memory Corruption Vulnerability (JSA10830)

Juniper Junos lo0 Firewall Bypass (PSN-2012-07-651)

Juniper Junos load factory-default Privilege Escalation (PSN-2012-07-646)

Juniper Junos MAC Move Limit Traffic Handling Remote DoS (JSA10833)

Juniper Junos Malformed RSVP RPD DoS (JSA10861)

Juniper Junos memory consumption denial of service (JSA10920)

Juniper Junos Memory Exhaustion RDP DOS with JET support (JSA10882)

Juniper Junos MGD-CLI Arbitrary Command Execution (PSN-2011-11-418)

Juniper Junos MPC Malformed Route Prefix Remote DoS (PSN-2011-08-327)

Juniper Junos MPLS DoS (PSN-2012-04-546)

Juniper Junos MPLS Packet Handling Remote DoS (JSA10831)

Juniper Junos Multiple CLI Command Handling Local Privilege Escalations (JSA10763)

Juniper Junos Multiple OpenSSL Vulnerabilities (JSA10629)

Juniper Junos Multiple OpenSSL Vulnerabilities (JSA10649)

Juniper Junos Multiple OpenSSL Vulnerabilities (JSA10679) (FREAK)

Juniper Junos Multiple OpenSSL Vulnerabilities (JSA10759) (SWEET32)

Juniper Junos Multiple OpenSSL Vulnerabilities (JSA10775)

Juniper Junos Multiple Privilege Escalation Vulnerabilities (JSA10674)

Juniper Junos Multiple Python Privilege Escalation (JSA10695)

Juniper Junos Multiple sfid Daemon Malformed Packet Remote DoS (PSN-2011-04-241)

Juniper Junos MX and T4000 Series MPC Reboot DoS (JSA10621)

Juniper Junos MX and T4000 Series Trinity uBFD Packet DoS (JSA10701)

Juniper Junos MX Malformed Packet - DOS (JSA10900)

Juniper Junos MX Series BBE Routers jpppd Remote DoS (JSA10665)

Juniper Junos MX Series Trio-based PFE Modules Security Bypass (JSA10666)

Juniper Junos Network Topology Loop DoS (JSA10719)

Juniper Junos Next-Gen MVPN Senario Malformed Message Handling Remote DoS (PSN-2011-10-391)

Juniper Junos NTP Server Amplification Remote DoS (JSA10613)

Juniper Junos OpenSSL ASN.1 Memory Corruption (PSN-2012-07-645)

Juniper Junos OpenSSL Heartbeat Information Disclosure (JSA10623) (Heartbleed)

Juniper Junos OpenSSL Multiple Vulnerabilities (JSA10575)

Juniper Junos OSPF Protocol Vulnerability (JSA10582)

Juniper Junos Oversized BGP UPDATE Remote DoS (JSA10609)

Juniper Junos Packet Forwarding Engine Potential RCE (JSA10906)

Juniper Junos PHP multiple vulnerabilities (JSA10804)

Juniper Junos PIM DoS (PSN-2012-07-648)

Juniper Junos PIM Hello DoS (PSN-2012-10-732)

Juniper Junos PIM Join Flood DoS (PSN-2013-01-808)

Juniper Junos PIM Remote Denial of Service (JSA10548)

Juniper Junos PIM rpd Crafted Boot Message Remote DoS (PSN-2011-07-296)

Juniper Junos Privilege Escalation (JSA10857)

Juniper Junos Protocol Daemon (RPD) BGP OPEN Message Handling DoS (JSA10779)

Juniper Junos Proxy ARP DoS (PSN-2013-04-913)

Juniper Junos proxy-arp/arp-resp DoS (JSA10576)

Juniper Junos QFX / EX Series 'Etherleak' Improper Padding Memory Disclosure (JSA10773)

Juniper Junos QFX Low Entropy Vulnerability (JSA10678)

Juniper Junos RADIUS Security Bypass (JSA10654)

Juniper Junos Remote Execution Vulnerability (JSA10818)

Juniper Junos Routing Process Daemon (RPD) BGP UPDATE Packet Handling Unspecified Remote DoS (JSA10848)

Juniper Junos Routing Process Daemon BGP UPDATE DoS (JSA10778)

Juniper Junos Routing Protocol Daemon LDP Packet DoS (JSA10777)

Juniper Junos rpd BGP add-path DoS (JSA10771)

Juniper Junos rpd MPLS Ping Packet Handling DoS (JSA10795)

Juniper Junos RPD MPLS RCE (JSA10877)

Juniper Junos rpd RIP DoS (JSA10772)

Juniper Junos RPD Routing Process DoS (JSA10715)

Juniper Junos RSVP 'rpd' Remote DoS (JSA10652)

Juniper Junos RTSP Packet Handling flowd DoS (JSA10721)

Juniper Junos Security Bypass Stateless Firewall Deactivation (JSA10859)

Juniper Junos sendmsg Local Privilege Escalation (JSA10797)

Juniper Junos Short MacSec Keys Configuration CKN / CAK Key Extension Brute-force Mitm Spoofing (JSA10854)

Juniper Junos SIP DoS (PSN-2013-04-911)

Juniper Junos SNMP MIB-II Subagent Daemon (mib2d) Unspecified Remote DoS (JSA10847)

Juniper Junos snmpd SNMP Packet Handling RCE (JSA10793)

Juniper Junos Sockets Library Buffer Overflow Privilege Escalation (JSA10792)

Juniper Junos Space 11.1x < 13.1R1.6 Multiple Vulnerabilities (JSA10585)

Juniper Junos Space 17.1 < 17.1R1 Patch v1 / 16.1 < 16.1R3 Authentication Bypass (JSA10824)

Juniper Junos Space 18.4.x < 18.4R1 Multiple Vulnerabilities (JSA10917)

Juniper Junos Space < 12.3P2.8 Password Disclosure (JSA10567)

Juniper Junos Space < 13.1R1 MySQL Multiple Vulnerabilities (JSA10601)

Juniper Junos Space < 13.3R1.8 Arbitrary Command Execution (JSA10626)

Juniper Junos Space < 13.3R1.8 Multiple Vulnerabilities (JSA10627)

Juniper Junos Space < 14.1R1 Multiple Vulnerabilities (JSA10659)

Juniper Junos Space < 15.1R1 Multiple Vulnerabilities (JSA10698)

Juniper Junos Space < 15.1R2 Multiple Vulnerabilities (JSA10727) (Bar Mitzvah) (Logjam)

Juniper Junos Space < 15.1R3 Multiple Vulnerabilities (JSA10727)

Juniper Junos Space < 17.1R1 Multiple Vulnerabilities (JSA10826)

Juniper Junos Space < 17.2R1 Multiple Vulnerabilities (JSA10838)

Juniper Junos Space < 17.2R2 Persistent XSS Vulnerability (JSA10881)

Juniper Junos Space < 18.2R1 Multiple Vulnerabilities (JSA10880)

Juniper Junos Space < 18.3R1 Multiple Vulnerabilities (JSA10917)

Juniper Junos Space < 19.2R1 Multiple Vulnerabilities (JSA10951)

Juniper Junos Space GNU Bash Command Injection Vulnerability (JSA10648) (Shellshock)

Juniper Junos Space Unsupported Release

Juniper Junos SRX Cluster Synchronization Failover Errors (JSA10806)

Juniper Junos SRX crafted packets destined to fxp0 denial of service (JSA10927)

Juniper Junos SRX DHCP flowd DHCP Packet Handling DoS (JSA10789)

Juniper Junos SRX Flowd Crash Vulnerability (JSA10811)

Juniper Junos SRX Flowd Crash Vulnerability (JSA10813)

Juniper Junos SRX IDP Remote Command Injection (JSA10801)

Juniper Junos SRX Integrated User Firewall Hardcoded Credentials (JSA10791)

Juniper Junos SRX MACsec Feature Secure Link Failure Silent Fallback Information Disclosure (JSA10790)

Juniper Junos SRX Series 'log-out-on-disconnect' Persistent Admin Access (JSA10672)

Juniper Junos SRX Series 'set system ports console insecure' Local Privilege Escalation (JSA10683)

Juniper Junos SRX Series ALG 'flowd' Remote DoS (JSA10650)

Juniper Junos SRX Series Application Layer Gateway DoS (JSA10751)

Juniper Junos SRX Series Dynamic IPsec VPN DoS (JSA10620)

Juniper Junos SRX Series Dynamic VPN XSS (JSA10677)

Juniper Junos SRX Series flowd DoS (JSA10622)

Juniper Junos SRX Series flowd Remote DoS (JSA10596)

Juniper Junos SRX Series flowd Remote DoS (JSA10610)

Juniper Junos SRX Series flowd Remote DoS (JSA10611)

Juniper Junos SRX Series flowd telnet Messages Remote Code Execution (JSA10594)

Juniper Junos SRX Series for the Data Center Memory Corruption (PSN-2012-04-548)

Juniper Junos SRX Series FTP ALG ftps-extension TCP Port Exposure (JSA10706)

Juniper Junos SRX Series Gateway Chassis Cluster flowd Multicast Session DoS (JSA10768)

Juniper Junos SRX Series MSRPC DoS (JSA10578)

Juniper Junos SRX Series NAT IPv6 to IPv4 Remote DoS (JSA10635)

Juniper Junos SRX Series NAT IPv6 to IPv4 Remote DoS (JSA10641)

Juniper Junos SRX Series Network Security Daemon DoS (JSA10692)

Juniper Junos SRX Series PIM DoS (JSA10573)

Juniper Junos SRX Series SIP ALG Remote DoS (JSA10633)

Juniper Junos SRX Series TCP ALG DoS (JSA10577)

Juniper Junos SRX Series UAC Enforcer HTTP Remote Code Execution (JSA10574)

Juniper Junos SRX Series Unauthenticated Access (JSA10593)

Juniper Junos SRX Series Upgrade Handling Local Root Authentication Bypass (JSA10753)

Juniper Junos SRX Series Web Authentication XSS (JSA10640)

Juniper Junos SRX, vSRX, and J-Series ISC BIND DoS (JSA10799)

Juniper Junos SRX1400/3400/3600 Etherleak Information Disclosure (JSA10579)

Juniper Junos SRX5000-series J-Web DoS (JSA10700)

Juniper Junos SSH TACACS+ Incorrect Permissions (PSN-2012-04-545)

Juniper Junos SSL/TLS Renegotiation DoS (JSA10580)

Juniper Junos SYN Cookie Protection DoS (PSN-2012-07-643)

Juniper Junos TACACS+ Double Quotes Privilege Escalation (JSA10667)

Juniper Junos TCP Packet Processing Remote DoS (JSA10638)

Juniper Junos TKEY Query Handling DoS (JSA10718)

Juniper Junos ttymodem() DoS (PSN-2012-08-699)

Juniper Junos UDP/IP DoS (PSN-2012-07-652)

Juniper Junos Unnumbered Interface Cache Poisoning Remote DoS and Information Disclosure (JSA10595)

Juniper Junos Unspecified DoS (PSN-2013-01-818)

Juniper Junos Unsupported Version Detection

Juniper Junos User Authentication Bypass (JSA10802)

Juniper Junos Virtualized Environment Guest-To-Host Privilege Escalation (JSA10787)

Juniper Junos VLAN authentication processing DoS (JSA10834)

Juniper Junos vMX 14.1 < 14.1R8 / 15.1 < 15.1F5 Local Information Disclosure (JSA10766)

Juniper Junos vMX Predictable IP ID Sequence Numbers (JSA10903)

Juniper Junos VPLS Ethernet Frame MAC Address Remote DoS (JSA10750)

Juniper Junos VPLS Routing MPLS Packet Handling mbuf Exhaustion Remote DoS (JSA10845)

Juniper Junos VPLS Routing MPLS Packet Handling mbuf Exhaustion Remote DoS (JSA10855)

Juniper Junos web-authentication Policy Not Enforced (PSN-2012-10-735)

Juniper Junos X-Frame-Options Clickjacking (JSA10675)

Juniper Junos XNM Command Remote DoS (JSA10607)

Juniper JunosE Malformed IP Option Remote DoS

Juniper Stateless IP Firewall Bypass Vulnerability (JSA10983)

Junos Operating System On Extended Support

Junos OS Default Credentials Vulnerability (JSA10998)

Junos OS Firewall Filters Failure Vulnerability (JSA10942)

Junos OS Multiple vulnerabilities (JSA10981)

Junos OS: app-id Signature Update MitM (JSA10952)

Junos OS: Broadband Edge Service Denial of Service (DoS) Vulnerability (JSA10987)

Junos OS: Clear Text Authentication Credentials (JSA10969)

Junos OS: Crafted HTTP traffic may cause UTM to consume all mbufs, leading to Denial of Service (JSA10910)

Junos OS: Cross-Site Scripting (XSS) in J-Web (JSA10986)

Junos OS: Deleted dynamic VPN users are allowed to establish VPN connections until reboot (JSA10915)

Junos OS: EX2300 and EX3400 series: Certain stateless firewall filter rules might not take effect (JSA10901)

Junos OS: EX2300 and EX3400 series: High disk I/O operations may disrupt the communication between RE and PFE (JSA10909)

Junos OS: flowd DoS (JSA10963)

Junos OS: FPC process crashes after J-Flow processes a malformed packet (JSA10914)

Junos OS: Improper handling of specific IPv6 packets (JSA10982)

Junos OS: Insecure PKI key pair export file permissions (JSA10974)

Junos OS: J-Web Session Fixation Vulnerability (JSA10961)

Junos OS: Kernel crash after processing specific incoming packet to the out of band management interface (JSA10911)

Junos OS: MC-LAG DoS (JSA10966)

Junos OS: Multicast flowd DoS (JSA10968)

Junos OS: Multiple vulnerabilities in libxml2 (JSA10902)

Junos OS: Multiple vulnerabilities in libxml2 (JSA10916)

Junos OS: NG-mVPN rpd DoS (JSA10965)

Junos OS: OpenSSL Security Advisories [16 Apr 2018] and [12 June 2018] (JSA10919)

Junos OS: Path traversal vulnerability in J-Web (JSA10985)

Junos OS: pccd DoS (JSA10980)

Junos OS: pd crash on VPLS PE upon receipt of specific BGP message (JSA10912)

Junos OS: processing of specific transit IP packets in flowd, leading to a Denial of Service Vulnerability (JSA10964)

Junos OS: processing of specific transit IP packets in flowd, leading to Denial of Service (JSA10959)

Junos OS: rdp Memory Leak DoS (JSA10957)

Junos OS: RPD crash upon receipt of malformed PIM packet (JSA10913)

Junos OS: SIP ALG flowd DoS (JSA10953)

Junos OS: srxpfe DoS (JSA10972)

Junos OS: srxpfe PIM DoS (JSA10976)

Junos OS: SSL-Proxy DoS (JSA10973)

Junos OS: Stateless firewall filter ignores IPv6 extension headers (JSA10905)

Junos Version Detection

Multiple Vulnerabilities in Juniper Junos (JSA10954)

NFX Series: Authentication Bypass Vulnerability Juniper Device Manager (JDM) (JSA10955)

NFX Series: Insecure sshd configuration in Juniper Device Manager (JDM) and host OS (JSA10878)

# Huawei Local Security Checks

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2016-1010)

EulerOS 2.0 SP1 : mercurial (EulerOS-SA-2016-1019)

EulerOS 2.0 SP1 : 389-ds-base (EulerOS-SA-2018-1032)

EulerOS 2.0 SP1 : 389-ds-base (EulerOS-SA-2018-1076)

EulerOS 2.0 SP1 : apr (EulerOS-SA-2017-1303)

EulerOS 2.0 SP1 : augeas (EulerOS-SA-2017-1250)

EulerOS 2.0 SP1 : authconfig (EulerOS-SA-2017-1195)

EulerOS 2.0 SP1 : bash (EulerOS-SA-2017-1031)

EulerOS 2.0 SP1 : bash (EulerOS-SA-2017-1163)

EulerOS 2.0 SP1 : bind (EulerOS-SA-2016-1052)

EulerOS 2.0 SP1 : bind (EulerOS-SA-2016-1079)

EulerOS 2.0 SP1 : bind (EulerOS-SA-2017-1025)

EulerOS 2.0 SP1 : bind (EulerOS-SA-2017-1077)

EulerOS 2.0 SP1 : bind (EulerOS-SA-2017-1140)

EulerOS 2.0 SP1 : bind (EulerOS-SA-2018-1037)

EulerOS 2.0 SP1 : binutils (EulerOS-SA-2017-1278)

EulerOS 2.0 SP1 : binutils (EulerOS-SA-2017-1285)

EulerOS 2.0 SP1 : binutils (EulerOS-SA-2017-1338)

EulerOS 2.0 SP1 : binutils (EulerOS-SA-2018-1062)

EulerOS 2.0 SP1 : binutils (EulerOS-SA-2018-1098)

EulerOS 2.0 SP1 : compat-libtiff3 (EulerOS-SA-2017-1044)

EulerOS 2.0 SP1 : cpio (EulerOS-SA-2016-1041)

EulerOS 2.0 SP1 : cups (EulerOS-SA-2018-1079)

EulerOS 2.0 SP1 : curl (EulerOS-SA-2016-1074)

EulerOS 2.0 SP1 : curl (EulerOS-SA-2017-1036)

EulerOS 2.0 SP1 : curl (EulerOS-SA-2017-1287)

EulerOS 2.0 SP1 : curl (EulerOS-SA-2017-1312)

EulerOS 2.0 SP1 : curl (EulerOS-SA-2018-1039)

EulerOS 2.0 SP1 : curl (EulerOS-SA-2018-1109)

EulerOS 2.0 SP1 : cyrus-imapd (EulerOS-SA-2016-1040)

EulerOS 2.0 SP1 : dbus (EulerOS-SA-2016-1037)

EulerOS 2.0 SP1 : dhcp (EulerOS-SA-2016-1065)

EulerOS 2.0 SP1 : dhcp (EulerOS-SA-2018-1035)

EulerOS 2.0 SP1 : dhcp (EulerOS-SA-2018-1072)

EulerOS 2.0 SP1 : dhcp (EulerOS-SA-2018-1122)

EulerOS 2.0 SP1 : dnsmasq (EulerOS-SA-2016-1044)

EulerOS 2.0 SP1 : dnsmasq (EulerOS-SA-2017-1239)

EulerOS 2.0 SP1 : docker (EulerOS-SA-2016-1016)

EulerOS 2.0 SP1 : dovecot (EulerOS-SA-2018-1056)

EulerOS 2.0 SP1 : dracut (EulerOS-SA-2018-1020)

EulerOS 2.0 SP1 : e2fsprogs (EulerOS-SA-2016-1038)

EulerOS 2.0 SP1 : elfutils (EulerOS-SA-2017-1142)

EulerOS 2.0 SP1 : emacs (EulerOS-SA-2017-1235)

EulerOS 2.0 SP1 : evince (EulerOS-SA-2017-1221)

EulerOS 2.0 SP1 : evince (EulerOS-SA-2018-1009)

EulerOS 2.0 SP1 : exempi (EulerOS-SA-2018-1124)

EulerOS 2.0 SP1 : expat (EulerOS-SA-2017-1002)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2016-1002)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2016-1046)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2016-1085)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1012)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1048)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1092)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1126)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1197)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1248)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1299)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2017-1326)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2018-1043)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2018-1117)

EulerOS 2.0 SP1 : firefox (EulerOS-SA-2018-1125)

EulerOS 2.0 SP1 : fontconfig (EulerOS-SA-2016-1077)

EulerOS 2.0 SP1 : freeradius (EulerOS-SA-2017-1134)

EulerOS 2.0 SP1 : freeradius (EulerOS-SA-2017-1167)

EulerOS 2.0 SP1 : freetype (EulerOS-SA-2017-1114)

EulerOS 2.0 SP1 : gd (EulerOS-SA-2017-1045)

EulerOS 2.0 SP1 : gdk-pixbuf2 (EulerOS-SA-2018-1045)

EulerOS 2.0 SP1 : gdm (EulerOS-SA-2017-1173)

EulerOS 2.0 SP1 : ghostscript (EulerOS-SA-2016-1050)

EulerOS 2.0 SP1 : ghostscript (EulerOS-SA-2017-1100)

EulerOS 2.0 SP1 : ghostscript (EulerOS-SA-2017-1144)

EulerOS 2.0 SP1 : gimp gimp-help (EulerOS-SA-2016-1075)

EulerOS 2.0 SP1 : gimp (EulerOS-SA-2018-1022)

EulerOS 2.0 SP1 : git (EulerOS-SA-2016-1009)

EulerOS 2.0 SP1 : git (EulerOS-SA-2017-1187)

EulerOS 2.0 SP1 : git (EulerOS-SA-2017-1265)

EulerOS 2.0 SP1 : glibc (EulerOS-SA-2016-1073)

EulerOS 2.0 SP1 : glibc (EulerOS-SA-2017-1146)

EulerOS 2.0 SP1 : glibc (EulerOS-SA-2017-1199)

EulerOS 2.0 SP1 : glibc (EulerOS-SA-2017-1267)

EulerOS 2.0 SP1 : glibc (EulerOS-SA-2018-1047)

EulerOS 2.0 SP1 : gnutls (EulerOS-SA-2017-1042)

EulerOS 2.0 SP1 : gnutls (EulerOS-SA-2017-1115)

EulerOS 2.0 SP1 : gnutls (EulerOS-SA-2017-1203)

EulerOS 2.0 SP1 : graphite2 (EulerOS-SA-2016-1013)

EulerOS 2.0 SP1 : graphite2 (EulerOS-SA-2017-1152)

EulerOS 2.0 SP1 : graphite2 (EulerOS-SA-2018-1106)

EulerOS 2.0 SP1 : gstreamer (EulerOS-SA-2017-1205)

EulerOS 2.0 SP1 : gstreamer-plugins-bad-free (EulerOS-SA-2017-1010)

EulerOS 2.0 SP1 : gstreamer-plugins-good (EulerOS-SA-2017-1062)

EulerOS 2.0 SP1 : gstreamer1-plugins-bad-free (EulerOS-SA-2017-1008)

EulerOS 2.0 SP1 : gstreamer1-plugins-good (EulerOS-SA-2017-1064)

EulerOS 2.0 SP1 : gtk-vnc (EulerOS-SA-2017-1181)

EulerOS 2.0 SP1 : httpd (EulerOS-SA-2016-1030)

EulerOS 2.0 SP1 : httpd (EulerOS-SA-2016-1039)

EulerOS 2.0 SP1 : httpd (EulerOS-SA-2017-1085)

EulerOS 2.0 SP1 : httpd (EulerOS-SA-2017-1177)

EulerOS 2.0 SP1 : httpd (EulerOS-SA-2017-1252)

EulerOS 2.0 SP1 : httpd (EulerOS-SA-2018-1151)

EulerOS 2.0 SP1 : icoutils (EulerOS-SA-2017-1089)

EulerOS 2.0 SP1 : icu (EulerOS-SA-2017-1305)

EulerOS 2.0 SP1 : ImageMagick (EulerOS-SA-2016-1021)

EulerOS 2.0 SP1 : ImageMagick (EulerOS-SA-2016-1029)

EulerOS 2.0 SP1 : ImageMagick (EulerOS-SA-2017-1116)

EulerOS 2.0 SP1 : ImageMagick (EulerOS-SA-2017-1257)

EulerOS 2.0 SP1 : ImageMagick (EulerOS-SA-2018-1127)

EulerOS 2.0 SP1 : ipa (EulerOS-SA-2016-1042)

EulerOS 2.0 SP1 : ipa (EulerOS-SA-2017-1013)

EulerOS 2.0 SP1 : irssi (EulerOS-SA-2017-1117)

EulerOS 2.0 SP1 : irssi (EulerOS-SA-2017-1283)

EulerOS 2.0 SP1 : irssi (EulerOS-SA-2018-1060)

EulerOS 2.0 SP1 : jasper (EulerOS-SA-2017-1094)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2016-1015)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2016-1032)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2016-1080)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2017-1027)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2017-1098)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2017-1207)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2017-1272)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2017-1330)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2018-1058)

EulerOS 2.0 SP1 : java-1.7.0-openjdk (EulerOS-SA-2018-1128)

EulerOS 2.0 SP1 : java-1.8.0-openjdk (EulerOS-SA-2017-1015)

EulerOS 2.0 SP1 : java-1.8.0-openjdk (EulerOS-SA-2017-1073)

EulerOS 2.0 SP1 : java-1.8.0-openjdk (EulerOS-SA-2017-1150)

EulerOS 2.0 SP1 : java-1.8.0-openjdk (EulerOS-SA-2017-1254)

EulerOS 2.0 SP1 : java-1.8.0-openjdk (EulerOS-SA-2018-1027)

EulerOS 2.0 SP1 : java-1.8.0-openjdk (EulerOS-SA-2018-1130)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1007)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1018)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1020)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1024)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1026)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1028)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1043)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1048)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1051)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2016-1089)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1001)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1057)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1071)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1122)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1154)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1159)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1245)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1271)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1291)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2017-1318)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2018-1002)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2018-1031)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2018-1054)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2018-1085)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2018-1119)

EulerOS 2.0 SP1 : kernel (EulerOS-SA-2018-1132)

EulerOS 2.0 SP1 : krb5 (EulerOS-SA-2016-1012)

EulerOS 2.0 SP1 : krb5 (EulerOS-SA-2016-1076)

EulerOS 2.0 SP1 : krb5 (EulerOS-SA-2018-1007)

EulerOS 2.0 SP1 : ldns (EulerOS-SA-2017-1336)

EulerOS 2.0 SP1 : libarchive (EulerOS-SA-2016-1045)

EulerOS 2.0 SP1 : libcdio (EulerOS-SA-2018-1081)

EulerOS 2.0 SP1 : libevent (EulerOS-SA-2017-1090)

EulerOS 2.0 SP1 : libexif (EulerOS-SA-2017-1276)

EulerOS 2.0 SP1 : libgcrypt (EulerOS-SA-2016-1081)

EulerOS 2.0 SP1 : liblouis (EulerOS-SA-2017-1289)

EulerOS 2.0 SP1 : liblouis (EulerOS-SA-2017-1328)

EulerOS 2.0 SP1 : libndp (EulerOS-SA-2016-1022)

EulerOS 2.0 SP1 : libnl3 (EulerOS-SA-2016-1067)

EulerOS 2.0 SP1 : libnl3 (EulerOS-SA-2017-1161)

EulerOS 2.0 SP1 : librelp (EulerOS-SA-2018-1134)

EulerOS 2.0 SP1 : libreswan (EulerOS-SA-2016-1078)

EulerOS 2.0 SP1 : librsvg2 (EulerOS-SA-2017-1136)

EulerOS 2.0 SP1 : libsndfile (EulerOS-SA-2017-1243)

EulerOS 2.0 SP1 : libsoup (EulerOS-SA-2017-1209)

EulerOS 2.0 SP1 : libssh2 (EulerOS-SA-2016-1005)

EulerOS 2.0 SP1 : libtasn1 (EulerOS-SA-2017-1171)

EulerOS 2.0 SP1 : libtiff (EulerOS-SA-2016-1034)

EulerOS 2.0 SP1 : libtiff (EulerOS-SA-2017-1019)

EulerOS 2.0 SP1 : libtiff (EulerOS-SA-2018-1102)

EulerOS 2.0 SP1 : libtirpc (EulerOS-SA-2017-1096)

EulerOS 2.0 SP1 : libvirt (EulerOS-SA-2017-1053)

EulerOS 2.0 SP1 : libvirt (EulerOS-SA-2018-1016)

EulerOS 2.0 SP1 : libvncserver (EulerOS-SA-2017-1046)

EulerOS 2.0 SP1 : libvncserver (EulerOS-SA-2018-1139)

EulerOS 2.0 SP1 : libvorbis (EulerOS-SA-2018-1018)

EulerOS 2.0 SP1 : libvorbis (EulerOS-SA-2018-1104)

EulerOS 2.0 SP1 : libwpd (EulerOS-SA-2017-1274)

EulerOS 2.0 SP1 : libXcursor (EulerOS-SA-2018-1003)

EulerOS 2.0 SP1 : libxml2 (EulerOS-SA-2017-1069)

EulerOS 2.0 SP1 : libxml2 (EulerOS-SA-2017-1237)

EulerOS 2.0 SP1 : libxml2 (EulerOS-SA-2018-1070)

EulerOS 2.0 SP1 : libxml2 (EulerOS-SA-2018-1088)

EulerOS 2.0 SP1 : libXpm libXdmcp libICE (EulerOS-SA-2017-1211)

EulerOS 2.0 SP1 : log4j (EulerOS-SA-2017-1213)

EulerOS 2.0 SP1 : mailman (EulerOS-SA-2018-1086)

EulerOS 2.0 SP1 : mariadb (EulerOS-SA-2016-1011)

EulerOS 2.0 SP1 : mariadb (EulerOS-SA-2016-1035)

EulerOS 2.0 SP1 : mariadb (EulerOS-SA-2016-1062)

EulerOS 2.0 SP1 : mariadb (EulerOS-SA-2017-1169)

EulerOS 2.0 SP1 : mariadb (EulerOS-SA-2017-1322)

EulerOS 2.0 SP1 : memcached (EulerOS-SA-2016-1086)

EulerOS 2.0 SP1 : memcached (EulerOS-SA-2018-1138)

EulerOS 2.0 SP1 : mercurial (EulerOS-SA-2017-1132)

EulerOS 2.0 SP1 : mercurial (EulerOS-SA-2017-1217)

EulerOS 2.0 SP1 : mercurial (EulerOS-SA-2018-1142)

EulerOS 2.0 SP1 : mod\_nss (EulerOS-SA-2016-1070)

EulerOS 2.0 SP1 : mpfr (EulerOS-SA-2017-1293)

EulerOS 2.0 SP1 : nasm (EulerOS-SA-2017-1297)

EulerOS 2.0 SP1 : nautilus (EulerOS-SA-2018-1053)

EulerOS 2.0 SP1 : ncurses (EulerOS-SA-2018-1005)

EulerOS 2.0 SP1 : nettle (EulerOS-SA-2016-1061)

EulerOS 2.0 SP1 : nss nspr nss-softokn nss-util (EulerOS-SA-2016-1017)

EulerOS 2.0 SP1 : nss nss-util (EulerOS-SA-2016-1084)

EulerOS 2.0 SP1 : nss nss-util (EulerOS-SA-2017-1075)

EulerOS 2.0 SP1 : nss (EulerOS-SA-2017-1108)

EulerOS 2.0 SP1 : nss (EulerOS-SA-2017-1246)

EulerOS 2.0 SP1 : nss-util (EulerOS-SA-2016-1003)

EulerOS 2.0 SP1 : ntp (EulerOS-SA-2016-1060)

EulerOS 2.0 SP1 : ntp (EulerOS-SA-2017-1023)

EulerOS 2.0 SP1 : ntp (EulerOS-SA-2017-1124)

EulerOS 2.0 SP1 : openjpeg (EulerOS-SA-2017-1088)

EulerOS 2.0 SP1 : openjpeg (EulerOS-SA-2018-1094)

EulerOS 2.0 SP1 : openldap (EulerOS-SA-2017-1201)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2016-1008)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2016-1053)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2017-1006)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2017-1055)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2017-1138)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2017-1189)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2018-1068)

EulerOS 2.0 SP1 : openssh (EulerOS-SA-2018-1140)

EulerOS 2.0 SP1 : openssl (EulerOS-SA-2016-1047)

EulerOS 2.0 SP1 : openssl (EulerOS-SA-2017-1029)

EulerOS 2.0 SP1 : openssl098e (EulerOS-SA-2017-1040)

EulerOS 2.0 SP1 : patch (EulerOS-SA-2018-1146)

EulerOS 2.0 SP1 : pcre (EulerOS-SA-2016-1023)

EulerOS 2.0 SP1 : php (EulerOS-SA-2016-1063)

EulerOS 2.0 SP1 : php (EulerOS-SA-2017-1067)

EulerOS 2.0 SP1 : php (EulerOS-SA-2017-1301)

EulerOS 2.0 SP1 : php (EulerOS-SA-2018-1096)

EulerOS 2.0 SP1 : pidgin (EulerOS-SA-2017-1165)

EulerOS 2.0 SP1 : pki-core (EulerOS-SA-2017-1183)

EulerOS 2.0 SP1 : policycoreutils (EulerOS-SA-2016-1083)

EulerOS 2.0 SP1 : poppler (EulerOS-SA-2016-1059)

EulerOS 2.0 SP1 : poppler (EulerOS-SA-2017-1229)

EulerOS 2.0 SP1 : poppler (EulerOS-SA-2017-1259)

EulerOS 2.0 SP1 : posrgresql (EulerOS-SA-2017-1215)

EulerOS 2.0 SP1 : postgresql (EulerOS-SA-2016-1001)

EulerOS 2.0 SP1 : postgresql (EulerOS-SA-2016-1058)

EulerOS 2.0 SP1 : postgresql (EulerOS-SA-2017-1231)

EulerOS 2.0 SP1 : postgresql (EulerOS-SA-2017-1340)

EulerOS 2.0 SP1 : procmail (EulerOS-SA-2017-1316)

EulerOS 2.0 SP1 : python (EulerOS-SA-2016-1036)

EulerOS 2.0 SP1 : python (EulerOS-SA-2016-1090)

EulerOS 2.0 SP1 : python (EulerOS-SA-2017-1003)

EulerOS 2.0 SP1 : python (EulerOS-SA-2017-1185)

EulerOS 2.0 SP1 : python (EulerOS-SA-2017-1334)

EulerOS 2.0 SP1 : python (EulerOS-SA-2018-1078)

EulerOS 2.0 SP1 : python-pillow (EulerOS-SA-2017-1049)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2016-1066)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2017-1037)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2017-1079)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2017-1118)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2017-1156)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2017-1223)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2017-1320)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2018-1014)

EulerOS 2.0 SP1 : qemu-kvm (EulerOS-SA-2018-1144)

EulerOS 2.0 SP1 : quagga (EulerOS-SA-2017-1058)

EulerOS 2.0 SP1 : quagga (EulerOS-SA-2017-1307)

EulerOS 2.0 SP1 : quagga (EulerOS-SA-2018-1064)

EulerOS 2.0 SP1 : resteasy-base (EulerOS-SA-2016-1057)

EulerOS 2.0 SP1 : rpcbind (EulerOS-SA-2017-1102)

EulerOS 2.0 SP1 : rsync (EulerOS-SA-2017-1332)

EulerOS 2.0 SP1 : rsync (EulerOS-SA-2018-1011)

EulerOS 2.0 SP1 : rsync (EulerOS-SA-2018-1049)

EulerOS 2.0 SP1 : ruby (EulerOS-SA-2017-1050)

EulerOS 2.0 SP1 : ruby (EulerOS-SA-2018-1029)

EulerOS 2.0 SP1 : ruby (EulerOS-SA-2018-1066)

EulerOS 2.0 SP1 : ruby (EulerOS-SA-2018-1143)

EulerOS 2.0 SP1 : samba (EulerOS-SA-2016-1006)

EulerOS 2.0 SP1 : samba (EulerOS-SA-2016-1014)

EulerOS 2.0 SP1 : samba (EulerOS-SA-2016-1031)

EulerOS 2.0 SP1 : samba (EulerOS-SA-2017-1104)

EulerOS 2.0 SP1 : samba (EulerOS-SA-2017-1219)

EulerOS 2.0 SP1 : samba (EulerOS-SA-2017-1233)

EulerOS 2.0 SP1 : samba (EulerOS-SA-2017-1314)

EulerOS 2.0 SP1 : setroubleshoot setroubleshoot-plugins (EulerOS-SA-2016-1033)

EulerOS 2.0 SP1 : slf4j (EulerOS-SA-2018-1092)

EulerOS 2.0 SP1 : sox (EulerOS-SA-2018-1083)

EulerOS 2.0 SP1 : spice-gtk (EulerOS-SA-2018-1149)

EulerOS 2.0 SP1 : spice-vdagent (EulerOS-SA-2018-1051)

EulerOS 2.0 SP1 : sqlite (EulerOS-SA-2018-1136)

EulerOS 2.0 SP1 : squid (EulerOS-SA-2016-1025)

EulerOS 2.0 SP1 : squid (EulerOS-SA-2016-1056)

EulerOS 2.0 SP1 : squid (EulerOS-SA-2017-1017)

EulerOS 2.0 SP1 : squid (EulerOS-SA-2018-1074)

EulerOS 2.0 SP1 : sssd (EulerOS-SA-2017-1324)

EulerOS 2.0 SP1 : subscription-manager python-rhsm (EulerOS-SA-2016-1069)

EulerOS 2.0 SP1 : subversion (EulerOS-SA-2017-1175)

EulerOS 2.0 SP1 : sudo (EulerOS-SA-2016-1055)

EulerOS 2.0 SP1 : sudo (EulerOS-SA-2017-1004)

EulerOS 2.0 SP1 : sudo (EulerOS-SA-2017-1106)

EulerOS 2.0 SP1 : sudo (EulerOS-SA-2017-1120)

EulerOS 2.0 SP1 : tcpdump (EulerOS-SA-2017-1179)

EulerOS 2.0 SP1 : tcpdump (EulerOS-SA-2017-1280)

EulerOS 2.0 SP1 : tigervnc (EulerOS-SA-2017-1227)

EulerOS 2.0 SP1 : tomcat (EulerOS-SA-2016-1049)

EulerOS 2.0 SP1 : tomcat (EulerOS-SA-2016-1054)

EulerOS 2.0 SP1 : tomcat (EulerOS-SA-2017-1081)

EulerOS 2.0 SP1 : tomcat (EulerOS-SA-2017-1191)

EulerOS 2.0 SP1 : tomcat (EulerOS-SA-2017-1261)

EulerOS 2.0 SP1 : util-linux (EulerOS-SA-2016-1068)

EulerOS 2.0 SP1 : util-linux (EulerOS-SA-2017-1083)

EulerOS 2.0 SP1 : vim (EulerOS-SA-2017-1033)

EulerOS 2.0 SP1 : vim (EulerOS-SA-2017-1148)

EulerOS 2.0 SP1 : webkitgtk3 (EulerOS-SA-2017-1309)

EulerOS 2.0 SP1 : wget (EulerOS-SA-2016-1027)

EulerOS 2.0 SP1 : wget (EulerOS-SA-2016-1064)

EulerOS 2.0 SP1 : wget (EulerOS-SA-2017-1269)

EulerOS 2.0 SP1 : wireshark (EulerOS-SA-2018-1041)

EulerOS 2.0 SP1 : wpa\_supplicant (EulerOS-SA-2017-1241)

EulerOS 2.0 SP1 : xdg-user-dirs (EulerOS-SA-2018-1024)

EulerOS 2.0 SP1 : xerces-c (EulerOS-SA-2016-1004)

EulerOS 2.0 SP1 : xerces-c (EulerOS-SA-2018-1100)

EulerOS 2.0 SP1 : xmlsec1 (EulerOS-SA-2017-1193)

EulerOS 2.0 SP1 : xorg-x11-server (EulerOS-SA-2017-1295)

EulerOS 2.0 SP1 : zsh (EulerOS-SA-2018-1090)

EulerOS 2.0 SP2 : gstreamer1-plugins-bad-free (EulerOS-SA-2017-1007)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2017-1087)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2018-1033)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2018-1077)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2018-1190)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2018-1357)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2018-1439)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2019-1046)

EulerOS 2.0 SP2 : 389-ds-base (EulerOS-SA-2019-2369)

EulerOS 2.0 SP2 : accountsservice (EulerOS-SA-2019-2443)

EulerOS 2.0 SP2 : apr (EulerOS-SA-2017-1304)

EulerOS 2.0 SP2 : audit (EulerOS-SA-2019-2385)

EulerOS 2.0 SP2 : augeas (EulerOS-SA-2017-1251)

EulerOS 2.0 SP2 : authconfig (EulerOS-SA-2017-1196)

EulerOS 2.0 SP2 : avahi (EulerOS-SA-2019-1734)

EulerOS 2.0 SP2 : bash (EulerOS-SA-2017-1032)

EulerOS 2.0 SP2 : bash (EulerOS-SA-2017-1164)

EulerOS 2.0 SP2 : bash (EulerOS-SA-2019-1563)

EulerOS 2.0 SP2 : bind (EulerOS-SA-2017-1026)

EulerOS 2.0 SP2 : bind (EulerOS-SA-2017-1078)

EulerOS 2.0 SP2 : bind (EulerOS-SA-2017-1141)

EulerOS 2.0 SP2 : bind (EulerOS-SA-2018-1038)

EulerOS 2.0 SP2 : bind (EulerOS-SA-2018-1281)

EulerOS 2.0 SP2 : bind (EulerOS-SA-2019-1730)

EulerOS 2.0 SP2 : bind (EulerOS-SA-2019-2453)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2017-1279)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2017-1286)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2017-1339)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2018-1063)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2018-1099)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2018-1283)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2018-1426)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2019-1728)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2019-1836)

EulerOS 2.0 SP2 : binutils (EulerOS-SA-2019-2450)

EulerOS 2.0 SP2 : bluez (EulerOS-SA-2019-2380)

EulerOS 2.0 SP2 : bzip2 (EulerOS-SA-2019-1837)

EulerOS 2.0 SP2 : bzip2 (EulerOS-SA-2019-2411)

EulerOS 2.0 SP2 : c-ares (EulerOS-SA-2019-1838)

EulerOS 2.0 SP2 : cairo (EulerOS-SA-2019-2495)

EulerOS 2.0 SP2 : chrony (EulerOS-SA-2017-1158)

EulerOS 2.0 SP2 : cifs-utils (EulerOS-SA-2019-2366)

EulerOS 2.0 SP2 : compat-libtiff3 (EulerOS-SA-2017-1043)

EulerOS 2.0 SP2 : coreutils (EulerOS-SA-2019-2417)

EulerOS 2.0 SP2 : cracklib (EulerOS-SA-2019-2439)

EulerOS 2.0 SP2 : cronie (EulerOS-SA-2019-2496)

EulerOS 2.0 SP2 : cups (EulerOS-SA-2018-1080)

EulerOS 2.0 SP2 : cups (EulerOS-SA-2019-1566)

EulerOS 2.0 SP2 : cups (EulerOS-SA-2019-2422)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2017-1035)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2017-1288)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2017-1313)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2018-1040)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2018-1110)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2018-1202)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2018-1427)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2019-1047)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2019-1751)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2019-1839)

EulerOS 2.0 SP2 : curl (EulerOS-SA-2019-2410)

EulerOS 2.0 SP2 : dbus (EulerOS-SA-2019-1727)

EulerOS 2.0 SP2 : dcraw (EulerOS-SA-2019-1840)

EulerOS 2.0 SP2 : dcraw (EulerOS-SA-2019-2489)

EulerOS 2.0 SP2 : dhcp (EulerOS-SA-2018-1036)

EulerOS 2.0 SP2 : dhcp (EulerOS-SA-2018-1073)

EulerOS 2.0 SP2 : dhcp (EulerOS-SA-2018-1123)

EulerOS 2.0 SP2 : dhcp (EulerOS-SA-2019-2500)

EulerOS 2.0 SP2 : dnsmasq (EulerOS-SA-2017-1240)

EulerOS 2.0 SP2 : dnsmasq (EulerOS-SA-2018-1285)

EulerOS 2.0 SP2 : docker-engine (EulerOS-SA-2019-1061)

EulerOS 2.0 SP2 : dom4j (EulerOS-SA-2019-2405)

EulerOS 2.0 SP2 : dosfstools (EulerOS-SA-2019-2356)

EulerOS 2.0 SP2 : dovecot (EulerOS-SA-2018-1057)

EulerOS 2.0 SP2 : dovecot (EulerOS-SA-2019-1279)

EulerOS 2.0 SP2 : dovecot (EulerOS-SA-2019-2372)

EulerOS 2.0 SP2 : dracut (EulerOS-SA-2018-1021)

EulerOS 2.0 SP2 : dump (EulerOS-SA-2019-1740)

EulerOS 2.0 SP2 : ed (EulerOS-SA-2019-2507)

EulerOS 2.0 SP2 : elfutils (EulerOS-SA-2017-1143)

EulerOS 2.0 SP2 : elfutils (EulerOS-SA-2019-1109)

EulerOS 2.0 SP2 : elfutils (EulerOS-SA-2019-2510)

EulerOS 2.0 SP2 : elinks (EulerOS-SA-2019-2376)

EulerOS 2.0 SP2 : emacs (EulerOS-SA-2017-1236)

EulerOS 2.0 SP2 : evince (EulerOS-SA-2017-1222)

EulerOS 2.0 SP2 : evince (EulerOS-SA-2018-1010)

EulerOS 2.0 SP2 : exempi (EulerOS-SA-2018-1111)

EulerOS 2.0 SP2 : exempi (EulerOS-SA-2019-2373)

EulerOS 2.0 SP2 : exiv2 (EulerOS-SA-2018-1286)

EulerOS 2.0 SP2 : exiv2 (EulerOS-SA-2019-2375)

EulerOS 2.0 SP2 : expat (EulerOS-SA-2019-1742)

EulerOS 2.0 SP2 : expat (EulerOS-SA-2019-1841)

EulerOS 2.0 SP2 : expat (EulerOS-SA-2019-2433)

EulerOS 2.0 SP2 : file (EulerOS-SA-2019-2449)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1011)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1047)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1093)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1127)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1198)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1249)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1300)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2017-1327)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2018-1044)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2018-1118)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2018-1126)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2018-1359)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2018-1414)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2019-1282)

EulerOS 2.0 SP2 : firefox (EulerOS-SA-2019-1570)

EulerOS 2.0 SP2 : firewalld (EulerOS-SA-2019-2377)

EulerOS 2.0 SP2 : flex (EulerOS-SA-2019-2448)

EulerOS 2.0 SP2 : foomatic (EulerOS-SA-2019-2412)

EulerOS 2.0 SP2 : freeradius (EulerOS-SA-2017-1135)

EulerOS 2.0 SP2 : freeradius (EulerOS-SA-2017-1168)

EulerOS 2.0 SP2 : freeradius (EulerOS-SA-2019-1572)

EulerOS 2.0 SP2 : freeradius (EulerOS-SA-2019-1747)

EulerOS 2.0 SP2 : freerdp (EulerOS-SA-2019-1283)

EulerOS 2.0 SP2 : freerdp (EulerOS-SA-2019-2455)

EulerOS 2.0 SP2 : freetype (EulerOS-SA-2017-1110)

EulerOS 2.0 SP2 : freetype (EulerOS-SA-2019-2514)

EulerOS 2.0 SP2 : fuse (EulerOS-SA-2019-1048)

EulerOS 2.0 SP2 : fuse (EulerOS-SA-2019-1286)

EulerOS 2.0 SP2 : gc (EulerOS-SA-2019-2451)

EulerOS 2.0 SP2 : gcc (EulerOS-SA-2018-1116)

EulerOS 2.0 SP2 : gd (EulerOS-SA-2017-1128)

EulerOS 2.0 SP2 : gd (EulerOS-SA-2019-1715)

EulerOS 2.0 SP2 : gd (EulerOS-SA-2019-1842)

EulerOS 2.0 SP2 : gd (EulerOS-SA-2019-2521)

EulerOS 2.0 SP2 : gdb (EulerOS-SA-2019-2479)

EulerOS 2.0 SP2 : gdk-pixbuf2 (EulerOS-SA-2018-1046)

EulerOS 2.0 SP2 : gdk-pixbuf2 (EulerOS-SA-2019-2386)

EulerOS 2.0 SP2 : gdm (EulerOS-SA-2017-1174)

EulerOS 2.0 SP2 : gettext (EulerOS-SA-2019-2505)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2017-1101)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2017-1145)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2018-1430)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2019-1049)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2019-1110)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2019-1288)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2019-1731)

EulerOS 2.0 SP2 : ghostscript (EulerOS-SA-2019-2370)

EulerOS 2.0 SP2 : giflib (EulerOS-SA-2019-2498)

EulerOS 2.0 SP2 : gimp (EulerOS-SA-2018-1023)

EulerOS 2.0 SP2 : gimp (EulerOS-SA-2019-1741)

EulerOS 2.0 SP2 : gimp (EulerOS-SA-2019-2471)

EulerOS 2.0 SP2 : git (EulerOS-SA-2017-1188)

EulerOS 2.0 SP2 : git (EulerOS-SA-2017-1266)

EulerOS 2.0 SP2 : git (EulerOS-SA-2018-1215)

EulerOS 2.0 SP2 : git (EulerOS-SA-2019-1843)

EulerOS 2.0 SP2 : git (EulerOS-SA-2019-2389)

EulerOS 2.0 SP2 : glib2 (EulerOS-SA-2019-2409)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2017-1147)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2017-1200)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2017-1268)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2018-1048)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2018-1289)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2019-1050)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2019-1111)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2019-1721)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2019-1844)

EulerOS 2.0 SP2 : glibc (EulerOS-SA-2019-2476)

EulerOS 2.0 SP2 : glusterfs (EulerOS-SA-2018-1441)

EulerOS 2.0 SP2 : gnupg2 (EulerOS-SA-2018-1221)

EulerOS 2.0 SP2 : gnupg2 (EulerOS-SA-2019-2393)

EulerOS 2.0 SP2 : gnutls (EulerOS-SA-2017-1041)

EulerOS 2.0 SP2 : gnutls (EulerOS-SA-2017-1111)

EulerOS 2.0 SP2 : gnutls (EulerOS-SA-2017-1204)

EulerOS 2.0 SP2 : gnutls (EulerOS-SA-2018-1444)

EulerOS 2.0 SP2 : gnutls (EulerOS-SA-2019-1112)

EulerOS 2.0 SP2 : gnutls (EulerOS-SA-2019-1743)

EulerOS 2.0 SP2 : gnutls (EulerOS-SA-2019-2432)

EulerOS 2.0 SP2 : golang (EulerOS-SA-2017-1225)

EulerOS 2.0 SP2 : golang (EulerOS-SA-2017-1311)

EulerOS 2.0 SP2 : gpgme (EulerOS-SA-2019-2406)

EulerOS 2.0 SP2 : graphite2 (EulerOS-SA-2017-1153)

EulerOS 2.0 SP2 : graphite2 (EulerOS-SA-2018-1107)

EulerOS 2.0 SP2 : graphviz (EulerOS-SA-2019-1726)

EulerOS 2.0 SP2 : graphviz (EulerOS-SA-2019-2355)

EulerOS 2.0 SP2 : grub2 (EulerOS-SA-2019-1735)

EulerOS 2.0 SP2 : gstreamer (EulerOS-SA-2017-1206)

EulerOS 2.0 SP2 : gstreamer-plugins-bad-free (EulerOS-SA-2017-1009)

EulerOS 2.0 SP2 : gstreamer-plugins-base (EulerOS-SA-2019-1577)

EulerOS 2.0 SP2 : gstreamer-plugins-good (EulerOS-SA-2017-1063)

EulerOS 2.0 SP2 : gstreamer1-plugins-base (EulerOS-SA-2019-1738)

EulerOS 2.0 SP2 : gstreamer1-plugins-good (EulerOS-SA-2017-1065)

EulerOS 2.0 SP2 : gtk-vnc (EulerOS-SA-2017-1182)

EulerOS 2.0 SP2 : guile (EulerOS-SA-2019-2424)

EulerOS 2.0 SP2 : gvfs (EulerOS-SA-2019-1749)

EulerOS 2.0 SP2 : httpcomponents-client (EulerOS-SA-2019-2518)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2017-1086)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2017-1178)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2017-1253)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2018-1152)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2018-1212)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2019-1113)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2019-1293)

EulerOS 2.0 SP2 : httpd (EulerOS-SA-2019-2402)

EulerOS 2.0 SP2 : icoutils (EulerOS-SA-2017-1059)

EulerOS 2.0 SP2 : icu (EulerOS-SA-2017-1129)

EulerOS 2.0 SP2 : icu (EulerOS-SA-2017-1306)

EulerOS 2.0 SP2 : icu (EulerOS-SA-2019-2390)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2017-1112)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2017-1258)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2017-1264)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2018-1114)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2018-1290)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2019-1114)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2019-1296)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2019-1581)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2019-1729)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2019-1845)

EulerOS 2.0 SP2 : ImageMagick (EulerOS-SA-2019-2354)

EulerOS 2.0 SP2 : ipa (EulerOS-SA-2017-1014)

EulerOS 2.0 SP2 : ipsilon (EulerOS-SA-2018-1013)

EulerOS 2.0 SP2 : irssi (EulerOS-SA-2017-1113)

EulerOS 2.0 SP2 : irssi (EulerOS-SA-2017-1284)

EulerOS 2.0 SP2 : irssi (EulerOS-SA-2018-1061)

EulerOS 2.0 SP2 : irssi (EulerOS-SA-2019-2477)

EulerOS 2.0 SP2 : jakarta-commons-httpclient (EulerOS-SA-2019-2397)

EulerOS 2.0 SP2 : jansson (EulerOS-SA-2019-2396)

EulerOS 2.0 SP2 : jasper (EulerOS-SA-2017-1095)

EulerOS 2.0 SP2 : jasper (EulerOS-SA-2018-1417)

EulerOS 2.0 SP2 : jasper (EulerOS-SA-2019-2490)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2017-1028)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2017-1099)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2017-1208)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2017-1273)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2017-1331)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2018-1059)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2018-1129)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2018-1192)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2018-1292)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2019-1115)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2019-1745)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2019-1846)

EulerOS 2.0 SP2 : java-1.7.0-openjdk (EulerOS-SA-2019-2460)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2017-1016)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2017-1074)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2017-1151)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2017-1255)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2018-1028)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2018-1131)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2018-1194)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2018-1294)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2018-1416)

EulerOS 2.0 SP2 : java-1.8.0-openjdk (EulerOS-SA-2019-2374)

EulerOS 2.0 SP2 : keepalived (EulerOS-SA-2019-1739)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1056)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1066)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1072)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1123)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1155)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1160)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1256)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1282)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1292)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1319)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2017-1342)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1001)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1026)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1055)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1120)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1133)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1153)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1278)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1296)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1360)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2018-1432)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-1062)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-1131)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-1302)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-1586)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-1639)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-1793)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-1847)

EulerOS 2.0 SP2 : kernel (EulerOS-SA-2019-2353)

EulerOS 2.0 SP2 : krb5 (EulerOS-SA-2018-1008)

EulerOS 2.0 SP2 : krb5 (EulerOS-SA-2018-1354)

EulerOS 2.0 SP2 : krb5 (EulerOS-SA-2018-1425)

EulerOS 2.0 SP2 : krb5 (EulerOS-SA-2019-1848)

EulerOS 2.0 SP2 : krb5 (EulerOS-SA-2019-2378)

EulerOS 2.0 SP2 : lcms2 (EulerOS-SA-2019-2401)

EulerOS 2.0 SP2 : ldns (EulerOS-SA-2017-1337)

EulerOS 2.0 SP2 : less (EulerOS-SA-2019-2475)

EulerOS 2.0 SP2 : lftp (EulerOS-SA-2019-2485)

EulerOS 2.0 SP2 : libarchive (EulerOS-SA-2019-1725)

EulerOS 2.0 SP2 : libarchive (EulerOS-SA-2019-1849)

EulerOS 2.0 SP2 : libarchive (EulerOS-SA-2019-2379)

EulerOS 2.0 SP2 : libcdio (EulerOS-SA-2018-1082)

EulerOS 2.0 SP2 : libcdio (EulerOS-SA-2018-1418)

EulerOS 2.0 SP2 : libcgroup (EulerOS-SA-2019-2512)

EulerOS 2.0 SP2 : libcroco (EulerOS-SA-2019-2520)

EulerOS 2.0 SP2 : libevent (EulerOS-SA-2017-1091)

EulerOS 2.0 SP2 : libevent (EulerOS-SA-2019-2515)

EulerOS 2.0 SP2 : libexif (EulerOS-SA-2017-1277)

EulerOS 2.0 SP2 : libexif (EulerOS-SA-2019-1116)

EulerOS 2.0 SP2 : libexif (EulerOS-SA-2019-1850)

EulerOS 2.0 SP2 : libgcrypt (EulerOS-SA-2019-1750)

EulerOS 2.0 SP2 : libgsf (EulerOS-SA-2019-2363)

EulerOS 2.0 SP2 : libguestfs (EulerOS-SA-2017-1061)

EulerOS 2.0 SP2 : libgxps (EulerOS-SA-2018-1428)

EulerOS 2.0 SP2 : libgxps (EulerOS-SA-2019-2416)

EulerOS 2.0 SP2 : libical (EulerOS-SA-2019-2457)

EulerOS 2.0 SP2 : libidn (EulerOS-SA-2019-1851)

EulerOS 2.0 SP2 : libidn (EulerOS-SA-2019-2392)

EulerOS 2.0 SP2 : libimobiledevice (EulerOS-SA-2019-2436)

EulerOS 2.0 SP2 : libjpeg-turbo (EulerOS-SA-2018-1298)

EulerOS 2.0 SP2 : libjpeg-turbo (EulerOS-SA-2019-1305)

EulerOS 2.0 SP2 : libjpeg-turbo (EulerOS-SA-2019-2407)

EulerOS 2.0 SP2 : liblouis (EulerOS-SA-2017-1290)

EulerOS 2.0 SP2 : liblouis (EulerOS-SA-2017-1329)

EulerOS 2.0 SP2 : liblouis (EulerOS-SA-2018-1222)

EulerOS 2.0 SP2 : liblouis (EulerOS-SA-2018-1300)

EulerOS 2.0 SP2 : libmspack (EulerOS-SA-2018-1435)

EulerOS 2.0 SP2 : libmspack (EulerOS-SA-2019-1852)

EulerOS 2.0 SP2 : libmspack (EulerOS-SA-2019-2454)

EulerOS 2.0 SP2 : libmtp (EulerOS-SA-2019-2452)

EulerOS 2.0 SP2 : libndp (EulerOS-SA-2019-2497)

EulerOS 2.0 SP2 : libnl (EulerOS-SA-2019-1853)

EulerOS 2.0 SP2 : libnl3 (EulerOS-SA-2017-1162)

EulerOS 2.0 SP2 : libosinfo (EulerOS-SA-2019-1854)

EulerOS 2.0 SP2 : libpcap (EulerOS-SA-2019-2456)

EulerOS 2.0 SP2 : libplist (EulerOS-SA-2019-2395)

EulerOS 2.0 SP2 : libpng (EulerOS-SA-2019-1117)

EulerOS 2.0 SP2 : libpng (EulerOS-SA-2019-1855)

EulerOS 2.0 SP2 : libpng (EulerOS-SA-2019-2383)

EulerOS 2.0 SP2 : librelp (EulerOS-SA-2018-1135)

EulerOS 2.0 SP2 : librsvg2 (EulerOS-SA-2017-1137)

EulerOS 2.0 SP2 : librsvg2 (EulerOS-SA-2019-2493)

EulerOS 2.0 SP2 : libsamplerate (EulerOS-SA-2019-2398)

EulerOS 2.0 SP2 : libseccomp (EulerOS-SA-2019-1856)

EulerOS 2.0 SP2 : libsndfile (EulerOS-SA-2017-1244)

EulerOS 2.0 SP2 : libsndfile (EulerOS-SA-2018-1447)

EulerOS 2.0 SP2 : libsndfile (EulerOS-SA-2019-1590)

EulerOS 2.0 SP2 : libsndfile (EulerOS-SA-2019-2513)

EulerOS 2.0 SP2 : libsoup (EulerOS-SA-2017-1210)

EulerOS 2.0 SP2 : libsoup (EulerOS-SA-2018-1419)

EulerOS 2.0 SP2 : libsrtp (EulerOS-SA-2019-2472)

EulerOS 2.0 SP2 : libssh2 (EulerOS-SA-2019-1308)

EulerOS 2.0 SP2 : libssh2 (EulerOS-SA-2019-2473)

EulerOS 2.0 SP2 : libtar (EulerOS-SA-2019-2444)

EulerOS 2.0 SP2 : libtasn1 (EulerOS-SA-2017-1172)

EulerOS 2.0 SP2 : libtasn1 (EulerOS-SA-2018-1445)

EulerOS 2.0 SP2 : libtasn1 (EulerOS-SA-2019-1311)

EulerOS 2.0 SP2 : libtasn1 (EulerOS-SA-2019-2470)

EulerOS 2.0 SP2 : libtiff (EulerOS-SA-2017-1020)

EulerOS 2.0 SP2 : libtiff (EulerOS-SA-2018-1103)

EulerOS 2.0 SP2 : libtiff (EulerOS-SA-2019-1857)

EulerOS 2.0 SP2 : libtiff (EulerOS-SA-2019-2466)

EulerOS 2.0 SP2 : libtirpc (EulerOS-SA-2017-1097)

EulerOS 2.0 SP2 : libvirt (EulerOS-SA-2017-1052)

EulerOS 2.0 SP2 : libvirt (EulerOS-SA-2018-1017)

EulerOS 2.0 SP2 : libvirt (EulerOS-SA-2019-1118)

EulerOS 2.0 SP2 : libvirt (EulerOS-SA-2019-1724)

EulerOS 2.0 SP2 : libvirt (EulerOS-SA-2019-2468)

EulerOS 2.0 SP2 : libvncserver (EulerOS-SA-2019-1051)

EulerOS 2.0 SP2 : libvncsever (EulerOS-SA-2017-1130)

EulerOS 2.0 SP2 : libvorbis (EulerOS-SA-2018-1019)

EulerOS 2.0 SP2 : libvorbis (EulerOS-SA-2018-1105)

EulerOS 2.0 SP2 : libvorbis (EulerOS-SA-2019-2502)

EulerOS 2.0 SP2 : libwmf (EulerOS-SA-2019-2492)

EulerOS 2.0 SP2 : libwpd (EulerOS-SA-2017-1275)

EulerOS 2.0 SP2 : libX11 (EulerOS-SA-2019-2480)

EulerOS 2.0 SP2 : libXcursor (EulerOS-SA-2018-1004)

EulerOS 2.0 SP2 : libxcursor (EulerOS-SA-2018-1437)

EulerOS 2.0 SP2 : libXfixes (EulerOS-SA-2019-2481)

EulerOS 2.0 SP2 : libXfont (EulerOS-SA-2019-2357)

EulerOS 2.0 SP2 : libXi (EulerOS-SA-2019-2434)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2017-1070)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2017-1238)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2018-1071)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2018-1089)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2018-1446)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2019-1315)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2019-1858)

EulerOS 2.0 SP2 : libxml2 (EulerOS-SA-2019-2491)

EulerOS 2.0 SP2 : libXpm libXdmcp libICE (EulerOS-SA-2017-1212)

EulerOS 2.0 SP2 : libXrender (EulerOS-SA-2019-2458)

EulerOS 2.0 SP2 : libxslt (EulerOS-SA-2019-1052)

EulerOS 2.0 SP2 : libxslt (EulerOS-SA-2019-1317)

EulerOS 2.0 SP2 : libxslt (EulerOS-SA-2019-2519)

EulerOS 2.0 SP2 : libXtst (EulerOS-SA-2020-1093)

EulerOS 2.0 SP2 : libXvMC (EulerOS-SA-2019-2441)

EulerOS 2.0 SP2 : log4j (EulerOS-SA-2017-1214)

EulerOS 2.0 SP2 : lua (EulerOS-SA-2019-2382)

EulerOS 2.0 SP2 : lz4 (EulerOS-SA-2019-2360)

EulerOS 2.0 SP2 : mailman (EulerOS-SA-2018-1087)

EulerOS 2.0 SP2 : mariadb (EulerOS-SA-2017-1170)

EulerOS 2.0 SP2 : mariadb (EulerOS-SA-2017-1323)

EulerOS 2.0 SP2 : mariadb (EulerOS-SA-2018-1302)

EulerOS 2.0 SP2 : mariadb (EulerOS-SA-2019-1859)

EulerOS 2.0 SP2 : memcached (EulerOS-SA-2019-2391)

EulerOS 2.0 SP2 : mercurial (EulerOS-SA-2017-1133)

EulerOS 2.0 SP2 : mercurial (EulerOS-SA-2017-1218)

EulerOS 2.0 SP2 : mercurial (EulerOS-SA-2018-1112)

EulerOS 2.0 SP2 : mod\_auth\_mellon (EulerOS-SA-2019-1319)

EulerOS 2.0 SP2 : mod\_auth\_mellon (EulerOS-SA-2019-2388)

EulerOS 2.0 SP2 : mod\_wsgi (EulerOS-SA-2019-2367)

EulerOS 2.0 SP2 : mpfr (EulerOS-SA-2017-1294)

EulerOS 2.0 SP2 : mutt (EulerOS-SA-2018-1304)

EulerOS 2.0 SP2 : mutt (EulerOS-SA-2019-2508)

EulerOS 2.0 SP2 : nasm (EulerOS-SA-2017-1298)

EulerOS 2.0 SP2 : nautilus (EulerOS-SA-2018-1034)

EulerOS 2.0 SP2 : ncurses (EulerOS-SA-2018-1006)

EulerOS 2.0 SP2 : ncurses (EulerOS-SA-2018-1218)

EulerOS 2.0 SP2 : ncurses (EulerOS-SA-2019-2420)

EulerOS 2.0 SP2 : net-snmp (EulerOS-SA-2019-1716)

EulerOS 2.0 SP2 : netpbm (EulerOS-SA-2019-2426)

EulerOS 2.0 SP2 : NetworkManager (EulerOS-SA-2019-1119)

EulerOS 2.0 SP2 : NetworkManager (EulerOS-SA-2019-2371)

EulerOS 2.0 SP2 : nss nss-util (EulerOS-SA-2017-1076)

EulerOS 2.0 SP2 : nss (EulerOS-SA-2017-1109)

EulerOS 2.0 SP2 : nss (EulerOS-SA-2017-1247)

EulerOS 2.0 SP2 : nss (EulerOS-SA-2018-1358)

EulerOS 2.0 SP2 : nss (EulerOS-SA-2019-2467)

EulerOS 2.0 SP2 : ntp (EulerOS-SA-2017-1024)

EulerOS 2.0 SP2 : ntp (EulerOS-SA-2017-1125)

EulerOS 2.0 SP2 : ntp (EulerOS-SA-2019-1053)

EulerOS 2.0 SP2 : ntp (EulerOS-SA-2019-1719)

EulerOS 2.0 SP2 : ntp (EulerOS-SA-2019-1860)

EulerOS 2.0 SP2 : ntp (EulerOS-SA-2019-2446)

EulerOS 2.0 SP2 : OpenEXR (EulerOS-SA-2019-2469)

EulerOS 2.0 SP2 : openjpeg (EulerOS-SA-2017-1060)

EulerOS 2.0 SP2 : openjpeg (EulerOS-SA-2018-1095)

EulerOS 2.0 SP2 : openjpeg (EulerOS-SA-2019-2503)

EulerOS 2.0 SP2 : openldap (EulerOS-SA-2017-1202)

EulerOS 2.0 SP2 : openldap (EulerOS-SA-2019-2358)

EulerOS 2.0 SP2 : openslp (EulerOS-SA-2018-1210)

EulerOS 2.0 SP2 : openslp (EulerOS-SA-2019-2394)

EulerOS 2.0 SP2 : openssh (EulerOS-SA-2017-1054)

EulerOS 2.0 SP2 : openssh (EulerOS-SA-2017-1139)

EulerOS 2.0 SP2 : openssh (EulerOS-SA-2017-1190)

EulerOS 2.0 SP2 : openssh (EulerOS-SA-2018-1069)

EulerOS 2.0 SP2 : openssh (EulerOS-SA-2018-1141)

EulerOS 2.0 SP2 : openssh (EulerOS-SA-2018-1431)

EulerOS 2.0 SP2 : openssh (EulerOS-SA-2019-2483)

EulerOS 2.0 SP2 : openssl (EulerOS-SA-2017-1030)

EulerOS 2.0 SP2 : openssl (EulerOS-SA-2018-1115)

EulerOS 2.0 SP2 : openssl (EulerOS-SA-2018-1420)

EulerOS 2.0 SP2 : openssl (EulerOS-SA-2019-1325)

EulerOS 2.0 SP2 : openssl (EulerOS-SA-2019-1732)

EulerOS 2.0 SP2 : openssl (EulerOS-SA-2019-2464)

EulerOS 2.0 SP2 : openssl098e (EulerOS-SA-2017-1039)

EulerOS 2.0 SP2 : openssl098e (EulerOS-SA-2019-1861)

EulerOS 2.0 SP2 : openssl098e (EulerOS-SA-2019-2509)

EulerOS 2.0 SP2 : openssl110f (EulerOS-SA-2018-1306)

EulerOS 2.0 SP2 : openssl110f (EulerOS-SA-2019-1327)

EulerOS 2.0 SP2 : openssl110f (EulerOS-SA-2019-1862)

EulerOS 2.0 SP2 : openssl110f (EulerOS-SA-2019-2430)

EulerOS 2.0 SP2 : openwsman (EulerOS-SA-2019-1329)

EulerOS 2.0 SP2 : oprofile (EulerOS-SA-2019-2516)

EulerOS 2.0 SP2 : PackageKit (EulerOS-SA-2018-1148)

EulerOS 2.0 SP2 : patch (EulerOS-SA-2018-1147)

EulerOS 2.0 SP2 : patch (EulerOS-SA-2019-1863)

EulerOS 2.0 SP2 : patch (EulerOS-SA-2019-2428)

EulerOS 2.0 SP2 : pcre (EulerOS-SA-2019-1733)

EulerOS 2.0 SP2 : pcre (EulerOS-SA-2019-2486)

EulerOS 2.0 SP2 : pcsc-lite (EulerOS-SA-2019-2474)

EulerOS 2.0 SP2 : perl (EulerOS-SA-2018-1307)

EulerOS 2.0 SP2 : perl (EulerOS-SA-2019-1717)

EulerOS 2.0 SP2 : perl (EulerOS-SA-2019-1864)

EulerOS 2.0 SP2 : perl (EulerOS-SA-2019-2419)

EulerOS 2.0 SP2 : perl-Archive-Tar (EulerOS-SA-2019-2415)

EulerOS 2.0 SP2 : php (EulerOS-SA-2017-1068)

EulerOS 2.0 SP2 : php (EulerOS-SA-2017-1302)

EulerOS 2.0 SP2 : php (EulerOS-SA-2018-1097)

EulerOS 2.0 SP2 : php (EulerOS-SA-2018-1217)

EulerOS 2.0 SP2 : php (EulerOS-SA-2018-1309)

EulerOS 2.0 SP2 : php (EulerOS-SA-2019-1120)

EulerOS 2.0 SP2 : php (EulerOS-SA-2019-1332)

EulerOS 2.0 SP2 : php (EulerOS-SA-2019-1723)

EulerOS 2.0 SP2 : php (EulerOS-SA-2019-1865)

EulerOS 2.0 SP2 : php (EulerOS-SA-2019-2438)

EulerOS 2.0 SP2 : php-pear (EulerOS-SA-2019-1121)

EulerOS 2.0 SP2 : pidgin (EulerOS-SA-2017-1131)

EulerOS 2.0 SP2 : pidgin (EulerOS-SA-2017-1166)

EulerOS 2.0 SP2 : pidgin (EulerOS-SA-2019-2387)

EulerOS 2.0 SP2 : pixman (EulerOS-SA-2019-2487)

EulerOS 2.0 SP2 : pki-core (EulerOS-SA-2017-1184)

EulerOS 2.0 SP2 : policycoreutils (EulerOS-SA-2019-2400)

EulerOS 2.0 SP2 : polkit (EulerOS-SA-2019-1122)

EulerOS 2.0 SP2 : polkit (EulerOS-SA-2019-1752)

EulerOS 2.0 SP2 : polkit (EulerOS-SA-2019-2404)

EulerOS 2.0 SP2 : poppler (EulerOS-SA-2017-1230)

EulerOS 2.0 SP2 : poppler (EulerOS-SA-2017-1260)

EulerOS 2.0 SP2 : poppler (EulerOS-SA-2017-1263)

EulerOS 2.0 SP2 : poppler (EulerOS-SA-2018-1219)

EulerOS 2.0 SP2 : poppler (EulerOS-SA-2019-1054)

EulerOS 2.0 SP2 : poppler (EulerOS-SA-2019-1123)

EulerOS 2.0 SP2 : poppler (EulerOS-SA-2019-2499)

EulerOS 2.0 SP2 : posrgresql (EulerOS-SA-2017-1216)

EulerOS 2.0 SP2 : postfix (EulerOS-SA-2018-1204)

EulerOS 2.0 SP2 : postgresql (EulerOS-SA-2017-1232)

EulerOS 2.0 SP2 : postgresql (EulerOS-SA-2017-1341)

EulerOS 2.0 SP2 : postgresql (EulerOS-SA-2018-1311)

EulerOS 2.0 SP2 : ppp (EulerOS-SA-2019-2399)

EulerOS 2.0 SP2 : procmail (EulerOS-SA-2017-1317)

EulerOS 2.0 SP2 : procps-ng (EulerOS-SA-2018-1198)

EulerOS 2.0 SP2 : python (EulerOS-SA-2017-1186)

EulerOS 2.0 SP2 : python (EulerOS-SA-2017-1335)

EulerOS 2.0 SP2 : python (EulerOS-SA-2019-1055)

EulerOS 2.0 SP2 : python (EulerOS-SA-2019-1124)

EulerOS 2.0 SP2 : python (EulerOS-SA-2019-1336)

EulerOS 2.0 SP2 : python (EulerOS-SA-2019-1866)

EulerOS 2.0 SP2 : python (EulerOS-SA-2019-2442)

EulerOS 2.0 SP2 : python-crypto (EulerOS-SA-2019-2511)

EulerOS 2.0 SP2 : python-jinja2 (EulerOS-SA-2019-1722)

EulerOS 2.0 SP2 : python-paramiko (EulerOS-SA-2018-1443)

EulerOS 2.0 SP2 : python-pillow (EulerOS-SA-2019-2437)

EulerOS 2.0 SP2 : python-urllib3 (EulerOS-SA-2019-2362)

EulerOS 2.0 SP2 : PyYAML (EulerOS-SA-2019-1056)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2017-1038)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2017-1080)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2017-1119)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2017-1157)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2017-1224)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2017-1321)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2018-1015)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2018-1113)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2018-1145)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2018-1200)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2018-1313)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2019-1867)

EulerOS 2.0 SP2 : qemu-kvm (EulerOS-SA-2019-2431)

EulerOS 2.0 SP2 : qpdf (EulerOS-SA-2019-2465)

EulerOS 2.0 SP2 : qt (EulerOS-SA-2019-1057)

EulerOS 2.0 SP2 : qt (EulerOS-SA-2019-1746)

EulerOS 2.0 SP2 : qt (EulerOS-SA-2019-2381)

EulerOS 2.0 SP2 : quagga (EulerOS-SA-2017-1308)

EulerOS 2.0 SP2 : quagga (EulerOS-SA-2018-1065)

EulerOS 2.0 SP2 : quagga (EulerOS-SA-2019-2408)

EulerOS 2.0 SP2 : rpcbind (EulerOS-SA-2017-1103)

EulerOS 2.0 SP2 : rpm (EulerOS-SA-2018-1353)

EulerOS 2.0 SP2 : rpm (EulerOS-SA-2019-2384)

EulerOS 2.0 SP2 : rsync (EulerOS-SA-2017-1333)

EulerOS 2.0 SP2 : rsync (EulerOS-SA-2018-1012)

EulerOS 2.0 SP2 : rsync (EulerOS-SA-2018-1050)

EulerOS 2.0 SP2 : rsyslog (EulerOS-SA-2019-1058)

EulerOS 2.0 SP2 : rsyslog (EulerOS-SA-2019-2418)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2017-1051)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2018-1030)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2018-1067)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2018-1108)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2018-1206)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2019-1718)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2019-1868)

EulerOS 2.0 SP2 : ruby (EulerOS-SA-2019-2403)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2017-1105)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2017-1220)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2017-1234)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2017-1315)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2019-1125)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2019-1744)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2019-1869)

EulerOS 2.0 SP2 : samba (EulerOS-SA-2019-2484)

EulerOS 2.0 SP2 : sblim-sfcb (EulerOS-SA-2019-2365)

EulerOS 2.0 SP2 : screen (EulerOS-SA-2019-1059)

EulerOS 2.0 SP2 : SDL (EulerOS-SA-2019-1126)

EulerOS 2.0 SP2 : SDL (EulerOS-SA-2019-2368)

EulerOS 2.0 SP2 : sendmail (EulerOS-SA-2019-2440)

EulerOS 2.0 SP2 : setup (EulerOS-SA-2018-1421)

EulerOS 2.0 SP2 : shadow-utils (EulerOS-SA-2019-2427)

EulerOS 2.0 SP2 : slf4j (EulerOS-SA-2018-1093)

EulerOS 2.0 SP2 : socat (EulerOS-SA-2019-2359)

EulerOS 2.0 SP2 : sox (EulerOS-SA-2018-1084)

EulerOS 2.0 SP2 : spice (EulerOS-SA-2017-1021)

EulerOS 2.0 SP2 : spice (EulerOS-SA-2017-1226)

EulerOS 2.0 SP2 : spice (EulerOS-SA-2018-1356)

EulerOS 2.0 SP2 : spice (EulerOS-SA-2019-1127)

EulerOS 2.0 SP2 : spice-gtk (EulerOS-SA-2018-1150)

EulerOS 2.0 SP2 : spice-gtk (EulerOS-SA-2018-1355)

EulerOS 2.0 SP2 : spice-vdagent (EulerOS-SA-2018-1052)

EulerOS 2.0 SP2 : sqlite (EulerOS-SA-2018-1137)

EulerOS 2.0 SP2 : sqlite (EulerOS-SA-2019-1720)

EulerOS 2.0 SP2 : sqlite (EulerOS-SA-2019-1870)

EulerOS 2.0 SP2 : sqlite (EulerOS-SA-2019-2461)

EulerOS 2.0 SP2 : squashfs-tools (EulerOS-SA-2019-1871)

EulerOS 2.0 SP2 : squid (EulerOS-SA-2017-1018)

EulerOS 2.0 SP2 : squid (EulerOS-SA-2018-1075)

EulerOS 2.0 SP2 : squid (EulerOS-SA-2019-2445)

EulerOS 2.0 SP2 : sssd (EulerOS-SA-2017-1325)

EulerOS 2.0 SP2 : sssd (EulerOS-SA-2018-1429)

EulerOS 2.0 SP2 : sssd (EulerOS-SA-2019-1754)

EulerOS 2.0 SP2 : sssd (EulerOS-SA-2019-2517)

EulerOS 2.0 SP2 : strongimcv (EulerOS-SA-2019-2447)

EulerOS 2.0 SP2 : subversion (EulerOS-SA-2017-1176)

EulerOS 2.0 SP2 : subversion (EulerOS-SA-2019-2504)

EulerOS 2.0 SP2 : sudo (EulerOS-SA-2017-1107)

EulerOS 2.0 SP2 : sudo (EulerOS-SA-2017-1121)

EulerOS 2.0 SP2 : sudo (EulerOS-SA-2019-2414)

EulerOS 2.0 SP2 : systemd (EulerOS-SA-2019-1060)

EulerOS 2.0 SP2 : systemd (EulerOS-SA-2019-1128)

EulerOS 2.0 SP2 : systemd (EulerOS-SA-2019-1344)

EulerOS 2.0 SP2 : systemd (EulerOS-SA-2019-1748)

EulerOS 2.0 SP2 : systemd (EulerOS-SA-2019-1872)

EulerOS 2.0 SP2 : systemd (EulerOS-SA-2019-2364)

EulerOS 2.0 SP2 : taglib (EulerOS-SA-2019-2482)

EulerOS 2.0 SP2 : tar (EulerOS-SA-2019-1129)

EulerOS 2.0 SP2 : tar (EulerOS-SA-2019-1600)

EulerOS 2.0 SP2 : tar (EulerOS-SA-2019-2423)

EulerOS 2.0 SP2 : tcpdump (EulerOS-SA-2017-1180)

EulerOS 2.0 SP2 : tcpdump (EulerOS-SA-2017-1281)

EulerOS 2.0 SP2 : tcpdump (EulerOS-SA-2019-2435)

EulerOS 2.0 SP2 : texlive (EulerOS-SA-2019-1873)

EulerOS 2.0 SP2 : tigervnc (EulerOS-SA-2017-1228)

EulerOS 2.0 SP2 : tomcat (EulerOS-SA-2017-1082)

EulerOS 2.0 SP2 : tomcat (EulerOS-SA-2017-1192)

EulerOS 2.0 SP2 : tomcat (EulerOS-SA-2017-1262)

EulerOS 2.0 SP2 : tomcat (EulerOS-SA-2018-1220)

EulerOS 2.0 SP2 : tomcat (EulerOS-SA-2018-1415)

EulerOS 2.0 SP2 : tomcat (EulerOS-SA-2019-2361)

EulerOS 2.0 SP2 : unbound (EulerOS-SA-2019-2488)

EulerOS 2.0 SP2 : unixODBC (EulerOS-SA-2019-2494)

EulerOS 2.0 SP2 : unzip (EulerOS-SA-2019-1348)

EulerOS 2.0 SP2 : unzip (EulerOS-SA-2019-2429)

EulerOS 2.0 SP2 : util-linux (EulerOS-SA-2017-1084)

EulerOS 2.0 SP2 : util-linux (EulerOS-SA-2019-1737)

EulerOS 2.0 SP2 : util-linux (EulerOS-SA-2019-2463)

EulerOS 2.0 SP2 : vim (EulerOS-SA-2017-1034)

EulerOS 2.0 SP2 : vim (EulerOS-SA-2017-1149)

EulerOS 2.0 SP2 : vim (EulerOS-SA-2019-1753)

EulerOS 2.0 SP2 : vim (EulerOS-SA-2019-2462)

EulerOS 2.0 SP2 : wavpack (EulerOS-SA-2019-1874)

EulerOS 2.0 SP2 : wavpack (EulerOS-SA-2019-2413)

EulerOS 2.0 SP2 : webkitgtk3 (EulerOS-SA-2017-1310)

EulerOS 2.0 SP2 : wget (EulerOS-SA-2017-1270)

EulerOS 2.0 SP2 : wget (EulerOS-SA-2018-1315)

EulerOS 2.0 SP2 : wget (EulerOS-SA-2019-1130)

EulerOS 2.0 SP2 : wget (EulerOS-SA-2019-1736)

EulerOS 2.0 SP2 : wget (EulerOS-SA-2019-2501)

EulerOS 2.0 SP2 : wireshark (EulerOS-SA-2018-1042)

EulerOS 2.0 SP2 : wireshark (EulerOS-SA-2019-2425)

EulerOS 2.0 SP2 : wpa\_supplicant (EulerOS-SA-2017-1242)

EulerOS 2.0 SP2 : wpa\_supplicant (EulerOS-SA-2018-1317)

EulerOS 2.0 SP2 : wpa\_supplicant (EulerOS-SA-2019-1875)

EulerOS 2.0 SP2 : xdelta (EulerOS-SA-2019-2506)

EulerOS 2.0 SP2 : xdg-user-dirs (EulerOS-SA-2018-1025)

EulerOS 2.0 SP2 : xerces-c (EulerOS-SA-2018-1101)

EulerOS 2.0 SP2 : xerces-c (EulerOS-SA-2018-1422)

EulerOS 2.0 SP2 : xmlsec1 (EulerOS-SA-2017-1194)

EulerOS 2.0 SP2 : xorg-x11-server (EulerOS-SA-2017-1296)

EulerOS 2.0 SP2 : xorg-x11-server (EulerOS-SA-2019-2421)

EulerOS 2.0 SP2 : yum-utils (EulerOS-SA-2018-1319)

EulerOS 2.0 SP2 : zip (EulerOS-SA-2019-1876)

EulerOS 2.0 SP2 : zsh (EulerOS-SA-2018-1091)

EulerOS 2.0 SP2 : zsh (EulerOS-SA-2018-1208)

EulerOS 2.0 SP2 : zsh (EulerOS-SA-2018-1424)

EulerOS 2.0 SP2 : zsh (EulerOS-SA-2019-2459)

EulerOS 2.0 SP2 : zziplib (EulerOS-SA-2018-1423)

EulerOS 2.0 SP2 : zziplib (EulerOS-SA-2019-2478)

EulerOS 2.0 SP3 : 389-ds-base (EulerOS-SA-2018-1191)

EulerOS 2.0 SP3 : 389-ds-base (EulerOS-SA-2018-1365)

EulerOS 2.0 SP3 : 389-ds-base (EulerOS-SA-2018-1440)

EulerOS 2.0 SP3 : 389-ds-base (EulerOS-SA-2019-1561)

EulerOS 2.0 SP3 : 389-ds-base (EulerOS-SA-2019-2554)

EulerOS 2.0 SP3 : accountsservice (EulerOS-SA-2019-2555)

EulerOS 2.0 SP3 : audit (EulerOS-SA-2019-2556)

EulerOS 2.0 SP3 : avahi (EulerOS-SA-2019-2038)

EulerOS 2.0 SP3 : bash (EulerOS-SA-2019-1564)

EulerOS 2.0 SP3 : bind (EulerOS-SA-2018-1282)

EulerOS 2.0 SP3 : bind (EulerOS-SA-2019-2040)

EulerOS 2.0 SP3 : bind (EulerOS-SA-2019-2557)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2018-1154)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2018-1284)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2018-1400)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2019-1089)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2019-1278)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2019-2041)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2019-2558)

EulerOS 2.0 SP3 : binutils (EulerOS-SA-2020-1372)

EulerOS 2.0 SP3 : bluez (EulerOS-SA-2019-2559)

EulerOS 2.0 SP3 : bubblewrap (EulerOS-SA-2019-2046)

EulerOS 2.0 SP3 : bzip2 (EulerOS-SA-2019-2057)

EulerOS 2.0 SP3 : bzip2 (EulerOS-SA-2019-2560)

EulerOS 2.0 SP3 : c-ares (EulerOS-SA-2019-2017)

EulerOS 2.0 SP3 : cairo (EulerOS-SA-2018-1161)

EulerOS 2.0 SP3 : cairo (EulerOS-SA-2019-2268)

EulerOS 2.0 SP3 : cairo (EulerOS-SA-2019-2561)

EulerOS 2.0 SP3 : cifs-utils (EulerOS-SA-2019-2562)

EulerOS 2.0 SP3 : cloud-init (EulerOS-SA-2020-1373)

EulerOS 2.0 SP3 : compat-libtiff3 (EulerOS-SA-2019-2244)

EulerOS 2.0 SP3 : coreutils (EulerOS-SA-2019-2563)

EulerOS 2.0 SP3 : coreutils (EulerOS-SA-2020-1374)

EulerOS 2.0 SP3 : cpio (EulerOS-SA-2020-1375)

EulerOS 2.0 SP3 : cronie (EulerOS-SA-2019-2564)

EulerOS 2.0 SP3 : cups (EulerOS-SA-2019-1567)

EulerOS 2.0 SP3 : cups (EulerOS-SA-2019-2565)

EulerOS 2.0 SP3 : curl (EulerOS-SA-2018-1203)

EulerOS 2.0 SP3 : curl (EulerOS-SA-2018-1401)

EulerOS 2.0 SP3 : curl (EulerOS-SA-2019-1090)

EulerOS 2.0 SP3 : curl (EulerOS-SA-2019-2054)

EulerOS 2.0 SP3 : curl (EulerOS-SA-2019-2252)

EulerOS 2.0 SP3 : curl (EulerOS-SA-2019-2566)

EulerOS 2.0 SP3 : curl (EulerOS-SA-2020-1376)

EulerOS 2.0 SP3 : cyrus-sasl (EulerOS-SA-2020-1377)

EulerOS 2.0 SP3 : dbus (EulerOS-SA-2019-2022)

EulerOS 2.0 SP3 : dcraw (EulerOS-SA-2019-2002)

EulerOS 2.0 SP3 : dcraw (EulerOS-SA-2019-2567)

EulerOS 2.0 SP3 : dhcp (EulerOS-SA-2018-1162)

EulerOS 2.0 SP3 : dhcp (EulerOS-SA-2018-1188)

EulerOS 2.0 SP3 : dhcp (EulerOS-SA-2019-2568)

EulerOS 2.0 SP3 : dnsmasq (EulerOS-SA-2020-1378)

EulerOS 2.0 SP3 : dom4j (EulerOS-SA-2019-2569)

EulerOS 2.0 SP3 : dosfstools (EulerOS-SA-2019-2570)

EulerOS 2.0 SP3 : dovecot (EulerOS-SA-2019-1569)

EulerOS 2.0 SP3 : dovecot (EulerOS-SA-2019-2243)

EulerOS 2.0 SP3 : dovecot (EulerOS-SA-2019-2571)

EulerOS 2.0 SP3 : dump (EulerOS-SA-2019-2029)

EulerOS 2.0 SP3 : e2fsprogs (EulerOS-SA-2020-1379)

EulerOS 2.0 SP3 : ed (EulerOS-SA-2019-2572)

EulerOS 2.0 SP3 : elfutils (EulerOS-SA-2019-1281)

EulerOS 2.0 SP3 : elfutils (EulerOS-SA-2019-2272)

EulerOS 2.0 SP3 : elfutils (EulerOS-SA-2019-2573)

EulerOS 2.0 SP3 : elinks (EulerOS-SA-2019-2574)

EulerOS 2.0 SP3 : eog (EulerOS-SA-2019-2026)

EulerOS 2.0 SP3 : exempi (EulerOS-SA-2018-1173)

EulerOS 2.0 SP3 : exempi (EulerOS-SA-2019-2575)

EulerOS 2.0 SP3 : exiv2 (EulerOS-SA-2018-1287)

EulerOS 2.0 SP3 : exiv2 (EulerOS-SA-2019-1995)

EulerOS 2.0 SP3 : exiv2 (EulerOS-SA-2019-2576)

EulerOS 2.0 SP3 : exiv2 (EulerOS-SA-2020-1380)

EulerOS 2.0 SP3 : expat (EulerOS-SA-2019-2063)

EulerOS 2.0 SP3 : expat (EulerOS-SA-2019-2256)

EulerOS 2.0 SP3 : fence-agents (EulerOS-SA-2019-2577)

EulerOS 2.0 SP3 : file (EulerOS-SA-2019-2578)

EulerOS 2.0 SP3 : file (EulerOS-SA-2020-1381)

EulerOS 2.0 SP3 : firefox (EulerOS-SA-2018-1189)

EulerOS 2.0 SP3 : firefox (EulerOS-SA-2018-1288)

EulerOS 2.0 SP3 : firefox (EulerOS-SA-2018-1367)

EulerOS 2.0 SP3 : firefox (EulerOS-SA-2018-1384)

EulerOS 2.0 SP3 : firefox (EulerOS-SA-2019-1571)

EulerOS 2.0 SP3 : flex (EulerOS-SA-2019-2050)

EulerOS 2.0 SP3 : foomatic (EulerOS-SA-2019-2579)

EulerOS 2.0 SP3 : freeradius (EulerOS-SA-2019-1573)

EulerOS 2.0 SP3 : freeradius (EulerOS-SA-2019-2065)

EulerOS 2.0 SP3 : freerdp (EulerOS-SA-2019-1284)

EulerOS 2.0 SP3 : freerdp (EulerOS-SA-2019-2262)

EulerOS 2.0 SP3 : freerdp (EulerOS-SA-2019-2580)

EulerOS 2.0 SP3 : freetype (EulerOS-SA-2019-2581)

EulerOS 2.0 SP3 : freetype (EulerOS-SA-2020-1382)

EulerOS 2.0 SP3 : fuse (EulerOS-SA-2018-1387)

EulerOS 2.0 SP3 : fuse (EulerOS-SA-2019-1575)

EulerOS 2.0 SP3 : gc (EulerOS-SA-2019-2582)

EulerOS 2.0 SP3 : gcc (EulerOS-SA-2018-1174)

EulerOS 2.0 SP3 : gcc (EulerOS-SA-2020-1383)

EulerOS 2.0 SP3 : gd (EulerOS-SA-2019-1091)

EulerOS 2.0 SP3 : gd (EulerOS-SA-2019-2583)

EulerOS 2.0 SP3 : gd (EulerOS-SA-2020-1384)

EulerOS 2.0 SP3 : gdb (EulerOS-SA-2019-2584)

EulerOS 2.0 SP3 : gdk-pixbuf2 (EulerOS-SA-2019-2585)

EulerOS 2.0 SP3 : gettext (EulerOS-SA-2019-2270)

EulerOS 2.0 SP3 : ghostscript (EulerOS-SA-2018-1404)

EulerOS 2.0 SP3 : ghostscript (EulerOS-SA-2019-1022)

EulerOS 2.0 SP3 : ghostscript (EulerOS-SA-2019-1092)

EulerOS 2.0 SP3 : ghostscript (EulerOS-SA-2019-1289)

EulerOS 2.0 SP3 : ghostscript (EulerOS-SA-2019-2031)

EulerOS 2.0 SP3 : ghostscript (EulerOS-SA-2019-2242)

EulerOS 2.0 SP3 : ghostscript (EulerOS-SA-2019-2586)

EulerOS 2.0 SP3 : giflib (EulerOS-SA-2019-2587)

EulerOS 2.0 SP3 : giflib (EulerOS-SA-2020-1385)

EulerOS 2.0 SP3 : gimp (EulerOS-SA-2019-2021)

EulerOS 2.0 SP3 : git (EulerOS-SA-2018-1216)

EulerOS 2.0 SP3 : git (EulerOS-SA-2018-1388)

EulerOS 2.0 SP3 : git (EulerOS-SA-2019-2028)

EulerOS 2.0 SP3 : git (EulerOS-SA-2020-1386)

EulerOS 2.0 SP3 : glib2 (EulerOS-SA-2019-2588)

EulerOS 2.0 SP3 : glib2 (EulerOS-SA-2020-1387)

EulerOS 2.0 SP3 : glibc (EulerOS-SA-2019-1024)

EulerOS 2.0 SP3 : glibc (EulerOS-SA-2019-2030)

EulerOS 2.0 SP3 : glibc (EulerOS-SA-2020-1388)

EulerOS 2.0 SP3 : glusterfs (EulerOS-SA-2018-1185)

EulerOS 2.0 SP3 : glusterfs (EulerOS-SA-2018-1229)

EulerOS 2.0 SP3 : glusterfs (EulerOS-SA-2018-1442)

EulerOS 2.0 SP3 : gnupg2 (EulerOS-SA-2018-1223)

EulerOS 2.0 SP3 : gnupg2 (EulerOS-SA-2019-2589)

EulerOS 2.0 SP3 : gnutls (EulerOS-SA-2019-1026)

EulerOS 2.0 SP3 : gnutls (EulerOS-SA-2019-1292)

EulerOS 2.0 SP3 : gnutls (EulerOS-SA-2019-2016)

EulerOS 2.0 SP3 : gnutls (EulerOS-SA-2019-2590)

EulerOS 2.0 SP3 : gpgme (EulerOS-SA-2019-2591)

EulerOS 2.0 SP3 : graphite2 (EulerOS-SA-2018-1172)

EulerOS 2.0 SP3 : graphviz (EulerOS-SA-2019-2064)

EulerOS 2.0 SP3 : graphviz (EulerOS-SA-2019-2592)

EulerOS 2.0 SP3 : grub2 (EulerOS-SA-2019-2011)

EulerOS 2.0 SP3 : gstreamer-plugins-base (EulerOS-SA-2019-1578)

EulerOS 2.0 SP3 : gvfs (EulerOS-SA-2019-2039)

EulerOS 2.0 SP3 : http-parser (EulerOS-SA-2019-2238)

EulerOS 2.0 SP3 : httpd (EulerOS-SA-2018-1213)

EulerOS 2.0 SP3 : httpd (EulerOS-SA-2019-1294)

EulerOS 2.0 SP3 : httpd (EulerOS-SA-2019-1580)

EulerOS 2.0 SP3 : httpd (EulerOS-SA-2019-2249)

EulerOS 2.0 SP3 : httpd (EulerOS-SA-2019-2593)

EulerOS 2.0 SP3 : icu (EulerOS-SA-2019-2248)

EulerOS 2.0 SP3 : icu (EulerOS-SA-2019-2594)

EulerOS 2.0 SP3 : icu (EulerOS-SA-2020-1389)

EulerOS 2.0 SP3 : ImageMagick (EulerOS-SA-2018-1175)

EulerOS 2.0 SP3 : ImageMagick (EulerOS-SA-2018-1291)

EulerOS 2.0 SP3 : ImageMagick (EulerOS-SA-2019-1297)

EulerOS 2.0 SP3 : ImageMagick (EulerOS-SA-2019-1582)

EulerOS 2.0 SP3 : ImageMagick (EulerOS-SA-2019-2024)

EulerOS 2.0 SP3 : ImageMagick (EulerOS-SA-2020-1390)

EulerOS 2.0 SP3 : ipa (EulerOS-SA-2020-1391)

EulerOS 2.0 SP3 : ipmitool (EulerOS-SA-2020-1392)

EulerOS 2.0 SP3 : irssi (EulerOS-SA-2019-1093)

EulerOS 2.0 SP3 : irssi (EulerOS-SA-2019-2595)

EulerOS 2.0 SP3 : iscsi-initiator-utils (EulerOS-SA-2019-2596)

EulerOS 2.0 SP3 : jakarta-commons-httpclient (EulerOS-SA-2019-2027)

EulerOS 2.0 SP3 : jansson (EulerOS-SA-2019-2597)

EulerOS 2.0 SP3 : jasper (EulerOS-SA-2018-1163)

EulerOS 2.0 SP3 : jasper (EulerOS-SA-2018-1389)

EulerOS 2.0 SP3 : jasper (EulerOS-SA-2019-2598)

EulerOS 2.0 SP3 : jasper (EulerOS-SA-2020-1393)

EulerOS 2.0 SP3 : java-1.7.0-openjdk (EulerOS-SA-2018-1193)

EulerOS 2.0 SP3 : java-1.7.0-openjdk (EulerOS-SA-2018-1293)

EulerOS 2.0 SP3 : java-1.7.0-openjdk (EulerOS-SA-2019-1299)

EulerOS 2.0 SP3 : java-1.7.0-openjdk (EulerOS-SA-2019-2007)

EulerOS 2.0 SP3 : java-1.7.0-openjdk (EulerOS-SA-2019-2263)

EulerOS 2.0 SP3 : java-1.7.0-openjdk (EulerOS-SA-2020-1394)

EulerOS 2.0 SP3 : java-1.8.0-openjdk (EulerOS-SA-2018-1195)

EulerOS 2.0 SP3 : java-1.8.0-openjdk (EulerOS-SA-2018-1295)

EulerOS 2.0 SP3 : java-1.8.0-openjdk (EulerOS-SA-2018-1386)

EulerOS 2.0 SP3 : java-1.8.0-openjdk (EulerOS-SA-2019-1300)

EulerOS 2.0 SP3 : java-1.8.0-openjdk (EulerOS-SA-2019-1585)

EulerOS 2.0 SP3 : java-1.8.0-openjdk (EulerOS-SA-2019-2245)

EulerOS 2.0 SP3 : java-1.8.0-openjdk (EulerOS-SA-2020-1395)

EulerOS 2.0 SP3 : keepalived (EulerOS-SA-2019-2044)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2018-1121)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2018-1196)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2018-1279)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2018-1297)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2018-1362)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2018-1406)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2018-1433)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-1027)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-1108)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-1303)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-1587)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-1672)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-2068)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-2274)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2019-2599)

EulerOS 2.0 SP3 : kernel (EulerOS-SA-2020-1396)

EulerOS 2.0 SP3 : krb5 (EulerOS-SA-2018-1361)

EulerOS 2.0 SP3 : krb5 (EulerOS-SA-2018-1398)

EulerOS 2.0 SP3 : krb5 (EulerOS-SA-2019-2058)

EulerOS 2.0 SP3 : krb5 (EulerOS-SA-2019-2600)

EulerOS 2.0 SP3 : lcms2 (EulerOS-SA-2019-2601)

EulerOS 2.0 SP3 : less (EulerOS-SA-2019-2602)

EulerOS 2.0 SP3 : lftp (EulerOS-SA-2019-2603)

EulerOS 2.0 SP3 : libarchive (EulerOS-SA-2019-1094)

EulerOS 2.0 SP3 : libarchive (EulerOS-SA-2019-2014)

EulerOS 2.0 SP3 : libarchive (EulerOS-SA-2019-2604)

EulerOS 2.0 SP3 : libarchive (EulerOS-SA-2020-1397)

EulerOS 2.0 SP3 : libcdio (EulerOS-SA-2018-1390)

EulerOS 2.0 SP3 : libcgroup (EulerOS-SA-2019-2001)

EulerOS 2.0 SP3 : libcroco (EulerOS-SA-2019-2605)

EulerOS 2.0 SP3 : libdwarf (EulerOS-SA-2020-1398)

EulerOS 2.0 SP3 : libesmtp (EulerOS-SA-2020-1399)

EulerOS 2.0 SP3 : libevent (EulerOS-SA-2018-1164)

EulerOS 2.0 SP3 : libexif (EulerOS-SA-2019-1095)

EulerOS 2.0 SP3 : libexif (EulerOS-SA-2019-2036)

EulerOS 2.0 SP3 : libgcrypt (EulerOS-SA-2019-2006)

EulerOS 2.0 SP3 : libgcrypt (EulerOS-SA-2020-1400)

EulerOS 2.0 SP3 : libgsf (EulerOS-SA-2019-2240)

EulerOS 2.0 SP3 : libguestfs-winsupport (EulerOS-SA-2019-2253)

EulerOS 2.0 SP3 : libgxps (EulerOS-SA-2018-1402)

EulerOS 2.0 SP3 : libgxps (EulerOS-SA-2019-2606)

EulerOS 2.0 SP3 : libgxps (EulerOS-SA-2020-1401)

EulerOS 2.0 SP3 : libical (EulerOS-SA-2019-2607)

EulerOS 2.0 SP3 : libidn (EulerOS-SA-2019-2049)

EulerOS 2.0 SP3 : libidn (EulerOS-SA-2019-2608)

EulerOS 2.0 SP3 : libimobiledevice (EulerOS-SA-2019-2258)

EulerOS 2.0 SP3 : libjpeg-turbo (EulerOS-SA-2018-1299)

EulerOS 2.0 SP3 : libjpeg-turbo (EulerOS-SA-2019-1589)

EulerOS 2.0 SP3 : libjpeg-turbo (EulerOS-SA-2019-2251)

EulerOS 2.0 SP3 : libjpeg-turbo (EulerOS-SA-2020-1402)

EulerOS 2.0 SP3 : liblouis (EulerOS-SA-2018-1228)

EulerOS 2.0 SP3 : liblouis (EulerOS-SA-2018-1301)

EulerOS 2.0 SP3 : libmspack (EulerOS-SA-2018-1436)

EulerOS 2.0 SP3 : libmspack (EulerOS-SA-2019-2034)

EulerOS 2.0 SP3 : libmspack (EulerOS-SA-2019-2261)

EulerOS 2.0 SP3 : libmspack (EulerOS-SA-2019-2609)

EulerOS 2.0 SP3 : libmspack (EulerOS-SA-2020-1403)

EulerOS 2.0 SP3 : libmtp (EulerOS-SA-2019-2610)

EulerOS 2.0 SP3 : libndp (EulerOS-SA-2019-2611)

EulerOS 2.0 SP3 : libnl (EulerOS-SA-2019-2051)

EulerOS 2.0 SP3 : libosinfo (EulerOS-SA-2019-2003)

EulerOS 2.0 SP3 : libpcap (EulerOS-SA-2019-2612)

EulerOS 2.0 SP3 : libplist (EulerOS-SA-2019-2613)

EulerOS 2.0 SP3 : libplist (EulerOS-SA-2020-1404)

EulerOS 2.0 SP3 : libpng (EulerOS-SA-2019-1307)

EulerOS 2.0 SP3 : libpng (EulerOS-SA-2019-2048)

EulerOS 2.0 SP3 : libpng (EulerOS-SA-2019-2247)

EulerOS 2.0 SP3 : librelp (EulerOS-SA-2018-1182)

EulerOS 2.0 SP3 : librsvg2 (EulerOS-SA-2019-2614)

EulerOS 2.0 SP3 : libsamplerate (EulerOS-SA-2019-2615)

EulerOS 2.0 SP3 : libseccomp (EulerOS-SA-2019-2025)

EulerOS 2.0 SP3 : libsndfile (EulerOS-SA-2019-1029)

EulerOS 2.0 SP3 : libsndfile (EulerOS-SA-2019-1591)

EulerOS 2.0 SP3 : libsndfile (EulerOS-SA-2019-2037)

EulerOS 2.0 SP3 : libsndfile (EulerOS-SA-2019-2616)

EulerOS 2.0 SP3 : libsolv (EulerOS-SA-2019-2033)

EulerOS 2.0 SP3 : libsolv (EulerOS-SA-2019-2260)

EulerOS 2.0 SP3 : libsoup (EulerOS-SA-2018-1391)

EulerOS 2.0 SP3 : libsrtp (EulerOS-SA-2019-2617)

EulerOS 2.0 SP3 : libssh (EulerOS-SA-2019-2067)

EulerOS 2.0 SP3 : libssh2 (EulerOS-SA-2019-1309)

EulerOS 2.0 SP3 : libssh2 (EulerOS-SA-2019-2618)

EulerOS 2.0 SP3 : libssh2 (EulerOS-SA-2020-1405)

EulerOS 2.0 SP3 : libtar (EulerOS-SA-2019-2619)

EulerOS 2.0 SP3 : libtasn1 (EulerOS-SA-2019-1031)

EulerOS 2.0 SP3 : libtasn1 (EulerOS-SA-2019-1312)

EulerOS 2.0 SP3 : libtasn1 (EulerOS-SA-2019-2620)

EulerOS 2.0 SP3 : libtiff (EulerOS-SA-2018-1165)

EulerOS 2.0 SP3 : libtiff (EulerOS-SA-2019-2056)

EulerOS 2.0 SP3 : libtiff (EulerOS-SA-2019-2265)

EulerOS 2.0 SP3 : libtiff (EulerOS-SA-2019-2621)

EulerOS 2.0 SP3 : libuser (EulerOS-SA-2020-1406)

EulerOS 2.0 SP3 : libvirt (EulerOS-SA-2018-1197)

EulerOS 2.0 SP3 : libvirt (EulerOS-SA-2019-1314)

EulerOS 2.0 SP3 : libvirt (EulerOS-SA-2019-2020)

EulerOS 2.0 SP3 : libvncserver (EulerOS-SA-2018-1176)

EulerOS 2.0 SP3 : libvncserver (EulerOS-SA-2019-1032)

EulerOS 2.0 SP3 : libvncserver (EulerOS-SA-2019-1096)

EulerOS 2.0 SP3 : libvorbis (EulerOS-SA-2018-1155)

EulerOS 2.0 SP3 : libvorbis (EulerOS-SA-2019-2622)

EulerOS 2.0 SP3 : libwmf (EulerOS-SA-2019-2623)

EulerOS 2.0 SP3 : libwpd (EulerOS-SA-2020-1407)

EulerOS 2.0 SP3 : libX11 (EulerOS-SA-2019-2624)

EulerOS 2.0 SP3 : libxcursor (EulerOS-SA-2018-1438)

EulerOS 2.0 SP3 : libXfont (EulerOS-SA-2019-2625)

EulerOS 2.0 SP3 : libxml2 (EulerOS-SA-2018-1156)

EulerOS 2.0 SP3 : libxml2 (EulerOS-SA-2018-1186)

EulerOS 2.0 SP3 : libxml2 (EulerOS-SA-2019-1034)

EulerOS 2.0 SP3 : libxml2 (EulerOS-SA-2019-2013)

EulerOS 2.0 SP3 : libxml2 (EulerOS-SA-2019-2626)

EulerOS 2.0 SP3 : libxml2 (EulerOS-SA-2020-1408)

EulerOS 2.0 SP3 : libxslt (EulerOS-SA-2019-1592)

EulerOS 2.0 SP3 : libxslt (EulerOS-SA-2019-2032)

EulerOS 2.0 SP3 : libxslt (EulerOS-SA-2019-2627)

EulerOS 2.0 SP3 : libxslt (EulerOS-SA-2020-1409)

EulerOS 2.0 SP3 : libXvMC (EulerOS-SA-2019-2628)

EulerOS 2.0 SP3 : lua (EulerOS-SA-2019-2629)

EulerOS 2.0 SP3 : lynx (EulerOS-SA-2020-1410)

EulerOS 2.0 SP3 : lz4 (EulerOS-SA-2019-2630)

EulerOS 2.0 SP3 : mariadb (EulerOS-SA-2018-1187)

EulerOS 2.0 SP3 : mariadb (EulerOS-SA-2018-1303)

EulerOS 2.0 SP3 : mariadb (EulerOS-SA-2020-1411)

EulerOS 2.0 SP3 : memcached (EulerOS-SA-2018-1177)

EulerOS 2.0 SP3 : memcached (EulerOS-SA-2019-2631)

EulerOS 2.0 SP3 : mercurial (EulerOS-SA-2018-1178)

EulerOS 2.0 SP3 : mercurial (EulerOS-SA-2019-2273)

EulerOS 2.0 SP3 : mod\_auth\_mellon (EulerOS-SA-2019-1320)

EulerOS 2.0 SP3 : mod\_auth\_mellon (EulerOS-SA-2019-2009)

EulerOS 2.0 SP3 : mod\_auth\_mellon (EulerOS-SA-2019-2632)

EulerOS 2.0 SP3 : mod\_wsgi (EulerOS-SA-2019-2633)

EulerOS 2.0 SP3 : mutt (EulerOS-SA-2018-1305)

EulerOS 2.0 SP3 : mutt (EulerOS-SA-2020-1412)

EulerOS 2.0 SP3 : ncurses (EulerOS-SA-2018-1166)

EulerOS 2.0 SP3 : ncurses (EulerOS-SA-2018-1225)

EulerOS 2.0 SP3 : ncurses (EulerOS-SA-2019-2634)

EulerOS 2.0 SP3 : net-snmp (EulerOS-SA-2019-1035)

EulerOS 2.0 SP3 : netpbm (EulerOS-SA-2019-2635)

EulerOS 2.0 SP3 : NetworkManager (EulerOS-SA-2019-1322)

EulerOS 2.0 SP3 : NetworkManager (EulerOS-SA-2019-2636)

EulerOS 2.0 SP3 : nginx (EulerOS-SA-2018-1399)

EulerOS 2.0 SP3 : nginx (EulerOS-SA-2020-1413)

EulerOS 2.0 SP3 : nss (EulerOS-SA-2018-1366)

EulerOS 2.0 SP3 : nss-softokn (EulerOS-SA-2019-2246)

EulerOS 2.0 SP3 : nss-softokn (EulerOS-SA-2020-1414)

EulerOS 2.0 SP3 : nss-util (EulerOS-SA-2020-1415)

EulerOS 2.0 SP3 : ntp (EulerOS-SA-2019-1037)

EulerOS 2.0 SP3 : ntp (EulerOS-SA-2019-2066)

EulerOS 2.0 SP3 : ntp (EulerOS-SA-2019-2637)

EulerOS 2.0 SP3 : OpenEXR (EulerOS-SA-2019-2638)

EulerOS 2.0 SP3 : OpenEXR (EulerOS-SA-2020-1416)

EulerOS 2.0 SP3 : openjpeg (EulerOS-SA-2018-1157)

EulerOS 2.0 SP3 : openjpeg (EulerOS-SA-2019-2639)

EulerOS 2.0 SP3 : openldap (EulerOS-SA-2019-1996)

EulerOS 2.0 SP3 : openldap (EulerOS-SA-2019-2640)

EulerOS 2.0 SP3 : opensc (EulerOS-SA-2020-1417)

EulerOS 2.0 SP3 : openslp (EulerOS-SA-2018-1211)

EulerOS 2.0 SP3 : openslp (EulerOS-SA-2019-2641)

EulerOS 2.0 SP3 : openslp (EulerOS-SA-2020-1418)

EulerOS 2.0 SP3 : openssh (EulerOS-SA-2018-1405)

EulerOS 2.0 SP3 : openssh (EulerOS-SA-2019-1097)

EulerOS 2.0 SP3 : openssh (EulerOS-SA-2020-1419)

EulerOS 2.0 SP3 : openssl (EulerOS-SA-2018-1179)

EulerOS 2.0 SP3 : openssl (EulerOS-SA-2018-1392)

EulerOS 2.0 SP3 : openssl (EulerOS-SA-2019-1326)

EulerOS 2.0 SP3 : openssl (EulerOS-SA-2019-2008)

EulerOS 2.0 SP3 : openssl (EulerOS-SA-2019-2264)

EulerOS 2.0 SP3 : openssl (EulerOS-SA-2019-2642)

EulerOS 2.0 SP3 : openssl098e (EulerOS-SA-2019-2271)

EulerOS 2.0 SP3 : openssl098e (EulerOS-SA-2019-2643)

EulerOS 2.0 SP3 : openssl098e (EulerOS-SA-2020-1420)

EulerOS 2.0 SP3 : openssl1.1.0f (EulerOS-SA-2019-2005)

EulerOS 2.0 SP3 : openssl1.1.0f (EulerOS-SA-2019-2254)

EulerOS 2.0 SP3 : openssl110f (EulerOS-SA-2018-1214)

EulerOS 2.0 SP3 : openssl110f (EulerOS-SA-2018-1434)

EulerOS 2.0 SP3 : openssl110f (EulerOS-SA-2019-1328)

EulerOS 2.0 SP3 : openwsman (EulerOS-SA-2019-1330)

EulerOS 2.0 SP3 : oprofile (EulerOS-SA-2019-2644)

EulerOS 2.0 SP3 : PackageKit (EulerOS-SA-2018-1183)

EulerOS 2.0 SP3 : patch (EulerOS-SA-2018-1184)

EulerOS 2.0 SP3 : patch (EulerOS-SA-2019-2004)

EulerOS 2.0 SP3 : patch (EulerOS-SA-2019-2645)

EulerOS 2.0 SP3 : pcre (EulerOS-SA-2018-1167)

EulerOS 2.0 SP3 : pcre (EulerOS-SA-2019-1098)

EulerOS 2.0 SP3 : pcre (EulerOS-SA-2019-2646)

EulerOS 2.0 SP3 : pcsc-lite (EulerOS-SA-2019-2647)

EulerOS 2.0 SP3 : perl (EulerOS-SA-2018-1308)

EulerOS 2.0 SP3 : perl (EulerOS-SA-2019-1099)

EulerOS 2.0 SP3 : perl (EulerOS-SA-2019-2035)

EulerOS 2.0 SP3 : perl (EulerOS-SA-2019-2648)

EulerOS 2.0 SP3 : perl (EulerOS-SA-2020-1421)

EulerOS 2.0 SP3 : php (EulerOS-SA-2018-1158)

EulerOS 2.0 SP3 : php (EulerOS-SA-2018-1224)

EulerOS 2.0 SP3 : php (EulerOS-SA-2018-1310)

EulerOS 2.0 SP3 : php (EulerOS-SA-2019-1100)

EulerOS 2.0 SP3 : php (EulerOS-SA-2019-1333)

EulerOS 2.0 SP3 : php (EulerOS-SA-2019-1593)

EulerOS 2.0 SP3 : php (EulerOS-SA-2019-2043)

EulerOS 2.0 SP3 : php (EulerOS-SA-2019-2649)

EulerOS 2.0 SP3 : pidgin (EulerOS-SA-2019-2650)

EulerOS 2.0 SP3 : pixman (EulerOS-SA-2020-1422)

EulerOS 2.0 SP3 : policycoreutils (EulerOS-SA-2020-1423)

EulerOS 2.0 SP3 : polkit (EulerOS-SA-2019-1101)

EulerOS 2.0 SP3 : polkit (EulerOS-SA-2019-2042)

EulerOS 2.0 SP3 : polkit (EulerOS-SA-2019-2651)

EulerOS 2.0 SP3 : polkit (EulerOS-SA-2020-1424)

EulerOS 2.0 SP3 : poppler (EulerOS-SA-2018-1226)

EulerOS 2.0 SP3 : poppler (EulerOS-SA-2018-1393)

EulerOS 2.0 SP3 : poppler (EulerOS-SA-2019-1102)

EulerOS 2.0 SP3 : poppler (EulerOS-SA-2019-1335)

EulerOS 2.0 SP3 : poppler (EulerOS-SA-2019-2015)

EulerOS 2.0 SP3 : poppler (EulerOS-SA-2019-2269)

EulerOS 2.0 SP3 : poppler (EulerOS-SA-2020-1425)

EulerOS 2.0 SP3 : postfix (EulerOS-SA-2018-1205)

EulerOS 2.0 SP3 : postgresql (EulerOS-SA-2018-1312)

EulerOS 2.0 SP3 : ppp (EulerOS-SA-2019-2652)

EulerOS 2.0 SP3 : ppp (EulerOS-SA-2020-1426)

EulerOS 2.0 SP3 : procps-ng (EulerOS-SA-2018-1199)

EulerOS 2.0 SP3 : procps-ng (EulerOS-SA-2018-1230)

EulerOS 2.0 SP3 : python (EulerOS-SA-2019-1337)

EulerOS 2.0 SP3 : python (EulerOS-SA-2019-1594)

EulerOS 2.0 SP3 : python (EulerOS-SA-2019-2019)

EulerOS 2.0 SP3 : python (EulerOS-SA-2019-2259)

EulerOS 2.0 SP3 : python (EulerOS-SA-2019-2653)

EulerOS 2.0 SP3 : python (EulerOS-SA-2020-1427)

EulerOS 2.0 SP3 : python-crypto (EulerOS-SA-2018-1168)

EulerOS 2.0 SP3 : python-jinja2 (EulerOS-SA-2019-2000)

EulerOS 2.0 SP3 : python-pillow (EulerOS-SA-2019-2654)

EulerOS 2.0 SP3 : python-reportlab (EulerOS-SA-2020-1428)

EulerOS 2.0 SP3 : python-requests (EulerOS-SA-2020-1429)

EulerOS 2.0 SP3 : python-urllib3 (EulerOS-SA-2019-2239)

EulerOS 2.0 SP3 : PyYAML (EulerOS-SA-2019-1040)

EulerOS 2.0 SP3 : qemu-kvm (EulerOS-SA-2018-1201)

EulerOS 2.0 SP3 : qemu-kvm (EulerOS-SA-2018-1314)

EulerOS 2.0 SP3 : qemu-kvm (EulerOS-SA-2019-1999)

EulerOS 2.0 SP3 : qemu-kvm (EulerOS-SA-2019-2255)

EulerOS 2.0 SP3 : qemu-kvm (EulerOS-SA-2020-1430)

EulerOS 2.0 SP3 : qpdf (EulerOS-SA-2019-2655)

EulerOS 2.0 SP3 : qt (EulerOS-SA-2019-1103)

EulerOS 2.0 SP3 : qt (EulerOS-SA-2019-2012)

EulerOS 2.0 SP3 : qt (EulerOS-SA-2019-2656)

EulerOS 2.0 SP3 : qt (EulerOS-SA-2020-1431)

EulerOS 2.0 SP3 : quagga (EulerOS-SA-2019-2657)

EulerOS 2.0 SP3 : rpm (EulerOS-SA-2019-1043)

EulerOS 2.0 SP3 : rpm (EulerOS-SA-2019-2658)

EulerOS 2.0 SP3 : rsyslog (EulerOS-SA-2019-1104)

EulerOS 2.0 SP3 : rsyslog (EulerOS-SA-2019-2659)

EulerOS 2.0 SP3 : ruby (EulerOS-SA-2018-1207)

EulerOS 2.0 SP3 : ruby (EulerOS-SA-2019-1340)

EulerOS 2.0 SP3 : ruby (EulerOS-SA-2019-2250)

EulerOS 2.0 SP3 : ruby (EulerOS-SA-2020-1432)

EulerOS 2.0 SP3 : samba (EulerOS-SA-2019-1342)

EulerOS 2.0 SP3 : samba (EulerOS-SA-2019-2018)

EulerOS 2.0 SP3 : sblim-sfcb (EulerOS-SA-2019-2660)

EulerOS 2.0 SP3 : screen (EulerOS-SA-2020-1433)

EulerOS 2.0 SP3 : SDL (EulerOS-SA-2019-1343)

EulerOS 2.0 SP3 : SDL (EulerOS-SA-2019-2045)

EulerOS 2.0 SP3 : SDL (EulerOS-SA-2019-2241)

EulerOS 2.0 SP3 : sendmail (EulerOS-SA-2019-2661)

EulerOS 2.0 SP3 : setup (EulerOS-SA-2018-1394)

EulerOS 2.0 SP3 : shadow-utils (EulerOS-SA-2018-1169)

EulerOS 2.0 SP3 : shadow-utils (EulerOS-SA-2019-2662)

EulerOS 2.0 SP3 : slf4j (EulerOS-SA-2018-1159)

EulerOS 2.0 SP3 : socat (EulerOS-SA-2019-2663)

EulerOS 2.0 SP3 : spice (EulerOS-SA-2018-1364)

EulerOS 2.0 SP3 : spice (EulerOS-SA-2019-1105)

EulerOS 2.0 SP3 : spice-gtk (EulerOS-SA-2018-1363)

EulerOS 2.0 SP3 : spice-gtk (EulerOS-SA-2019-2266)

EulerOS 2.0 SP3 : sqlite (EulerOS-SA-2018-1180)

EulerOS 2.0 SP3 : sqlite (EulerOS-SA-2019-1106)

EulerOS 2.0 SP3 : sqlite (EulerOS-SA-2019-2060)

EulerOS 2.0 SP3 : sqlite (EulerOS-SA-2019-2664)

EulerOS 2.0 SP3 : sqlite (EulerOS-SA-2020-1434)

EulerOS 2.0 SP3 : squashfs-tools (EulerOS-SA-2019-2665)

EulerOS 2.0 SP3 : squid (EulerOS-SA-2019-1044)

EulerOS 2.0 SP3 : squid (EulerOS-SA-2019-2053)

EulerOS 2.0 SP3 : squid (EulerOS-SA-2019-2666)

EulerOS 2.0 SP3 : sssd (EulerOS-SA-2018-1403)

EulerOS 2.0 SP3 : sssd (EulerOS-SA-2019-2052)

EulerOS 2.0 SP3 : sssd (EulerOS-SA-2019-2667)

EulerOS 2.0 SP3 : strongimcv (EulerOS-SA-2019-2668)

EulerOS 2.0 SP3 : subversion (EulerOS-SA-2019-2669)

EulerOS 2.0 SP3 : sudo (EulerOS-SA-2019-2670)

EulerOS 2.0 SP3 : sudo (EulerOS-SA-2020-1435)

EulerOS 2.0 SP3 : systemd (EulerOS-SA-2019-1107)

EulerOS 2.0 SP3 : systemd (EulerOS-SA-2019-1345)

EulerOS 2.0 SP3 : systemd (EulerOS-SA-2019-1599)

EulerOS 2.0 SP3 : systemd (EulerOS-SA-2019-1998)

EulerOS 2.0 SP3 : systemd (EulerOS-SA-2019-2671)

EulerOS 2.0 SP3 : systemd (EulerOS-SA-2020-1436)

EulerOS 2.0 SP3 : taglib (EulerOS-SA-2019-2672)

EulerOS 2.0 SP3 : tar (EulerOS-SA-2019-1346)

EulerOS 2.0 SP3 : tar (EulerOS-SA-2019-1601)

EulerOS 2.0 SP3 : tar (EulerOS-SA-2019-2673)

EulerOS 2.0 SP3 : tcpdump (EulerOS-SA-2019-2257)

EulerOS 2.0 SP3 : tcpdump (EulerOS-SA-2019-2674)

EulerOS 2.0 SP3 : tcpdump (EulerOS-SA-2020-1437)

EulerOS 2.0 SP3 : texlive (EulerOS-SA-2019-2062)

EulerOS 2.0 SP3 : tomcat (EulerOS-SA-2018-1227)

EulerOS 2.0 SP3 : tomcat (EulerOS-SA-2018-1385)

EulerOS 2.0 SP3 : tomcat (EulerOS-SA-2019-2047)

EulerOS 2.0 SP3 : tomcat (EulerOS-SA-2019-2675)

EulerOS 2.0 SP3 : tomcat (EulerOS-SA-2020-1438)

EulerOS 2.0 SP3 : unbound (EulerOS-SA-2019-2676)

EulerOS 2.0 SP3 : unixODBC (EulerOS-SA-2019-2267)

EulerOS 2.0 SP3 : unzip (EulerOS-SA-2018-1170)

EulerOS 2.0 SP3 : unzip (EulerOS-SA-2019-1603)

EulerOS 2.0 SP3 : unzip (EulerOS-SA-2019-2010)

EulerOS 2.0 SP3 : unzip (EulerOS-SA-2019-2677)

EulerOS 2.0 SP3 : unzip (EulerOS-SA-2020-1439)

EulerOS 2.0 SP3 : util-linux (EulerOS-SA-2019-2061)

EulerOS 2.0 SP3 : util-linux (EulerOS-SA-2019-2678)

EulerOS 2.0 SP3 : vim (EulerOS-SA-2018-1171)

EulerOS 2.0 SP3 : vim (EulerOS-SA-2019-1997)

EulerOS 2.0 SP3 : vim (EulerOS-SA-2019-2679)

EulerOS 2.0 SP3 : wavpack (EulerOS-SA-2019-2680)

EulerOS 2.0 SP3 : wget (EulerOS-SA-2018-1316)

EulerOS 2.0 SP3 : wget (EulerOS-SA-2019-1350)

EulerOS 2.0 SP3 : wget (EulerOS-SA-2019-2023)

EulerOS 2.0 SP3 : wget (EulerOS-SA-2019-2681)

EulerOS 2.0 SP3 : wpa\_supplicant (EulerOS-SA-2018-1318)

EulerOS 2.0 SP3 : wpa\_supplicant (EulerOS-SA-2019-2055)

EulerOS 2.0 SP3 : xdelta (EulerOS-SA-2019-2682)

EulerOS 2.0 SP3 : xdg-user-dirs (EulerOS-SA-2018-1181)

EulerOS 2.0 SP3 : xerces-c (EulerOS-SA-2018-1160)

EulerOS 2.0 SP3 : xerces-c (EulerOS-SA-2018-1395)

EulerOS 2.0 SP3 : xguest (EulerOS-SA-2020-1440)

EulerOS 2.0 SP3 : xorg-x11-server (EulerOS-SA-2019-2683)

EulerOS 2.0 SP3 : yum-utils (EulerOS-SA-2018-1320)

EulerOS 2.0 SP3 : zip (EulerOS-SA-2019-2059)

EulerOS 2.0 SP3 : zsh (EulerOS-SA-2018-1209)

EulerOS 2.0 SP3 : zsh (EulerOS-SA-2018-1396)

EulerOS 2.0 SP3 : zsh (EulerOS-SA-2019-2684)

EulerOS 2.0 SP3 : zsh (EulerOS-SA-2020-1441)

EulerOS 2.0 SP3 : zziplib (EulerOS-SA-2018-1397)

EulerOS 2.0 SP3 : zziplib (EulerOS-SA-2019-2685)

EulerOS 2.0 SP5 : 389-ds-base (EulerOS-SA-2019-1562)

EulerOS 2.0 SP5 : 389-ds-base (EulerOS-SA-2019-2127)

EulerOS 2.0 SP5 : accountsservice (EulerOS-SA-2019-2709)

EulerOS 2.0 SP5 : avahi (EulerOS-SA-2019-1958)

EulerOS 2.0 SP5 : bash (EulerOS-SA-2019-1565)

EulerOS 2.0 SP5 : bash (EulerOS-SA-2019-1911)

EulerOS 2.0 SP5 : bash (EulerOS-SA-2020-1303)

EulerOS 2.0 SP5 : bind (EulerOS-SA-2019-1664)

EulerOS 2.0 SP5 : bind (EulerOS-SA-2019-2128)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-1019)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-1132)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-1799)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-1887)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-1959)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-2129)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-2522)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2019-2686)

EulerOS 2.0 SP5 : binutils (EulerOS-SA-2020-1094)

EulerOS 2.0 SP5 : blktrace (EulerOS-SA-2020-1095)

EulerOS 2.0 SP5 : bzip2 (EulerOS-SA-2019-1020)

EulerOS 2.0 SP5 : bzip2 (EulerOS-SA-2019-1757)

EulerOS 2.0 SP5 : c-ares (EulerOS-SA-2019-1805)

EulerOS 2.0 SP5 : cairo (EulerOS-SA-2019-2130)

EulerOS 2.0 SP5 : cifs-utils (EulerOS-SA-2019-2131)

EulerOS 2.0 SP5 : cloud-init (EulerOS-SA-2019-2132)

EulerOS 2.0 SP5 : cloud-init (EulerOS-SA-2020-1304)

EulerOS 2.0 SP5 : compat-libtiff3 (EulerOS-SA-2019-2133)

EulerOS 2.0 SP5 : compat-poppler022 (EulerOS-SA-2019-1803)

EulerOS 2.0 SP5 : coreutils (EulerOS-SA-2019-2134)

EulerOS 2.0 SP5 : cpio (EulerOS-SA-2019-2687)

EulerOS 2.0 SP5 : cronie (EulerOS-SA-2019-1893)

EulerOS 2.0 SP5 : cups (EulerOS-SA-2019-1568)

EulerOS 2.0 SP5 : cups (EulerOS-SA-2019-2135)

EulerOS 2.0 SP5 : cups (EulerOS-SA-2020-1096)

EulerOS 2.0 SP5 : curl (EulerOS-SA-2019-1002)

EulerOS 2.0 SP5 : curl (EulerOS-SA-2019-1021)

EulerOS 2.0 SP5 : curl (EulerOS-SA-2019-1665)

EulerOS 2.0 SP5 : curl (EulerOS-SA-2019-1809)

EulerOS 2.0 SP5 : curl (EulerOS-SA-2019-2136)

EulerOS 2.0 SP5 : dbus (EulerOS-SA-2019-1673)

EulerOS 2.0 SP5 : dcraw (EulerOS-SA-2019-1879)

EulerOS 2.0 SP5 : dhcp (EulerOS-SA-2019-2137)

EulerOS 2.0 SP5 : dnsmasq (EulerOS-SA-2020-1097)

EulerOS 2.0 SP5 : docker-engine (EulerOS-SA-2019-1074)

EulerOS 2.0 SP5 : dom4j (EulerOS-SA-2019-1960)

EulerOS 2.0 SP5 : dosfstools (EulerOS-SA-2019-1961)

EulerOS 2.0 SP5 : dovecot (EulerOS-SA-2019-1280)

EulerOS 2.0 SP5 : dovecot (EulerOS-SA-2019-2138)

EulerOS 2.0 SP5 : dpdk (EulerOS-SA-2019-2688)

EulerOS 2.0 SP5 : dump (EulerOS-SA-2019-2139)

EulerOS 2.0 SP5 : e2fsprogs (EulerOS-SA-2019-2140)

EulerOS 2.0 SP5 : e2fsprogs (EulerOS-SA-2020-1098)

EulerOS 2.0 SP5 : ed (EulerOS-SA-2019-1962)

EulerOS 2.0 SP5 : elfutils (EulerOS-SA-2019-1133)

EulerOS 2.0 SP5 : elfutils (EulerOS-SA-2019-2141)

EulerOS 2.0 SP5 : elfutils (EulerOS-SA-2019-2523)

EulerOS 2.0 SP5 : elinks (EulerOS-SA-2019-2142)

EulerOS 2.0 SP5 : evince (EulerOS-SA-2019-1906)

EulerOS 2.0 SP5 : exempi (EulerOS-SA-2019-2143)

EulerOS 2.0 SP5 : exempi (EulerOS-SA-2019-2524)

EulerOS 2.0 SP5 : exiv2 (EulerOS-SA-2019-1804)

EulerOS 2.0 SP5 : exiv2 (EulerOS-SA-2019-1900)

EulerOS 2.0 SP5 : exiv2 (EulerOS-SA-2019-2144)

EulerOS 2.0 SP5 : exiv2 (EulerOS-SA-2019-2710)

EulerOS 2.0 SP5 : exiv2 (EulerOS-SA-2020-1099)

EulerOS 2.0 SP5 : expat (EulerOS-SA-2019-1666)

EulerOS 2.0 SP5 : expat (EulerOS-SA-2019-1758)

EulerOS 2.0 SP5 : expat (EulerOS-SA-2019-1896)

EulerOS 2.0 SP5 : expat (EulerOS-SA-2019-2145)

EulerOS 2.0 SP5 : fence-agents (EulerOS-SA-2019-1897)

EulerOS 2.0 SP5 : file (EulerOS-SA-2019-2525)

EulerOS 2.0 SP5 : flatpak (EulerOS-SA-2019-1134)

EulerOS 2.0 SP5 : flatpak (EulerOS-SA-2019-2146)

EulerOS 2.0 SP5 : flatpak (EulerOS-SA-2020-1305)

EulerOS 2.0 SP5 : flex (EulerOS-SA-2019-1963)

EulerOS 2.0 SP5 : foomatic (EulerOS-SA-2019-1964)

EulerOS 2.0 SP5 : freeradius (EulerOS-SA-2019-1574)

EulerOS 2.0 SP5 : freeradius (EulerOS-SA-2019-1674)

EulerOS 2.0 SP5 : freerdp (EulerOS-SA-2019-1285)

EulerOS 2.0 SP5 : freerdp (EulerOS-SA-2019-2147)

EulerOS 2.0 SP5 : freetype (EulerOS-SA-2019-2148)

EulerOS 2.0 SP5 : fuse (EulerOS-SA-2019-1003)

EulerOS 2.0 SP5 : fuse (EulerOS-SA-2019-1287)

EulerOS 2.0 SP5 : gc (EulerOS-SA-2019-2526)

EulerOS 2.0 SP5 : gd (EulerOS-SA-2019-1064)

EulerOS 2.0 SP5 : gd (EulerOS-SA-2019-2149)

EulerOS 2.0 SP5 : gd (EulerOS-SA-2019-2527)

EulerOS 2.0 SP5 : gdb (EulerOS-SA-2019-1965)

EulerOS 2.0 SP5 : gegl (EulerOS-SA-2019-2150)

EulerOS 2.0 SP5 : gettext (EulerOS-SA-2019-1966)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-1004)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-1023)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-1065)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-1290)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-1576)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-2151)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-2528)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2019-2689)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2020-1100)

EulerOS 2.0 SP5 : ghostscript (EulerOS-SA-2020-1306)

EulerOS 2.0 SP5 : giflib (EulerOS-SA-2019-2152)

EulerOS 2.0 SP5 : gimp (EulerOS-SA-2019-1675)

EulerOS 2.0 SP5 : git (EulerOS-SA-2019-1291)

EulerOS 2.0 SP5 : git (EulerOS-SA-2019-1917)

EulerOS 2.0 SP5 : git (EulerOS-SA-2019-2153)

EulerOS 2.0 SP5 : git (EulerOS-SA-2020-1101)

EulerOS 2.0 SP5 : glib2 (EulerOS-SA-2019-1894)

EulerOS 2.0 SP5 : glib2 (EulerOS-SA-2019-2154)

EulerOS 2.0 SP5 : glib2 (EulerOS-SA-2019-2690)

EulerOS 2.0 SP5 : glibc (EulerOS-SA-2019-1025)

EulerOS 2.0 SP5 : glibc (EulerOS-SA-2019-1135)

EulerOS 2.0 SP5 : glibc (EulerOS-SA-2019-1667)

EulerOS 2.0 SP5 : glibc (EulerOS-SA-2019-2155)

EulerOS 2.0 SP5 : glibc (EulerOS-SA-2020-1102)

EulerOS 2.0 SP5 : glusterfs (EulerOS-SA-2020-1103)

EulerOS 2.0 SP5 : gnupg2 (EulerOS-SA-2020-1104)

EulerOS 2.0 SP5 : gnutls (EulerOS-SA-2019-1005)

EulerOS 2.0 SP5 : gnutls (EulerOS-SA-2019-1136)

EulerOS 2.0 SP5 : gnutls (EulerOS-SA-2019-1676)

EulerOS 2.0 SP5 : golang (EulerOS-SA-2019-1916)

EulerOS 2.0 SP5 : golang (EulerOS-SA-2019-1967)

EulerOS 2.0 SP5 : golang (EulerOS-SA-2019-2529)

EulerOS 2.0 SP5 : gpgme (EulerOS-SA-2019-2125)

EulerOS 2.0 SP5 : graphviz (EulerOS-SA-2019-1677)

EulerOS 2.0 SP5 : gstreamer-plugins-base (EulerOS-SA-2019-1579)

EulerOS 2.0 SP5 : gstreamer1-plugins-base (EulerOS-SA-2019-1678)

EulerOS 2.0 SP5 : gvfs (EulerOS-SA-2019-1907)

EulerOS 2.0 SP5 : gvfs (EulerOS-SA-2019-1968)

EulerOS 2.0 SP5 : gvfs (EulerOS-SA-2019-2156)

EulerOS 2.0 SP5 : haproxy (EulerOS-SA-2020-1105)

EulerOS 2.0 SP5 : http-parser (EulerOS-SA-2019-2158)

EulerOS 2.0 SP5 : httpd (EulerOS-SA-2019-1137)

EulerOS 2.0 SP5 : httpd (EulerOS-SA-2019-1295)

EulerOS 2.0 SP5 : httpd (EulerOS-SA-2019-2157)

EulerOS 2.0 SP5 : httpd (EulerOS-SA-2019-2691)

EulerOS 2.0 SP5 : icedtea-web (EulerOS-SA-2019-1905)

EulerOS 2.0 SP5 : icu (EulerOS-SA-2019-1969)

EulerOS 2.0 SP5 : icu (EulerOS-SA-2019-2159)

EulerOS 2.0 SP5 : icu (EulerOS-SA-2020-1106)

EulerOS 2.0 SP5 : ImageMagick (EulerOS-SA-2019-1138)

EulerOS 2.0 SP5 : ImageMagick (EulerOS-SA-2019-1298)

EulerOS 2.0 SP5 : ImageMagick (EulerOS-SA-2019-1583)

EulerOS 2.0 SP5 : ImageMagick (EulerOS-SA-2019-1679)

EulerOS 2.0 SP5 : ImageMagick (EulerOS-SA-2019-1889)

EulerOS 2.0 SP5 : ImageMagick (EulerOS-SA-2019-1970)

EulerOS 2.0 SP5 : ImageMagick (EulerOS-SA-2019-2160)

EulerOS 2.0 SP5 : ipa (EulerOS-SA-2020-1107)

EulerOS 2.0 SP5 : ipmitool (EulerOS-SA-2020-1108)

EulerOS 2.0 SP5 : irssi (EulerOS-SA-2019-1066)

EulerOS 2.0 SP5 : irssi (EulerOS-SA-2019-1971)

EulerOS 2.0 SP5 : irssi (EulerOS-SA-2019-2161)

EulerOS 2.0 SP5 : jakarta-commons-httpclient (EulerOS-SA-2020-1109)

EulerOS 2.0 SP5 : jasper (EulerOS-SA-2019-2237)

EulerOS 2.0 SP5 : jasper (EulerOS-SA-2019-2530)

EulerOS 2.0 SP5 : java-1.7.0-openjdk (EulerOS-SA-2019-1139)

EulerOS 2.0 SP5 : java-1.7.0-openjdk (EulerOS-SA-2019-1584)

EulerOS 2.0 SP5 : java-1.7.0-openjdk (EulerOS-SA-2019-1759)

EulerOS 2.0 SP5 : java-1.7.0-openjdk (EulerOS-SA-2019-1903)

EulerOS 2.0 SP5 : java-1.7.0-openjdk (EulerOS-SA-2019-2200)

EulerOS 2.0 SP5 : java-1.7.0-openjdk (EulerOS-SA-2020-1110)

EulerOS 2.0 SP5 : java-1.8.0-openjdk (EulerOS-SA-2019-1140)

EulerOS 2.0 SP5 : java-1.8.0-openjdk (EulerOS-SA-2019-1301)

EulerOS 2.0 SP5 : java-1.8.0-openjdk (EulerOS-SA-2020-1111)

EulerOS 2.0 SP5 : java-1.8.0-openjdk (EulerOS-SA-2020-1307)

EulerOS 2.0 SP5 : keepalived (EulerOS-SA-2019-1680)

EulerOS 2.0 SP5 : keepalived (EulerOS-SA-2019-2692)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1028)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1076)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1156)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1304)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1588)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1671)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1692)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1813)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1919)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-1972)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-2201)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-2531)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2019-2693)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2020-1112)

EulerOS 2.0 SP5 : kernel (EulerOS-SA-2020-1308)

EulerOS 2.0 SP5 : krb5 (EulerOS-SA-2019-2162)

EulerOS 2.0 SP5 : krb5 (EulerOS-SA-2019-2532)

EulerOS 2.0 SP5 : lcms2 (EulerOS-SA-2019-2163)

EulerOS 2.0 SP5 : less (EulerOS-SA-2019-2164)

EulerOS 2.0 SP5 : lftp (EulerOS-SA-2019-2165)

EulerOS 2.0 SP5 : libarchive (EulerOS-SA-2019-1067)

EulerOS 2.0 SP5 : libarchive (EulerOS-SA-2019-1681)

EulerOS 2.0 SP5 : libarchive (EulerOS-SA-2019-1882)

EulerOS 2.0 SP5 : libarchive (EulerOS-SA-2019-1973)

EulerOS 2.0 SP5 : libarchive (EulerOS-SA-2019-2202)

EulerOS 2.0 SP5 : libarchive (EulerOS-SA-2019-2533)

EulerOS 2.0 SP5 : libcdio (EulerOS-SA-2019-1682)

EulerOS 2.0 SP5 : libcgroup (EulerOS-SA-2019-1918)

EulerOS 2.0 SP5 : libcroco (EulerOS-SA-2019-2203)

EulerOS 2.0 SP5 : libcroco (EulerOS-SA-2019-2694)

EulerOS 2.0 SP5 : libdb (EulerOS-SA-2019-1974)

EulerOS 2.0 SP5 : libdwarf (EulerOS-SA-2019-2204)

EulerOS 2.0 SP5 : libesmtp (EulerOS-SA-2020-1113)

EulerOS 2.0 SP5 : libexif (EulerOS-SA-2019-1141)

EulerOS 2.0 SP5 : libffi (EulerOS-SA-2019-1756)

EulerOS 2.0 SP5 : libgcrypt (EulerOS-SA-2019-2205)

EulerOS 2.0 SP5 : libgcrypt (EulerOS-SA-2019-2695)

EulerOS 2.0 SP5 : libgcrypt (EulerOS-SA-2020-1114)

EulerOS 2.0 SP5 : libgsf (EulerOS-SA-2019-2166)

EulerOS 2.0 SP5 : libguestfs-winsupport (EulerOS-SA-2019-2126)

EulerOS 2.0 SP5 : libgxps (EulerOS-SA-2019-1142)

EulerOS 2.0 SP5 : libgxps (EulerOS-SA-2019-2167)

EulerOS 2.0 SP5 : libical (EulerOS-SA-2019-1915)

EulerOS 2.0 SP5 : libidn (EulerOS-SA-2019-2206)

EulerOS 2.0 SP5 : libjpeg-turbo (EulerOS-SA-2019-1306)

EulerOS 2.0 SP5 : libjpeg-turbo (EulerOS-SA-2019-1892)

EulerOS 2.0 SP5 : libjpeg-turbo (EulerOS-SA-2020-1115)

EulerOS 2.0 SP5 : libmspack (EulerOS-SA-2019-1899)

EulerOS 2.0 SP5 : libmspack (EulerOS-SA-2019-2534)

EulerOS 2.0 SP5 : libmwaw (EulerOS-SA-2019-2535)

EulerOS 2.0 SP5 : libnl (EulerOS-SA-2019-2168)

EulerOS 2.0 SP5 : libosinfo (EulerOS-SA-2019-1888)

EulerOS 2.0 SP5 : libpcap (EulerOS-SA-2019-2712)

EulerOS 2.0 SP5 : libplist (EulerOS-SA-2019-2207)

EulerOS 2.0 SP5 : libpng (EulerOS-SA-2019-1810)

EulerOS 2.0 SP5 : libpng (EulerOS-SA-2019-1912)

EulerOS 2.0 SP5 : libpng (EulerOS-SA-2019-1975)

EulerOS 2.0 SP5 : librabbitmq (EulerOS-SA-2020-1116)

EulerOS 2.0 SP5 : libreoffice (EulerOS-SA-2019-1976)

EulerOS 2.0 SP5 : libreoffice (EulerOS-SA-2019-2169)

EulerOS 2.0 SP5 : libsamplerate (EulerOS-SA-2019-2170)

EulerOS 2.0 SP5 : libseccomp (EulerOS-SA-2019-1794)

EulerOS 2.0 SP5 : libsndfile (EulerOS-SA-2019-1030)

EulerOS 2.0 SP5 : libsndfile (EulerOS-SA-2019-2208)

EulerOS 2.0 SP5 : libsolv (EulerOS-SA-2019-1910)

EulerOS 2.0 SP5 : libsoup (EulerOS-SA-2019-1143)

EulerOS 2.0 SP5 : libsoup (EulerOS-SA-2020-1309)

EulerOS 2.0 SP5 : libsrtp (EulerOS-SA-2019-2706)

EulerOS 2.0 SP5 : libssh2 (EulerOS-SA-2019-1310)

EulerOS 2.0 SP5 : libssh2 (EulerOS-SA-2019-2536)

EulerOS 2.0 SP5 : libtasn1 (EulerOS-SA-2019-1006)

EulerOS 2.0 SP5 : libtasn1 (EulerOS-SA-2019-2171)

EulerOS 2.0 SP5 : libtiff (EulerOS-SA-2019-1313)

EulerOS 2.0 SP5 : libtiff (EulerOS-SA-2019-1683)

EulerOS 2.0 SP5 : libtiff (EulerOS-SA-2019-1807)

EulerOS 2.0 SP5 : libtiff (EulerOS-SA-2019-2209)

EulerOS 2.0 SP5 : libtiff (EulerOS-SA-2019-2707)

EulerOS 2.0 SP5 : libvirt (EulerOS-SA-2019-1144)

EulerOS 2.0 SP5 : libvirt (EulerOS-SA-2019-1684)

EulerOS 2.0 SP5 : libvirt (EulerOS-SA-2019-1796)

EulerOS 2.0 SP5 : libvirt (EulerOS-SA-2019-2210)

EulerOS 2.0 SP5 : libvncserver (EulerOS-SA-2019-1033)

EulerOS 2.0 SP5 : libvncserver (EulerOS-SA-2019-1068)

EulerOS 2.0 SP5 : libvorbis (EulerOS-SA-2019-1977)

EulerOS 2.0 SP5 : libwmf (EulerOS-SA-2019-2537)

EulerOS 2.0 SP5 : libwpd (EulerOS-SA-2019-2708)

EulerOS 2.0 SP5 : libx11 (EulerOS-SA-2019-1884)

EulerOS 2.0 SP5 : libX11 (EulerOS-SA-2019-2538)

EulerOS 2.0 SP5 : libXfont (EulerOS-SA-2019-2172)

EulerOS 2.0 SP5 : libXfont (EulerOS-SA-2019-2539)

EulerOS 2.0 SP5 : libxkbcommon (EulerOS-SA-2019-2540)

EulerOS 2.0 SP5 : libxkbcommon (EulerOS-SA-2019-2696)

EulerOS 2.0 SP5 : libxml2 (EulerOS-SA-2019-1007)

EulerOS 2.0 SP5 : libxml2 (EulerOS-SA-2019-1316)

EulerOS 2.0 SP5 : libxml2 (EulerOS-SA-2019-1685)

EulerOS 2.0 SP5 : libxml2 (EulerOS-SA-2019-1798)

EulerOS 2.0 SP5 : libxml2 (EulerOS-SA-2019-2211)

EulerOS 2.0 SP5 : libxml2 (EulerOS-SA-2020-1117)

EulerOS 2.0 SP5 : libxml2 (EulerOS-SA-2020-1310)

EulerOS 2.0 SP5 : libxslt (EulerOS-SA-2019-1318)

EulerOS 2.0 SP5 : libxslt (EulerOS-SA-2019-1913)

EulerOS 2.0 SP5 : libxslt (EulerOS-SA-2019-2212)

EulerOS 2.0 SP5 : libxslt (EulerOS-SA-2019-2541)

EulerOS 2.0 SP5 : libxslt (EulerOS-SA-2019-2697)

EulerOS 2.0 SP5 : lua (EulerOS-SA-2019-1978)

EulerOS 2.0 SP5 : lvm2 (EulerOS-SA-2020-1311)

EulerOS 2.0 SP5 : lz4 (EulerOS-SA-2019-2542)

EulerOS 2.0 SP5 : mariadb (EulerOS-SA-2019-2543)

EulerOS 2.0 SP5 : memcached (EulerOS-SA-2019-2213)

EulerOS 2.0 SP5 : mercurial (EulerOS-SA-2019-2214)

EulerOS 2.0 SP5 : mod\_auth\_mellon (EulerOS-SA-2019-1321)

EulerOS 2.0 SP5 : mod\_wsgi (EulerOS-SA-2019-2711)

EulerOS 2.0 SP5 : mutt (EulerOS-SA-2020-1312)

EulerOS 2.0 SP5 : ncurses (EulerOS-SA-2019-2544)

EulerOS 2.0 SP5 : ncurses (EulerOS-SA-2020-1118)

EulerOS 2.0 SP5 : net-snmp (EulerOS-SA-2019-1036)

EulerOS 2.0 SP5 : netpbm (EulerOS-SA-2019-2173)

EulerOS 2.0 SP5 : nettle (EulerOS-SA-2020-1313)

EulerOS 2.0 SP5 : NetworkManager (EulerOS-SA-2019-2698)

EulerOS 2.0 SP5 : nginx (EulerOS-SA-2020-1119)

EulerOS 2.0 SP5 : nss (EulerOS-SA-2019-2174)

EulerOS 2.0 SP5 : nss-softokn (EulerOS-SA-2019-1979)

EulerOS 2.0 SP5 : nss-softokn (EulerOS-SA-2019-2175)

EulerOS 2.0 SP5 : ntp (EulerOS-SA-2019-1014)

EulerOS 2.0 SP5 : ntp (EulerOS-SA-2019-1323)

EulerOS 2.0 SP5 : ntp (EulerOS-SA-2019-1878)

EulerOS 2.0 SP5 : ntp (EulerOS-SA-2019-2215)

EulerOS 2.0 SP5 : ntp (EulerOS-SA-2020-1314)

EulerOS 2.0 SP5 : numpy (EulerOS-SA-2020-1315)

EulerOS 2.0 SP5 : openjpeg (EulerOS-SA-2019-1909)

EulerOS 2.0 SP5 : openjpeg (EulerOS-SA-2019-2177)

EulerOS 2.0 SP5 : openldap (EulerOS-SA-2019-1914)

EulerOS 2.0 SP5 : openldap (EulerOS-SA-2019-2178)

EulerOS 2.0 SP5 : openslp (EulerOS-SA-2019-2176)

EulerOS 2.0 SP5 : openslp (EulerOS-SA-2020-1120)

EulerOS 2.0 SP5 : openssh (EulerOS-SA-2019-1008)

EulerOS 2.0 SP5 : openssh (EulerOS-SA-2019-1038)

EulerOS 2.0 SP5 : openssh (EulerOS-SA-2019-1324)

EulerOS 2.0 SP5 : openssh (EulerOS-SA-2019-1908)

EulerOS 2.0 SP5 : openssh (EulerOS-SA-2020-1316)

EulerOS 2.0 SP5 : openssl (EulerOS-SA-2019-1009)

EulerOS 2.0 SP5 : openssl (EulerOS-SA-2019-1145)

EulerOS 2.0 SP5 : openssl (EulerOS-SA-2019-1755)

EulerOS 2.0 SP5 : openssl (EulerOS-SA-2019-2216)

EulerOS 2.0 SP5 : openssl (EulerOS-SA-2019-2699)

EulerOS 2.0 SP5 : openssl098e (EulerOS-SA-2019-1980)

EulerOS 2.0 SP5 : openssl098e (EulerOS-SA-2019-2217)

EulerOS 2.0 SP5 : openssl098e (EulerOS-SA-2020-1121)

EulerOS 2.0 SP5 : openssl110h (EulerOS-SA-2019-1890)

EulerOS 2.0 SP5 : openssl110h (EulerOS-SA-2019-1981)

EulerOS 2.0 SP5 : openssl110h (EulerOS-SA-2019-2218)

EulerOS 2.0 SP5 : openwsman (EulerOS-SA-2019-1331)

EulerOS 2.0 SP5 : openwsman (EulerOS-SA-2019-2179)

EulerOS 2.0 SP5 : PackageKit (EulerOS-SA-2019-2700)

EulerOS 2.0 SP5 : patch (EulerOS-SA-2019-1801)

EulerOS 2.0 SP5 : patch (EulerOS-SA-2019-1982)

EulerOS 2.0 SP5 : patch (EulerOS-SA-2019-2219)

EulerOS 2.0 SP5 : patch (EulerOS-SA-2020-1317)

EulerOS 2.0 SP5 : pcre (EulerOS-SA-2019-1802)

EulerOS 2.0 SP5 : pcre (EulerOS-SA-2019-2180)

EulerOS 2.0 SP5 : pcre2 (EulerOS-SA-2019-1983)

EulerOS 2.0 SP5 : pcsc-lite (EulerOS-SA-2019-2545)

EulerOS 2.0 SP5 : perl (EulerOS-SA-2019-1039)

EulerOS 2.0 SP5 : perl (EulerOS-SA-2019-1800)

EulerOS 2.0 SP5 : perl (EulerOS-SA-2019-2220)

EulerOS 2.0 SP5 : perl (EulerOS-SA-2020-1122)

EulerOS 2.0 SP5 : perl (EulerOS-SA-2020-1318)

EulerOS 2.0 SP5 : perl-Archive-Tar (EulerOS-SA-2019-2181)

EulerOS 2.0 SP5 : perl-Data-Dumper (EulerOS-SA-2020-1123)

EulerOS 2.0 SP5 : perl-File-Path (EulerOS-SA-2019-2182)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-1069)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-1146)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-1334)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-1686)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-1795)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-1881)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-1984)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-2221)

EulerOS 2.0 SP5 : php (EulerOS-SA-2019-2546)

EulerOS 2.0 SP5 : php (EulerOS-SA-2020-1124)

EulerOS 2.0 SP5 : php-pear (EulerOS-SA-2019-1147)

EulerOS 2.0 SP5 : pidgin (EulerOS-SA-2019-1985)

EulerOS 2.0 SP5 : pidgin (EulerOS-SA-2019-2222)

EulerOS 2.0 SP5 : polkit (EulerOS-SA-2019-1070)

EulerOS 2.0 SP5 : polkit (EulerOS-SA-2019-2223)

EulerOS 2.0 SP5 : poppler (EulerOS-SA-2019-1010)

EulerOS 2.0 SP5 : poppler (EulerOS-SA-2019-1071)

EulerOS 2.0 SP5 : poppler (EulerOS-SA-2019-1148)

EulerOS 2.0 SP5 : poppler (EulerOS-SA-2019-1898)

EulerOS 2.0 SP5 : poppler (EulerOS-SA-2019-1986)

EulerOS 2.0 SP5 : poppler (EulerOS-SA-2019-2224)

EulerOS 2.0 SP5 : poppler (EulerOS-SA-2020-1125)

EulerOS 2.0 SP5 : ppp (EulerOS-SA-2019-1987)

EulerOS 2.0 SP5 : ppp (EulerOS-SA-2019-2183)

EulerOS 2.0 SP5 : ppp (EulerOS-SA-2020-1319)

EulerOS 2.0 SP5 : pyOpenSSL (EulerOS-SA-2020-1320)

EulerOS 2.0 SP5 : python (EulerOS-SA-2019-1072)

EulerOS 2.0 SP5 : python (EulerOS-SA-2019-1149)

EulerOS 2.0 SP5 : python (EulerOS-SA-2019-1338)

EulerOS 2.0 SP5 : python (EulerOS-SA-2019-1797)

EulerOS 2.0 SP5 : python (EulerOS-SA-2019-2225)

EulerOS 2.0 SP5 : python (EulerOS-SA-2020-1126)

EulerOS 2.0 SP5 : python (EulerOS-SA-2020-1321)

EulerOS 2.0 SP5 : python-jinja2 (EulerOS-SA-2019-1595)

EulerOS 2.0 SP5 : python-jinja2 (EulerOS-SA-2020-1127)

EulerOS 2.0 SP5 : python-paramiko (EulerOS-SA-2019-1339)

EulerOS 2.0 SP5 : python-pillow (EulerOS-SA-2019-1687)

EulerOS 2.0 SP5 : python-pillow (EulerOS-SA-2019-2226)

EulerOS 2.0 SP5 : python-pillow (EulerOS-SA-2019-2701)

EulerOS 2.0 SP5 : python-pillow (EulerOS-SA-2020-1128)

EulerOS 2.0 SP5 : python-pillow (EulerOS-SA-2020-1322)

EulerOS 2.0 SP5 : python-reportlab (EulerOS-SA-2020-1129)

EulerOS 2.0 SP5 : python-requests (EulerOS-SA-2019-1886)

EulerOS 2.0 SP5 : python-urllib3 (EulerOS-SA-2019-1596)

EulerOS 2.0 SP5 : python-urllib3 (EulerOS-SA-2019-1877)

EulerOS 2.0 SP5 : python-urllib3 (EulerOS-SA-2019-2184)

EulerOS 2.0 SP5 : PyYAML (EulerOS-SA-2019-1041)

EulerOS 2.0 SP5 : qemu-kvm (EulerOS-SA-2019-1811)

EulerOS 2.0 SP5 : qemu-kvm (EulerOS-SA-2019-1988)

EulerOS 2.0 SP5 : qemu-kvm (EulerOS-SA-2019-2227)

EulerOS 2.0 SP5 : qpdf (EulerOS-SA-2019-2185)

EulerOS 2.0 SP5 : qt (EulerOS-SA-2019-1042)

EulerOS 2.0 SP5 : qt (EulerOS-SA-2019-1688)

EulerOS 2.0 SP5 : qt (EulerOS-SA-2019-1904)

EulerOS 2.0 SP5 : qt (EulerOS-SA-2019-2186)

EulerOS 2.0 SP5 : qt (EulerOS-SA-2020-1323)

EulerOS 2.0 SP5 : quagga (EulerOS-SA-2019-2228)

EulerOS 2.0 SP5 : rpm (EulerOS-SA-2019-1011)

EulerOS 2.0 SP5 : rsync (EulerOS-SA-2019-1806)

EulerOS 2.0 SP5 : rsync (EulerOS-SA-2019-1989)

EulerOS 2.0 SP5 : rsyslog (EulerOS-SA-2019-1073)

EulerOS 2.0 SP5 : rsyslog (EulerOS-SA-2019-2229)

EulerOS 2.0 SP5 : ruby (EulerOS-SA-2019-1341)

EulerOS 2.0 SP5 : ruby (EulerOS-SA-2019-1597)

EulerOS 2.0 SP5 : ruby (EulerOS-SA-2019-1895)

EulerOS 2.0 SP5 : ruby (EulerOS-SA-2019-1990)

EulerOS 2.0 SP5 : ruby (EulerOS-SA-2019-2230)

EulerOS 2.0 SP5 : ruby (EulerOS-SA-2020-1130)

EulerOS 2.0 SP5 : ruby (EulerOS-SA-2020-1324)

EulerOS 2.0 SP5 : samba (EulerOS-SA-2019-1150)

EulerOS 2.0 SP5 : samba (EulerOS-SA-2019-1598)

EulerOS 2.0 SP5 : samba (EulerOS-SA-2019-1689)

EulerOS 2.0 SP5 : samba (EulerOS-SA-2019-1902)

EulerOS 2.0 SP5 : samba (EulerOS-SA-2019-2547)

EulerOS 2.0 SP5 : samba (EulerOS-SA-2020-1131)

EulerOS 2.0 SP5 : samba (EulerOS-SA-2020-1325)

EulerOS 2.0 SP5 : screen (EulerOS-SA-2019-2548)

EulerOS 2.0 SP5 : SDL (EulerOS-SA-2019-1151)

EulerOS 2.0 SP5 : SDL (EulerOS-SA-2019-1883)

EulerOS 2.0 SP5 : SDL (EulerOS-SA-2019-2187)

EulerOS 2.0 SP5 : sendmail (EulerOS-SA-2019-2549)

EulerOS 2.0 SP5 : shadow-utils (EulerOS-SA-2019-2188)

EulerOS 2.0 SP5 : spice (EulerOS-SA-2019-1012)

EulerOS 2.0 SP5 : spice (EulerOS-SA-2019-1075)

EulerOS 2.0 SP5 : spice-gtk (EulerOS-SA-2019-1013)

EulerOS 2.0 SP5 : spice-gtk (EulerOS-SA-2019-2189)

EulerOS 2.0 SP5 : sqlite (EulerOS-SA-2019-1152)

EulerOS 2.0 SP5 : sqlite (EulerOS-SA-2019-1668)

EulerOS 2.0 SP5 : sqlite (EulerOS-SA-2019-1991)

EulerOS 2.0 SP5 : sqlite (EulerOS-SA-2020-1132)

EulerOS 2.0 SP5 : squid (EulerOS-SA-2019-2231)

EulerOS 2.0 SP5 : squid (EulerOS-SA-2020-1133)

EulerOS 2.0 SP5 : squid (EulerOS-SA-2020-1326)

EulerOS 2.0 SP5 : sssd (EulerOS-SA-2019-1669)

EulerOS 2.0 SP5 : sssd (EulerOS-SA-2019-2190)

EulerOS 2.0 SP5 : strongimcv (EulerOS-SA-2019-2702)

EulerOS 2.0 SP5 : strongimcv (EulerOS-SA-2020-1134)

EulerOS 2.0 SP5 : subversion (EulerOS-SA-2019-2550)

EulerOS 2.0 SP5 : sudo (EulerOS-SA-2019-2191)

EulerOS 2.0 SP5 : sudo (EulerOS-SA-2020-1135)

EulerOS 2.0 SP5 : systemd (EulerOS-SA-2019-1045)

EulerOS 2.0 SP5 : systemd (EulerOS-SA-2019-1153)

EulerOS 2.0 SP5 : systemd (EulerOS-SA-2019-1808)

EulerOS 2.0 SP5 : systemd (EulerOS-SA-2019-2232)

EulerOS 2.0 SP5 : tar (EulerOS-SA-2019-1154)

EulerOS 2.0 SP5 : tar (EulerOS-SA-2019-1347)

EulerOS 2.0 SP5 : tar (EulerOS-SA-2019-2192)

EulerOS 2.0 SP5 : tcpdump (EulerOS-SA-2019-2233)

EulerOS 2.0 SP5 : tcpdump (EulerOS-SA-2019-2551)

EulerOS 2.0 SP5 : tcpdump (EulerOS-SA-2019-2703)

EulerOS 2.0 SP5 : tomcat (EulerOS-SA-2019-1602)

EulerOS 2.0 SP5 : tomcat (EulerOS-SA-2019-1885)

EulerOS 2.0 SP5 : tomcat (EulerOS-SA-2019-1992)

EulerOS 2.0 SP5 : tomcat (EulerOS-SA-2020-1136)

EulerOS 2.0 SP5 : tomcat (EulerOS-SA-2020-1327)

EulerOS 2.0 SP5 : udisks2 (EulerOS-SA-2019-2193)

EulerOS 2.0 SP5 : unbound (EulerOS-SA-2019-2194)

EulerOS 2.0 SP5 : unixODBC (EulerOS-SA-2019-1993)

EulerOS 2.0 SP5 : unzip (EulerOS-SA-2019-1349)

EulerOS 2.0 SP5 : unzip (EulerOS-SA-2019-1880)

EulerOS 2.0 SP5 : unzip (EulerOS-SA-2019-2234)

EulerOS 2.0 SP5 : unzip (EulerOS-SA-2020-1137)

EulerOS 2.0 SP5 : util-linux (EulerOS-SA-2019-1670)

EulerOS 2.0 SP5 : util-linux (EulerOS-SA-2019-1994)

EulerOS 2.0 SP5 : vim (EulerOS-SA-2019-1690)

EulerOS 2.0 SP5 : vim (EulerOS-SA-2020-1138)

EulerOS 2.0 SP5 : wavpack (EulerOS-SA-2019-1901)

EulerOS 2.0 SP5 : wavpack (EulerOS-SA-2019-2195)

EulerOS 2.0 SP5 : webkitgtk3 (EulerOS-SA-2019-2196)

EulerOS 2.0 SP5 : webkitgtk4 (EulerOS-SA-2019-2197)

EulerOS 2.0 SP5 : webkitgtk4 (EulerOS-SA-2020-1328)

EulerOS 2.0 SP5 : wget (EulerOS-SA-2019-1155)

EulerOS 2.0 SP5 : wget (EulerOS-SA-2019-1691)

EulerOS 2.0 SP5 : wget (EulerOS-SA-2019-2198)

EulerOS 2.0 SP5 : wireshark (EulerOS-SA-2020-1139)

EulerOS 2.0 SP5 : wpa\_supplicant (EulerOS-SA-2019-1891)

EulerOS 2.0 SP5 : xdelta (EulerOS-SA-2019-2552)

EulerOS 2.0 SP5 : xerces-c (EulerOS-SA-2019-2199)

EulerOS 2.0 SP5 : xorg-x11-server (EulerOS-SA-2019-2553)

EulerOS 2.0 SP5 : zip (EulerOS-SA-2019-1812)

EulerOS 2.0 SP5 : zlib (EulerOS-SA-2019-2704)

EulerOS 2.0 SP5 : zsh (EulerOS-SA-2019-2235)

EulerOS 2.0 SP5 : zsh (EulerOS-SA-2019-2705)

EulerOS 2.0 SP5 : zsh (EulerOS-SA-2020-1329)

EulerOS 2.0 SP5 : zziplib (EulerOS-SA-2019-2236)

EulerOS 2.0 SP8 : avahi (EulerOS-SA-2019-1640)

EulerOS 2.0 SP8 : bash (EulerOS-SA-2020-1140)

EulerOS 2.0 SP8 : bind (EulerOS-SA-2019-1641)

EulerOS 2.0 SP8 : bind (EulerOS-SA-2019-1822)

EulerOS 2.0 SP8 : bind (EulerOS-SA-2019-2096)

EulerOS 2.0 SP8 : bind (EulerOS-SA-2019-2275)

EulerOS 2.0 SP8 : bind (EulerOS-SA-2020-1141)

EulerOS 2.0 SP8 : binutils (EulerOS-SA-2019-1642)

EulerOS 2.0 SP8 : binutils (EulerOS-SA-2019-1790)

EulerOS 2.0 SP8 : binutils (EulerOS-SA-2019-2069)

EulerOS 2.0 SP8 : binutils (EulerOS-SA-2019-2099)

EulerOS 2.0 SP8 : binutils (EulerOS-SA-2019-2276)

EulerOS 2.0 SP8 : binutils (EulerOS-SA-2020-1001)

EulerOS 2.0 SP8 : binutils (EulerOS-SA-2020-1142)

EulerOS 2.0 SP8 : bubblewrap (EulerOS-SA-2019-1762)

EulerOS 2.0 SP8 : bzip2 (EulerOS-SA-2019-1782)

EulerOS 2.0 SP8 : ceph (EulerOS-SA-2019-1791)

EulerOS 2.0 SP8 : ceph (EulerOS-SA-2020-1285)

EulerOS 2.0 SP8 : cloud-init (EulerOS-SA-2020-1286)

EulerOS 2.0 SP8 : cockpit (EulerOS-SA-2020-1143)

EulerOS 2.0 SP8 : compat-openssl10 (EulerOS-SA-2019-1643)

EulerOS 2.0 SP8 : compat-openssl10 (EulerOS-SA-2019-1828)

EulerOS 2.0 SP8 : compat-openssl10 (EulerOS-SA-2019-2098)

EulerOS 2.0 SP8 : cpio (EulerOS-SA-2020-1002)

EulerOS 2.0 SP8 : cronie (EulerOS-SA-2019-2100)

EulerOS 2.0 SP8 : cups (EulerOS-SA-2019-2070)

EulerOS 2.0 SP8 : curl (EulerOS-SA-2019-1786)

EulerOS 2.0 SP8 : curl (EulerOS-SA-2019-2101)

EulerOS 2.0 SP8 : curl (EulerOS-SA-2020-1144)

EulerOS 2.0 SP8 : cyrus-sasl (EulerOS-SA-2020-1145)

EulerOS 2.0 SP8 : dbus (EulerOS-SA-2019-1767)

EulerOS 2.0 SP8 : dcraw (EulerOS-SA-2019-1817)

EulerOS 2.0 SP8 : dhcp (EulerOS-SA-2019-1826)

EulerOS 2.0 SP8 : docker-engine (EulerOS-SA-2020-1283)

EulerOS 2.0 SP8 : dovecot (EulerOS-SA-2019-1644)

EulerOS 2.0 SP8 : dovecot (EulerOS-SA-2019-2071)

EulerOS 2.0 SP8 : dovecot (EulerOS-SA-2020-1146)

EulerOS 2.0 SP8 : dpdk (EulerOS-SA-2020-1039)

EulerOS 2.0 SP8 : e2fsprogs (EulerOS-SA-2020-1287)

EulerOS 2.0 SP8 : elfutils (EulerOS-SA-2019-2102)

EulerOS 2.0 SP8 : exempi (EulerOS-SA-2019-1645)

EulerOS 2.0 SP8 : exiv2 (EulerOS-SA-2019-1784)

EulerOS 2.0 SP8 : exiv2 (EulerOS-SA-2019-1830)

EulerOS 2.0 SP8 : exiv2 (EulerOS-SA-2019-2072)

EulerOS 2.0 SP8 : exiv2 (EulerOS-SA-2019-2277)

EulerOS 2.0 SP8 : exiv2 (EulerOS-SA-2020-1003)

EulerOS 2.0 SP8 : exiv2 (EulerOS-SA-2020-1147)

EulerOS 2.0 SP8 : expat (EulerOS-SA-2019-1783)

EulerOS 2.0 SP8 : expat (EulerOS-SA-2019-2103)

EulerOS 2.0 SP8 : file (EulerOS-SA-2019-2278)

EulerOS 2.0 SP8 : flatpak (EulerOS-SA-2020-1004)

EulerOS 2.0 SP8 : freeradius (EulerOS-SA-2019-1763)

EulerOS 2.0 SP8 : freeradius (EulerOS-SA-2020-1005)

EulerOS 2.0 SP8 : freerdp (EulerOS-SA-2019-1646)

EulerOS 2.0 SP8 : freetype (EulerOS-SA-2020-1148)

EulerOS 2.0 SP8 : fribidi (EulerOS-SA-2020-1149)

EulerOS 2.0 SP8 : gcc (EulerOS-SA-2019-1825)

EulerOS 2.0 SP8 : gcc (EulerOS-SA-2019-2073)

EulerOS 2.0 SP8 : gd (EulerOS-SA-2019-1647)

EulerOS 2.0 SP8 : gd (EulerOS-SA-2019-2074)

EulerOS 2.0 SP8 : gdb (EulerOS-SA-2019-2279)

EulerOS 2.0 SP8 : gettext (EulerOS-SA-2019-2075)

EulerOS 2.0 SP8 : ghostscript (EulerOS-SA-2019-1823)

EulerOS 2.0 SP8 : ghostscript (EulerOS-SA-2019-2076)

EulerOS 2.0 SP8 : ghostscript (EulerOS-SA-2020-1006)

EulerOS 2.0 SP8 : ghostscript (EulerOS-SA-2020-1150)

EulerOS 2.0 SP8 : giflib (EulerOS-SA-2019-2104)

EulerOS 2.0 SP8 : giflib (EulerOS-SA-2019-2280)

EulerOS 2.0 SP8 : gimp (EulerOS-SA-2019-1761)

EulerOS 2.0 SP8 : git (EulerOS-SA-2020-1151)

EulerOS 2.0 SP8 : glib2 (EulerOS-SA-2019-2077)

EulerOS 2.0 SP8 : glibc (EulerOS-SA-2019-1648)

EulerOS 2.0 SP8 : glibc (EulerOS-SA-2019-2307)

EulerOS 2.0 SP8 : glibc (EulerOS-SA-2020-1007)

EulerOS 2.0 SP8 : glibc (EulerOS-SA-2020-1152)

EulerOS 2.0 SP8 : glibc (EulerOS-SA-2020-1288)

EulerOS 2.0 SP8 : gnupg2 (EulerOS-SA-2020-1153)

EulerOS 2.0 SP8 : gnutls (EulerOS-SA-2019-1649)

EulerOS 2.0 SP8 : golang (EulerOS-SA-2019-2078)

EulerOS 2.0 SP8 : golang (EulerOS-SA-2020-1008)

EulerOS 2.0 SP8 : gperftools (EulerOS-SA-2020-1154)

EulerOS 2.0 SP8 : graphviz (EulerOS-SA-2019-1760)

EulerOS 2.0 SP8 : grub2 (EulerOS-SA-2020-1009)

EulerOS 2.0 SP8 : gvfs (EulerOS-SA-2019-1768)

EulerOS 2.0 SP8 : gvfs (EulerOS-SA-2019-2079)

EulerOS 2.0 SP8 : haproxy (EulerOS-SA-2019-1650)

EulerOS 2.0 SP8 : httpd (EulerOS-SA-2019-1835)

EulerOS 2.0 SP8 : httpd (EulerOS-SA-2019-2080)

EulerOS 2.0 SP8 : httpd (EulerOS-SA-2020-1155)

EulerOS 2.0 SP8 : httpd (EulerOS-SA-2020-1289)

EulerOS 2.0 SP8 : ImageMagick (EulerOS-SA-2019-1651)

EulerOS 2.0 SP8 : ImageMagick (EulerOS-SA-2019-1764)

EulerOS 2.0 SP8 : ImageMagick (EulerOS-SA-2019-1820)

EulerOS 2.0 SP8 : ImageMagick (EulerOS-SA-2019-2281)

EulerOS 2.0 SP8 : ImageMagick (EulerOS-SA-2020-1010)

EulerOS 2.0 SP8 : ipmitool (EulerOS-SA-2020-1156)

EulerOS 2.0 SP8 : iSulad-kit (EulerOS-SA-2020-1290)

EulerOS 2.0 SP8 : jasper (EulerOS-SA-2019-2282)

EulerOS 2.0 SP8 : jasper (EulerOS-SA-2020-1011)

EulerOS 2.0 SP8 : java-1.8.0-openjdk (EulerOS-SA-2019-1777)

EulerOS 2.0 SP8 : java-1.8.0-openjdk (EulerOS-SA-2019-2105)

EulerOS 2.0 SP8 : keepalived (EulerOS-SA-2019-1770)

EulerOS 2.0 SP8 : keepalived (EulerOS-SA-2020-1157)

EulerOS 2.0 SP8 : keepalived (EulerOS-SA-2020-1291)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2019-1792)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2019-2081)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2019-2106)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2019-2283)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2020-1012)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2020-1158)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2020-1186)

EulerOS 2.0 SP8 : kernel (EulerOS-SA-2020-1292)

EulerOS 2.0 SP8 : libarchive (EulerOS-SA-2020-1013)

EulerOS 2.0 SP8 : libarchive (EulerOS-SA-2020-1159)

EulerOS 2.0 SP8 : libcomps (EulerOS-SA-2020-1293)

EulerOS 2.0 SP8 : libcroco (EulerOS-SA-2019-2284)

EulerOS 2.0 SP8 : libesmtp (EulerOS-SA-2020-1160)

EulerOS 2.0 SP8 : libexif (EulerOS-SA-2019-1781)

EulerOS 2.0 SP8 : libgcrypt (EulerOS-SA-2019-2107)

EulerOS 2.0 SP8 : libidn2 (EulerOS-SA-2020-1161)

EulerOS 2.0 SP8 : libmspack (EulerOS-SA-2019-1829)

EulerOS 2.0 SP8 : libmspack (EulerOS-SA-2019-2285)

EulerOS 2.0 SP8 : libmspack (EulerOS-SA-2020-1014)

EulerOS 2.0 SP8 : libosinfo (EulerOS-SA-2019-1821)

EulerOS 2.0 SP8 : libpcap (EulerOS-SA-2019-2286)

EulerOS 2.0 SP8 : libpng (EulerOS-SA-2019-1787)

EulerOS 2.0 SP8 : libpng (EulerOS-SA-2020-1015)

EulerOS 2.0 SP8 : libpng (EulerOS-SA-2020-1162)

EulerOS 2.0 SP8 : librabbitmq (EulerOS-SA-2020-1163)

EulerOS 2.0 SP8 : libreoffice (EulerOS-SA-2019-2082)

EulerOS 2.0 SP8 : libsndfile (EulerOS-SA-2020-1016)

EulerOS 2.0 SP8 : libsolv (EulerOS-SA-2019-1652)

EulerOS 2.0 SP8 : libssh (EulerOS-SA-2020-1164)

EulerOS 2.0 SP8 : libssh2 (EulerOS-SA-2019-2287)

EulerOS 2.0 SP8 : libtiff (EulerOS-SA-2019-1785)

EulerOS 2.0 SP8 : libtiff (EulerOS-SA-2019-1834)

EulerOS 2.0 SP8 : libtiff (EulerOS-SA-2019-2108)

EulerOS 2.0 SP8 : libtiff (EulerOS-SA-2019-2288)

EulerOS 2.0 SP8 : libvirt (EulerOS-SA-2019-1653)

EulerOS 2.0 SP8 : libvirt (EulerOS-SA-2019-1774)

EulerOS 2.0 SP8 : libvirt (EulerOS-SA-2019-2289)

EulerOS 2.0 SP8 : libvpx (EulerOS-SA-2020-1185)

EulerOS 2.0 SP8 : libwpd (EulerOS-SA-2019-2109)

EulerOS 2.0 SP8 : libxml2 (EulerOS-SA-2020-1165)

EulerOS 2.0 SP8 : libxslt (EulerOS-SA-2019-2290)

EulerOS 2.0 SP8 : libxslt (EulerOS-SA-2020-1017)

EulerOS 2.0 SP8 : libxslt (EulerOS-SA-2020-1166)

EulerOS 2.0 SP8 : lua (EulerOS-SA-2019-1776)

EulerOS 2.0 SP8 : lz4 (EulerOS-SA-2019-2291)

EulerOS 2.0 SP8 : ncurses (EulerOS-SA-2019-2292)

EulerOS 2.0 SP8 : nghttp2 (EulerOS-SA-2019-2083)

EulerOS 2.0 SP8 : nginx (EulerOS-SA-2019-2084)

EulerOS 2.0 SP8 : nginx (EulerOS-SA-2020-1167)

EulerOS 2.0 SP8 : nmap (EulerOS-SA-2019-2085)

EulerOS 2.0 SP8 : nmap (EulerOS-SA-2020-1018)

EulerOS 2.0 SP8 : ntp (EulerOS-SA-2019-1769)

EulerOS 2.0 SP8 : oniguruma (EulerOS-SA-2019-2086)

EulerOS 2.0 SP8 : oniguruma (EulerOS-SA-2020-1019)

EulerOS 2.0 SP8 : openjpeg (EulerOS-SA-2019-2110)

EulerOS 2.0 SP8 : openjpeg2 (EulerOS-SA-2019-1775)

EulerOS 2.0 SP8 : openjpeg2 (EulerOS-SA-2019-2111)

EulerOS 2.0 SP8 : openjpeg2 (EulerOS-SA-2020-1020)

EulerOS 2.0 SP8 : openjpeg2 (EulerOS-SA-2020-1168)

EulerOS 2.0 SP8 : openldap (EulerOS-SA-2019-2087)

EulerOS 2.0 SP8 : openldap (EulerOS-SA-2019-2112)

EulerOS 2.0 SP8 : openldap (EulerOS-SA-2020-1169)

EulerOS 2.0 SP8 : opensc (EulerOS-SA-2019-2293)

EulerOS 2.0 SP8 : openslp (EulerOS-SA-2020-1038)

EulerOS 2.0 SP8 : openssh (EulerOS-SA-2019-2113)

EulerOS 2.0 SP8 : openssh (EulerOS-SA-2019-2294)

EulerOS 2.0 SP8 : openssh (EulerOS-SA-2020-1170)

EulerOS 2.0 SP8 : openssl (EulerOS-SA-2019-1654)

EulerOS 2.0 SP8 : openssl (EulerOS-SA-2019-2097)

EulerOS 2.0 SP8 : openssl (EulerOS-SA-2020-1021)

EulerOS 2.0 SP8 : pango (EulerOS-SA-2019-2088)

EulerOS 2.0 SP8 : patch (EulerOS-SA-2020-1022)

EulerOS 2.0 SP8 : patch (EulerOS-SA-2020-1171)

EulerOS 2.0 SP8 : php (EulerOS-SA-2019-1655)

EulerOS 2.0 SP8 : php (EulerOS-SA-2019-2089)

EulerOS 2.0 SP8 : php (EulerOS-SA-2019-2295)

EulerOS 2.0 SP8 : php (EulerOS-SA-2020-1023)

EulerOS 2.0 SP8 : php (EulerOS-SA-2020-1172)

EulerOS 2.0 SP8 : polkit (EulerOS-SA-2019-1656)

EulerOS 2.0 SP8 : poppler (EulerOS-SA-2019-1827)

EulerOS 2.0 SP8 : poppler (EulerOS-SA-2019-2296)

EulerOS 2.0 SP8 : poppler (EulerOS-SA-2020-1173)

EulerOS 2.0 SP8 : postgresql (EulerOS-SA-2019-1824)

EulerOS 2.0 SP8 : postgresql (EulerOS-SA-2019-2090)

EulerOS 2.0 SP8 : postgresql (EulerOS-SA-2019-2297)

EulerOS 2.0 SP8 : ppp (EulerOS-SA-2019-2298)

EulerOS 2.0 SP8 : ppp (EulerOS-SA-2020-1294)

EulerOS 2.0 SP8 : python-jinja2 (EulerOS-SA-2019-1816)

EulerOS 2.0 SP8 : python-pillow (EulerOS-SA-2020-1026)

EulerOS 2.0 SP8 : python-pip (EulerOS-SA-2020-1176)

EulerOS 2.0 SP8 : python-requests (EulerOS-SA-2020-1027)

EulerOS 2.0 SP8 : python-urllib3 (EulerOS-SA-2020-1028)

EulerOS 2.0 SP8 : python-urllib3 (EulerOS-SA-2020-1177)

EulerOS 2.0 SP8 : python2 (EulerOS-SA-2019-1657)

EulerOS 2.0 SP8 : python2 (EulerOS-SA-2019-1771)

EulerOS 2.0 SP8 : python2 (EulerOS-SA-2019-2114)

EulerOS 2.0 SP8 : python2 (EulerOS-SA-2020-1024)

EulerOS 2.0 SP8 : python2 (EulerOS-SA-2020-1174)

EulerOS 2.0 SP8 : python2 (EulerOS-SA-2020-1295)

EulerOS 2.0 SP8 : python3 (EulerOS-SA-2019-1658)

EulerOS 2.0 SP8 : python3 (EulerOS-SA-2019-1778)

EulerOS 2.0 SP8 : python3 (EulerOS-SA-2019-2091)

EulerOS 2.0 SP8 : python3 (EulerOS-SA-2019-2115)

EulerOS 2.0 SP8 : python3 (EulerOS-SA-2020-1025)

EulerOS 2.0 SP8 : python3 (EulerOS-SA-2020-1175)

EulerOS 2.0 SP8 : python3 (EulerOS-SA-2020-1296)

EulerOS 2.0 SP8 : PyYAML (EulerOS-SA-2019-2299)

EulerOS 2.0 SP8 : PyYAML (EulerOS-SA-2020-1297)

EulerOS 2.0 SP8 : qemu (EulerOS-SA-2019-2300)

EulerOS 2.0 SP8 : qemu (EulerOS-SA-2020-1029)

EulerOS 2.0 SP8 : qemu (EulerOS-SA-2020-1298)

EulerOS 2.0 SP8 : qemu-kvm (EulerOS-SA-2019-1815)

EulerOS 2.0 SP8 : qpdf (EulerOS-SA-2020-1030)

EulerOS 2.0 SP8 : qt (EulerOS-SA-2019-1833)

EulerOS 2.0 SP8 : qt (EulerOS-SA-2019-2301)

EulerOS 2.0 SP8 : qt (EulerOS-SA-2020-1299)

EulerOS 2.0 SP8 : rsync (EulerOS-SA-2019-1659)

EulerOS 2.0 SP8 : rsyslog (EulerOS-SA-2019-2302)

EulerOS 2.0 SP8 : ruby (EulerOS-SA-2020-1031)

EulerOS 2.0 SP8 : ruby (EulerOS-SA-2020-1178)

EulerOS 2.0 SP8 : samba (EulerOS-SA-2019-1780)

EulerOS 2.0 SP8 : samba (EulerOS-SA-2019-1832)

EulerOS 2.0 SP8 : samba (EulerOS-SA-2019-2116)

EulerOS 2.0 SP8 : samba (EulerOS-SA-2019-2303)

EulerOS 2.0 SP8 : samba (EulerOS-SA-2020-1032)

EulerOS 2.0 SP8 : samba (EulerOS-SA-2020-1179)

EulerOS 2.0 SP8 : SDL (EulerOS-SA-2019-2117)

EulerOS 2.0 SP8 : SDL2 (EulerOS-SA-2019-2118)

EulerOS 2.0 SP8 : sqlite (EulerOS-SA-2019-1814)

EulerOS 2.0 SP8 : sqlite (EulerOS-SA-2019-2119)

EulerOS 2.0 SP8 : sqlite (EulerOS-SA-2020-1033)

EulerOS 2.0 SP8 : sqlite (EulerOS-SA-2020-1180)

EulerOS 2.0 SP8 : sqlite (EulerOS-SA-2020-1300)

EulerOS 2.0 SP8 : squashfs-tools (EulerOS-SA-2019-2092)

EulerOS 2.0 SP8 : squid (EulerOS-SA-2019-2093)

EulerOS 2.0 SP8 : squid (EulerOS-SA-2020-1034)

EulerOS 2.0 SP8 : sssd (EulerOS-SA-2019-1660)

EulerOS 2.0 SP8 : subversion (EulerOS-SA-2019-1789)

EulerOS 2.0 SP8 : sudo (EulerOS-SA-2019-2304)

EulerOS 2.0 SP8 : sudo (EulerOS-SA-2020-1181)

EulerOS 2.0 SP8 : sysstat (EulerOS-SA-2019-2120)

EulerOS 2.0 SP8 : systemd (EulerOS-SA-2019-1661)

EulerOS 2.0 SP8 : systemd (EulerOS-SA-2019-2121)

EulerOS 2.0 SP8 : systemd (EulerOS-SA-2020-1301)

EulerOS 2.0 SP8 : taglib (EulerOS-SA-2019-1662)

EulerOS 2.0 SP8 : tar (EulerOS-SA-2020-1035)

EulerOS 2.0 SP8 : tcpdump (EulerOS-SA-2019-2305)

EulerOS 2.0 SP8 : tomcat (EulerOS-SA-2019-1772)

EulerOS 2.0 SP8 : tomcat (EulerOS-SA-2019-1819)

EulerOS 2.0 SP8 : tomcat (EulerOS-SA-2019-2094)

EulerOS 2.0 SP8 : tomcat (EulerOS-SA-2020-1182)

EulerOS 2.0 SP8 : tomcat (EulerOS-SA-2020-1302)

EulerOS 2.0 SP8 : unbound (EulerOS-SA-2020-1183)

EulerOS 2.0 SP8 : unzip (EulerOS-SA-2019-1773)

EulerOS 2.0 SP8 : unzip (EulerOS-SA-2019-1818)

EulerOS 2.0 SP8 : unzip (EulerOS-SA-2020-1184)

EulerOS 2.0 SP8 : vim (EulerOS-SA-2019-1766)

EulerOS 2.0 SP8 : wavpack (EulerOS-SA-2019-1831)

EulerOS 2.0 SP8 : wavpack (EulerOS-SA-2019-2095)

EulerOS 2.0 SP8 : wavpack (EulerOS-SA-2019-2122)

EulerOS 2.0 SP8 : wget (EulerOS-SA-2019-1663)

EulerOS 2.0 SP8 : wget (EulerOS-SA-2019-1765)

EulerOS 2.0 SP8 : wpa\_supplicant (EulerOS-SA-2019-1779)

EulerOS 2.0 SP8 : wpa\_supplicant (EulerOS-SA-2019-2306)

EulerOS 2.0 SP8 : wpa\_supplicant (EulerOS-SA-2020-1036)

EulerOS 2.0 SP8 : xorg-x11-server (EulerOS-SA-2019-2123)

EulerOS 2.0 SP8 : xorg-x11-server (EulerOS-SA-2020-1037)

EulerOS 2.0 SP8 : zip (EulerOS-SA-2019-1788)

EulerOS 2.0 SP8 : zziplib (EulerOS-SA-2019-2124)

EulerOS Virtualization 2.5.0 : bind (EulerOS-SA-2018-1343)

EulerOS Virtualization 2.5.0 : cups (EulerOS-SA-2018-1329)

EulerOS Virtualization 2.5.0 : curl (EulerOS-SA-2018-1237)

EulerOS Virtualization 2.5.0 : curl (EulerOS-SA-2018-1330)

EulerOS Virtualization 2.5.0 : dhcp (EulerOS-SA-2018-1241)

EulerOS Virtualization 2.5.0 : dhcp (EulerOS-SA-2018-1250)

EulerOS Virtualization 2.5.0 : gcc (EulerOS-SA-2018-1331)

EulerOS Virtualization 2.5.0 : glibc (EulerOS-SA-2018-1239)

EulerOS Virtualization 2.5.0 : glibc (EulerOS-SA-2018-1344)

EulerOS Virtualization 2.5.0 : gnupg2 (EulerOS-SA-2018-1333)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1232)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1234)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1235)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1236)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1245)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1246)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1260)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1262)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1266)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1270)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1345)

EulerOS Virtualization 2.5.0 : kernel (EulerOS-SA-2018-1368)

EulerOS Virtualization 2.5.0 : krb5 (EulerOS-SA-2018-1240)

EulerOS Virtualization 2.5.0 : kvm (EulerOS-SA-2018-1233)

EulerOS Virtualization 2.5.0 : kvm (EulerOS-SA-2018-1264)

EulerOS Virtualization 2.5.0 : kvm (EulerOS-SA-2018-1271)

EulerOS Virtualization 2.5.0 : kvm (EulerOS-SA-2018-1350)

EulerOS Virtualization 2.5.0 : ldns (EulerOS-SA-2018-1231)

EulerOS Virtualization 2.5.0 : libtasn1 (EulerOS-SA-2018-1334)

EulerOS Virtualization 2.5.0 : libvirt (EulerOS-SA-2018-1277)

EulerOS Virtualization 2.5.0 : libxml2 (EulerOS-SA-2018-1255)

EulerOS Virtualization 2.5.0 : libxml2 (EulerOS-SA-2018-1258)

EulerOS Virtualization 2.5.0 : libxml2 (EulerOS-SA-2018-1336)

EulerOS Virtualization 2.5.0 : mariadb (EulerOS-SA-2018-1242)

EulerOS Virtualization 2.5.0 : mariadb (EulerOS-SA-2018-1251)

EulerOS Virtualization 2.5.0 : mariadb (EulerOS-SA-2018-1346)

EulerOS Virtualization 2.5.0 : ncurses (EulerOS-SA-2018-1252)

EulerOS Virtualization 2.5.0 : ncurses (EulerOS-SA-2018-1338)

EulerOS Virtualization 2.5.0 : openssh (EulerOS-SA-2018-1254)

EulerOS Virtualization 2.5.0 : openssl (EulerOS-SA-2018-1339)

EulerOS Virtualization 2.5.0 : php (EulerOS-SA-2018-1249)

EulerOS Virtualization 2.5.0 : procps-ng (EulerOS-SA-2018-1340)

EulerOS Virtualization 2.5.0 : qemu-kvm (EulerOS-SA-2018-1247)

EulerOS Virtualization 2.5.0 : rsync (EulerOS-SA-2018-1244)

EulerOS Virtualization 2.5.0 : ruby (EulerOS-SA-2018-1248)

EulerOS Virtualization 2.5.0 : ruby (EulerOS-SA-2018-1347)

EulerOS Virtualization 2.5.0 : samba (EulerOS-SA-2018-1238)

EulerOS Virtualization 2.5.0 : sqlite (EulerOS-SA-2018-1341)

EulerOS Virtualization 2.5.0 : systemd (EulerOS-SA-2018-1243)

EulerOS Virtualization 2.5.0 : wget (EulerOS-SA-2018-1348)

EulerOS Virtualization 2.5.0 : yum-utils (EulerOS-SA-2018-1349)

EulerOS Virtualization 2.5.1 : bind (EulerOS-SA-2018-1328)

EulerOS Virtualization 2.5.1 : freetype (EulerOS-SA-2018-1381)

EulerOS Virtualization 2.5.1 : ghostscript (EulerOS-SA-2019-1016)

EulerOS Virtualization 2.5.1 : git (EulerOS-SA-2018-1377)

EulerOS Virtualization 2.5.1 : glibc (EulerOS-SA-2018-1272)

EulerOS Virtualization 2.5.1 : glibc (EulerOS-SA-2018-1332)

EulerOS Virtualization 2.5.1 : gnupg2 (EulerOS-SA-2018-1324)

EulerOS Virtualization 2.5.1 : httpd (EulerOS-SA-2019-1015)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1256)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1261)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1263)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1267)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1280)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1322)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1323)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2018-1410)

EulerOS Virtualization 2.5.1 : kernel (EulerOS-SA-2019-1638)

EulerOS Virtualization 2.5.1 : krb5 (EulerOS-SA-2018-1376)

EulerOS Virtualization 2.5.1 : kvm (EulerOS-SA-2018-1265)

EulerOS Virtualization 2.5.1 : kvm (EulerOS-SA-2018-1269)

EulerOS Virtualization 2.5.1 : libtasn1 (EulerOS-SA-2018-1335)

EulerOS Virtualization 2.5.1 : libvirt (EulerOS-SA-2018-1253)

EulerOS Virtualization 2.5.1 : libxml2 (EulerOS-SA-2018-1257)

EulerOS Virtualization 2.5.1 : mariadb (EulerOS-SA-2018-1337)

EulerOS Virtualization 2.5.1 : mariadb (EulerOS-SA-2019-1001)

EulerOS Virtualization 2.5.1 : openssh (EulerOS-SA-2018-1411)

EulerOS Virtualization 2.5.1 : openssl (EulerOS-SA-2018-1383)

EulerOS Virtualization 2.5.1 : openssl098e (EulerOS-SA-2018-1379)

EulerOS Virtualization 2.5.1 : pam (EulerOS-SA-2018-1375)

EulerOS Virtualization 2.5.1 : patch (EulerOS-SA-2018-1378)

EulerOS Virtualization 2.5.1 : php (EulerOS-SA-2018-1325)

EulerOS Virtualization 2.5.1 : procps-ng (EulerOS-SA-2018-1274)

EulerOS Virtualization 2.5.1 : procps-ng (EulerOS-SA-2018-1326)

EulerOS Virtualization 2.5.1 : qemu-kvm (EulerOS-SA-2018-1259)

EulerOS Virtualization 2.5.1 : qemu-kvm (EulerOS-SA-2018-1268)

EulerOS Virtualization 2.5.1 : qemu-kvm (EulerOS-SA-2018-1321)

EulerOS Virtualization 2.5.1 : ruby (EulerOS-SA-2018-1275)

EulerOS Virtualization 2.5.1 : ruby (EulerOS-SA-2018-1374)

EulerOS Virtualization 2.5.1 : sssd (EulerOS-SA-2018-1273)

EulerOS Virtualization 2.5.1 : sudo (EulerOS-SA-2018-1380)

EulerOS Virtualization 2.5.1 : wget (EulerOS-SA-2018-1342)

EulerOS Virtualization 2.5.1 : yum-utils (EulerOS-SA-2018-1327)

EulerOS Virtualization 2.5.2 : bind (EulerOS-SA-2019-1081)

EulerOS Virtualization 2.5.2 : curl (EulerOS-SA-2019-1083)

EulerOS Virtualization 2.5.2 : fuse (EulerOS-SA-2018-1409)

EulerOS Virtualization 2.5.2 : ghostscript (EulerOS-SA-2018-1412)

EulerOS Virtualization 2.5.2 : ghostscript (EulerOS-SA-2019-1087)

EulerOS Virtualization 2.5.2 : ghostscript (EulerOS-SA-2019-1088)

EulerOS Virtualization 2.5.2 : glibc (EulerOS-SA-2019-1086)

EulerOS Virtualization 2.5.2 : gnupg2 (EulerOS-SA-2019-1077)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1351)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1352)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1369)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1370)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1372)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1373)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1382)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2018-1407)

EulerOS Virtualization 2.5.2 : kernel (EulerOS-SA-2019-1637)

EulerOS Virtualization 2.5.2 : krb5 (EulerOS-SA-2018-1408)

EulerOS Virtualization 2.5.2 : libjpeg-turbo (EulerOS-SA-2019-1079)

EulerOS Virtualization 2.5.2 : libtasn1 (EulerOS-SA-2019-1017)

EulerOS Virtualization 2.5.2 : libtasn1 (EulerOS-SA-2019-1018)

EulerOS Virtualization 2.5.2 : libtasn1 (EulerOS-SA-2019-1082)

EulerOS Virtualization 2.5.2 : ncurses (EulerOS-SA-2018-1276)

EulerOS Virtualization 2.5.2 : openssh (EulerOS-SA-2018-1413)

EulerOS Virtualization 2.5.2 : openssl (EulerOS-SA-2019-1084)

EulerOS Virtualization 2.5.2 : perl (EulerOS-SA-2019-1078)

EulerOS Virtualization 2.5.2 : systemd (EulerOS-SA-2018-1371)

EulerOS Virtualization 2.5.2 : systemd (EulerOS-SA-2019-1063)

EulerOS Virtualization 2.5.2 : wget (EulerOS-SA-2019-1085)

EulerOS Virtualization 2.5.2 : yum-utils (EulerOS-SA-2019-1080)

EulerOS Virtualization 2.5.3 : bind (EulerOS-SA-2019-1161)

EulerOS Virtualization 2.5.3 : binutils (EulerOS-SA-2019-1266)

EulerOS Virtualization 2.5.3 : binutils (EulerOS-SA-2019-1270)

EulerOS Virtualization 2.5.3 : bzip2 (EulerOS-SA-2019-1171)

EulerOS Virtualization 2.5.3 : cups (EulerOS-SA-2019-1352)

EulerOS Virtualization 2.5.3 : curl (EulerOS-SA-2019-1163)

EulerOS Virtualization 2.5.3 : curl (EulerOS-SA-2019-1172)

EulerOS Virtualization 2.5.3 : curl (EulerOS-SA-2019-1179)

EulerOS Virtualization 2.5.3 : curl (EulerOS-SA-2019-1240)

EulerOS Virtualization 2.5.3 : curl (EulerOS-SA-2019-1269)

EulerOS Virtualization 2.5.3 : cyrus-sasl (EulerOS-SA-2019-1173)

EulerOS Virtualization 2.5.3 : dnsmasq (EulerOS-SA-2019-1174)

EulerOS Virtualization 2.5.3 : elfutils (EulerOS-SA-2019-1261)

EulerOS Virtualization 2.5.3 : fuse (EulerOS-SA-2019-1186)

EulerOS Virtualization 2.5.3 : fuse (EulerOS-SA-2019-1351)

EulerOS Virtualization 2.5.3 : ghostscript (EulerOS-SA-2019-1176)

EulerOS Virtualization 2.5.3 : ghostscript (EulerOS-SA-2019-1177)

EulerOS Virtualization 2.5.3 : ghostscript (EulerOS-SA-2019-1205)

EulerOS Virtualization 2.5.3 : ghostscript (EulerOS-SA-2019-1241)

EulerOS Virtualization 2.5.3 : ghostscript (EulerOS-SA-2019-1254)

EulerOS Virtualization 2.5.3 : ghostscript (EulerOS-SA-2019-1361)

EulerOS Virtualization 2.5.3 : ghostscript (EulerOS-SA-2019-1364)

EulerOS Virtualization 2.5.3 : git (EulerOS-SA-2019-1183)

EulerOS Virtualization 2.5.3 : glibc (EulerOS-SA-2019-1166)

EulerOS Virtualization 2.5.3 : glibc (EulerOS-SA-2019-1228)

EulerOS Virtualization 2.5.3 : glibc (EulerOS-SA-2019-1257)

EulerOS Virtualization 2.5.3 : glibc (EulerOS-SA-2019-1260)

EulerOS Virtualization 2.5.3 : gnupg2 (EulerOS-SA-2019-1157)

EulerOS Virtualization 2.5.3 : gnutls (EulerOS-SA-2019-1272)

EulerOS Virtualization 2.5.3 : httpd (EulerOS-SA-2019-1271)

EulerOS Virtualization 2.5.3 : httpd (EulerOS-SA-2019-1354)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1178)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1182)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1188)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1197)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1220)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1221)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1244)

EulerOS Virtualization 2.5.3 : kernel (EulerOS-SA-2019-1259)

EulerOS Virtualization 2.5.3 : krb5 (EulerOS-SA-2019-1167)

EulerOS Virtualization 2.5.3 : krb5 (EulerOS-SA-2019-1184)

EulerOS Virtualization 2.5.3 : kvm (EulerOS-SA-2019-1255)

EulerOS Virtualization 2.5.3 : kvm (EulerOS-SA-2019-1369)

EulerOS Virtualization 2.5.3 : kvm (EulerOS-SA-2019-1370)

EulerOS Virtualization 2.5.3 : libidn (EulerOS-SA-2019-1268)

EulerOS Virtualization 2.5.3 : libjpeg-turbo (EulerOS-SA-2019-1159)

EulerOS Virtualization 2.5.3 : libssh2 (EulerOS-SA-2019-1360)

EulerOS Virtualization 2.5.3 : libssh2 (EulerOS-SA-2019-1362)

EulerOS Virtualization 2.5.3 : libtasn1 (EulerOS-SA-2019-1162)

EulerOS Virtualization 2.5.3 : libtasn1 (EulerOS-SA-2019-1190)

EulerOS Virtualization 2.5.3 : libtasn1 (EulerOS-SA-2019-1208)

EulerOS Virtualization 2.5.3 : libvirt (EulerOS-SA-2019-1367)

EulerOS Virtualization 2.5.3 : libxml2 (EulerOS-SA-2019-1353)

EulerOS Virtualization 2.5.3 : nss (EulerOS-SA-2019-1169)

EulerOS Virtualization 2.5.3 : ntp (EulerOS-SA-2019-1207)

EulerOS Virtualization 2.5.3 : ntp (EulerOS-SA-2019-1222)

EulerOS Virtualization 2.5.3 : ntp (EulerOS-SA-2019-1230)

EulerOS Virtualization 2.5.3 : ntp (EulerOS-SA-2019-1356)

EulerOS Virtualization 2.5.3 : openssh (EulerOS-SA-2019-1198)

EulerOS Virtualization 2.5.3 : openssh (EulerOS-SA-2019-1252)

EulerOS Virtualization 2.5.3 : openssh (EulerOS-SA-2019-1355)

EulerOS Virtualization 2.5.3 : openssl (EulerOS-SA-2019-1164)

EulerOS Virtualization 2.5.3 : openssl (EulerOS-SA-2019-1185)

EulerOS Virtualization 2.5.3 : openssl (EulerOS-SA-2019-1258)

EulerOS Virtualization 2.5.3 : openssl (EulerOS-SA-2019-1267)

EulerOS Virtualization 2.5.3 : perl (EulerOS-SA-2019-1158)

EulerOS Virtualization 2.5.3 : perl (EulerOS-SA-2019-1239)

EulerOS Virtualization 2.5.3 : php (EulerOS-SA-2019-1247)

EulerOS Virtualization 2.5.3 : php (EulerOS-SA-2019-1251)

EulerOS Virtualization 2.5.3 : php (EulerOS-SA-2019-1264)

EulerOS Virtualization 2.5.3 : php (EulerOS-SA-2019-1265)

EulerOS Virtualization 2.5.3 : php (EulerOS-SA-2019-1274)

EulerOS Virtualization 2.5.3 : php (EulerOS-SA-2019-1358)

EulerOS Virtualization 2.5.3 : php (EulerOS-SA-2019-1363)

EulerOS Virtualization 2.5.3 : python (EulerOS-SA-2019-1246)

EulerOS Virtualization 2.5.3 : python (EulerOS-SA-2019-1277)

EulerOS Virtualization 2.5.3 : python (EulerOS-SA-2019-1357)

EulerOS Virtualization 2.5.3 : python (EulerOS-SA-2019-1359)

EulerOS Virtualization 2.5.3 : qemu-kvm (EulerOS-SA-2019-1368)

EulerOS Virtualization 2.5.3 : rsyslog (EulerOS-SA-2019-1243)

EulerOS Virtualization 2.5.3 : samba (EulerOS-SA-2019-1273)

EulerOS Virtualization 2.5.3 : spice-gtk (EulerOS-SA-2019-1170)

EulerOS Virtualization 2.5.3 : sqlite (EulerOS-SA-2019-1275)

EulerOS Virtualization 2.5.3 : sqlite (EulerOS-SA-2019-1365)

EulerOS Virtualization 2.5.3 : systemd (EulerOS-SA-2019-1180)

EulerOS Virtualization 2.5.3 : systemd (EulerOS-SA-2019-1195)

EulerOS Virtualization 2.5.3 : systemd (EulerOS-SA-2019-1227)

EulerOS Virtualization 2.5.3 : systemd (EulerOS-SA-2019-1256)

EulerOS Virtualization 2.5.3 : tar (EulerOS-SA-2019-1262)

EulerOS Virtualization 2.5.3 : tar (EulerOS-SA-2019-1366)

EulerOS Virtualization 2.5.3 : util-linux (EulerOS-SA-2019-1175)

EulerOS Virtualization 2.5.3 : wget (EulerOS-SA-2019-1165)

EulerOS Virtualization 2.5.3 : wget (EulerOS-SA-2019-1263)

EulerOS Virtualization 2.5.3 : yum-utils (EulerOS-SA-2019-1160)

EulerOS Virtualization 2.5.3 : zlib (EulerOS-SA-2019-1276)

EulerOS Virtualization 2.5.4 : binutils (EulerOS-SA-2019-1219)

EulerOS Virtualization 2.5.4 : binutils (EulerOS-SA-2019-1231)

EulerOS Virtualization 2.5.4 : curl (EulerOS-SA-2019-1206)

EulerOS Virtualization 2.5.4 : curl (EulerOS-SA-2019-1237)

EulerOS Virtualization 2.5.4 : gd (EulerOS-SA-2019-1250)

EulerOS Virtualization 2.5.4 : ghostscript (EulerOS-SA-2019-1202)

EulerOS Virtualization 2.5.4 : ghostscript (EulerOS-SA-2019-1209)

EulerOS Virtualization 2.5.4 : ghostscript (EulerOS-SA-2019-1215)

EulerOS Virtualization 2.5.4 : glibc (EulerOS-SA-2019-1225)

EulerOS Virtualization 2.5.4 : glibc (EulerOS-SA-2019-1371)

EulerOS Virtualization 2.5.4 : glusterfs (EulerOS-SA-2019-1192)

EulerOS Virtualization 2.5.4 : gnutls (EulerOS-SA-2019-1203)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1168)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1181)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1187)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1189)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1204)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1218)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1223)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1226)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1229)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1232)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1234)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1236)

EulerOS Virtualization 2.5.4 : kernel (EulerOS-SA-2019-1253)

EulerOS Virtualization 2.5.4 : kvm (EulerOS-SA-2019-1372)

EulerOS Virtualization 2.5.4 : libtasn1 (EulerOS-SA-2019-1212)

EulerOS Virtualization 2.5.4 : libXcursor (EulerOS-SA-2019-1191)

EulerOS Virtualization 2.5.4 : libxml2 (EulerOS-SA-2019-1211)

EulerOS Virtualization 2.5.4 : net-snmp (EulerOS-SA-2019-1214)

EulerOS Virtualization 2.5.4 : ntp (EulerOS-SA-2019-1213)

EulerOS Virtualization 2.5.4 : openssh (EulerOS-SA-2019-1199)

EulerOS Virtualization 2.5.4 : openssh (EulerOS-SA-2019-1235)

EulerOS Virtualization 2.5.4 : openssl (EulerOS-SA-2019-1201)

EulerOS Virtualization 2.5.4 : perl (EulerOS-SA-2019-1238)

EulerOS Virtualization 2.5.4 : php (EulerOS-SA-2019-1249)

EulerOS Virtualization 2.5.4 : python (EulerOS-SA-2019-1248)

EulerOS Virtualization 2.5.4 : PyYAML (EulerOS-SA-2019-1224)

EulerOS Virtualization 2.5.4 : qemu-kvm (EulerOS-SA-2019-1373)

EulerOS Virtualization 2.5.4 : rpm (EulerOS-SA-2019-1210)

EulerOS Virtualization 2.5.4 : rsyslog (EulerOS-SA-2019-1245)

EulerOS Virtualization 2.5.4 : spice-gtk (EulerOS-SA-2019-1200)

EulerOS Virtualization 2.5.4 : sssd (EulerOS-SA-2019-1193)

EulerOS Virtualization 2.5.4 : systemd (EulerOS-SA-2019-1196)

EulerOS Virtualization 2.5.4 : systemd (EulerOS-SA-2019-1216)

EulerOS Virtualization 2.5.4 : systemd (EulerOS-SA-2019-1217)

EulerOS Virtualization 2.5.4 : systemd (EulerOS-SA-2019-1233)

EulerOS Virtualization 2.5.4 : systemd (EulerOS-SA-2019-1242)

EulerOS Virtualization 2.5.4 : wpa\_supplicant (EulerOS-SA-2019-1194)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1510)

EulerOS Virtualization 3.0.1.0 : apr (EulerOS-SA-2019-1452)

EulerOS Virtualization 3.0.1.0 : bash (EulerOS-SA-2019-1418)

EulerOS Virtualization 3.0.1.0 : bash (EulerOS-SA-2019-1609)

EulerOS Virtualization 3.0.1.0 : bind (EulerOS-SA-2019-1433)

EulerOS Virtualization 3.0.1.0 : binutils (EulerOS-SA-2019-1431)

EulerOS Virtualization 3.0.1.0 : cups (EulerOS-SA-2019-1432)

EulerOS Virtualization 3.0.1.0 : cups (EulerOS-SA-2019-1605)

EulerOS Virtualization 3.0.1.0 : curl (EulerOS-SA-2019-1549)

EulerOS Virtualization 3.0.1.0 : curl (EulerOS-SA-2019-1550)

EulerOS Virtualization 3.0.1.0 : cvs (EulerOS-SA-2019-1455)

EulerOS Virtualization 3.0.1.0 : dhcp (EulerOS-SA-2019-1443)

EulerOS Virtualization 3.0.1.0 : dnsmasq (EulerOS-SA-2019-1423)

EulerOS Virtualization 3.0.1.0 : expat (EulerOS-SA-2019-1446)

EulerOS Virtualization 3.0.1.0 : file (EulerOS-SA-2019-1424)

EulerOS Virtualization 3.0.1.0 : flac (EulerOS-SA-2019-1451)

EulerOS Virtualization 3.0.1.0 : fuse (EulerOS-SA-2019-1442)

EulerOS Virtualization 3.0.1.0 : fuse (EulerOS-SA-2019-1607)

EulerOS Virtualization 3.0.1.0 : gcc (EulerOS-SA-2019-1461)

EulerOS Virtualization 3.0.1.0 : gd (EulerOS-SA-2019-1463)

EulerOS Virtualization 3.0.1.0 : gdk-pixbuf2 (EulerOS-SA-2019-1438)

EulerOS Virtualization 3.0.1.0 : ghostscript (EulerOS-SA-2019-1465)

EulerOS Virtualization 3.0.1.0 : git (EulerOS-SA-2019-1420)

EulerOS Virtualization 3.0.1.0 : glibc (EulerOS-SA-2019-1551)

EulerOS Virtualization 3.0.1.0 : glibc (EulerOS-SA-2019-1552)

EulerOS Virtualization 3.0.1.0 : gnupg2 (EulerOS-SA-2019-1457)

EulerOS Virtualization 3.0.1.0 : httpd (EulerOS-SA-2019-1419)

EulerOS Virtualization 3.0.1.0 : httpd (EulerOS-SA-2019-1560)

EulerOS Virtualization 3.0.1.0 : icu (EulerOS-SA-2019-1453)

EulerOS Virtualization 3.0.1.0 : jbigkit (EulerOS-SA-2019-1430)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1473)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1475)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1477)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1479)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1480)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1481)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1483)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1485)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1487)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1488)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1489)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1491)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1492)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1494)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1496)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1498)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1499)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1501)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1502)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1504)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1507)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1509)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1511)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1512)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1514)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1515)

EulerOS Virtualization 3.0.1.0 : kernel (EulerOS-SA-2019-1612)

EulerOS Virtualization 3.0.1.0 : kvm (EulerOS-SA-2019-1450)

EulerOS Virtualization 3.0.1.0 : kvm (EulerOS-SA-2019-1611)

EulerOS Virtualization 3.0.1.0 : libarchive (EulerOS-SA-2019-1470)

EulerOS Virtualization 3.0.1.0 : libevent (EulerOS-SA-2019-1439)

EulerOS Virtualization 3.0.1.0 : libgcrypt (EulerOS-SA-2019-1448)

EulerOS Virtualization 3.0.1.0 : libidn (EulerOS-SA-2019-1454)

EulerOS Virtualization 3.0.1.0 : libjpeg-turbo (EulerOS-SA-2019-1468)

EulerOS Virtualization 3.0.1.0 : libpng (EulerOS-SA-2019-1421)

EulerOS Virtualization 3.0.1.0 : libsndfile (EulerOS-SA-2019-1441)

EulerOS Virtualization 3.0.1.0 : libssh2 (EulerOS-SA-2019-1429)

EulerOS Virtualization 3.0.1.0 : libtar (EulerOS-SA-2019-1440)

EulerOS Virtualization 3.0.1.0 : libtiff (EulerOS-SA-2019-1437)

EulerOS Virtualization 3.0.1.0 : libvirt (EulerOS-SA-2019-1456)

EulerOS Virtualization 3.0.1.0 : libvirt (EulerOS-SA-2019-1610)

EulerOS Virtualization 3.0.1.0 : libxml2 (EulerOS-SA-2019-1559)

EulerOS Virtualization 3.0.1.0 : libxslt (EulerOS-SA-2019-1606)

EulerOS Virtualization 3.0.1.0 : libyaml (EulerOS-SA-2019-1445)

EulerOS Virtualization 3.0.1.0 : mariadb (EulerOS-SA-2019-1553)

EulerOS Virtualization 3.0.1.0 : mariadb (EulerOS-SA-2019-1554)

EulerOS Virtualization 3.0.1.0 : memcached (EulerOS-SA-2019-1435)

EulerOS Virtualization 3.0.1.0 : net-snmp (EulerOS-SA-2019-1436)

EulerOS Virtualization 3.0.1.0 : ntp (EulerOS-SA-2019-1555)

EulerOS Virtualization 3.0.1.0 : ntp (EulerOS-SA-2019-1556)

EulerOS Virtualization 3.0.1.0 : ntp (EulerOS-SA-2019-1557)

EulerOS Virtualization 3.0.1.0 : openssh (EulerOS-SA-2019-1426)

EulerOS Virtualization 3.0.1.0 : openssl (EulerOS-SA-2019-1546)

EulerOS Virtualization 3.0.1.0 : openssl (EulerOS-SA-2019-1547)

EulerOS Virtualization 3.0.1.0 : openssl (EulerOS-SA-2019-1548)

EulerOS Virtualization 3.0.1.0 : pcre (EulerOS-SA-2019-1558)

EulerOS Virtualization 3.0.1.0 : perl (EulerOS-SA-2019-1464)

EulerOS Virtualization 3.0.1.0 : php (EulerOS-SA-2019-1543)

EulerOS Virtualization 3.0.1.0 : php (EulerOS-SA-2019-1544)

EulerOS Virtualization 3.0.1.0 : php (EulerOS-SA-2019-1545)

EulerOS Virtualization 3.0.1.0 : python (EulerOS-SA-2019-1434)

EulerOS Virtualization 3.0.1.0 : python-urllib3 (EulerOS-SA-2019-1604)

EulerOS Virtualization 3.0.1.0 : qemu (EulerOS-SA-2019-1444)

EulerOS Virtualization 3.0.1.0 : rpm (EulerOS-SA-2019-1466)

EulerOS Virtualization 3.0.1.0 : rsync (EulerOS-SA-2019-1460)

EulerOS Virtualization 3.0.1.0 : ruby (EulerOS-SA-2019-1428)

EulerOS Virtualization 3.0.1.0 : samba (EulerOS-SA-2019-1447)

EulerOS Virtualization 3.0.1.0 : scsi-target-utils (EulerOS-SA-2019-1427)

EulerOS Virtualization 3.0.1.0 : SDL (EulerOS-SA-2019-1469)

EulerOS Virtualization 3.0.1.0 : sqlite (EulerOS-SA-2019-1425)

EulerOS Virtualization 3.0.1.0 : squashfs-tools (EulerOS-SA-2019-1459)

EulerOS Virtualization 3.0.1.0 : sudo (EulerOS-SA-2019-1449)

EulerOS Virtualization 3.0.1.0 : systemd (EulerOS-SA-2019-1416)

EulerOS Virtualization 3.0.1.0 : tar (EulerOS-SA-2019-1608)

EulerOS Virtualization 3.0.1.0 : thrift (EulerOS-SA-2019-1458)

EulerOS Virtualization 3.0.1.0 : unzip (EulerOS-SA-2019-1467)

EulerOS Virtualization 3.0.1.0 : util-linux (EulerOS-SA-2019-1462)

EulerOS Virtualization 3.0.1.0 : wget (EulerOS-SA-2019-1417)

EulerOS Virtualization 3.0.1.0 : wpa\_supplicant (EulerOS-SA-2019-1422)

EulerOS Virtualization 3.0.2.2 : avahi (EulerOS-SA-2020-1450)

EulerOS Virtualization 3.0.2.2 : bind (EulerOS-SA-2020-1460)

EulerOS Virtualization 3.0.2.2 : binutils (EulerOS-SA-2020-1466)

EulerOS Virtualization 3.0.2.2 : c-ares (EulerOS-SA-2020-1480)

EulerOS Virtualization 3.0.2.2 : cifs-utils (EulerOS-SA-2020-1495)

EulerOS Virtualization 3.0.2.2 : coreutils (EulerOS-SA-2020-1484)

EulerOS Virtualization 3.0.2.2 : cronie (EulerOS-SA-2020-1468)

EulerOS Virtualization 3.0.2.2 : cups (EulerOS-SA-2020-1461)

EulerOS Virtualization 3.0.2.2 : curl (EulerOS-SA-2020-1271)

EulerOS Virtualization 3.0.2.2 : curl-openssl (EulerOS-SA-2020-1278)

EulerOS Virtualization 3.0.2.2 : dhcp (EulerOS-SA-2020-1273)

EulerOS Virtualization 3.0.2.2 : dhcp-noddns (EulerOS-SA-2020-1267)

EulerOS Virtualization 3.0.2.2 : dosfstools (EulerOS-SA-2020-1458)

EulerOS Virtualization 3.0.2.2 : e2fsprogs (EulerOS-SA-2020-1272)

EulerOS Virtualization 3.0.2.2 : elfutils (EulerOS-SA-2020-1448)

EulerOS Virtualization 3.0.2.2 : expat (EulerOS-SA-2020-1445)

EulerOS Virtualization 3.0.2.2 : freetype (EulerOS-SA-2020-1491)

EulerOS Virtualization 3.0.2.2 : gd (EulerOS-SA-2020-1464)

EulerOS Virtualization 3.0.2.2 : gettext (EulerOS-SA-2020-1469)

EulerOS Virtualization 3.0.2.2 : ghostscript (EulerOS-SA-2020-1499)

EulerOS Virtualization 3.0.2.2 : glib2 (EulerOS-SA-2020-1456)

EulerOS Virtualization 3.0.2.2 : glibc (EulerOS-SA-2020-1478)

EulerOS Virtualization 3.0.2.2 : gnupg2 (EulerOS-SA-2020-1489)

EulerOS Virtualization 3.0.2.2 : gpgme (EulerOS-SA-2020-1494)

EulerOS Virtualization 3.0.2.2 : http-parser (EulerOS-SA-2020-1486)

EulerOS Virtualization 3.0.2.2 : httpd (EulerOS-SA-2020-1455)

EulerOS Virtualization 3.0.2.2 : icu (EulerOS-SA-2020-1454)

EulerOS Virtualization 3.0.2.2 : ipmitool (EulerOS-SA-2020-1479)

EulerOS Virtualization 3.0.2.2 : keepalived (EulerOS-SA-2020-1493)

EulerOS Virtualization 3.0.2.2 : kernel (EulerOS-SA-2020-1269)

EulerOS Virtualization 3.0.2.2 : kernel (EulerOS-SA-2020-1452)

EulerOS Virtualization 3.0.2.2 : krb5 (EulerOS-SA-2020-1467)

EulerOS Virtualization 3.0.2.2 : lcms2 (EulerOS-SA-2020-1492)

EulerOS Virtualization 3.0.2.2 : libarchive (EulerOS-SA-2020-1488)

EulerOS Virtualization 3.0.2.2 : libcroco (EulerOS-SA-2020-1475)

EulerOS Virtualization 3.0.2.2 : libgcrypt (EulerOS-SA-2020-1498)

EulerOS Virtualization 3.0.2.2 : libjpeg-turbo (EulerOS-SA-2020-1483)

EulerOS Virtualization 3.0.2.2 : libnl (EulerOS-SA-2020-1490)

EulerOS Virtualization 3.0.2.2 : libpcap (EulerOS-SA-2020-1487)

EulerOS Virtualization 3.0.2.2 : libpng (EulerOS-SA-2020-1496)

EulerOS Virtualization 3.0.2.2 : libssh2 (EulerOS-SA-2020-1282)

EulerOS Virtualization 3.0.2.2 : libtiff (EulerOS-SA-2020-1447)

EulerOS Virtualization 3.0.2.2 : libX11 (EulerOS-SA-2020-1471)

EulerOS Virtualization 3.0.2.2 : libXfont (EulerOS-SA-2020-1459)

EulerOS Virtualization 3.0.2.2 : libxml2 (EulerOS-SA-2020-1268)

EulerOS Virtualization 3.0.2.2 : libxml2 (EulerOS-SA-2020-1474)

EulerOS Virtualization 3.0.2.2 : libxslt (EulerOS-SA-2020-1442)

EulerOS Virtualization 3.0.2.2 : lua (EulerOS-SA-2020-1477)

EulerOS Virtualization 3.0.2.2 : netpbm (EulerOS-SA-2020-1470)

EulerOS Virtualization 3.0.2.2 : ntp (EulerOS-SA-2020-1457)

EulerOS Virtualization 3.0.2.2 : openldap (EulerOS-SA-2020-1481)

EulerOS Virtualization 3.0.2.2 : openssl (EulerOS-SA-2020-1274)

EulerOS Virtualization 3.0.2.2 : openssl (EulerOS-SA-2020-1444)

EulerOS Virtualization 3.0.2.2 : patch (EulerOS-SA-2020-1446)

EulerOS Virtualization 3.0.2.2 : pcre (EulerOS-SA-2020-1485)

EulerOS Virtualization 3.0.2.2 : perl (EulerOS-SA-2020-1476)

EulerOS Virtualization 3.0.2.2 : polkit (EulerOS-SA-2020-1463)

EulerOS Virtualization 3.0.2.2 : python (EulerOS-SA-2020-1275)

EulerOS Virtualization 3.0.2.2 : python (EulerOS-SA-2020-1472)

EulerOS Virtualization 3.0.2.2 : python-pillow (EulerOS-SA-2020-1473)

EulerOS Virtualization 3.0.2.2 : python-urllib3 (EulerOS-SA-2020-1277)

EulerOS Virtualization 3.0.2.2 : qemu-kvm (EulerOS-SA-2020-1500)

EulerOS Virtualization 3.0.2.2 : rsync (EulerOS-SA-2020-1497)

EulerOS Virtualization 3.0.2.2 : rsyslog (EulerOS-SA-2020-1276)

EulerOS Virtualization 3.0.2.2 : ruby (EulerOS-SA-2020-1443)

EulerOS Virtualization 3.0.2.2 : samba (EulerOS-SA-2020-1270)

EulerOS Virtualization 3.0.2.2 : sqlite (EulerOS-SA-2020-1280)

EulerOS Virtualization 3.0.2.2 : sssd (EulerOS-SA-2020-1453)

EulerOS Virtualization 3.0.2.2 : sudo (EulerOS-SA-2020-1279)

EulerOS Virtualization 3.0.2.2 : systemd (EulerOS-SA-2020-1451)

EulerOS Virtualization 3.0.2.2 : tar (EulerOS-SA-2020-1449)

EulerOS Virtualization 3.0.2.2 : unbound (EulerOS-SA-2020-1482)

EulerOS Virtualization 3.0.2.2 : unzip (EulerOS-SA-2020-1462)

EulerOS Virtualization 3.0.2.2 : wget (EulerOS-SA-2020-1281)

EulerOS Virtualization 3.0.2.2 : zip (EulerOS-SA-2020-1465)

EulerOS Virtualization for ARM 64 3.0.1.0 : apr (EulerOS-SA-2019-1374)

EulerOS Virtualization for ARM 64 3.0.1.0 : augeas (EulerOS-SA-2019-1375)

EulerOS Virtualization for ARM 64 3.0.1.0 : bind (EulerOS-SA-2019-1376)

EulerOS Virtualization for ARM 64 3.0.1.0 : binutils (EulerOS-SA-2019-1377)

EulerOS Virtualization for ARM 64 3.0.1.0 : bluez (EulerOS-SA-2019-1378)

EulerOS Virtualization for ARM 64 3.0.1.0 : curl (EulerOS-SA-2019-1540)

EulerOS Virtualization for ARM 64 3.0.1.0 : dhcp (EulerOS-SA-2019-1379)

EulerOS Virtualization for ARM 64 3.0.1.0 : dnsmasq (EulerOS-SA-2019-1380)

EulerOS Virtualization for ARM 64 3.0.1.0 : emacs (EulerOS-SA-2019-1381)

EulerOS Virtualization for ARM 64 3.0.1.0 : fuse (EulerOS-SA-2019-1382)

EulerOS Virtualization for ARM 64 3.0.1.0 : ghostscript (EulerOS-SA-2019-1384)

EulerOS Virtualization for ARM 64 3.0.1.0 : git (EulerOS-SA-2019-1385)

EulerOS Virtualization for ARM 64 3.0.1.0 : glibc (EulerOS-SA-2019-1386)

EulerOS Virtualization for ARM 64 3.0.1.0 : glusterfs (EulerOS-SA-2019-1387)

EulerOS Virtualization for ARM 64 3.0.1.0 : gnutls (EulerOS-SA-2019-1388)

EulerOS Virtualization for ARM 64 3.0.1.0 : httpd (EulerOS-SA-2019-1389)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1471)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1472)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1474)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1476)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1478)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1482)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1484)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1486)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1490)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1493)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1495)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1497)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1500)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1503)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1505)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1506)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1508)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1513)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1516)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1517)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1518)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1519)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1520)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1521)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1522)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1523)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1524)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1525)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1526)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1527)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1528)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1529)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1530)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1531)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1532)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1533)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1534)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1535)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1536)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1537)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1538)

EulerOS Virtualization for ARM 64 3.0.1.0 : kernel (EulerOS-SA-2019-1539)

EulerOS Virtualization for ARM 64 3.0.1.0 : krb5 (EulerOS-SA-2019-1383)

EulerOS Virtualization for ARM 64 3.0.1.0 : libarchive (EulerOS-SA-2019-1390)

EulerOS Virtualization for ARM 64 3.0.1.0 : libpng12 (EulerOS-SA-2019-1391)

EulerOS Virtualization for ARM 64 3.0.1.0 : libsoup (EulerOS-SA-2019-1392)

EulerOS Virtualization for ARM 64 3.0.1.0 : libssh2 (EulerOS-SA-2019-1393)

EulerOS Virtualization for ARM 64 3.0.1.0 : libvirt (EulerOS-SA-2019-1394)

EulerOS Virtualization for ARM 64 3.0.1.0 : libXcursor (EulerOS-SA-2019-1395)

EulerOS Virtualization for ARM 64 3.0.1.0 : mariadb (EulerOS-SA-2019-1541)

EulerOS Virtualization for ARM 64 3.0.1.0 : mariadb (EulerOS-SA-2019-1542)

EulerOS Virtualization for ARM 64 3.0.1.0 : memcached (EulerOS-SA-2019-1396)

EulerOS Virtualization for ARM 64 3.0.1.0 : nss (EulerOS-SA-2019-1397)

EulerOS Virtualization for ARM 64 3.0.1.0 : ntp (EulerOS-SA-2019-1398)

EulerOS Virtualization for ARM 64 3.0.1.0 : openssh (EulerOS-SA-2019-1399)

EulerOS Virtualization for ARM 64 3.0.1.0 : openssl (EulerOS-SA-2019-1400)

EulerOS Virtualization for ARM 64 3.0.1.0 : perl (EulerOS-SA-2019-1401)

EulerOS Virtualization for ARM 64 3.0.1.0 : php (EulerOS-SA-2019-1402)

EulerOS Virtualization for ARM 64 3.0.1.0 : python (EulerOS-SA-2019-1403)

EulerOS Virtualization for ARM 64 3.0.1.0 : python-paramiko (EulerOS-SA-2019-1404)

EulerOS Virtualization for ARM 64 3.0.1.0 : qemu-kvm (EulerOS-SA-2019-1405)

EulerOS Virtualization for ARM 64 3.0.1.0 : rsyslog (EulerOS-SA-2019-1406)

EulerOS Virtualization for ARM 64 3.0.1.0 : ruby (EulerOS-SA-2019-1407)

EulerOS Virtualization for ARM 64 3.0.1.0 : samba (EulerOS-SA-2019-1408)

EulerOS Virtualization for ARM 64 3.0.1.0 : setup (EulerOS-SA-2019-1409)

EulerOS Virtualization for ARM 64 3.0.1.0 : sqlite (EulerOS-SA-2019-1410)

EulerOS Virtualization for ARM 64 3.0.1.0 : sssd (EulerOS-SA-2019-1411)

EulerOS Virtualization for ARM 64 3.0.1.0 : systemd (EulerOS-SA-2019-1412)

EulerOS Virtualization for ARM 64 3.0.1.0 : wget (EulerOS-SA-2019-1413)

EulerOS Virtualization for ARM 64 3.0.1.0 : wpa\_supplicant (EulerOS-SA-2019-1414)

EulerOS Virtualization for ARM 64 3.0.1.0 : yum-utils (EulerOS-SA-2019-1415)

EulerOS Virtualization for ARM 64 3.0.2.0 : avahi (EulerOS-SA-2020-1228)

EulerOS Virtualization for ARM 64 3.0.2.0 : bash (EulerOS-SA-2019-1621)

EulerOS Virtualization for ARM 64 3.0.2.0 : bash (EulerOS-SA-2019-1942)

EulerOS Virtualization for ARM 64 3.0.2.0 : bind (EulerOS-SA-2019-1704)

EulerOS Virtualization for ARM 64 3.0.2.0 : bind (EulerOS-SA-2020-1203)

EulerOS Virtualization for ARM 64 3.0.2.0 : binutils (EulerOS-SA-2019-1940)

EulerOS Virtualization for ARM 64 3.0.2.0 : binutils (EulerOS-SA-2020-1205)

EulerOS Virtualization for ARM 64 3.0.2.0 : bzip2 (EulerOS-SA-2019-1920)

EulerOS Virtualization for ARM 64 3.0.2.0 : c-ares (EulerOS-SA-2019-1950)

EulerOS Virtualization for ARM 64 3.0.2.0 : cairo (EulerOS-SA-2020-1260)

EulerOS Virtualization for ARM 64 3.0.2.0 : cifs-utils (EulerOS-SA-2020-1253)

EulerOS Virtualization for ARM 64 3.0.2.0 : coreutils (EulerOS-SA-2020-1194)

EulerOS Virtualization for ARM 64 3.0.2.0 : cronie (EulerOS-SA-2019-1933)

EulerOS Virtualization for ARM 64 3.0.2.0 : cups (EulerOS-SA-2019-1622)

EulerOS Virtualization for ARM 64 3.0.2.0 : cups (EulerOS-SA-2020-1227)

EulerOS Virtualization for ARM 64 3.0.2.0 : curl (EulerOS-SA-2019-1695)

EulerOS Virtualization for ARM 64 3.0.2.0 : curl (EulerOS-SA-2019-1696)

EulerOS Virtualization for ARM 64 3.0.2.0 : curl (EulerOS-SA-2019-1697)

EulerOS Virtualization for ARM 64 3.0.2.0 : curl (EulerOS-SA-2019-1924)

EulerOS Virtualization for ARM 64 3.0.2.0 : curl (EulerOS-SA-2020-1233)

EulerOS Virtualization for ARM 64 3.0.2.0 : dbus (EulerOS-SA-2019-1706)

EulerOS Virtualization for ARM 64 3.0.2.0 : dhcp (EulerOS-SA-2020-1204)

EulerOS Virtualization for ARM 64 3.0.2.0 : dosfstools (EulerOS-SA-2020-1230)

EulerOS Virtualization for ARM 64 3.0.2.0 : elfutils (EulerOS-SA-2020-1190)

EulerOS Virtualization for ARM 64 3.0.2.0 : expat (EulerOS-SA-2019-1698)

EulerOS Virtualization for ARM 64 3.0.2.0 : expat (EulerOS-SA-2019-1935)

EulerOS Virtualization for ARM 64 3.0.2.0 : expat (EulerOS-SA-2020-1217)

EulerOS Virtualization for ARM 64 3.0.2.0 : file (EulerOS-SA-2020-1201)

EulerOS Virtualization for ARM 64 3.0.2.0 : freetype (EulerOS-SA-2020-1224)

EulerOS Virtualization for ARM 64 3.0.2.0 : fuse (EulerOS-SA-2019-1623)

EulerOS Virtualization for ARM 64 3.0.2.0 : gcc (EulerOS-SA-2019-2308)

EulerOS Virtualization for ARM 64 3.0.2.0 : gettext (EulerOS-SA-2020-1248)

EulerOS Virtualization for ARM 64 3.0.2.0 : ghostscript (EulerOS-SA-2019-1613)

EulerOS Virtualization for ARM 64 3.0.2.0 : ghostscript (EulerOS-SA-2020-1240)

EulerOS Virtualization for ARM 64 3.0.2.0 : git (EulerOS-SA-2019-1930)

EulerOS Virtualization for ARM 64 3.0.2.0 : glib2 (EulerOS-SA-2019-1927)

EulerOS Virtualization for ARM 64 3.0.2.0 : glib2 (EulerOS-SA-2020-1239)

EulerOS Virtualization for ARM 64 3.0.2.0 : glibc (EulerOS-SA-2019-1703)

EulerOS Virtualization for ARM 64 3.0.2.0 : glibc (EulerOS-SA-2020-1229)

EulerOS Virtualization for ARM 64 3.0.2.0 : gnupg2 (EulerOS-SA-2020-1232)

EulerOS Virtualization for ARM 64 3.0.2.0 : gnutls (EulerOS-SA-2019-1693)

EulerOS Virtualization for ARM 64 3.0.2.0 : gpgme (EulerOS-SA-2020-1254)

EulerOS Virtualization for ARM 64 3.0.2.0 : gstreamer1-plugins-base (EulerOS-SA-2019-1712)

EulerOS Virtualization for ARM 64 3.0.2.0 : http-parser (EulerOS-SA-2020-1198)

EulerOS Virtualization for ARM 64 3.0.2.0 : httpd (EulerOS-SA-2019-1631)

EulerOS Virtualization for ARM 64 3.0.2.0 : httpd (EulerOS-SA-2020-1250)

EulerOS Virtualization for ARM 64 3.0.2.0 : icu (EulerOS-SA-2019-1946)

EulerOS Virtualization for ARM 64 3.0.2.0 : icu (EulerOS-SA-2020-1261)

EulerOS Virtualization for ARM 64 3.0.2.0 : jasper (EulerOS-SA-2020-1188)

EulerOS Virtualization for ARM 64 3.0.2.0 : keepalived (EulerOS-SA-2019-1710)

EulerOS Virtualization for ARM 64 3.0.2.0 : kernel (EulerOS-SA-2019-1635)

EulerOS Virtualization for ARM 64 3.0.2.0 : kernel (EulerOS-SA-2019-1636)

EulerOS Virtualization for ARM 64 3.0.2.0 : kernel (EulerOS-SA-2019-1702)

EulerOS Virtualization for ARM 64 3.0.2.0 : kernel (EulerOS-SA-2019-1926)

EulerOS Virtualization for ARM 64 3.0.2.0 : kernel (EulerOS-SA-2020-1197)

EulerOS Virtualization for ARM 64 3.0.2.0 : krb5 (EulerOS-SA-2020-1192)

EulerOS Virtualization for ARM 64 3.0.2.0 : lcms2 (EulerOS-SA-2020-1211)

EulerOS Virtualization for ARM 64 3.0.2.0 : less (EulerOS-SA-2020-1238)

EulerOS Virtualization for ARM 64 3.0.2.0 : lftp (EulerOS-SA-2020-1259)

EulerOS Virtualization for ARM 64 3.0.2.0 : libarchive (EulerOS-SA-2019-1714)

EulerOS Virtualization for ARM 64 3.0.2.0 : libarchive (EulerOS-SA-2019-1954)

EulerOS Virtualization for ARM 64 3.0.2.0 : libarchive (EulerOS-SA-2020-1226)

EulerOS Virtualization for ARM 64 3.0.2.0 : libcgroup (EulerOS-SA-2019-1953)

EulerOS Virtualization for ARM 64 3.0.2.0 : libcroco (EulerOS-SA-2020-1251)

EulerOS Virtualization for ARM 64 3.0.2.0 : libffi (EulerOS-SA-2019-1941)

EulerOS Virtualization for ARM 64 3.0.2.0 : libgcrypt (EulerOS-SA-2020-1189)

EulerOS Virtualization for ARM 64 3.0.2.0 : libidn (EulerOS-SA-2020-1265)

EulerOS Virtualization for ARM 64 3.0.2.0 : libjpeg-turbo (EulerOS-SA-2019-1628)

EulerOS Virtualization for ARM 64 3.0.2.0 : libjpeg-turbo (EulerOS-SA-2019-1955)

EulerOS Virtualization for ARM 64 3.0.2.0 : libnl (EulerOS-SA-2020-1258)

EulerOS Virtualization for ARM 64 3.0.2.0 : libosinfo (EulerOS-SA-2019-1952)

EulerOS Virtualization for ARM 64 3.0.2.0 : libpcap (EulerOS-SA-2020-1249)

EulerOS Virtualization for ARM 64 3.0.2.0 : libpng (EulerOS-SA-2019-1951)

EulerOS Virtualization for ARM 64 3.0.2.0 : libpng (EulerOS-SA-2020-1256)

EulerOS Virtualization for ARM 64 3.0.2.0 : libseccomp (EulerOS-SA-2019-1956)

EulerOS Virtualization for ARM 64 3.0.2.0 : libssh2 (EulerOS-SA-2020-1263)

EulerOS Virtualization for ARM 64 3.0.2.0 : libtasn1 (EulerOS-SA-2020-1234)

EulerOS Virtualization for ARM 64 3.0.2.0 : libtiff (EulerOS-SA-2019-1629)

EulerOS Virtualization for ARM 64 3.0.2.0 : libtiff (EulerOS-SA-2019-1700)

EulerOS Virtualization for ARM 64 3.0.2.0 : libtiff (EulerOS-SA-2019-1937)

EulerOS Virtualization for ARM 64 3.0.2.0 : libtiff (EulerOS-SA-2020-1235)

EulerOS Virtualization for ARM 64 3.0.2.0 : libvirt (EulerOS-SA-2019-1634)

EulerOS Virtualization for ARM 64 3.0.2.0 : libvirt (EulerOS-SA-2019-1957)

EulerOS Virtualization for ARM 64 3.0.2.0 : libvorbis (EulerOS-SA-2020-1247)

EulerOS Virtualization for ARM 64 3.0.2.0 : libX11 (EulerOS-SA-2019-1948)

EulerOS Virtualization for ARM 64 3.0.2.0 : libX11 (EulerOS-SA-2020-1191)

EulerOS Virtualization for ARM 64 3.0.2.0 : libXfont (EulerOS-SA-2020-1241)

EulerOS Virtualization for ARM 64 3.0.2.0 : libXfont2 (EulerOS-SA-2020-1242)

EulerOS Virtualization for ARM 64 3.0.2.0 : libxkbcommon (EulerOS-SA-2020-1246)

EulerOS Virtualization for ARM 64 3.0.2.0 : libxml2 (EulerOS-SA-2019-1614)

EulerOS Virtualization for ARM 64 3.0.2.0 : libxml2 (EulerOS-SA-2019-1711)

EulerOS Virtualization for ARM 64 3.0.2.0 : libxml2 (EulerOS-SA-2020-1208)

EulerOS Virtualization for ARM 64 3.0.2.0 : libxslt (EulerOS-SA-2019-1625)

EulerOS Virtualization for ARM 64 3.0.2.0 : libxslt (EulerOS-SA-2019-1929)

EulerOS Virtualization for ARM 64 3.0.2.0 : libxslt (EulerOS-SA-2020-1215)

EulerOS Virtualization for ARM 64 3.0.2.0 : lua (EulerOS-SA-2020-1220)

EulerOS Virtualization for ARM 64 3.0.2.0 : lz4 (EulerOS-SA-2020-1262)

EulerOS Virtualization for ARM 64 3.0.2.0 : ncurses (EulerOS-SA-2020-1206)

EulerOS Virtualization for ARM 64 3.0.2.0 : netpbm (EulerOS-SA-2020-1255)

EulerOS Virtualization for ARM 64 3.0.2.0 : nss (EulerOS-SA-2020-1214)

EulerOS Virtualization for ARM 64 3.0.2.0 : nss-softokn (EulerOS-SA-2020-1252)

EulerOS Virtualization for ARM 64 3.0.2.0 : ntp (EulerOS-SA-2019-1938)

EulerOS Virtualization for ARM 64 3.0.2.0 : ntp (EulerOS-SA-2020-1210)

EulerOS Virtualization for ARM 64 3.0.2.0 : openldap (EulerOS-SA-2019-1939)

EulerOS Virtualization for ARM 64 3.0.2.0 : openldap (EulerOS-SA-2020-1200)

EulerOS Virtualization for ARM 64 3.0.2.0 : openssh (EulerOS-SA-2019-1630)

EulerOS Virtualization for ARM 64 3.0.2.0 : openssl (EulerOS-SA-2019-1943)

EulerOS Virtualization for ARM 64 3.0.2.0 : openssl (EulerOS-SA-2020-1221)

EulerOS Virtualization for ARM 64 3.0.2.0 : patch (EulerOS-SA-2019-1922)

EulerOS Virtualization for ARM 64 3.0.2.0 : patch (EulerOS-SA-2020-1225)

EulerOS Virtualization for ARM 64 3.0.2.0 : pcre (EulerOS-SA-2019-1931)

EulerOS Virtualization for ARM 64 3.0.2.0 : pcre (EulerOS-SA-2020-1219)

EulerOS Virtualization for ARM 64 3.0.2.0 : perl (EulerOS-SA-2020-1196)

EulerOS Virtualization for ARM 64 3.0.2.0 : perl-File-Path (EulerOS-SA-2020-1187)

EulerOS Virtualization for ARM 64 3.0.2.0 : php (EulerOS-SA-2019-1632)

EulerOS Virtualization for ARM 64 3.0.2.0 : php (EulerOS-SA-2019-1705)

EulerOS Virtualization for ARM 64 3.0.2.0 : php (EulerOS-SA-2019-1928)

EulerOS Virtualization for ARM 64 3.0.2.0 : polkit (EulerOS-SA-2020-1193)

EulerOS Virtualization for ARM 64 3.0.2.0 : python (EulerOS-SA-2019-1626)

EulerOS Virtualization for ARM 64 3.0.2.0 : python (EulerOS-SA-2019-1934)

EulerOS Virtualization for ARM 64 3.0.2.0 : python (EulerOS-SA-2020-1212)

EulerOS Virtualization for ARM 64 3.0.2.0 : python-jinja2 (EulerOS-SA-2019-1619)

EulerOS Virtualization for ARM 64 3.0.2.0 : python-pillow (EulerOS-SA-2019-1709)

EulerOS Virtualization for ARM 64 3.0.2.0 : python-pillow (EulerOS-SA-2020-1244)

EulerOS Virtualization for ARM 64 3.0.2.0 : python-requests (EulerOS-SA-2019-1947)

EulerOS Virtualization for ARM 64 3.0.2.0 : python-urllib3 (EulerOS-SA-2019-1620)

EulerOS Virtualization for ARM 64 3.0.2.0 : python-urllib3 (EulerOS-SA-2019-1936)

EulerOS Virtualization for ARM 64 3.0.2.0 : python-urllib3 (EulerOS-SA-2020-1213)

EulerOS Virtualization for ARM 64 3.0.2.0 : PyYAML (EulerOS-SA-2019-1615)

EulerOS Virtualization for ARM 64 3.0.2.0 : qemu-kvm (EulerOS-SA-2019-1633)

EulerOS Virtualization for ARM 64 3.0.2.0 : qemu-kvm (EulerOS-SA-2020-1266)

EulerOS Virtualization for ARM 64 3.0.2.0 : rpm (EulerOS-SA-2019-1616)

EulerOS Virtualization for ARM 64 3.0.2.0 : rsync (EulerOS-SA-2019-1944)

EulerOS Virtualization for ARM 64 3.0.2.0 : rsync (EulerOS-SA-2020-1257)

EulerOS Virtualization for ARM 64 3.0.2.0 : rsyslog (EulerOS-SA-2020-1218)

EulerOS Virtualization for ARM 64 3.0.2.0 : ruby (EulerOS-SA-2019-1617)

EulerOS Virtualization for ARM 64 3.0.2.0 : ruby (EulerOS-SA-2019-1932)

EulerOS Virtualization for ARM 64 3.0.2.0 : ruby (EulerOS-SA-2020-1195)

EulerOS Virtualization for ARM 64 3.0.2.0 : samba (EulerOS-SA-2019-1618)

EulerOS Virtualization for ARM 64 3.0.2.0 : samba (EulerOS-SA-2019-1708)

EulerOS Virtualization for ARM 64 3.0.2.0 : samba (EulerOS-SA-2019-1921)

EulerOS Virtualization for ARM 64 3.0.2.0 : samba (EulerOS-SA-2020-1231)

EulerOS Virtualization for ARM 64 3.0.2.0 : shadow-utils (EulerOS-SA-2020-1237)

EulerOS Virtualization for ARM 64 3.0.2.0 : sqlite (EulerOS-SA-2019-1713)

EulerOS Virtualization for ARM 64 3.0.2.0 : sqlite (EulerOS-SA-2020-1207)

EulerOS Virtualization for ARM 64 3.0.2.0 : sssd (EulerOS-SA-2019-1701)

EulerOS Virtualization for ARM 64 3.0.2.0 : sssd (EulerOS-SA-2020-1209)

EulerOS Virtualization for ARM 64 3.0.2.0 : sudo (EulerOS-SA-2020-1223)

EulerOS Virtualization for ARM 64 3.0.2.0 : systemd (EulerOS-SA-2019-1923)

EulerOS Virtualization for ARM 64 3.0.2.0 : systemd (EulerOS-SA-2020-1216)

EulerOS Virtualization for ARM 64 3.0.2.0 : tar (EulerOS-SA-2019-1624)

EulerOS Virtualization for ARM 64 3.0.2.0 : tar (EulerOS-SA-2020-1245)

EulerOS Virtualization for ARM 64 3.0.2.0 : unbound (EulerOS-SA-2020-1264)

EulerOS Virtualization for ARM 64 3.0.2.0 : unzip (EulerOS-SA-2019-1627)

EulerOS Virtualization for ARM 64 3.0.2.0 : unzip (EulerOS-SA-2019-1949)

EulerOS Virtualization for ARM 64 3.0.2.0 : unzip (EulerOS-SA-2020-1222)

EulerOS Virtualization for ARM 64 3.0.2.0 : util-linux (EulerOS-SA-2019-1694)

EulerOS Virtualization for ARM 64 3.0.2.0 : util-linux (EulerOS-SA-2020-1243)

EulerOS Virtualization for ARM 64 3.0.2.0 : vim (EulerOS-SA-2019-1699)

EulerOS Virtualization for ARM 64 3.0.2.0 : webkitgtk4 (EulerOS-SA-2020-1199)

EulerOS Virtualization for ARM 64 3.0.2.0 : wget (EulerOS-SA-2019-1707)

EulerOS Virtualization for ARM 64 3.0.2.0 : wget (EulerOS-SA-2020-1202)

EulerOS Virtualization for ARM 64 3.0.2.0 : wpa\_supplicant (EulerOS-SA-2019-1945)

EulerOS Virtualization for ARM 64 3.0.2.0 : xorg-x11-server (EulerOS-SA-2020-1236)

EulerOS Virtualization for ARM 64 3.0.2.0 : zip (EulerOS-SA-2019-1925)

EulerOS Virtualization for ARM 64 3.0.3.0 : avahi (EulerOS-SA-2019-2315)

EulerOS Virtualization for ARM 64 3.0.3.0 : bind (EulerOS-SA-2019-2321)

EulerOS Virtualization for ARM 64 3.0.3.0 : blktrace (EulerOS-SA-2019-2328)

EulerOS Virtualization for ARM 64 3.0.3.0 : coreutils (EulerOS-SA-2019-2333)

EulerOS Virtualization for ARM 64 3.0.3.0 : cups (EulerOS-SA-2019-2346)

EulerOS Virtualization for ARM 64 3.0.3.0 : dhcp (EulerOS-SA-2019-2336)

EulerOS Virtualization for ARM 64 3.0.3.0 : elfutils (EulerOS-SA-2019-2313)

EulerOS Virtualization for ARM 64 3.0.3.0 : file (EulerOS-SA-2019-2317)

EulerOS Virtualization for ARM 64 3.0.3.0 : flac (EulerOS-SA-2019-2327)

EulerOS Virtualization for ARM 64 3.0.3.0 : gd (EulerOS-SA-2019-2335)

EulerOS Virtualization for ARM 64 3.0.3.0 : gettext (EulerOS-SA-2019-2320)

EulerOS Virtualization for ARM 64 3.0.3.0 : ghostscript (EulerOS-SA-2019-2338)

EulerOS Virtualization for ARM 64 3.0.3.0 : git (EulerOS-SA-2019-2310)

EulerOS Virtualization for ARM 64 3.0.3.0 : glib2 (EulerOS-SA-2019-2325)

EulerOS Virtualization for ARM 64 3.0.3.0 : gnupg2 (EulerOS-SA-2019-2349)

EulerOS Virtualization for ARM 64 3.0.3.0 : gnutls (EulerOS-SA-2019-2324)

EulerOS Virtualization for ARM 64 3.0.3.0 : haproxy (EulerOS-SA-2019-2329)

EulerOS Virtualization for ARM 64 3.0.3.0 : httpd (EulerOS-SA-2019-2311)

EulerOS Virtualization for ARM 64 3.0.3.0 : icu (EulerOS-SA-2019-2312)

EulerOS Virtualization for ARM 64 3.0.3.0 : jasper (EulerOS-SA-2019-2332)

EulerOS Virtualization for ARM 64 3.0.3.0 : kernel (EulerOS-SA-2019-2309)

EulerOS Virtualization for ARM 64 3.0.3.0 : lcms2 (EulerOS-SA-2019-2342)

EulerOS Virtualization for ARM 64 3.0.3.0 : libarchive (EulerOS-SA-2019-2322)

EulerOS Virtualization for ARM 64 3.0.3.0 : libidn (EulerOS-SA-2019-2337)

EulerOS Virtualization for ARM 64 3.0.3.0 : libjpeg-turbo (EulerOS-SA-2019-2318)

EulerOS Virtualization for ARM 64 3.0.3.0 : libpng (EulerOS-SA-2019-2331)

EulerOS Virtualization for ARM 64 3.0.3.0 : libsndfile (EulerOS-SA-2019-2351)

EulerOS Virtualization for ARM 64 3.0.3.0 : libtiff (EulerOS-SA-2019-2323)

EulerOS Virtualization for ARM 64 3.0.3.0 : libvorbis (EulerOS-SA-2019-2345)

EulerOS Virtualization for ARM 64 3.0.3.0 : libXfont2 (EulerOS-SA-2019-2347)

EulerOS Virtualization for ARM 64 3.0.3.0 : lua (EulerOS-SA-2019-2339)

EulerOS Virtualization for ARM 64 3.0.3.0 : memcached (EulerOS-SA-2019-2330)

EulerOS Virtualization for ARM 64 3.0.3.0 : net-snmp (EulerOS-SA-2019-2316)

EulerOS Virtualization for ARM 64 3.0.3.0 : nmap (EulerOS-SA-2019-2350)

EulerOS Virtualization for ARM 64 3.0.3.0 : pango (EulerOS-SA-2019-2344)

EulerOS Virtualization for ARM 64 3.0.3.0 : patch (EulerOS-SA-2019-2343)

EulerOS Virtualization for ARM 64 3.0.3.0 : perl (EulerOS-SA-2019-2326)

EulerOS Virtualization for ARM 64 3.0.3.0 : perl-DBD-MySQL (EulerOS-SA-2019-2340)

EulerOS Virtualization for ARM 64 3.0.3.0 : polkit (EulerOS-SA-2019-2314)

EulerOS Virtualization for ARM 64 3.0.3.0 : qemu-kvm (EulerOS-SA-2019-2352)

EulerOS Virtualization for ARM 64 3.0.3.0 : rsync (EulerOS-SA-2019-2334)

EulerOS Virtualization for ARM 64 3.0.3.0 : sqlite (EulerOS-SA-2019-2348)

EulerOS Virtualization for ARM 64 3.0.3.0 : systemd (EulerOS-SA-2019-2319)

EulerOS Virtualization for ARM 64 3.0.3.0 : unbound (EulerOS-SA-2019-2341)

EulerOS Virtualization for ARM 64 3.0.5.0 : bind (EulerOS-SA-2020-1047)

EulerOS Virtualization for ARM 64 3.0.5.0 : binutils (EulerOS-SA-2020-1074)

EulerOS Virtualization for ARM 64 3.0.5.0 : compat-openssl10 (EulerOS-SA-2020-1061)

EulerOS Virtualization for ARM 64 3.0.5.0 : cpio (EulerOS-SA-2020-1056)

EulerOS Virtualization for ARM 64 3.0.5.0 : cronie (EulerOS-SA-2020-1069)

EulerOS Virtualization for ARM 64 3.0.5.0 : curl (EulerOS-SA-2020-1070)

EulerOS Virtualization for ARM 64 3.0.5.0 : elfutils (EulerOS-SA-2020-1055)

EulerOS Virtualization for ARM 64 3.0.5.0 : expat (EulerOS-SA-2020-1075)

EulerOS Virtualization for ARM 64 3.0.5.0 : file (EulerOS-SA-2020-1052)

EulerOS Virtualization for ARM 64 3.0.5.0 : gdb (EulerOS-SA-2020-1088)

EulerOS Virtualization for ARM 64 3.0.5.0 : ghostscript (EulerOS-SA-2020-1059)

EulerOS Virtualization for ARM 64 3.0.5.0 : glibc (EulerOS-SA-2020-1041)

EulerOS Virtualization for ARM 64 3.0.5.0 : grub2 (EulerOS-SA-2020-1045)

EulerOS Virtualization for ARM 64 3.0.5.0 : jasper (EulerOS-SA-2020-1053)

EulerOS Virtualization for ARM 64 3.0.5.0 : kernel (EulerOS-SA-2020-1042)

EulerOS Virtualization for ARM 64 3.0.5.0 : libarchive (EulerOS-SA-2020-1080)

EulerOS Virtualization for ARM 64 3.0.5.0 : libcroco (EulerOS-SA-2020-1076)

EulerOS Virtualization for ARM 64 3.0.5.0 : libgcrypt (EulerOS-SA-2020-1085)

EulerOS Virtualization for ARM 64 3.0.5.0 : libmirage (EulerOS-SA-2020-1090)

EulerOS Virtualization for ARM 64 3.0.5.0 : libpcap (EulerOS-SA-2020-1082)

EulerOS Virtualization for ARM 64 3.0.5.0 : libpng (EulerOS-SA-2020-1078)

EulerOS Virtualization for ARM 64 3.0.5.0 : libsndfile (EulerOS-SA-2020-1066)

EulerOS Virtualization for ARM 64 3.0.5.0 : libssh2 (EulerOS-SA-2020-1089)

EulerOS Virtualization for ARM 64 3.0.5.0 : libtiff (EulerOS-SA-2020-1071)

EulerOS Virtualization for ARM 64 3.0.5.0 : libxslt (EulerOS-SA-2020-1050)

EulerOS Virtualization for ARM 64 3.0.5.0 : lz4 (EulerOS-SA-2020-1057)

EulerOS Virtualization for ARM 64 3.0.5.0 : ncurses (EulerOS-SA-2020-1064)

EulerOS Virtualization for ARM 64 3.0.5.0 : nmap (EulerOS-SA-2020-1081)

EulerOS Virtualization for ARM 64 3.0.5.0 : openjpeg2 (EulerOS-SA-2020-1049)

EulerOS Virtualization for ARM 64 3.0.5.0 : openldap (EulerOS-SA-2020-1077)

EulerOS Virtualization for ARM 64 3.0.5.0 : openssh (EulerOS-SA-2020-1046)

EulerOS Virtualization for ARM 64 3.0.5.0 : openssl (EulerOS-SA-2020-1063)

EulerOS Virtualization for ARM 64 3.0.5.0 : patch (EulerOS-SA-2020-1065)

EulerOS Virtualization for ARM 64 3.0.5.0 : php (EulerOS-SA-2020-1058)

EulerOS Virtualization for ARM 64 3.0.5.0 : python-pillow (EulerOS-SA-2020-1087)

EulerOS Virtualization for ARM 64 3.0.5.0 : python-requests (EulerOS-SA-2020-1043)

EulerOS Virtualization for ARM 64 3.0.5.0 : python-urllib3 (EulerOS-SA-2020-1084)

EulerOS Virtualization for ARM 64 3.0.5.0 : python2 (EulerOS-SA-2020-1044)

EulerOS Virtualization for ARM 64 3.0.5.0 : python3 (EulerOS-SA-2020-1048)

EulerOS Virtualization for ARM 64 3.0.5.0 : PyYAML (EulerOS-SA-2020-1083)

EulerOS Virtualization for ARM 64 3.0.5.0 : qemu-kvm (EulerOS-SA-2020-1091)

EulerOS Virtualization for ARM 64 3.0.5.0 : rsyslog (EulerOS-SA-2020-1060)

EulerOS Virtualization for ARM 64 3.0.5.0 : ruby (EulerOS-SA-2020-1051)

EulerOS Virtualization for ARM 64 3.0.5.0 : samba (EulerOS-SA-2020-1040)

EulerOS Virtualization for ARM 64 3.0.5.0 : spdk (EulerOS-SA-2020-1092)

EulerOS Virtualization for ARM 64 3.0.5.0 : sqlite (EulerOS-SA-2020-1079)

EulerOS Virtualization for ARM 64 3.0.5.0 : sudo (EulerOS-SA-2020-1086)

EulerOS Virtualization for ARM 64 3.0.5.0 : sysstat (EulerOS-SA-2020-1067)

EulerOS Virtualization for ARM 64 3.0.5.0 : systemd (EulerOS-SA-2020-1054)

EulerOS Virtualization for ARM 64 3.0.5.0 : tar (EulerOS-SA-2020-1068)

EulerOS Virtualization for ARM 64 3.0.5.0 : tcpdump (EulerOS-SA-2020-1072)

EulerOS Virtualization for ARM 64 3.0.5.0 : wpa\_supplicant (EulerOS-SA-2020-1073)

EulerOS Virtualization for ARM 64 3.0.5.0 : xorg-x11-server (EulerOS-SA-2020-1062)

EulerOS Virtualization for ARM 64 3.0.6.0 : bash (EulerOS-SA-2020-1343)

EulerOS Virtualization for ARM 64 3.0.6.0 : bind (EulerOS-SA-2020-1355)

EulerOS Virtualization for ARM 64 3.0.6.0 : binutils (EulerOS-SA-2020-1363)

EulerOS Virtualization for ARM 64 3.0.6.0 : cloud-init (EulerOS-SA-2020-1356)

EulerOS Virtualization for ARM 64 3.0.6.0 : compat-openssl10 (EulerOS-SA-2020-1333)

EulerOS Virtualization for ARM 64 3.0.6.0 : curl (EulerOS-SA-2020-1345)

EulerOS Virtualization for ARM 64 3.0.6.0 : cyrus-sasl (EulerOS-SA-2020-1336)

EulerOS Virtualization for ARM 64 3.0.6.0 : e2fsprogs (EulerOS-SA-2020-1347)

EulerOS Virtualization for ARM 64 3.0.6.0 : fribidi (EulerOS-SA-2020-1351)

EulerOS Virtualization for ARM 64 3.0.6.0 : ghostscript (EulerOS-SA-2020-1348)

EulerOS Virtualization for ARM 64 3.0.6.0 : git (EulerOS-SA-2020-1361)

EulerOS Virtualization for ARM 64 3.0.6.0 : glibc (EulerOS-SA-2020-1330)

EulerOS Virtualization for ARM 64 3.0.6.0 : glibc (EulerOS-SA-2020-1369)

EulerOS Virtualization for ARM 64 3.0.6.0 : gnupg2 (EulerOS-SA-2020-1358)

EulerOS Virtualization for ARM 64 3.0.6.0 : gperftools (EulerOS-SA-2020-1366)

EulerOS Virtualization for ARM 64 3.0.6.0 : httpd (EulerOS-SA-2020-1359)

EulerOS Virtualization for ARM 64 3.0.6.0 : httpd (EulerOS-SA-2020-1370)

EulerOS Virtualization for ARM 64 3.0.6.0 : ipmitool (EulerOS-SA-2020-1337)

EulerOS Virtualization for ARM 64 3.0.6.0 : keepalived (EulerOS-SA-2020-1357)

EulerOS Virtualization for ARM 64 3.0.6.0 : kernel (EulerOS-SA-2020-1342)

EulerOS Virtualization for ARM 64 3.0.6.0 : kernel (EulerOS-SA-2020-1368)

EulerOS Virtualization for ARM 64 3.0.6.0 : libarchive (EulerOS-SA-2020-1362)

EulerOS Virtualization for ARM 64 3.0.6.0 : libidn2 (EulerOS-SA-2020-1338)

EulerOS Virtualization for ARM 64 3.0.6.0 : libpng (EulerOS-SA-2020-1334)

EulerOS Virtualization for ARM 64 3.0.6.0 : libssh (EulerOS-SA-2020-1332)

EulerOS Virtualization for ARM 64 3.0.6.0 : openjpeg2 (EulerOS-SA-2020-1365)

EulerOS Virtualization for ARM 64 3.0.6.0 : openldap (EulerOS-SA-2020-1353)

EulerOS Virtualization for ARM 64 3.0.6.0 : openssh (EulerOS-SA-2020-1360)

EulerOS Virtualization for ARM 64 3.0.6.0 : patch (EulerOS-SA-2020-1335)

EulerOS Virtualization for ARM 64 3.0.6.0 : php (EulerOS-SA-2020-1350)

EulerOS Virtualization for ARM 64 3.0.6.0 : python-pip (EulerOS-SA-2020-1354)

EulerOS Virtualization for ARM 64 3.0.6.0 : python-urllib3 (EulerOS-SA-2020-1340)

EulerOS Virtualization for ARM 64 3.0.6.0 : python2 (EulerOS-SA-2020-1344)

EulerOS Virtualization for ARM 64 3.0.6.0 : python3 (EulerOS-SA-2020-1346)

EulerOS Virtualization for ARM 64 3.0.6.0 : PyYAML (EulerOS-SA-2020-1371)

EulerOS Virtualization for ARM 64 3.0.6.0 : qemu-kvm (EulerOS-SA-2020-1367)

EulerOS Virtualization for ARM 64 3.0.6.0 : ruby (EulerOS-SA-2020-1339)

EulerOS Virtualization for ARM 64 3.0.6.0 : samba (EulerOS-SA-2020-1341)

EulerOS Virtualization for ARM 64 3.0.6.0 : sqlite (EulerOS-SA-2020-1364)

EulerOS Virtualization for ARM 64 3.0.6.0 : sudo (EulerOS-SA-2020-1349)

EulerOS Virtualization for ARM 64 3.0.6.0 : systemd (EulerOS-SA-2020-1331)

EulerOS Virtualization for ARM 64 3.0.6.0 : unbound (EulerOS-SA-2020-1352)

Huawei AR Router Remote Command Execution (HWNSIRT-2013-0427)

Huawei Campus Series Switches Remote Buffer Overflow DoS (HWPSIRT-2015-02014)

Huawei Campus Switch DoS (HWPSIRT-2014-0112)

Huawei Campus Switch Information Disclosure (HWNSIRT-2013-0317)

Huawei Campus Switch Multiple Vulnerabilities (HWPSIRT-2014-0315 - HWPSIRT-2014-0318)

Huawei CloudEngine Switch Security Bypass (HWPSIRT-2013-1256)

Huawei Denial-of-Service Vulnerability

Huawei Device DoS (HWPSIRT-2014-0307)

Huawei eSap Platform DoS (HWPSIRT-2014-0111)

Huawei Eudemon8000E Firewall DoS (HWPSIRT-2014-0101)

Huawei Multiple Vulnerabilities

Huawei Quidway Switches DoS (HWPSIRT-2014-0301)

Huawei SSH DoS (HWPSIRT-2014-0701)

Huawei Switch DoS (HWPSIRT-2013-1165)

Huawei Switches Permission Control Privilege Escalation (HWPSIRT-2015-08048)

Huawei VP9610 / 9620 Fixed Session ID (HWNSIRT-2013-0318)

Information Leakage Vulnerability via MPLS Ping in Huawei VRP Platform (HWPSIRT-2014-0418)

Multiple XSRF Vulnerabilities in Huawei Products (HWPSIRT-2014-0406)

SSH Username Information Disclosure Vulnerability in Huawei Campus Series Switches

# HP-UX Local Security Checks

HP-UX PHCO\_14625 : s700\_800 11.00 bdf(1M) patch to skip autofs file systems

HP-UX PHCO\_16629 : s700\_800 11.00 libc cumulative patch

HP-UX PHCO\_17601 : s700\_800 11.00 libc cumulative patch

HP-UX PHCO\_18183 : HPSBUX9907-101 Security Vulnerability Software Distributor (SD) (rev.1)

HP-UX PHCO\_21534 : HPSBUX0005-113 Sec. Vulnerability with shutdown command (rev.1)

HP-UX PHCO\_21567 : HPSBUX0005-113 Sec. Vulnerability with shutdown command (rev.1)

HP-UX PHCO\_21993 : HPSBUX0011-130 Sec. Vulnerability in auto\_parms (rev.2)

HP-UX PHCO\_22096 : HPSBUX0008-118 Sec. Vulnerability in newgrp(1) (rev.1)

HP-UX PHCO\_22186 : HPSBUX0011-130 Sec. Vulnerability in auto\_parms (rev.2)

HP-UX PHCO\_22229 : HPSBUX0102-140 Sec. Vulnerability in Text editors (rev.1)

HP-UX PHCO\_22274 : HPSBUX0010-127 Sec. Vulnerability in bdf(1) + df(1) commands (rev.2)

HP-UX PHCO\_22276 : HPSBUX0010-127 Sec. Vulnerability in bdf(1) + df(1) commands (rev.2)

HP-UX PHCO\_22326 : HPSBUX0010-127 Sec. Vulnerability in bdf(1) + df(1) commands (rev.2)

HP-UX PHCO\_22327 : HPSBUX0010-127 Sec. Vulnerability in bdf(1) + df(1) commands (rev.2)

HP-UX PHCO\_22365 : HPSBUX0010-125 Sec. Vulnerability in lpspooler (rev.1)

HP-UX PHCO\_22526 : HPSBUX0102-143 Sec. Vulnerability in SD-UX (Rev.02)

HP-UX PHCO\_22665 : HPSBUX0012-135 Sec. Vulnerability in kermit(1) (rev.2)

HP-UX PHCO\_22686 : HPSBUX0012-134 Sec. Vulnerability in top(1) (rev.1)

HP-UX PHCO\_22766 : HP-UX cu(1), Local Denial of Service (DoS) (HPSBUX00167 SSRT071384 rev.2)

HP-UX PHCO\_22767 : HPSBUX0103-146 Sec. Vulnerability in crontab(1) (rev.1)

HP-UX PHCO\_22921 : HPSBUX0012-134 Sec. Vulnerability in top(1) (rev.1)

HP-UX PHCO\_23083 : HP-UX newgrp(1), Local Increased Privilege (HPSBUX00147 SSRT071380 rev.2)

HP-UX PHCO\_23088 : HPSBUX0101-138 Sec. Vulnerability in man(1) command (rev.1)

HP-UX PHCO\_23178 : HPSBUX0101-138 Sec. Vulnerability in man(1) command (rev.1)

HP-UX PHCO\_23354 : HPSBUX0102-140 Sec. Vulnerability in Text editors (rev.1)

HP-UX PHCO\_23424 : HP-UX cu(1), Local Denial of Service (DoS) (HPSBUX00167 SSRT071384 rev.2)

HP-UX PHCO\_23429 : HPSBUX0103-146 Sec. Vulnerability in crontab(1) (rev.1)

HP-UX PHCO\_23483 : HPSBUX0102-143 Sec. Vulnerability in SD-UX (Rev.02)

HP-UX PHCO\_23492 : HP-UX running dlkm, Local Unauthorized Increase in Privilege (HPSBUX00159 SSRT071344 rev.3)

HP-UX PHCO\_23900 : HP-UX running login(1), Local Increased Privilege (HPSBUX00160 SSRT071385 rev.3)

HP-UX PHCO\_23909 : HP-UX cu(1), Local Denial of Service (DoS) (HPSBUX00167 SSRT071384 rev.2)

HP-UX PHCO\_24083 : HP-UX running login(1), Local Increased Privilege (HPSBUX00160 SSRT071385 rev.3)

HP-UX PHCO\_24112 : HP-UX kmmodreg (1M), Local Denial of Service (DoS), Increased Privilege (HPSBUX00153 SSRT071381 rev.2)

HP-UX PHCO\_24147 : HP-UX kmmodreg (1M), Local Denial of Service (DoS), Increased Privilege (HPSBUX00153 SSRT071381 rev.2)

HP-UX PHCO\_24197 : HP-UX kmmodreg (1M), Local Denial of Service (DoS), Increased Privilege (HPSBUX00153 SSRT071381 rev.2)

HP-UX PHCO\_24418 : HP-UX running login(1), Local Increased Privilege (HPSBUX00160 SSRT071385 rev.3)

HP-UX PHCO\_24446 : HPSBUX0212-227 Sec. Vulnerability in ied(1)

HP-UX PHCO\_24700 : HP-UX running rlpdaemon, Remote Unauthorized Access, Increased Privilege (HPSBUX00163 SSRT071386 rev.2)

HP-UX PHCO\_24701 : HP-UX running rlpdaemon, Remote Unauthorized Access, Increased Privilege (HPSBUX00163 SSRT071386 rev.2)

HP-UX PHCO\_24723 : HPSBUX0304-257 SSRT3496 Potential Security Vulnerability in rexec

HP-UX PHCO\_24839 : HP-UX passwd(1), Local Denial of Service (DoS) (HPSBUX00191 SSRT071389 rev.2)

HP-UX PHCO\_24852 : HPSBUX0109-166 Sec. Vulnerability in libsecurity (VVOS) (rev.1)

HP-UX PHCO\_24868 : HP-UX running rlpdaemon, Remote Unauthorized Access, Increased Privilege (HPSBUX00163 SSRT071386 rev.2)

HP-UX PHCO\_25110 : HPSBUX0111-176 Sec. Vulnerability in rlpdaemon (rev.1)

HP-UX PHCO\_25111 : HPSBUX0111-176 Sec. Vulnerability in rlpdaemon (rev.1)

HP-UX PHCO\_25527 : HP-UX passwd(1), Local Denial of Service (DoS) (HPSBUX00191 SSRT071389 rev.2)

HP-UX PHCO\_25841 : HP-UX Running Portable File System (PFS), Remote Increase in Privilege (HPSBUX02203 SSRT071339 rev.1)

HP-UX PHCO\_25875 : HP-UX running SD, Local Unauthorized Access, Denial of Service (DoS) (HPSBUX00194 SSRT071391 rev.2)

HP-UX PHCO\_25887 : HP-UX running SD, Local Unauthorized Access, Denial of Service (DoS) (HPSBUX00194 SSRT071391 rev.2)

HP-UX PHCO\_25918 : HP-UX Running sort, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00237 SSRT3454 rev.2)

HP-UX PHCO\_26385 : HP-UX Running newgrp(1), Local Privilege Elevation (HPSBUX01102 SSRT4687 rev.2)

HP-UX PHCO\_26449 : HP-UX Running Portable File System (PFS), Remote Increase in Privilege (HPSBUX02203 SSRT071339 rev.1)

HP-UX PHCO\_26561 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_26904 : HP-UX passwd(1), Local Denial of Service (DoS) (HPSBUX00191 SSRT071389 rev.2)

HP-UX PHCO\_27019 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_27020 : HP-UX LP subsystem, Local Denial of Service (DoS) (HPSBUX00213 SSRT2331 rev.2)

HP-UX PHCO\_27132 : HP-UX LP subsystem, Local Denial of Service (DoS) (HPSBUX00213 SSRT2331 rev.2)

HP-UX PHCO\_27344 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_27345 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_27373 : HPSBUX0208-210 Sec. Vulnerability in VVOS passwd(1) (rev. 2)

HP-UX PHCO\_27418 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_27565 : HP-UX Running sort, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00237 SSRT3454 rev.2)

HP-UX PHCO\_27763 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_28125 : HP-UX Running System Administration Manager (SAM), Local Elevation of Privilege (HPSBUX01104 SSRT4699 rev.3)

HP-UX PHCO\_28425 : HP-UX calloc(3C), Local Denial of Service (DoS) (HPSBUX00310 SSRT2341 rev.2)

HP-UX PHCO\_28427 : HP-UX calloc(3C), Local Denial of Service (DoS) (HPSBUX00310 SSRT2341 rev.2)

HP-UX PHCO\_28467 : HP-UX Running sort, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00237 SSRT3454 rev.2)

HP-UX PHCO\_28480 : s700\_800 11.00 cumulative 10.20 libc compatibility support

HP-UX PHCO\_28481 : s700\_800 11.11 cumulative 10.20 libc compatibility support

HP-UX PHCO\_28718 : HP-UX Running wall(1), Local Privilege Increase, Denial of Service (DoS) (HPSBUX00258 SSRT3483 rev.2)

HP-UX PHCO\_28719 : HP-UX Running wall(1), Local Privilege Increase, Denial of Service (DoS) (HPSBUX00258 SSRT3483 rev.2)

HP-UX PHCO\_28847 : s700\_800 11.00 Software Distributor (SD) Cumulative Patch

HP-UX PHCO\_28848 : s700\_800 11.11 Software Distributor Cumulative Patch

HP-UX PHCO\_28954 : HP-UX Running shar(1), Local Execution of Arbitrary Code (HPSBUX00304 SSRT3639 rev.2)

HP-UX PHCO\_29010 : HP-UX Running shar(1), Local Execution of Arbitrary Code (HPSBUX00304 SSRT3639 rev.2)

HP-UX PHCO\_29043 : HPSBUX0305-260 SSRT3491 Potential Security Vulnerability in ipcs(1) (rev. 1)

HP-UX PHCO\_29085 : HP-UX Running wall(1), Local Privilege Increase, Denial of Service (DoS) (HPSBUX00258 SSRT3483 rev.2)

HP-UX PHCO\_29190 : s700\_800 11.04 (VVOS) libc cumulative patch

HP-UX PHCO\_29208 : HP-UX /usr/lbin/rwrite, Local Denial of Service (DoS) (HPSBUX00312 SSRT3556 rev.2)

HP-UX PHCO\_29209 : HP-UX /usr/lbin/rwrite, Local Denial of Service (DoS) (HPSBUX00312 SSRT3556 rev.2)

HP-UX PHCO\_29249 : s700\_800 11.00 libpam and libpam\_unix cumulative patch

HP-UX PHCO\_29284 : HP-UX NLSPath, Local Increase in Privilege (HPSBUX00294 SSRT3656 rev.2)

HP-UX PHCO\_29329 : HP-UX NLSPath, Local Increase in Privilege (HPSBUX00294 SSRT3656 rev.2)

HP-UX PHCO\_29381 : HP-UX uucp(1) and uusub(1), Local Increase in Privilege (HPSBUX00262 SSRT3461 rev.2)

HP-UX PHCO\_29382 : HP-UX uucp(1) and uusub(1), Local Increase in Privilege (HPSBUX00262 SSRT3461 rev.2)

HP-UX PHCO\_29495 : HP-UX NLSPath, Local Increase in Privilege (HPSBUX00294 SSRT3656 rev.2)

HP-UX PHCO\_29621 : HP-UX Local Elevation of Privilege Related to Directory Permissions (HPSBUX01006 SSRT2320 rev.2)

HP-UX PHCO\_29622 : HP-UX Local Elevation of Privilege Related to Directory Permissions (HPSBUX01006 SSRT2320 rev.2)

HP-UX PHCO\_29682 : HP-UX Running newgrp(1), Local Privilege Elevation (HPSBUX01102 SSRT4687 rev.2)

HP-UX PHCO\_29697 : HP-UX Running shar(1), Local Execution of Arbitrary Code (HPSBUX00304 SSRT3639 rev.2)

HP-UX PHCO\_29698 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_29702 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_29814 : HP-UX Shells, Local Increase of Privilege, Denial of Service (DoS) (HPSBUX00275 SSRT3618 rev.2)

HP-UX PHCO\_30006 : s700\_800 11.04 (VVOS) Software Distributor (SD) Cumulative

HP-UX PHCO\_30191 : HP-UX NLSPath, Local Increase in Privilege (HPSBUX00294 SSRT3656 rev.2)

HP-UX PHCO\_30402 : HP-UX Local Increased Privilege (HPSBUX02091 SSRT061099 rev.2)

HP-UX PHCO\_30407 : HP-UX Running RPC, Remote Unauthorized Access or Denial of Service (DoS) (HPSBUX00252 SSRT2439 rev.13)

HP-UX PHCO\_30519 : HP-UX Local Elevation of Privilege Related to Directory Permissions (HPSBUX01006 SSRT2320 rev.2)

HP-UX PHCO\_32036 : HPSBUX02128 SSRT5996 - rev.1 HP-UX mkdir(1) Local Unauthorized Access

HP-UX PHCO\_32149 : HP-UX passwd(1) Local Denial of Service (DoS) (HPSBUX02103 SSRT5953 rev.3)

HP-UX PHCO\_32280 : s700\_800 11.04 (VVOS) libpam, libpam\_unix cumulative patch

HP-UX PHCO\_32549 : HP-UX Running System Administration Manager (SAM), Local Elevation of Privilege (HPSBUX01104 SSRT4699 rev.3)

HP-UX PHCO\_32926 : s700\_800 11.23 libpam\_unix cumulative patch

HP-UX PHCO\_33142 : HP-UX usermod(1M) Local Unauthorized Access. (HPSBUX02102 SSRT051078 rev.4)

HP-UX PHCO\_33214 : HP-UX passwd(1) Local Denial of Service (DoS) (HPSBUX02103 SSRT5953 rev.3)

HP-UX PHCO\_33215 : s700\_800 11.11 libpam\_unix cumulative patch

HP-UX PHCO\_33219 : HP-UX passwd(1) Local Denial of Service (DoS) (HPSBUX02103 SSRT5953 rev.3)

HP-UX PHCO\_33822 : HP-UX Running Software Distributor (SD) Remote Unauthorized Access (HPSBUX02089 SSRT5983 rev.1)

HP-UX PHCO\_33967 : HP-UX envd, Local Execution of Privileged Code (HPSBUX02073 SSRT051012 rev.2)

HP-UX PHCO\_33989 : HP-UX envd, Local Execution of Privileged Code (HPSBUX02073 SSRT051012 rev.2)

HP-UX PHCO\_34151 : HPSBUX02128 SSRT5996 - rev.1 HP-UX mkdir(1) Local Unauthorized Access

HP-UX PHCO\_34214 : HP-UX in Trusted mode, Local Denial of Service (DoS) (HPSBUX02141 SSRT51153 rev.1)

HP-UX PHCO\_34215 : HP-UX in Trusted mode, Local Denial of Service (DoS) (HPSBUX02141 SSRT51153 rev.1)

HP-UX PHCO\_34533 : HPSBUX02128 SSRT5996 - rev.1 HP-UX mkdir(1) Local Unauthorized Access

HP-UX PHCO\_34539 : HP-UX Running Software Distributor Local Elevation of Privilege (HPSBUX02114 SSRT061115 rev.1)

HP-UX PHCO\_34545 : HP-UX su(1) Local Unauthorized Access (HPSBUX02111 SSRT061132 rev.2)

HP-UX PHCO\_34568 : HP-UX Running Software Distributor Local Elevation of Privilege (HPSBUX02114 SSRT061115 rev.1)

HP-UX PHCO\_34763 : HP-UX usermod(1M) Local Unauthorized Access. (HPSBUX02102 SSRT051078 rev.4)

HP-UX PHCO\_34764 : HP-UX usermod(1M) Local Unauthorized Access. (HPSBUX02102 SSRT051078 rev.4)

HP-UX PHCO\_34806 : HP-UX in Trusted mode, Local Denial of Service (DoS) (HPSBUX02141 SSRT51153 rev.1)

HP-UX PHCO\_34814 : HP-UX Running Software Distributor Local Elevation of Privilege (HPSBUX02114 SSRT061115 rev.1)

HP-UX PHCO\_34929 : HP-UX passwd(1) Local Denial of Service (DoS) (HPSBUX02103 SSRT5953 rev.3)

HP-UX PHCO\_35040 : HPSBUX02128 SSRT5996 - rev.1 HP-UX mkdir(1) Local Unauthorized Access

HP-UX PHCO\_35587 : HP-UX Running Software Distributor (SD), Remote Denial of Service (DoS) (HPSBUX02195 SSRT061237 rev.1)

HP-UX PHCO\_36003 : HP-UX Running logins(1M), Remote Unauthorized Access (HPSBUX02259 SSRT071439 rev.1)

HP-UX PHCO\_36562 : HP-UX Running System Administration Manager (SAM), Unintended Remote Access (HPSBUX02286 SSRT071466 rev.1)

HP-UX PHCO\_36563 : HP-UX Running System Administration Manager (SAM), Unintended Remote Access (HPSBUX02286 SSRT071466 rev.1)

HP-UX PHCO\_36808 : HP-UX Running logins(1M), Remote Unauthorized Access (HPSBUX02259 SSRT071439 rev.1)

HP-UX PHCO\_36809 : HP-UX Running logins(1M), Remote Unauthorized Access (HPSBUX02259 SSRT071439 rev.1)

HP-UX PHCO\_36953 : HP-UX Running useradd(1M), Local Unauthorized Access (HPSBUX02335 SSRT071454 rev.2)

HP-UX PHCO\_37290 : HP-UX Running useradd(1M), Local Unauthorized Access (HPSBUX02335 SSRT071454 rev.2)

HP-UX PHCO\_37291 : HP-UX Running useradd(1M), Local Unauthorized Access (HPSBUX02335 SSRT071454 rev.2)

HP-UX PHCO\_38048 : HP-UX Using libc, Remote Denial of Service (DoS) (HPSBUX02355 SSRT080023 rev.2)

HP-UX PHCO\_38273 : HP-UX Using libc, Remote Denial of Service (DoS) (HPSBUX02355 SSRT080023 rev.2)

HP-UX PHCO\_38491 : HPUX Running useradd(1M), Local Unauthorized Access (HPSBUX02366 SSRT080120 rev.2)

HP-UX PHCO\_38492 : HPUX Running useradd(1M), Local Unauthorized Access (HPSBUX02366 SSRT080120 rev.2)

HP-UX PHCO\_38547 : HPUX Running useradd(1M), Local Unauthorized Access (HPSBUX02366 SSRT080120 rev.2)

HP-UX PHCO\_38913 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHCO\_39027 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHCO\_39103 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHCO\_39104 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHCO\_39124 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHCO\_39132 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHCO\_40131 : HP-UX Running Role-Based Access Control (RBAC), Local Unauthorized Access (HPSBUX02457 SSRT090174 rev.1)

HP-UX PHCO\_40518 : HP-UX Running VRTSweb, Remote Execution of Arbitrary Code, Increase of Privilege (HPSBUX02480 SSRT090253 rev.1)

HP-UX PHCO\_40519 : HP-UX Running VRTSweb, Remote Execution of Arbitrary Code, Increase of Privilege (HPSBUX02480 SSRT090253 rev.1)

HP-UX PHCO\_40520 : HP-UX Running VRTSweb, Remote Execution of Arbitrary Code, Increase of Privilege (HPSBUX02480 SSRT090253 rev.1)

HP-UX PHCO\_41200 : HP-UX running Software Distributor (sd), Local Privilege Increase, Unauthorized Access (HPSBUX02552 SSRT100062 rev.1)

HP-UX PHCO\_41201 : HP-UX running Software Distributor (sd), Local Privilege Increase, Unauthorized Access (HPSBUX02552 SSRT100062 rev.1)

HP-UX PHCO\_41202 : HP-UX running Software Distributor (sd), Local Privilege Increase, Unauthorized Access (HPSBUX02552 SSRT100062 rev.1)

HP-UX PHCO\_42173 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42175 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42176 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42177 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42178 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42179 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42180 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42181 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42182 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42316 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_42317 : HP-UX running VEA, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02700 SSRT100506 rev.2)

HP-UX PHCO\_43835 : s700\_800 11.31 m4(1) cumulative patch

HP-UX PHCO\_43843 : s700\_800 11.23 m4(1) cumulative patch

HP-UX PHCO\_43873 : s700\_800 11.11 libpam\_updbe patch

HP-UX PHCO\_43874 : s700\_800 11.23 libpam\_updbe cumulative patch

HP-UX PHCO\_43875 : s700\_800 11.31 libpam\_updbe patch

HP-UX PHCO\_43917 : s700\_800 11.11 m4(1) cumulative patch

HP-UX PHKL\_15689 : s700\_800 11.0 AutoFS support patch

HP-UX PHKL\_22932 : HP-UX Filesystem Deadlock, Local Denial of Service (DoS) (HPSBUX00178 SSRT071361 rev.2)

HP-UX PHKL\_23335 : HP-UX Filesystem Deadlock, Local Denial of Service (DoS) (HPSBUX00178 SSRT071361 rev.2)

HP-UX PHKL\_23423 : HP-UX Running setrlimit(1M), Denial of Service (DoS) (HPSBUX00156 SSRT071363 rev.3)

HP-UX PHKL\_23628 : HP-UX Running setrlimit(1M), Denial of Service (DoS) (HPSBUX00156 SSRT071363 rev.3)

HP-UX PHKL\_23886 : HP-UX Running setrlimit(1M), Denial of Service (DoS) (HPSBUX00156 SSRT071363 rev.3)

HP-UX PHKL\_24201 : HPSBUX0210-223 Security Vulnerability with OnlineJFS 3.1 (rev. 1)

HP-UX PHKL\_25033 : HP-UX Filesystem Deadlock, Local Denial of Service (DoS) (HPSBUX00178 SSRT071361 rev.2)

HP-UX PHKL\_26233 : HP-UX, Local Denial of Service (DoS) (HPSBUX00183 SSRT071370 rev.2)

HP-UX PHKL\_26269 : HP-UX Running Portable File System (PFS), Remote Increase in Privilege (HPSBUX02203 SSRT071339 rev.1)

HP-UX PHKL\_26450 : HP-UX Running Portable File System (PFS), Remote Increase in Privilege (HPSBUX02203 SSRT071339 rev.1)

HP-UX PHKL\_27179 : HP-UX running ptrace(2), Local Denial of Service (DoS) (HPSBUX00206 SSRT071397 rev.2)

HP-UX PHKL\_27180 : HP-UX running ptrace(2), Local Denial of Service (DoS) (HPSBUX00206 SSRT071397 rev.2)

HP-UX PHKL\_27536 : HP-UX running ptrace(2), Local Denial of Service (DoS) (HPSBUX00206 SSRT071397 rev.2)

HP-UX PHKL\_27932 : HPSBUX0210-223 Security Vulnerability with OnlineJFS 3.1 (rev. 1)

HP-UX PHKL\_28025 : HP-UX Running Portable File System (PFS), Remote Increase in Privilege (HPSBUX02203 SSRT071339 rev.1)

HP-UX PHKL\_28060 : HP-UX Running Portable File System (PFS), Remote Increase in Privilege (HPSBUX02203 SSRT071339 rev.1)

HP-UX PHKL\_28401 : HPSBUX0303-247 SSRT3517 Sec. Vulnerability in VVOS HFS file system

HP-UX PHKL\_29896 : HPSBUX01218 SSRT4702 rev 2. - HP-UX Running Veritas VxFS 3.3/3.5, Local Unauthorized Access

HP-UX PHKL\_31500 : s700\_800 11.23 Sept04 base patch

HP-UX PHKL\_32669 : HPSBUX01218 SSRT4702 rev 2. - HP-UX Running Veritas VxFS 3.3/3.5, Local Unauthorized Access

HP-UX PHKL\_33285 : HPSBUX01218 SSRT4702 rev 2. - HP-UX Running Veritas VxFS 3.3/3.5, Local Unauthorized Access

HP-UX PHKL\_33713 : HP-UX Running on Itanium Platforms Local Denial of Service (DoS) (HPSBUX01233 SSRT5975 rev.2)

HP-UX PHKL\_33714 : HP-UX Running on Itanium Platforms Local Denial of Service (DoS) (HPSBUX01233 SSRT5975 rev.2)

HP-UX PHKL\_34192 : HPSBUX02127 SSRT051056 - rev.1 HP-UX Kernel Local Denial of Service (DoS)

HP-UX PHKL\_34193 : HPSBUX02127 SSRT051056 - rev.1 HP-UX Kernel Local Denial of Service (DoS)

HP-UX PHKL\_34194 : HPSBUX02127 SSRT051056 - rev.1 HP-UX Kernel Local Denial of Service (DoS)

HP-UX PHKL\_34406 : HP-UX Local Denial of Service (DoS) (HPSBUX02120 SSRT051057 rev.2)

HP-UX PHKL\_34940 : HP-UX Local Denial of Service (DoS) (HPSBUX02120 SSRT051057 rev.2)

HP-UX PHKL\_38795 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHKL\_38987 : HP-UX, Local Denial of Service (DoS) (HPSBUX02389 SSRT080141 rev.1)

HP-UX PHKL\_39029 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHKL\_39130 : HP-UX Running VERITAS File System (VRTSvxfs) or VERITAS Oracle Disk Manager (VRTSodm), Local Escalation of Privilege (HPSBUX02409 SSRT080171 rev.3)

HP-UX PHKL\_39133 : HP-UX Running Threaded Processes, Remote Denial of Service (DoS) (HPSBUX02611 SSRT090201 rev.1)

HP-UX PHKL\_39899 : HP-UX Running Threaded Processes, Remote Denial of Service (DoS) (HPSBUX02611 SSRT090201 rev.1)

HP-UX PHKL\_40197 : HP-UX ttrace(2), Local Denial of Service (DoS) (HPSBUX02450 SSRT090141 rev1)

HP-UX PHKL\_40845 : HP-UX running AudFilter rules enabled, Local Denial of Service (DoS) (HPSBUX02514 SSRT100010 rev.1)

HP-UX PHKL\_40888 : HP-UX, Local Denial of Service (DoS) (HPSBUX02518 SSRT100051 rev.1)

HP-UX PHKL\_40944 : HP-UX Running Threaded Processes, Remote Denial of Service (DoS) (HPSBUX02611 SSRT090201 rev.1)

HP-UX PHKL\_41944 : HP-UX, Local Denial of Service (DoS) (HPSBUX02646 SSRT100396 rev.1)

HP-UX PHKL\_41945 : HP-UX, Local Denial of Service (DoS) (HPSBUX02646 SSRT100396 rev.1)

HP-UX PHKL\_44278 : s700\_800 11.31 vm cumulative patch

HP-UX PHKL\_44285 : s700\_800 11.23 exec(2) cumulative patch

HP-UX PHKL\_44305 : s700\_800 11.11 exec(2) patch

HP-UX PHNE\_12957 : s700\_800 11.00 Bind 4.9.7 components

HP-UX PHNE\_14017 : s700\_800 11.00 cumulative ARPA Transport patch

HP-UX PHNE\_14479 : s700\_800 11.00 ftpd(1M) and ftp(1) patch

HP-UX PHNE\_16091 : s700\_800 11.00 r-commands cumulative patch

HP-UX PHNE\_16295 : s700\_800 11.00 vacation patch.

HP-UX PHNE\_16470 : s700\_800 11.0 ONC cumulative patch

HP-UX PHNE\_17030 : HP-UX Trusted System, Remote Unauthorized Access (HPSBUX01165 SSRT5899 rev.2)

HP-UX PHNE\_17190 : s700\_800 11.00 sendmail(1m) 8.8.6 patch

HP-UX PHNE\_17949 : s700\_800 11.00 Domain Management (DESMS B.01.12)

HP-UX PHNE\_18017 : s700\_800 11.00 Domain Management (DESMS-NS B.01.11)

HP-UX PHNE\_18377 : HPSBUX9912-106 Security Vulnerability in wu-ftp (rev.2)

HP-UX PHNE\_20371 : HPSBUX9910-104 Sec. Vulnerability regarding automountd (rev. 02)

HP-UX PHNE\_20619 : HPSBUX0005-114 Sec. Vulnerability in BIND (rev.1)

HP-UX PHNE\_20681 : HPSBUX9912-106 Security Vulnerability in wu-ftp (rev.2)

HP-UX PHNE\_21090 : HPSBUX0005-114 Sec. Vulnerability in BIND (rev.1)

HP-UX PHNE\_21155 : HPSBUX0010-123 Sec. Vulnerability in net.init (rev.1)

HP-UX PHNE\_21261 : HPSBUX0004-112 Sec. Vulnerability with VirtualVault (rev.1)

HP-UX PHNE\_21767 : HPSBUX0010-123 Sec. Vulnerability in net.init (rev.1)

HP-UX PHNE\_21835 : HPSBUX0101-136 Sec. Vulnerability in inetd(1M) (rev.1)

HP-UX PHNE\_21936 : HPSBUX0007-117 Sec. Vulnerability in ftpd (rev.5)

HP-UX PHNE\_22060 : HPSBUX0007-117 Sec. Vulnerability in ftpd (rev.5)

HP-UX PHNE\_22722 : HP-UX running xntpd(1M), Remote Execution of Arbitrary Commands, Increased Privilege (HPSBUX00148 SSRT071379 rev.4)

HP-UX PHNE\_22919 : HP-UX running BIND, Remote Denial of Service (DoS) (HPSBUX00144 SSRT071378 rev.2)

HP-UX PHNE\_23068 : HPSBUX0101-136 Sec. Vulnerability in inetd(1M) (rev.1)

HP-UX PHNE\_23274 : HP-UX running BIND, Remote Denial of Service (DoS) (HPSBUX00144 SSRT071378 rev.2)

HP-UX PHNE\_23275 : HP-UX running BIND, Remote Denial of Service (DoS) (HPSBUX00144 SSRT071378 rev.2)

HP-UX PHNE\_23697 : HP-UX running xntpd(1M), Remote Execution of Arbitrary Commands, Increased Privilege (HPSBUX00148 SSRT071379 rev.4)

HP-UX PHNE\_23949 : s700\_800 11.00 ftpd(1M) and ftp(1) patch

HP-UX PHNE\_23950 : HP-UX Running ftp and ftpd, Remote Unauthorized Access (HPSBUX00162 SSRT4883 rev.4)

HP-UX PHNE\_24034 : HP-UX Running rpcbind Software, Denial of Service (DoS) (HPSBUX00169 SSRT071366 rev.3)

HP-UX PHNE\_24035 : HP-UX Running rpcbind Software, Denial of Service (DoS) (HPSBUX00169 SSRT071366 rev.3)

HP-UX PHNE\_24077 : HP-UX running xntpd(1M), Remote Execution of Arbitrary Commands, Increased Privilege (HPSBUX00148 SSRT071379 rev.4)

HP-UX PHNE\_24164 : s700\_800 11.X CIFS/9000 Server A.01.06 Cumulative Patch

HP-UX PHNE\_24395 : s700\_800 11.04 (VVOS) ftpd(1M) and ftp(1) patch

HP-UX PHNE\_24419 : HP-UX running sendmail(1M), Remote Unauthorized Access (HPSBUX00179 SSRT071387 rev.3)

HP-UX PHNE\_24512 : HP-UX running xntpd, Remote Denial of Service (DoS) (HPSBUX00232 SSRT2370 rev.2)

HP-UX PHNE\_24715 : HPSBUX0309-283 SSRT3637 Potential Security Vulnerability in socket programs

HP-UX PHNE\_25077 : HP-UX Running rpcbind Software, Denial of Service (DoS) (HPSBUX00169 SSRT071366 rev.3)

HP-UX PHNE\_25184 : HP-UX running sendmail(1M), Remote Unauthorized Access (HPSBUX00179 SSRT071387 rev.3)

HP-UX PHNE\_25644 : s700\_800 11.11 cumulative ARPA Transport patch

HP-UX PHNE\_25984 : HP-UX running sendmail(1M), Remote Unauthorized Access (HPSBUX00179 SSRT071387 rev.3)

HP-UX PHNE\_26076 : HP-UX TCP/IP Remote Denial of Service (DoS) (HPSBUX01164 SSRT4884 rev.9)

HP-UX PHNE\_26101 : HP-UX Running ARPA Transport, Advisory, RFC 1948 ISN Randomization (HPSBUX00205 SSRT080009 rev.3)

HP-UX PHNE\_26125 : HP-UX TCP/IP Remote Denial of Service (DoS) (HPSBUX01164 SSRT4884 rev.9)

HP-UX PHNE\_26771 : HP-UX Running ARPA Transport, Advisory, RFC 1948 ISN Randomization (HPSBUX00205 SSRT080009 rev.3)

HP-UX PHNE\_26988 : HP-UX Running Advanced Server/9000 for HP-UX (AS/U) RFC-Netbios, Remote Denial of Service (DoS) (HPSBUX00198 SSRT071359 rev.2)

HP-UX PHNE\_27223 : HP-UX running xntpd, Remote Denial of Service (DoS) (HPSBUX00232 SSRT2370 rev.2)

HP-UX PHNE\_27442 : HP-UX running xntpd, Remote Denial of Service (DoS) (HPSBUX00232 SSRT2370 rev.2)

HP-UX PHNE\_27703 : HP-UX, Remote Execution of Arbitrary Code, Denial of Service (DoS) from Network Traffic (HPSBUX00271 SSRT2443 rev.3)

HP-UX PHNE\_27795 : HP-UX DNS and Resolver Libraries, Remote Execution of Arbitrary Code, Denial of Service (DoS) (HPSBUX00209 SSRT2316 rev.17)

HP-UX PHNE\_27796 : HP-UX DNS and Resolver Libraries, Remote Execution of Arbitrary Code, Denial of Service (DoS) (HPSBUX00209 SSRT2316 rev.17)

HP-UX PHNE\_27881 : HP-UX DNS and Resolver Libraries, Remote Execution of Arbitrary Code, Denial of Service (DoS) (HPSBUX00209 SSRT2316 rev.17)

HP-UX PHNE\_27902 : HP-UX, Remote Execution of Arbitrary Code, Denial of Service (DoS) from Network Traffic (HPSBUX00271 SSRT2443 rev.3)

HP-UX PHNE\_28102 : s700\_800 11.00 ONC/NFS General Release/Performance Patch

HP-UX PHNE\_28103 : s700\_800 11.11 ONC/NFS General Release/Performance Patch

HP-UX PHNE\_28138 : s700\_800 11.22 ONC/NFS General Release/Performance Patch

HP-UX PHNE\_28143 : HPSBUX0305-261 SSRT3451 Potential Security Vulnerability in HP-UX network drivers (Data Leakage) (rev. 01)

HP-UX PHNE\_28299 : HP-UX DNS and Resolver Libraries, Remote Execution of Arbitrary Code, Denial of Service (DoS) (HPSBUX00209 SSRT2316 rev.17)

HP-UX PHNE\_28409 : s700\_800 11.22 sendmail(1m) 8.11.1 patch

HP-UX PHNE\_28444 : HP-UX PHNE\_26413 and PHNE\_27128, Local Denial of Service (DoS) (HPSBUX00270 SSRT3585 rev.3)

HP-UX PHNE\_28449 : s700\_800 11.00 Bind 4.9.7 components

HP-UX PHNE\_28450 : s700\_800 11.11 Bind 8.1.2 Patch

HP-UX PHNE\_28490 : HP-UX DNS and Resolver Libraries, Remote Execution of Arbitrary Code, Denial of Service (DoS) (HPSBUX00209 SSRT2316 rev.17)

HP-UX PHNE\_28538 : HP-UX Running on HP9000 Series 700/800, Denial of Service (DoS) (HPSBUX00264 SSRT3460 rev.5)

HP-UX PHNE\_28636 : HPSBUX0305-261 SSRT3451 Potential Security Vulnerability in HP-UX network drivers (Data Leakage) (rev. 01)

HP-UX PHNE\_28828 : HP-UX Running tftpd, Remote Denial of Service (HPSBUX00266 SSRT3487 rev.6)

HP-UX PHNE\_28895 : HP-UX Running on HP9000 Series 700/800, Denial of Service (DoS) (HPSBUX00264 SSRT3460 rev.5)

HP-UX PHNE\_28982 : HP-UX Running RPC, Remote Unauthorized Access or Denial of Service (DoS) (HPSBUX00252 SSRT2439 rev.13)

HP-UX PHNE\_28983 : HP-UX Running RPC, Remote Unauthorized Access or Denial of Service (DoS) (HPSBUX00252 SSRT2439 rev.13)

HP-UX PHNE\_29210 : s700\_800 11.00 ONC/NFS General Release/Performance Patch

HP-UX PHNE\_29211 : s700\_800 11.11 ONC/NFS General Release/Performance Patch

HP-UX PHNE\_29231 : HP-UX PHNE\_26413 and PHNE\_27128, Local Denial of Service (DoS) (HPSBUX00270 SSRT3585 rev.3)

HP-UX PHNE\_29244 : HPSBUX0305-261 SSRT3451 Potential Security Vulnerability in HP-UX network drivers (Data Leakage) (rev. 01)

HP-UX PHNE\_29267 : HPSBUX0305-261 SSRT3451 Potential Security Vulnerability in HP-UX network drivers (Data Leakage) (rev. 01)

HP-UX PHNE\_29449 : s700\_800 11.22 ONC/NFS General Release/Performance Patch

HP-UX PHNE\_29453 : HP-UX Running on HP9000 Series 700/800, Denial of Service (DoS) (HPSBUX00264 SSRT3460 rev.5)

HP-UX PHNE\_29460 : s700\_800 11.00 ftpd(1M) and ftp(1) patch

HP-UX PHNE\_29461 : s700\_800 11.11 ftpd(1M) and ftp(1) patch

HP-UX PHNE\_29462 : s700\_800 11.22 ftpd(1M) and ftp(1) patch

HP-UX PHNE\_29473 : HP-UX Running ARPA Transport, Local Denial of Service (DoS) (HPSBUX01054 SSRT3552 rev.2)

HP-UX PHNE\_29525 : HP-UX, Remote Execution of Arbitrary Code, Denial of Service (DoS) from Network Traffic (HPSBUX00271 SSRT2443 rev.3)

HP-UX PHNE\_29526 : s700\_800 11.04 (VVOS) sendmail(1m) 8.9.3 patch

HP-UX PHNE\_29634 : s700\_800 11.04 (VVOS) Bind 4.9.7 components

HP-UX PHNE\_29783 : HP-UX Running rpc.ypupdated, Remote Unauthorized Access (HPSBUX01002 SSRT4688 rev.2)

HP-UX PHNE\_29785 : HP-UX Running rpc.ypupdated, Remote Unauthorized Access (HPSBUX01002 SSRT4688 rev.2)

HP-UX PHNE\_29887 : HP-UX Running ARPA Transport, Local Denial of Service (DoS) (HPSBUX01054 SSRT3552 rev.2)

HP-UX PHNE\_29912 : HP-UX sendmail, Remote Unauthorized Privileged Access (HPSBUX00281 SSRT3631 rev.11)

HP-UX PHNE\_30068 : HP-UX Running Bind 8.1.2, Remote Denial of Service (DoS) (HPSBUX00303 SSRT3653 rev.2)

HP-UX PHNE\_30084 : HP-UX Running rpc.ypupdated, Remote Unauthorized Access (HPSBUX01002 SSRT4688 rev.2)

HP-UX PHNE\_30090 : HP-UX Running RPC, Remote Denial of Service (DoS) (HPSBUX01020 SSRT2384 rev.2)

HP-UX PHNE\_30091 : HP-UX Running RPC, Remote Denial of Service (DoS) (HPSBUX01020 SSRT2384 rev.2)

HP-UX PHNE\_30092 : HP-UX Running RPC, Remote Denial of Service (DoS) (HPSBUX01020 SSRT2384 rev.2)

HP-UX PHNE\_30093 : HP-UX Running RPC, Remote Denial of Service (DoS) (HPSBUX01020 SSRT2384 rev.2)

HP-UX PHNE\_30094 : HP-UX Running RPC, Remote Denial of Service (DoS) (HPSBUX01020 SSRT2384 rev.2)

HP-UX PHNE\_30095 : HP-UX Running rpc.ypupdated, Remote Unauthorized Access (HPSBUX01002 SSRT4688 rev.2)

HP-UX PHNE\_30161 : HP-UX running TCP/IP Remote Denial of Service (DoS) (HPSBUX02087 SSRT4728 rev.5)

HP-UX PHNE\_30168 : HP-UX Running RPC, Remote Unauthorized Access or Denial of Service (DoS) (HPSBUX00252 SSRT2439 rev.13)

HP-UX PHNE\_30224 : HP-UX sendmail, Remote Unauthorized Privileged Access (HPSBUX00281 SSRT3631 rev.11)

HP-UX PHNE\_30589 : HP-UX Running tftpd, Remote Denial of Service (HPSBUX00266 SSRT3487 rev.6)

HP-UX PHNE\_30808 : HP-UX Running RPC, Remote Denial of Service (DoS) (HPSBUX01020 SSRT2384 rev.2)

HP-UX PHNE\_30905 : HP-UX Running ARPA Transport, Local Denial of Service (DoS) (HPSBUX01054 SSRT3552 rev.2)

HP-UX PHNE\_30983 : s700\_800 11.23 ftpd(1M) patch

HP-UX PHNE\_30989 : HP-UX ftpd, Remote Unauthorized Access (HPSBUX01119 SSRT4694 rev.2)

HP-UX PHNE\_30990 : HP-UX ftpd, Remote Unauthorized Access (HPSBUX01119 SSRT4694 rev.2)

HP-UX PHNE\_31034 : s700\_800 11.04 (VVOS) ftpd(1M) and ftp(1) patch

HP-UX PHNE\_31726 : HP-UX Running BIND v920, Remote Denial of Service (DoS) (HPSBUX00290 SSRT3622 rev.5)

HP-UX PHNE\_31732 : HP-UX Running wu-ftpd Local Unauthorized Access (HPSBUX01059 SSRT4704 rev.4)

HP-UX PHNE\_32006 : HP-UX Running sendmail, Remote Execution of Arbitrary Code (HPSBUX02108 SSRT061133 rev.15)

HP-UX PHNE\_32443 : HP-UX Running BIND v9.2.0, Remote Denial of Service (DoS) (HPSBUX01117 SSRT4861 rev.2)

HP-UX PHNE\_32449 : HP-UX Running tftpd, Remote Denial of Service (HPSBUX00266 SSRT3487 rev.6)

HP-UX PHNE\_32606 : s700\_800 11.23 cumulative ARPA Transport patch

HP-UX PHNE\_32813 : HP-UX ftpd, Remote Unauthorized Access (HPSBUX01119 SSRT4694 rev.2)

HP-UX PHNE\_33159 : s700\_800 11.11 cumulative ARPA Transport patch

HP-UX PHNE\_33395 : HP-UX TCP/IP Remote Denial of Service (DoS) (HPSBUX01164 SSRT4884 rev.9)

HP-UX PHNE\_33406 : HP-UX Running ftpd Remote Denial of Service (DoS) (HPSBUX02092 SSRT5971 rev.2)

HP-UX PHNE\_33412 : HP-UX Running ftpd Remote Denial of Service (DoS) (HPSBUX02092 SSRT5971 rev.2)

HP-UX PHNE\_33414 : HP-UX Running ftpd Remote Denial of Service (DoS) (HPSBUX02092 SSRT5971 rev.2)

HP-UX PHNE\_33427 : s700\_800 11.04 (VVOS) cumulative ARPA Transport patch

HP-UX PHNE\_33508 : HP-UX running SLP, Remote Unauthorized Access (HPSBUX02129 SSRT061149 rev.2)

HP-UX PHNE\_33790 : s700\_800 11.00 r-commands cumulative mega-patch

HP-UX PHNE\_33791 : s700\_800 11.11 r-commands cumulative mega-patch

HP-UX PHNE\_33792 : s700\_800 11.23 r-commands cumulative mega-patch

HP-UX PHNE\_34009 : HP-UX running X.25 Local Denial of Service (Dos) (HPSBUX02126 SSRT051019 rev.1)

HP-UX PHNE\_34077 : HP-UX Running ftpd Remote Denial of Service (DoS) (HPSBUX02092 SSRT5971 rev.2)

HP-UX PHNE\_34131 : HP-UX running TCP/IP Remote Denial of Service (DoS) (HPSBUX02087 SSRT4728 rev.5)

HP-UX PHNE\_34306 : HP-UX Running wu-ftpd Remote Denial of Service (DoS) (HPSBUX02110 SSRT061110 rev.1)

HP-UX PHNE\_34543 : HP-UX Running wu-ftpd Remote Denial of Service (DoS) (HPSBUX02110 SSRT061110 rev.1)

HP-UX PHNE\_34544 : HP-UX Running wu-ftpd Remote Denial of Service (DoS) (HPSBUX02110 SSRT061110 rev.1)

HP-UX PHNE\_34671 : HP-UX Running ARPA Transport Software, Local Denial of Service (DoS) (HPSBUX02151 SSRT051021 rev.1)

HP-UX PHNE\_34672 : HP-UX Running ARPA Transport Software, Local Denial of Service (DoS) (HPSBUX02151 SSRT051021 rev.1)

HP-UX PHNE\_34689 : HP-UX Sendmail MIME Remote Denial of Service (DoS) (HPSBUX02124 SSRT061159 rev.2)

HP-UX PHNE\_34900 : HP-UX Sendmail MIME Remote Denial of Service (DoS) (HPSBUX02124 SSRT061159 rev.2)

HP-UX PHNE\_34927 : s700\_800 11.04 (VVOS) sendmail(1m) 8.9.3 patch

HP-UX PHNE\_34936 : HP-UX Sendmail MIME Remote Denial of Service (DoS) (HPSBUX02124 SSRT061159 rev.2)

HP-UX PHNE\_34988 : HP-UX running X.25 Local Denial of Service (Dos) (HPSBUX02126 SSRT051019 rev.1)

HP-UX PHNE\_34999 : HP-UX running X.25 Local Denial of Service (Dos) (HPSBUX02126 SSRT051019 rev.1)

HP-UX PHNE\_35146 : HP-UX Running the LP Subsystem, remote Denial of Service (DoS) (HPSBUX02139 SSRT5981 rev.1)

HP-UX PHNE\_35182 : HP-UX Running ARPA Transport, Local Denial of Service (DoS) (HPSBUX02192 SSRT061233 rev.1)

HP-UX PHNE\_35183 : HP-UX Running ARPA Transport, Local Denial of Service (DoS) (HPSBUX02192 SSRT061233 rev.1)

HP-UX PHNE\_35351 : s700\_800 11.11 cumulative ARPA Transport patch

HP-UX PHNE\_35352 : HP-UX Running ARPA Transport, Remote Denial of Service (DoS) (HPSBUX02248 SSRT071437 rev.1)

HP-UX PHNE\_35483 : s700\_800 11.00 sendmail(1M) 8.9.3 patch

HP-UX PHNE\_35484 : s700\_800 11.11 sendmail(1M) 8.9.3 patch

HP-UX PHNE\_35485 : s700\_800 11.23 sendmail(1M) 8.11.1 patch

HP-UX PHNE\_35729 : HP-UX Running ARPA Transport, Local Denial of Service (DoS) (HPSBUX02205 SSRT061120 rev.1)

HP-UX PHNE\_35766 : s700\_800 11.23 cumulative ARPA Transport patch

HP-UX PHNE\_35920 : HP-UX Running BIND, Remote Denial of Service (DoS) (HPSBUX02219 SSRT061273 rev.1)

HP-UX PHNE\_36168 : HP-UX Running rpc.yppasswdd, Remote Denial of Service (DoS) (HPSBUX02295 SSRT071333 rev.1)

HP-UX PHNE\_36185 : HP-UX Running BIND 8, Remote DNS Cache Poisoning (HPSBUX02289 SSRT071461 rev.1)

HP-UX PHNE\_36192 : HP-UX Running ftp, Remote Denial of Service (DoS) (HPSBUX02334 SSRT071403 rev.2)

HP-UX PHNE\_36193 : HP-UX Running ftp, Remote Denial of Service (DoS) (HPSBUX02334 SSRT071403 rev.2)

HP-UX PHNE\_36260 : HP-UX Running rpc.yppasswdd, Remote Denial of Service (DoS) (HPSBUX02295 SSRT071333 rev.1)

HP-UX PHNE\_36281 : HP-UX Running ARPA Transport, Remote Denial of Service (DoS) (HPSBUX02306 SSRT071463 rev.2)

HP-UX PHNE\_36449 : HP-UX Running rpc.yppasswdd, Remote Denial of Service (DoS) (HPSBUX02295 SSRT071333 rev.1)

HP-UX PHNE\_36973 : HP-UX Running BIND, Remote DNS Cache Poisoning (HPSBUX02251 SSRT071449 rev.3)

HP-UX PHNE\_36982 : HP-UX Running rpcbind, Remote Denial of Service (DoS) (HPSBUX02370 SSRT071459 rev.1)

HP-UX PHNE\_37110 : HP-UX Running rpcbind, Remote Denial of Service (DoS) (HPSBUX02370 SSRT071459 rev.1)

HP-UX PHNE\_37865 : HP-UX Running BIND, Remote DNS Cache Poisoning (HPSBUX02351 SSRT080058 rev.6)

HP-UX PHNE\_37897 : HP-UX Running IPv6, Remote Denial of Service (DoS) and Unauthorized Access (HPSBUX02407 SSRT080107 rev.1)

HP-UX PHNE\_37898 : HP-UX Running IPv6, Remote Denial of Service (DoS) and Unauthorized Access (HPSBUX02407 SSRT080107 rev.1)

HP-UX PHNE\_38458 : HP-UX Running ftpd, Remote Privileged Access (HPSBUX02356 SSRT080051 rev.1)

HP-UX PHNE\_38680 : HP-UX Running IPv6, Remote Denial of Service (DoS) and Unauthorized Access (HPSBUX02407 SSRT080107 rev.1)

HP-UX PHNE\_39443 : HP-UX Running bootpd, Remote Denial of Service (DoS) (HPSBUX02458 SSRT090104 rev.1)

HP-UX PHNE\_39668 : HP-UX Running bootpd, Remote Denial of Service (DoS) (HPSBUX02458 SSRT090104 rev.1)

HP-UX PHNE\_39700 : HP-UX Running bootpd, Remote Denial of Service (DoS) (HPSBUX02458 SSRT090104 rev.1)

HP-UX PHNE\_39871 : HP-UX Running XNTP, Remote Execution of Arbitrary Code (HPSBUX02437 SSRT090038 rev.2)

HP-UX PHNE\_39872 : HP-UX Running XNTP, Remote Execution of Arbitrary Code (HPSBUX02437 SSRT090038 rev.2)

HP-UX PHNE\_39873 : HP-UX Running XNTP, Remote Execution of Arbitrary Code (HPSBUX02437 SSRT090038 rev.2)

HP-UX PHNE\_40339 : s700\_800 11.23 BIND 9.2.0 Revision 5.0

HP-UX PHNE\_40388 : HP-UX Running sendmail, Remote Denial of Service (DoS) (HPSBUX02495 SSRT090151 rev.2)

HP-UX PHNE\_40393 : HP-UX Running sendmail, Remote Denial of Service (DoS) (HPSBUX02495 SSRT090151 rev.2)

HP-UX PHNE\_41021 : HP-UX Running ONCplus rpc.pcnfsd, Remote Denial of Service (DoS), Increase in Privilege (HPSBUX02523 SSRT100036 rev.2)

HP-UX PHNE\_41023 : HP-UX Running ONCplus rpc.pcnfsd, Remote Denial of Service (DoS), Increase in Privilege (HPSBUX02523 SSRT100036 rev.2)

HP-UX PHNE\_41177 : HP-UX Running XNTP, Remote Denial of Service (DoS) (HPSBUX02639 SSRT100293 rev.1)

HP-UX PHNE\_41907 : HP-UX Running XNTP, Remote Denial of Service (DoS) (HPSBUX02639 SSRT100293 rev.1)

HP-UX PHNE\_41908 : HP-UX Running XNTP, Remote Denial of Service (DoS) (HPSBUX02639 SSRT100293 rev.1)

HP-UX PHNE\_42470 : s700\_800 11.31 cumulative ARPA Transport patch

HP-UX PHNE\_42727 : s700\_800 11.23 BIND 9.2.0 Revision 5.0

HP-UX PHNE\_43369 : s700\_800 11.23 BIND 9.2.0 Revision 5.0

HP-UX PHNE\_43577 : s700\_800 11.11 ONC/NFS General Release/Performance Patch

HP-UX PHNE\_43706 : s700\_800 11.23 Lock Manager cumulative patch

HP-UX PHNE\_43814 : s700\_800 11.31 cumulative ARPA Transport patch

HP-UX PHNE\_44235 : s700\_800 11.11 NTP timeservices upgrade plus utilities

HP-UX PHNE\_44236 : s700\_800 11.23 NTP timeservices upgrade plus utilities

HP-UX PHNE\_44295 : s700\_800 11.31 s700\_800 cumulative PPP patch

HP-UX PHNE\_44296 : s700\_800 11.23 cumulative PPP patch

HP-UX PHSS\_14592 : s700\_800 11.00 Predictive C.11.0[0,a-e] cumulative patch

HP-UX PHSS\_16148 : s700\_800 11.00 CDE Runtime AUG 98 Cumulative Patch

HP-UX PHSS\_16474 : s700\_800 11.00 OV OB2.55 patch - DA packet

HP-UX PHSS\_16534 : s700\_800 11.X OV OB2.55 patch - WinNT packet

HP-UX PHSS\_16649 : s700\_800 11.00 Receiver Services October 1998 Patch

HP-UX PHSS\_16846 : s700\_800 11.X OV EMANATE14.x Emanate Agent 14.2 patch

HP-UX PHSS\_17483 : s700\_800 11.00 MC/LockManager A.11.05 (English) Patch

HP-UX PHSS\_17484 : s700\_800 11.00 MC/LockManager A.11.05 (Japanese) Patch

HP-UX PHSS\_17581 : s700\_800 11.00 MC ServiceGuard 11.05 Cumulative Patch

HP-UX PHSS\_17810 : HPSBUX0308-273 SSRT3608 Potential security vulnerability in DCE

HP-UX PHSS\_19483 : HPSBUX9908-102 Security Vulnerability in rpc.cmsd (rev.2)

HP-UX PHSS\_19748 : HPSBUX9909-103 Security Vulnerability in CDE ttsession (Rev.01)

HP-UX PHSS\_21663 : HPSBUX0001-108 Sec. Vulnerability with Aserver (rev. 04)

HP-UX PHSS\_22062 : HPSBUX0008-119 Sec. Vulnerability OpenView NNM 6.1 (rev.1)

HP-UX PHSS\_22296 : HPSBUX0010-124 Sec. Vulnerability in VVOS NSAPI (rev.1)

HP-UX PHSS\_22320 : HPSBUX0011-128 Sec. Vulnerability in dtterm (rev.1)

HP-UX PHSS\_22407 : s700\_800 11.00 OV NNM6.1 pmd exception/core dump

HP-UX PHSS\_22540 : HP-UX MC/ServiceGuard, Local Denial of Service (DoS) (HPSBUX00129 SSRT071374 rev.2)

HP-UX PHSS\_22548 : HPSBUX0011-128 Sec. Vulnerability in dtterm (rev.1)

HP-UX PHSS\_22678 : HP-UX ContinentalClusters, Remote Unauthorized Access (HPSBUX00133 SSRT071376 rev.2)

HP-UX PHSS\_22915 : HPSBUX0102-142 Sec. Vulnerability in OV OmniBack (rev.1)

HP-UX PHSS\_23066 : HP-UX Running Support Tools Manager, Local Denial of Service (DoS) (HPSBUX00137 SSRT071336 rev.4)

HP-UX PHSS\_23067 : HP-UX Running Support Tools Manager, Local Denial of Service (DoS) (HPSBUX00137 SSRT071336 rev.4)

HP-UX PHSS\_23096 : HPSBUX0102-142 Sec. Vulnerability in OV OmniBack (rev.1)

HP-UX PHSS\_23104 : HPSBUX0102-142 Sec. Vulnerability in OV OmniBack (rev.1)

HP-UX PHSS\_23215 : HPSBUX0102-139 Sec. Vulnerability in iPlanet 4.X in VV4.0 (rev.1)

HP-UX PHSS\_23266 : HP-UX Running Support Tools Manager, Local Denial of Service (DoS) (HPSBUX00137 SSRT071336 rev.4)

HP-UX PHSS\_23269 : HP-UX Running Support Tools Manager, Local Denial of Service (DoS) (HPSBUX00137 SSRT071336 rev.4)

HP-UX PHSS\_23780 : HPSBUX0106-154 Sec. Vulnerability in OpenView NNM (rev.2)

HP-UX PHSS\_23797 : HP-UX running CDE, Local Increased Privilege, Denial of Service (DoS) (HPSBUX00151 SSRT071382 rev.2)

HP-UX PHSS\_24038 : HPSBUX0205-193 Sec. Vulnerability in Virtualvault 4.5 IWS

HP-UX PHSS\_24087 : HP-UX running CDE, Local Increased Privilege, Denial of Service (DoS) (HPSBUX00151 SSRT071382 rev.2)

HP-UX PHSS\_24091 : HP-UX running CDE, Local Increased Privilege, Denial of Service (DoS) (HPSBUX00151 SSRT071382 rev.2)

HP-UX PHSS\_24098 : HP-UX running CDE, Local Increased Privilege, Denial of Service (DoS) (HPSBUX00151 SSRT071382 rev.2)

HP-UX PHSS\_24108 : HPSBUX0106-152 Security Vul. in Virtualvault 4.0 w/ iPlanet WS (rev.1)

HP-UX PHSS\_24169 : HPSBUX0107-161 Sec. Vulnerability in VVOS mkacct (rev.1)

HP-UX PHSS\_24212 : HPSBUX0107-161 Sec. Vulnerability in VVOS mkacct (rev.1)

HP-UX PHSS\_24498 : HPSBUX0107-158 Security Vulnerability in ecsd (rev.1)

HP-UX PHSS\_24608 : s700\_800 11.00 AudioSubsystem July 2001 Periodic Patch

HP-UX PHSS\_24798 : s700\_800 11.00 OV NNM6.1 Consolidated Patch 4

HP-UX PHSS\_24823 : HPSBUX0110-173 Sec. Vulnerability in Tomcat 3.2.1 (VVOS) (rev.1)

HP-UX PHSS\_24843 : s700\_800 11.X OV NNM6.2 NNM mishandles large objectid

HP-UX PHSS\_24864 : HP-UX running PRM or WLM, Local Increased Privilege (HPSBUX00165 SSRT071392 rev.2)

HP-UX PHSS\_25138 : HP-UX running rpc.ttdbserverd, Remote Unauthorized Access, Increased Privilege (HPSBUX00168 SSRT071383 rev.5)

HP-UX PHSS\_25139 : HP-UX running rpc.ttdbserverd, Remote Unauthorized Access, Increased Privilege (HPSBUX00168 SSRT071383 rev.5)

HP-UX PHSS\_25221 : HPSBUX0110-173 Sec. Vulnerability in Tomcat 3.2.1 (VVOS) (rev.1)

HP-UX PHSS\_25291 : HPSBUX0301-238 SSRT2361 Security Vulnerability in the HP-UX 11.22 Xserver

HP-UX PHSS\_25420 : HP-UX running rpc.ttdbserverd, Remote Unauthorized Access, Increased Privilege (HPSBUX00168 SSRT071383 rev.5)

HP-UX PHSS\_25454 : HPSBUX0110-171 Sec. Vulnerability in IA HP-UX 11.20 only (rev.1)

HP-UX PHSS\_25787 : HP-UX running CDE dtspcd, Remote Unauthorized Access, Increased Privilege, Arbitrary Code Execution (HPSBUX00175 SSRT071388 rev.5)

HP-UX PHSS\_25788 : HP-UX running CDE dtspcd, Remote Unauthorized Access, Increased Privilege, Arbitrary Code Execution (HPSBUX00175 SSRT071388 rev.5)

HP-UX PHSS\_26030 : HP-UX running CDE dtspcd, Remote Unauthorized Access, Increased Privilege, Arbitrary Code Execution (HPSBUX00175 SSRT071388 rev.5)

HP-UX PHSS\_26138 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_26368 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_26478 : HPSBUX0203-189 Sec, Vulnerability in VVOS Web proxy (rev.1)

HP-UX PHSS\_26525 : HPSBUX0204-190 Sec. Vulnerability on Virtualvault4.5, Apache 1.3.19 (rev.1)

HP-UX PHSS\_26909 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_26919 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_26933 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_27182 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_27222 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_27258 : HP-UX with PHSS\_25710, PHSS\_26394, or PHSS\_26396, Remote Denial of Service (DoS) (HPSBUX00196 SSRT071360 rev.2)

HP-UX PHSS\_27259 : HP-UX with PHSS\_25710, PHSS\_26394, or PHSS\_26396, Remote Denial of Service (DoS) (HPSBUX00196 SSRT071360 rev.2)

HP-UX PHSS\_27263 : HPSBUX0209-217 Sec. Vulnerability in Apache OpenSSL (rev.2)

HP-UX PHSS\_27274 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_27361 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_27371 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_27411 : HP-UX Running ISEE Software, Local Elevated Privileges (HPSBUX00201 SSRT071373 rev.3)

HP-UX PHSS\_27423 : s700\_800 11.04 Virtualvault 4.6 Inside Server Update

HP-UX PHSS\_27427 : HP-UX Running rpc.ttdbserver, Remote Denial of Service(DoS), Privilege Increase (HPSBUX00199 SSRT071348 rev.6)

HP-UX PHSS\_27428 : HP-UX Running rpc.ttdbserver, Remote Denial of Service(DoS), Privilege Increase (HPSBUX00199 SSRT071348 rev.6)

HP-UX PHSS\_27438 : HP-UX, HP Jetdirect, HP Procurve Switches, HP OpenView Network Node Manager (NNM), OpenView Distributed Management (DM), HP TopTools Remote Control Card Running SNMP, Remote Unauthorized Access, Denial of Service (DoS) (HPSBUX00184 SSRT071347 rev.17)

HP-UX PHSS\_27476 : s700\_800 11.04 Virtualvault 4.6 inside server support

HP-UX PHSS\_27477 : s700\_800 11.04 Virtualvault 4.5 Inside Admin Server Update

HP-UX PHSS\_27499 : HPSBUX0208-211 Sec. Vulnerability in VVOS TGAD (rev.1)

HP-UX PHSS\_27500 : HPSBUX0208-211 Sec. Vulnerability in VVOS TGAD (rev.1)

HP-UX PHSS\_27501 : HPSBUX0208-211 Sec. Vulnerability in VVOS TGAD (rev.1)

HP-UX PHSS\_27547 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_27627 : s700\_800 11.04 Virtualvault 4.5 inside server support

HP-UX PHSS\_27637 : HPSBUX0209-217 Sec. Vulnerability in Apache OpenSSL (rev.2)

HP-UX PHSS\_27639 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_27655 : HPSBUX0209-217 Sec. Vulnerability in Apache OpenSSL (rev.2)

HP-UX PHSS\_27656 : HPSBUX0209-217 Sec. Vulnerability in Apache OpenSSL (rev.2)

HP-UX PHSS\_27668 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_27782 : HPSBUX0208-214 SSRT2334 Security Vulnerability in VJE.VJE-RUN (rev.1)

HP-UX PHSS\_27784 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_27850 : HP-UX Running OpenView EMANATE14.2, Unauthorized Access or Denial of Service (DoS) (HPSBUX00208 SSRT071349 rev.4)

HP-UX PHSS\_27921 : HPSBUX0209-222 Security Vulnerability in VVOS tomcat 3.2.x

HP-UX PHSS\_27922 : HPSBUX0209-222 Security Vulnerability in VVOS tomcat 3.2.x

HP-UX PHSS\_27936 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_28090 : HP-UX Running Apache, Increased Privileges or Denial of Service (DoS) or Execution of Arbitrary Code (HPSBUX00224 SSRT2393 rev.3)

HP-UX PHSS\_28098 : HP-UX Running Apache, Increased Privileges or Denial of Service (DoS) or Execution of Arbitrary Code (HPSBUX00224 SSRT2393 rev.3)

HP-UX PHSS\_28099 : HP-UX Running Apache, Increased Privileges or Denial of Service (DoS) or Execution of Arbitrary Code (HPSBUX00224 SSRT2393 rev.3)

HP-UX PHSS\_28111 : HP-UX Running Apache, Increased Privileges or Denial of Service (DoS) or Execution of Arbitrary Code (HPSBUX00224 SSRT2393 rev.3)

HP-UX PHSS\_28174 : HP-UX Running rpc.ttdbserver, Remote Denial of Service(DoS), Privilege Increase (HPSBUX00199 SSRT071348 rev.6)

HP-UX PHSS\_28469 : HP-UX Running X Font Server (xfs) Software, Remote Unauthorized Access or Denial of Service (DoS) (HPSBUX00228 SSRT2429 rev.3)

HP-UX PHSS\_28470 : HP-UX Running X Font Server (xfs) Software, Remote Unauthorized Access or Denial of Service (DoS) (HPSBUX00228 SSRT2429 rev.3)

HP-UX PHSS\_28471 : HP-UX Running X Font Server (xfs) Software, Remote Unauthorized Access or Denial of Service (DoS) (HPSBUX00228 SSRT2429 rev.3)

HP-UX PHSS\_28558 : HP-UX Running Sendmail and Using Bastille Sendmail.cf, Remote Unauthorized Disclosure of Information (HPSBUX00245 SSRT3450 rev.2)

HP-UX PHSS\_28675 : s700\_800 11.00 CDE Runtime Periodic Patch

HP-UX PHSS\_28676 : s700\_800 11.11 CDE Base Periodic Patch

HP-UX PHSS\_28677 : HP-UX running CDE, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX00263 SSRT2373 rev.3)

HP-UX PHSS\_28678 : HP-UX running CDE, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX00263 SSRT2373 rev.3)

HP-UX PHSS\_28679 : HP-UX running CDE, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX00263 SSRT2373 rev.3)

HP-UX PHSS\_28682 : s700\_800 11.22 CDE Base Periodic Patch

HP-UX PHSS\_28683 : HP-UX running CDE, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX00263 SSRT2373 rev.3)

HP-UX PHSS\_28685 : s700\_800 11.04 Virtualvault 4.5 OWS update

HP-UX PHSS\_28686 : s700\_800 11.04 Virtualvault 4.6 OWS update

HP-UX PHSS\_28688 : HP-UX Running OpenView EMANATE14.2, Unauthorized Access or Denial of Service (DoS) (HPSBUX00208 SSRT071349 rev.4)

HP-UX PHSS\_28705 : HP-UX Running Apache, Increased Privileges or Denial of Service (DoS) or Execution of Arbitrary Code (HPSBUX00224 SSRT2393 rev.3)

HP-UX PHSS\_29057 : HPSBUX0306-265 SSRT3570 Security Vulnerability in HP-UX VVOS OpenSSH

HP-UX PHSS\_29120 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_29121 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_29214 : HP-UX running CDE, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX00263 SSRT2373 rev.3)

HP-UX PHSS\_29338 : HP-UX SharedX, Local Unauthorized Access or Denial of Service (DoS) (HPSBUX00307 SSRT3476 rev.2)

HP-UX PHSS\_29367 : HP-UX dtprintinfo, Local Increased Privilege (HPSBUX00289 SSRT3589 rev.2)

HP-UX PHSS\_29371 : HP-UX dtprintinfo, Local Increased Privilege (HPSBUX00289 SSRT3589 rev.2)

HP-UX PHSS\_29373 : HP-UX dtprintinfo, Local Increased Privilege (HPSBUX00289 SSRT3589 rev.2)

HP-UX PHSS\_29541 : HPSBUX0310-285 SSRT3642 Potential Security Vulnerabilities Apache web server HP-UX VVOS and Webproxy.

HP-UX PHSS\_29542 : HPSBUX0310-285 SSRT3642 Potential Security Vulnerabilities Apache web server HP-UX VVOS and Webproxy.

HP-UX PHSS\_29545 : HPSBUX0310-285 SSRT3642 Potential Security Vulnerabilities Apache web server HP-UX VVOS and Webproxy.

HP-UX PHSS\_29546 : HPSBUX0310-285 SSRT3642 Potential Security Vulnerabilities Apache web server HP-UX VVOS and Webproxy.

HP-UX PHSS\_29547 : HPSBUX0310-285 SSRT3642 Potential Security Vulnerabilities Apache web server HP-UX VVOS and Webproxy.

HP-UX PHSS\_29550 : HP-UX SharedX, Local Unauthorized Access or Denial of Service (DoS) (HPSBUX00307 SSRT3476 rev.2)

HP-UX PHSS\_29626 : HP-UX OpenView DCE, Remote Denial of Service (DoS) (HPSBUX00274 SSRT3617 rev.3)

HP-UX PHSS\_29644 : HP-UX OpenView DCE, Remote Denial of Service (DoS) (HPSBUX00274 SSRT3617 rev.3)

HP-UX PHSS\_29645 : HP-UX OpenView DCE, Remote Denial of Service (DoS) (HPSBUX00274 SSRT3617 rev.3)

HP-UX PHSS\_29646 : HP-UX OpenView DCE, Remote Denial of Service (DoS) (HPSBUX00274 SSRT3617 rev.3)

HP-UX PHSS\_29690 : HPSBUX0310-284 SSRT3622 rev.3 HP-UX Apache HTTP Server Denial of Service,unauthorized access

HP-UX PHSS\_29691 : HPSBUX0310-284 SSRT3622 rev.3 HP-UX Apache HTTP Server Denial of Service,unauthorized access

HP-UX PHSS\_29734 : s700\_800 11.00 CDE Runtime Periodic Patch

HP-UX PHSS\_29735 : s700\_800 11.11 CDE Base Periodic Patch

HP-UX PHSS\_29736 : s700\_800 11.22 CDE Base Periodic Patch

HP-UX PHSS\_29737 : HP-UX Running dtmailpr Software, Local Root Privileges. (HPSBUX00300 SSRT3667 rev.2)

HP-UX PHSS\_29744 : HPSBUX0302-241 SSRT3472 rev.3 HP-UX stmkfont potential unauthorized access

HP-UX PHSS\_29886 : HPSBUX0311-302 SSRT3670 Rev.1 VirtualVault OpenSSH

HP-UX PHSS\_29891 : HPSBUX0310-284 SSRT3622 rev.3 HP-UX Apache HTTP Server Denial of Service,unauthorized access

HP-UX PHSS\_29892 : HPSBUX0310-284 SSRT3622 rev.3 HP-UX Apache HTTP Server Denial of Service,unauthorized access

HP-UX PHSS\_29893 : HPSBUX0310-284 SSRT3622 rev.3 HP-UX Apache HTTP Server Denial of Service,unauthorized access

HP-UX PHSS\_29894 : s700\_800 11.04 Webproxy server 2.0 update

HP-UX PHSS\_29963 : s700\_800 11.00 HP DCE/9000 1.7 Runtime cumulative patch

HP-UX PHSS\_29964 : s700\_800 11.11 HP DCE/9000 1.8 DCE Client IPv6 patch

HP-UX PHSS\_29966 : HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX00299 SSRT3660 rev.4)

HP-UX PHSS\_29987 : HP-UX Running Apache, Remote Denial of Service (DoS) or Elevation Privilege, or Execution of Arbitrary Code (HPSBUX00197 SSRT2332 rev.11)

HP-UX PHSS\_30010 : HP-UX Running CDE, Local Elevation of Privileges (HPSBUX00297 SSRT3657 rev.4)

HP-UX PHSS\_30011 : HP-UX Running CDE, Local Elevation of Privileges (HPSBUX00297 SSRT3657 rev.4)

HP-UX PHSS\_30012 : HP-UX Running CDE, Local Elevation of Privileges (HPSBUX00297 SSRT3657 rev.4)

HP-UX PHSS\_30013 : HP-UX Running CDE, Local Elevation of Privileges (HPSBUX00297 SSRT3657 rev.4)

HP-UX PHSS\_30055 : s700\_800 11.04 Virtualvault 4.7 IWS update

HP-UX PHSS\_30056 : s700\_800 11.04 Virtualvault 4.7 OWS update

HP-UX PHSS\_30057 : HPSBUX0310-284 SSRT3622 rev.3 HP-UX Apache HTTP Server Denial of Service,unauthorized access

HP-UX PHSS\_30058 : s700\_800 11.04 Webproxy server 2.1 update

HP-UX PHSS\_30110 : HPSBUX0311-302 SSRT3670 Rev.1 VirtualVault OpenSSH

HP-UX PHSS\_30153 : HPSBUX0401-305 SSRT4681 Apache 1.3.29 web server on VVOS

HP-UX PHSS\_30154 : HPSBUX0401-305 SSRT4681 Apache 1.3.29 web server on VVOS

HP-UX PHSS\_30159 : HPSBUX0401-305 SSRT4681 Apache 1.3.29 web server on VVOS

HP-UX PHSS\_30160 : HPSBUX0401-305 SSRT4681 Apache 1.3.29 web server on VVOS

HP-UX PHSS\_30167 : s700\_800 11.04 (VVOS) CDE Runtime Patch

HP-UX PHSS\_30171 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30172 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30173 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30181 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30302 : s700\_800 11.04 (VVOS) DCE/9000 1.7 Runtime cumulative patch

HP-UX PHSS\_30405 : s700\_800 11.04 Virtualvault 4.6 mod\_jk update

HP-UX PHSS\_30406 : s700\_800 11.04 Virtualvault 4.7 mod\_jk update

HP-UX PHSS\_30477 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30478 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30479 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30480 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30526 : HP OpenView Operations, Remote Unauthorized Access (HPSBMA01010 SSRT4727 rev.2)

HP-UX PHSS\_30538 : HP OpenView Operations, Remote Unauthorized Access (HPSBMA01010 SSRT4727 rev.2)

HP-UX PHSS\_30586 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30639 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30640 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30641 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30642 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30643 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30644 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30645 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30646 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30647 : s700\_800 11.04 Virtualvault 4.5 IWS Update

HP-UX PHSS\_30648 : s700\_800 11.04 Virtualvault 4.5 OWS update

HP-UX PHSS\_30649 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30650 : HP-UX Running Apache, Remote Denial of Service (DoS) (HPSBUX01019 SSRT4717 rev.3)

HP-UX PHSS\_30668 : HP-UX running CDE dtlogin, Remote Unauthorized Privileged Access, Denial of Service (DoS) (HPSBUX01038 SSRT4721 rev.2)

HP-UX PHSS\_30669 : HP-UX running CDE dtlogin, Remote Unauthorized Privileged Access, Denial of Service (DoS) (HPSBUX01038 SSRT4721 rev.2)

HP-UX PHSS\_30670 : HP-UX running CDE dtlogin, Remote Unauthorized Privileged Access, Denial of Service (DoS) (HPSBUX01038 SSRT4721 rev.2)

HP-UX PHSS\_30671 : HP-UX running CDE dtlogin, Remote Unauthorized Privileged Access, Denial of Service (DoS) (HPSBUX01038 SSRT4721 rev.2)

HP-UX PHSS\_30706 : HP-UX XFree86, Remote Unauthorized Privileged Access, Execution of Arbitrary Code (HPSBUX01018 SSRT4692 rev.2)

HP-UX PHSS\_30771 : HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX00299 SSRT3660 rev.4)

HP-UX PHSS\_30782 : s700\_800 11.04 Virtualvault A.04.50 TGA daemon Update

HP-UX PHSS\_30807 : HP-UX running CDE dtlogin, Remote Unauthorized Privileged Access, Denial of Service (DoS) (HPSBUX01038 SSRT4721 rev.2)

HP-UX PHSS\_30944 : s700\_800 11.04 Virtualvault 4.7 IWS update

HP-UX PHSS\_30946 : s700\_800 11.04 Virtualvault 4.6 IWS update

HP-UX PHSS\_30949 : s700\_800 11.04 Webproxy server 2.0 update

HP-UX PHSS\_30950 : s700\_800 11.04 Webproxy server 2.1 update

HP-UX PHSS\_31057 : s700\_800 11.04 Virtualvault 4.6 OWS update

HP-UX PHSS\_31058 : s700\_800 11.04 Virtualvault 4.7 OWS update

HP-UX PHSS\_31065 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31066 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31067 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31068 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31069 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31070 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31071 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31072 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31073 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31074 : HP-UX Running Serviceguard, Remote Increase in Privilege (HPSBUX01080 SSRT3526 rev.2)

HP-UX PHSS\_31104 : HPSBUX0302-241 SSRT3472 rev.3 HP-UX stmkfont potential unauthorized access

HP-UX PHSS\_31178 : HP-UX Running xfs and stmkfont, Remote Unauthorized Access (HPSBUX01061 SSRT4773 rev.2)

HP-UX PHSS\_31179 : HP-UX Running xfs and stmkfont, Remote Unauthorized Access (HPSBUX01061 SSRT4773 rev.2)

HP-UX PHSS\_31180 : HP-UX Running xfs and stmkfont, Remote Unauthorized Access (HPSBUX01061 SSRT4773 rev.2)

HP-UX PHSS\_31181 : HP-UX Running xfs and stmkfont, Remote Unauthorized Access (HPSBUX01061 SSRT4773 rev.2)

HP-UX PHSS\_31240 : HP-UX Running System Administration Manager (SAM), Local Elevation of Privilege (HPSBUX01104 SSRT4699 rev.3)

HP-UX PHSS\_31243 : HP-UX Running System Administration Manager (SAM), Local Elevation of Privilege (HPSBUX01104 SSRT4699 rev.3)

HP-UX PHSS\_31303 : HP-UX Running xfs and stmkfont, Remote Unauthorized Access (HPSBUX01061 SSRT4773 rev.2)

HP-UX PHSS\_31817 : HP-UX Running System Administration Manager (SAM), Local Elevation of Privilege (HPSBUX01104 SSRT4699 rev.3)

HP-UX PHSS\_31823 : s700\_800 11.04 Virtualvault 4.7 IWS update

HP-UX PHSS\_31824 : s700\_800 11.04 Virtualvault 4.7 OWS update

HP-UX PHSS\_31825 : s700\_800 11.04 Virtualvault 4.6 IWS update

HP-UX PHSS\_31826 : s700\_800 11.04 Virtualvault 4.6 OWS update

HP-UX PHSS\_31827 : s700\_800 11.04 Virtualvault 4.5 IWS Update

HP-UX PHSS\_31828 : s700\_800 11.04 Virtualvault 4.5 OWS update

HP-UX PHSS\_31829 : s700\_800 11.04 Webproxy server 2.0 update

HP-UX PHSS\_31830 : s700\_800 11.04 Webproxy server 2.1 update

HP-UX PHSS\_31933 : HP OpenView Operations (OVO), Remote Unauthorized Privilege Elevation (HPSBMA01092 SSRT4847 rev.2)

HP-UX PHSS\_31987 : HP-UX stmkfont Local Unauthorized Privileged Access (HPSBUX01088 SSRT4807 rev.2)

HP-UX PHSS\_31988 : HP-UX stmkfont Local Unauthorized Privileged Access (HPSBUX01088 SSRT4807 rev.2)

HP-UX PHSS\_31989 : HP-UX stmkfont Local Unauthorized Privileged Access (HPSBUX01088 SSRT4807 rev.2)

HP-UX PHSS\_31990 : HP-UX stmkfont Local Unauthorized Privileged Access (HPSBUX01088 SSRT4807 rev.2)

HP-UX PHSS\_32046 : HP OpenView Network Node Manager (OV NNM), Remote Denial of Service (DoS) (HPSBMA01125 SSRT4829 rev.2)

HP-UX PHSS\_32140 : s700\_800 11.04 Virtualvault 4.7 IWS update

HP-UX PHSS\_32141 : s700\_800 11.04 Virtualvault 4.5 IWS Update

HP-UX PHSS\_32175 : HP OpenView Operations (OVO), Remote Unauthorized Privilege Elevation (HPSBMA01092 SSRT4847 rev.2)

HP-UX PHSS\_32176 : HP OpenView Operations (OVO), Remote Unauthorized Privilege Elevation (HPSBMA01092 SSRT4847 rev.2)

HP-UX PHSS\_32182 : s700\_800 11.04 Virtualvault 4.7 OWS update

HP-UX PHSS\_32183 : s700\_800 11.04 Virtualvault 4.6 OWS update

HP-UX PHSS\_32184 : s700\_800 11.04 Virtualvault 4.5 OWS update

HP-UX PHSS\_32196 : HP-UX stmkfont Local Unauthorized Privileged Access (HPSBUX01088 SSRT4807 rev.2)

HP-UX PHSS\_32206 : s700\_800 11.04 Virtualvault 4.6 IWS update

HP-UX PHSS\_32357 : HP OpenView Network Node Manager (OV NNM), Remote Denial of Service (DoS) (HPSBMA01125 SSRT4829 rev.2)

HP-UX PHSS\_32358 : HP OpenView Network Node Manager (OV NNM), Remote Denial of Service (DoS) (HPSBMA01125 SSRT4829 rev.2)

HP-UX PHSS\_32362 : s700\_800 11.04 Webproxy server 2.1 (Apache 1.x) update

HP-UX PHSS\_32363 : s700\_800 11.04 Webproxy server 2.0 update

HP-UX PHSS\_32380 : HP OpenView Operations, Remote Unauthorized Access and Denial of Service (DoS) (HPSBMA02149 SSRT050968 rev.1)

HP-UX PHSS\_32406 : HP OpenView Operations and OpenView VantagePoint Java Runtime Environment (JRE), Remote Privileged Access (HPSBMA01234 SSRT051052 rev.2)

HP-UX PHSS\_32423 : HP OpenView Operations, Remote Unauthorized Access and Denial of Service (DoS) (HPSBMA02149 SSRT050968 rev.1)

HP-UX PHSS\_32507 : s700\_800 11.04 Virtualvault A.04.60 TGA daemon update

HP-UX PHSS\_32514 : HP OpenView Network Node Manager (OV NNM), Remote Denial of Service (DoS) (HPSBMA01125 SSRT4829 rev.2)

HP-UX PHSS\_32515 : HP OpenView Network Node Manager (OV NNM), Remote Denial of Service (DoS) (HPSBMA01125 SSRT4829 rev.2)

HP-UX PHSS\_32520 : s700\_800 11.04 Virtualvault A.04.70 TGA daemon update

HP-UX PHSS\_32543 : HP OpenView Network Node Manager (OV NNM), Remote Denial of Service (DoS) (HPSBMA01125 SSRT4829 rev.2)

HP-UX PHSS\_32690 : HP OpenView Network Node Manager (OV NNM), Remote Unauthorized Privileged Code Execution, Denial of Service (DoS) (HPSBMA01140 SSRT4795, SSRT4797, SSRT4864 rev.2)

HP-UX PHSS\_32692 : HP OpenView Network Node Manager (OV NNM), Remote Unauthorized Privileged Code Execution, Denial of Service (DoS) (HPSBMA01140 SSRT4795, SSRT4797, SSRT4864 rev.2)

HP-UX PHSS\_32693 : HP OpenView Network Node Manager (OV NNM), Remote Unauthorized Privileged Code Execution, Denial of Service (DoS) (HPSBMA01140 SSRT4795, SSRT4797, SSRT4864 rev.2)

HP-UX PHSS\_32738 : HPSBMA02088 SSRT051026 rev. 2 - HP-UX running WBEM Services Denial of Service (DoS)

HP-UX PHSS\_32781 : HP OpenView Network Node Manager (OV NNM), Remote Unauthorized Privileged Code Execution, Denial of Service (DoS) (HPSBMA01140 SSRT4795, SSRT4797, SSRT4864 rev.2)

HP-UX PHSS\_32918 : HP OpenView Event Correlation Services (OV ECS), Remote Unauthorized Privileged Code Execution, Denial of Service (DoS) (HPSBMA01141 SSRT4796, SSRT4873 rev.2)

HP-UX PHSS\_32919 : HP OpenView Event Correlation Services (OV ECS), Remote Unauthorized Privileged Code Execution, Denial of Service (DoS) (HPSBMA01141 SSRT4796, SSRT4873 rev.2)

HP-UX PHSS\_32960 : HP-UX Running Xserver Local Execution of Arbitrary Code, Privilege Elevation (HPSBUX02137 SSRT051024 rev.1)

HP-UX PHSS\_32965 : HP-UX Running Xserver Local Execution of Arbitrary Code, Privilege Elevation (HPSBUX02137 SSRT051024 rev.1)

HP-UX PHSS\_32966 : HP-UX Running Xserver Local Execution of Arbitrary Code, Privilege Elevation (HPSBUX02137 SSRT051024 rev.1)

HP-UX PHSS\_33038 : HP OpenView Network Node Manager (OV NNM), Remote Unauthorized Privileged Code Execution, Denial of Service (DoS) (HPSBMA01140 SSRT4795, SSRT4797, SSRT4864 rev.2)

HP-UX PHSS\_33075 : Apache on HP-UX, Remote Denial of Service (DoS), Bypass of SSLCipherSuite Settings (HPSBUX01123 SSRT5931 rev.2)

HP-UX PHSS\_33129 : HP-UX Running Motif Applications Remote Arbitrary Code Execution, Denial of Service (DoS) (HPSBUX02119 SSRT4848 rev.1)

HP-UX PHSS\_33130 : HP-UX Running Motif Applications Remote Arbitrary Code Execution, Denial of Service (DoS) (HPSBUX02119 SSRT4848 rev.1)

HP-UX PHSS\_33132 : HP-UX Running Motif Applications Remote Arbitrary Code Execution, Denial of Service (DoS) (HPSBUX02119 SSRT4848 rev.1)

HP-UX PHSS\_33252 : HP OpenView Operations, Remote Unauthorized Access and Denial of Service (DoS) (HPSBMA02149 SSRT050968 rev.1)

HP-UX PHSS\_33253 : HP OpenView Operations, Remote Unauthorized Access and Denial of Service (DoS) (HPSBMA02149 SSRT050968 rev.1)

HP-UX PHSS\_33256 : HP OpenView Operations, Remote Unauthorized Access and Denial of Service (DoS) (HPSBMA02149 SSRT050968 rev.1)

HP-UX PHSS\_33257 : HP OpenView Operations, Remote Unauthorized Access and Denial of Service (DoS) (HPSBMA02149 SSRT050968 rev.1)

HP-UX PHSS\_33280 : HP OpenView Operations, Remote Unauthorized Access and Denial of Service (DoS) (HPSBMA02149 SSRT050968 rev.1)

HP-UX PHSS\_33384 : HP-UX Kerberos Client Remote Unauthenticated Execution of Arbitrary Code (HPSBUX02152 SSRT5973 rev.1)

HP-UX PHSS\_33389 : HP-UX Kerberos Client Remote Unauthenticated Execution of Arbitrary Code (HPSBUX02152 SSRT5973 rev.1)

HP-UX PHSS\_33538 : HP OpenView Event Correlation Services (OV ECS), Remote Unauthorized Privileged Access (HPSBMA01225 SSRT051030 rev.2)

HP-UX PHSS\_33539 : HP OpenView Event Correlation Services (OV ECS), Remote Unauthorized Privileged Access (HPSBMA01225 SSRT051030 rev.2)

HP-UX PHSS\_33627 : HP OpenView Operations and OpenView VantagePoint Java Runtime Environment (JRE), Remote Privileged Access (HPSBMA01234 SSRT051052 rev.2)

HP-UX PHSS\_33659 : HP OpenView Event Correlation Services (OV ECS), Remote Unauthorized Privileged Access (HPSBMA01225 SSRT051030 rev.2)

HP-UX PHSS\_33783 : s700\_800 11.X OV NNM7.50 CGI PA RISC Intermediate Patch

HP-UX PHSS\_33784 : s700\_800 11.23 OV NNM7.50 CGI IA-64 Intermediate Patch

HP-UX PHSS\_33797 : HP OpenView Event Correlation Services (OV ECS), Remote Unauthorized Privileged Access (HPSBMA01225 SSRT051030 rev.2)

HP-UX PHSS\_33842 : s700\_800 11.X OV NNM7.01 Intermediate Patch 9

HP-UX PHSS\_33845 : HP OpenView Event Correlation Services (OV ECS), Remote Unauthorized Privileged Access (HPSBMA01225 SSRT051030 rev.2)

HP-UX PHSS\_33866 : HP OpenView Operations and OpenView VantagePoint Java Runtime Environment (JRE), Remote Privileged Access (HPSBMA01234 SSRT051052 rev.2)

HP-UX PHSS\_34008 : s700\_800 11.X OV NNM6.2 Intermediate Patch 18

HP-UX PHSS\_34098 : s700\_800 11.X OV NNM7.50 PA RISC Consolidated Patch 3

HP-UX PHSS\_34099 : s700\_800 11.23 OV NNM7.50 IA-64 Consolidated Patch 3

HP-UX PHSS\_34102 : HP-UX Running xterm Local Unauthorized Access (HPSBUX02075 SSRT051074 rev.5)

HP-UX PHSS\_34119 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34120 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34121 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34123 : Apache-based Web Server on HP-UX mod\_ssl, proxy\_http, Remote Execution of Arbitrary Code, Denial of Service (DoS), and Unauthorized Access (HPSBUX02074 SSRT051251 rev.2)

HP-UX PHSS\_34159 : HP-UX Running xterm Local Unauthorized Access (HPSBUX02075 SSRT051074 rev.5)

HP-UX PHSS\_34160 : HP-UX Running xterm Local Unauthorized Access (HPSBUX02075 SSRT051074 rev.5)

HP-UX PHSS\_34163 : Apache-based Web Server on HP-UX mod\_ssl, proxy\_http, Remote Execution of Arbitrary Code, Denial of Service (DoS), and Unauthorized Access (HPSBUX02074 SSRT051251 rev.2)

HP-UX PHSS\_34169 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34170 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34171 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34202 : s700\_800 11.X OV NNM6.4x/ET2.0x Intermediate Patch 14

HP-UX PHSS\_34203 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34204 : HP-UX VirtualVault running Apache 1.3.X Remote Unauthorized Access (HPSBUX02101 SSRT051128 rev.1)

HP-UX PHSS\_34288 : HP-UX running Support Tools Manager (xstm, cstm, stm) Local Denial of Service (DoS) (HPSBUX02115 SSRT061077 rev.2)

HP-UX PHSS\_34389 : HP-UX Running Xserver, Local Denial of Service (DoS) (HPSBUX02225 SSRT071295 rev.1)

HP-UX PHSS\_34392 : HP-UX Running Xserver, Remote Execution of Arbitrary Code (HPSBUX02381 SSRT080083 rev.2)

HP-UX PHSS\_34566 : HP-UX Secure Shell Remote Denial of Service (DoS) (HPSBUX02090 SSRT051058 rev.2)

HP-UX PHSS\_34567 : HP-UX Secure Shell Remote Denial of Service (DoS) (HPSBUX02090 SSRT051058 rev.2)

HP-UX PHSS\_34870 : s700\_800 11.X OV NNM7.50 PA RISC Consolidated Patch 4

HP-UX PHSS\_34871 : s700\_800 11.23 OV NNM7.50 IA-64 Consolidated Patch 4

HP-UX PHSS\_34887 : s700\_800 11.X OV DP5.10 patch - CORE packet

HP-UX PHSS\_34949 : s700\_800 11.X OV NNM6.4x/ET2.0x Intermediate Patch 15

HP-UX PHSS\_34991 : HP-UX running Kerberos, Remote Arbitrary Code Execution (HPSBUX02217 SSRT071337 rev.2)

HP-UX PHSS\_35110 : s700\_800 11.04 Webproxy server 2.0 update

HP-UX PHSS\_35111 : s700\_800 11.04 Webproxy 2.1 (Apache 1.x) update

HP-UX PHSS\_35113 : s700\_800 11.X OV NNM6.2 Intermediate Patch 19

HP-UX PHSS\_35142 : s700\_800 11.X OV DP5.50 PA-RISC patch - CORE packet

HP-UX PHSS\_35143 : s700\_800 11.23 OV DP5.50 IA-64 patch - CORE packet

HP-UX PHSS\_35164 : HP OpenView Storage Data Protector, Local Execution of Arbitrary Code (HPSBMA02190 SSRT071300 rev.1)

HP-UX PHSS\_35165 : HP OpenView Storage Data Protector, Local Execution of Arbitrary Code (HPSBMA02190 SSRT071300 rev.1)

HP-UX PHSS\_35433 : HP-UX Running dtmail, Local Execution of Arbitrary Code (HPSBUX02162 SSRT061223 rev.1)

HP-UX PHSS\_35434 : HP-UX Running dtmail, Local Execution of Arbitrary Code (HPSBUX02162 SSRT061223 rev.1)

HP-UX PHSS\_35435 : HP-UX Running dtmail, Local Execution of Arbitrary Code (HPSBUX02162 SSRT061223 rev.1)

HP-UX PHSS\_35436 : s700\_800 11.04 Virtualvault 4.7 OWS (Apache 2.x) update

HP-UX PHSS\_35437 : s700\_800 11.04 Webproxy server 2.1 (Apache 2.x) update

HP-UX PHSS\_35457 : HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution (HPSBMA02239 SSRT061260 rev.3)

HP-UX PHSS\_35458 : s700\_800 11.04 Virtualvault 4.5 IWS Update

HP-UX PHSS\_35459 : s700\_800 11.04 Virtualvault 4.6 IWS update

HP-UX PHSS\_35460 : s700\_800 11.04 Virtualvault 4.7 IWS update

HP-UX PHSS\_35461 : s700\_800 11.04 Virtualvault 4.5 OWS update

HP-UX PHSS\_35462 : s700\_800 11.04 Virtualvault 4.6 OWS update

HP-UX PHSS\_35463 : s700\_800 11.04 Virtualvault 4.7 (Apache 1.x) OWS update

HP-UX PHSS\_35480 : HP-UX VirtualVault Remote Unauthorized Access (HPSBUX02165 SSRT061266 rev.1)

HP-UX PHSS\_35481 : HP-UX VirtualVault Remote Unauthorized Access (HPSBUX02165 SSRT061266 rev.1)

HP-UX PHSS\_35528 : HP-UX Running Aries PA Emulator, Local Unauthorized Access (HPSBUX02285 SSRT071484 rev.1)

HP-UX PHSS\_35579 : s700\_800 11.X OV NNM7.01 PA RISC Intermediate Patch 10

HP-UX PHSS\_35843 : s700\_800 11.X OV NNM7.51 PA RISC Intermediate Patch 15

HP-UX PHSS\_35844 : s700\_800 11.23 OV NNM7.51 IA-64 Intermediate Patch 15

HP-UX PHSS\_36004 : HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX02294 SSRT071451 rev.1)

HP-UX PHSS\_36005 : HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX02294 SSRT071451 rev.1)

HP-UX PHSS\_36123 : HP-UX Running Xserver, Local Denial of Service (DoS) (HPSBUX02225 SSRT071295 rev.1)

HP-UX PHSS\_36278 : HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution (HPSBMA02239 SSRT061260 rev.3)

HP-UX PHSS\_36286 : HP-UX running Kerberos, Remote Arbitrary Code Execution (HPSBUX02217 SSRT071337 rev.2)

HP-UX PHSS\_36311 : HP-UX Running Aries PA Emulator, Local Unauthorized Access (HPSBUX02285 SSRT071484 rev.1)

HP-UX PHSS\_36361 : HP-UX running Kerberos, Remote Arbitrary Code Execution (HPSBUX02217 SSRT071337 rev.2)

HP-UX PHSS\_36385 : HP OpenView Network Node Manager (OV NNM) Running Apache, Remote Cross Site Scripting (XSS), Denial of Service (DoS), Execute Arbitrary Code (HPSBMA02328 SSRT071293 rev.2)

HP-UX PHSS\_36386 : HP OpenView Network Node Manager (OV NNM) Running Apache, Remote Cross Site Scripting (XSS), Denial of Service (DoS), Execute Arbitrary Code (HPSBMA02328 SSRT071293 rev.2)

HP-UX PHSS\_36452 : HP-UX Running Xserver, Local Denial of Service (DoS) (HPSBUX02225 SSRT071295 rev.1)

HP-UX PHSS\_36588 : s700\_800 11.X OV DP6.00 PA-RISC patch - CS packet

HP-UX PHSS\_36589 : s700\_800 11.X OV DP6.00 IA-64 patch - CS packet

HP-UX PHSS\_36622 : s700\_800 11.X OV DP6.00 PA-RISC patch - CORE packet

HP-UX PHSS\_36623 : s700\_800 11.X OV DP6.00 IA-64 patch - CORE packet

HP-UX PHSS\_36773 : s700\_800 11.X OV NNM7.01 Intermediate Patch 11

HP-UX PHSS\_36799 : s700\_800 11.X OV DP5.50 PA RISC patch - CS packet

HP-UX PHSS\_36800 : s700\_800 11.23 OV DP5.50 IA-64 patch - CS packet

HP-UX PHSS\_36869 : HP System Management Homepage (SMH) for HP-UX, XSS (HPSBMA02274 SSRT071445 rev.3)

HP-UX PHSS\_36870 : HP System Management Homepage (SMH) for HP-UX, XSS (HPSBMA02274 SSRT071445 rev.3)

HP-UX PHSS\_36871 : HP System Management Homepage (SMH) for HP-UX, XSS (HPSBMA02274 SSRT071445 rev.3)

HP-UX PHSS\_36901 : s700\_800 11.X OV NNM7.51 PA-RISC Intermediate Patch 17

HP-UX PHSS\_36902 : s700\_800 11.X OV NNM7.51 IA-64 Intermediate Patch 17

HP-UX PHSS\_37141 : s700\_800 11.X OV NNM6.4x/ET2.0x Intermediate Patch 17

HP-UX PHSS\_37182 : HP OpenView Operations (OVO) Running on HP-UX and Solaris, Remote Unauthorized Access, Denial of Service (DoS) (HPSBMA02288 SSRT071465 rev.1)

HP-UX PHSS\_37183 : HP OpenView Operations (OVO) Running on HP-UX and Solaris, Remote Unauthorized Access, Denial of Service (DoS) (HPSBMA02288 SSRT071465 rev.1)

HP-UX PHSS\_37197 : HP OpenView Operations (OVO) Running on HP-UX and Solaris, Remote Unauthorized Access, Denial of Service (DoS) (HPSBMA02288 SSRT071465 rev.1)

HP-UX PHSS\_37224 : HP-UX Running X Font Server (xfs) Software, Remote Execution of Arbitrary Code (HPSBUX02303 SSRT071468 rev.1)

HP-UX PHSS\_37225 : HP-UX Running X Font Server (xfs) Software, Remote Execution of Arbitrary Code (HPSBUX02303 SSRT071468 rev.1)

HP-UX PHSS\_37226 : HP-UX Running X Font Server (xfs) Software, Remote Execution of Arbitrary Code (HPSBUX02303 SSRT071468 rev.1)

HP-UX PHSS\_37273 : s700\_800 11.X OV NNM7.51 PA-RISC Intermediate Patch 18

HP-UX PHSS\_37274 : s700\_800 11.X OV NNM7.51 IA-64 Intermediate Patch 18

HP-UX PHSS\_37335 : HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution (HPSBMA02239 SSRT061260 rev.3)

HP-UX PHSS\_37336 : HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution (HPSBMA02239 SSRT061260 rev.3)

HP-UX PHSS\_37382 : s700\_800 11.X OV DP5.50 PA-RISC patch - CORE packet

HP-UX PHSS\_37383 : s700\_800 11.23 OV DP5.50 IA-64 patch - CORE packet

HP-UX PHSS\_37397 : HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution (HPSBMA02239 SSRT061260 rev.3)

HP-UX PHSS\_37398 : HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution (HPSBMA02239 SSRT061260 rev.3)

HP-UX PHSS\_37399 : HP OpenView Operations (OVO) Agents Running Shared Trace Service, Remote Arbitrary Code Execution (HPSBMA02239 SSRT061260 rev.3)

HP-UX PHSS\_37700 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_37701 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_37702 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_37703 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_37704 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_37891 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_37972 : HP-UX Running Xserver, Remote Execution of Arbitrary Code (HPSBUX02381 SSRT080083 rev.2)

HP-UX PHSS\_38009 : HP OpenView Network Node Manager (OV NNM), Remote Execution of Arbitrary Code, Denial of Service (DoS) (HPSBMA02340 SSRT080024, SSRT080041 rev.1)

HP-UX PHSS\_38147 : s700\_800 11.X OV NNM7.53 PA-RISC Intermediate Patch 19

HP-UX PHSS\_38148 : s700\_800 11.X OV NNM7.53 IA-64 Intermediate Patch 19

HP-UX PHSS\_38183 : HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX02393 SSRT080057 rev.1)

HP-UX PHSS\_38258 : HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX02393 SSRT080057 rev.1)

HP-UX PHSS\_38259 : HP-UX Running DCE, Remote Denial of Service (DoS) (HPSBUX02393 SSRT080057 rev.1)

HP-UX PHSS\_38488 : s700\_800 11.X OV NNM7.53 PA-RISC Intermediate Patch 20

HP-UX PHSS\_38489 : s700\_800 11.X OV NNM7.53 IA-64 Intermediate Patch 20

HP-UX PHSS\_38747 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_38748 : HP-UX running WBEM Services, Remote Execution of Arbitrary Code, Gain Extended Privileges (HPSBMA02331 SSRT080000 rev.3)

HP-UX PHSS\_38761 : s700\_800 11.X OV NNM7.01 Intermediate Patch 12

HP-UX PHSS\_38782 : HP OpenView Network Node Manager (OV NNM), Remote Execution of Arbitrary Code, Unauthorized Access to Data (HPSBMA02406 SSRT080100 rev.2)

HP-UX PHSS\_38783 : HP OpenView Network Node Manager (OV NNM), Remote Execution of Arbitrary Code, Unauthorized Access to Data (HPSBMA02406 SSRT080100 rev.2)

HP-UX PHSS\_38840 : HP-UX Running Xserver, Remote Execution of Arbitrary Code (HPSBUX02381 SSRT080083 rev.2)

HP-UX PHSS\_39015 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39016 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39105 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39106 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39245 : s700\_800 11.X OV NNM7.53 PA-RISC Intermediate Patch 22

HP-UX PHSS\_39246 : s700\_800 11.X OV NNM7.53 IA-64 Intermediate Patch 22

HP-UX PHSS\_39510 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39511 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39514 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39515 : HP OpenView Storage Data Protector, Local Unauthorized Access (HPSBMA02502 SSRT090171 rev.1)

HP-UX PHSS\_39639 : HP OpenView Network Node Manager (OV NNM), Remote Execution of Arbitrary Code (HPSBMA02416 SSRT090008 rev.5)

HP-UX PHSS\_39640 : HP OpenView Network Node Manager (OV NNM), Remote Execution of Arbitrary Code (HPSBMA02416 SSRT090008 rev.5)

HP-UX PHSS\_39765 : HP-UX Running Kerberos, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02421 SSRT090047 rev.2)

HP-UX PHSS\_39766 : HP-UX Running Kerberos, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02421 SSRT090047 rev.2)

HP-UX PHSS\_39774 : HP-UX Running Kerberos, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02421 SSRT090047 rev.2)

HP-UX PHSS\_39886 : HP OpenView SNMP Emanate Master Agent Remote Unauthorized Access (HPSBMA02439 SSRT080082 rev.3)

HP-UX PHSS\_39887 : HP OpenView SNMP Emanate Master Agent Remote Unauthorized Access (HPSBMA02439 SSRT080082 rev.3)

HP-UX PHSS\_40229 : HP Enterprise Cluster Master Toolkit (ECMT) running on HP-UX, Local Unauthorized Access (HPSBUX02464 SSRT090210 rev.1)

HP-UX PHSS\_40230 : HP Enterprise Cluster Master Toolkit (ECMT) running on HP-UX, Local Unauthorized Access (HPSBUX02464 SSRT090210 rev.1)

HP-UX PHSS\_40368 : HP Network Node Manager (NNM), Remote Execution of Arbitrary Commands (HPSBMA02484 SSRT090076 rev.1)

HP-UX PHSS\_40374 : s700\_800 11.X OV NNM7.53 PA-RISC Intermediate Patch 25

HP-UX PHSS\_40375 : s700\_800 11.X OV NNM7.53 IA-64 Intermediate Patch 25

HP-UX PHSS\_40705 : s700\_800 11.11 OV NNM7.01 Intermediate Patch 13

HP-UX PHSS\_40707 : s700\_800 11.X OV NNM7.53 PA-RISC Intermediate Patch 26

HP-UX PHSS\_40708 : s700\_800 11.X OV NNM7.53 IA-64 Intermediate Patch 26

HP-UX PHSS\_41166 : HP-UX Running Kerberos, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02544 SSRT100107 rev.1)

HP-UX PHSS\_41167 : HP-UX Running Kerberos, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02544 SSRT100107 rev.1)

HP-UX PHSS\_41168 : HP-UX Running Kerberos, Remote Denial of Service (DoS), Execution of Arbitrary Code (HPSBUX02544 SSRT100107 rev.1)

HP-UX PHSS\_41174 : HP-UX Running CDE Calendar Manager, Remote Execution of Arbitrary Code (HPSBUX02628 SSRT090183 rev.1)

HP-UX PHSS\_41363 : s700\_800 11.X OV DP6.11 HP-UX PA-Risc - Core patch

HP-UX PHSS\_41364 : s700\_800 11.X OV DP6.11 HP-UX IA64 - Core patch

HP-UX PHSS\_41606 : s700\_800 11.X OV NNM7.53 PA-RISC Intermediate Patch 28

HP-UX PHSS\_41607 : s700\_800 11.X OV NNM7.53 IA-64 Intermediate Patch 28

HP-UX PHSS\_41775 : HP-UX Running Kerberos, Remote Unauthorized Modification (HPSBUX02623 SSRT100355 rev.1)

HP-UX PHSS\_41788 : HP-UX Running CDE Calendar Manager, Remote Execution of Arbitrary Code (HPSBUX02628 SSRT090183 rev.1)

HP-UX PHSS\_41983 : HP Network Node Manager i (NNMi) for HP-UX, Linux, Solaris, and Windows, Remote Unauthorized Access (HPSBMA02659 SSRT100440 rev.2)

HP-UX PHSS\_42040 : HP-UX Dynamic Loader, Local Privilege Escalation, Denial of Service (DoS) (HPSBUX02688 SSRT100513 rev.1)

HP-UX PHSS\_42043 : HP-UX Dynamic Loader, Local Privilege Escalation, Denial of Service (DoS) (HPSBUX02688 SSRT100513 rev.1)

HP-UX PHSS\_42253 : HP-UX Dynamic Loader, Local Privilege Escalation, Denial of Service (DoS) (HPSBUX02688 SSRT100513 rev.1)

HP-UX PHSS\_42328 : s700\_800 11.X OV NNM9.00 NNM 9.0x Patch 5

HP-UX PHSS\_42793 : HP-UX 11.31 OV NNM9.20 NNM 9.2x Patch 1

HP-UX PHSS\_42852 : HP-UX running DCE, Remote Denial of Service (DoS) (HPSBUX02758 SSRT100774 rev.1)

HP-UX PHSS\_42853 : HP-UX running DCE, Remote Denial of Service (DoS) (HPSBUX02758 SSRT100774 rev.1)

HP-UX PHSS\_42865 : HP-UX running DCE, Remote Denial of Service (DoS) (HPSBUX02758 SSRT100774 rev.1)

HP-UX PHSS\_42866 : HP-UX running DCE, Remote Denial of Service (DoS) (HPSBUX02758 SSRT100774 rev.1)

HP-UX PHSS\_42987 : s700\_800 11.23 Serviceguard A.11.19.00

HP-UX PHSS\_42988 : s700\_800 11.31 Serviceguard A.11.19.00

HP-UX PHSS\_43094 : s700\_800 11.31 Serviceguard A.11.20.00

HP-UX PHSS\_43134 : s700\_800 11.31 X Font Server Patch

HP-UX PHSS\_43202 : s700\_800 11.23 X Font Server Patch

HP-UX PHSS\_43355 : s700\_800 11.11 X Font Server Patch

HP-UX PHSS\_43408 : HP-UX 11.31 OV NNM9.20 NNM 9.2x Patch 3

HP-UX PHSS\_43690 : s700\_800 11.31 X/Motif Runtime Patch

HP-UX PHSS\_43889 : s700\_800 11.X OV DP7.00 HP-UX IA/PA - Cell Server patch

HP-UX PHSS\_43890 : s700\_800 11.X OV DP7.00 HP-UX IA/PA - Core patch

HP-UX PHSS\_44149 : s700\_800 11.23 X/Motif Runtime Patch

HP-UX PHSS\_44188 : s700\_800 11.11 X/Motif Runtime Periodic Patch

HP-UX Running NFS/ONCplus, NFS Inadvertently Enabled (HPSBUX02509 SSRT100032 rev.1)

HP-UX Running NFS/ONCplus, Remote Denial of Service (DoS) (HPSBUX02653 SSRT100310)

HP-UX Security patch : PHCO\_10028

HP-UX Security patch : PHCO\_10048

HP-UX Security patch : PHCO\_10052

HP-UX Security patch : PHCO\_10059

HP-UX Security patch : PHCO\_10060

HP-UX Security patch : PHCO\_10061

HP-UX Security patch : PHCO\_10387

HP-UX Security patch : PHCO\_10652

HP-UX Security patch : PHCO\_11004

HP-UX Security patch : PHCO\_11183

HP-UX Security patch : PHCO\_11185

HP-UX Security patch : PHCO\_12326

HP-UX Security patch : PHCO\_12332

HP-UX Security patch : PHCO\_12342

HP-UX Security patch : PHCO\_12344

HP-UX Security patch : PHCO\_12922

HP-UX Security patch : PHCO\_13777

HP-UX Security patch : PHCO\_14253

HP-UX Security patch : PHCO\_14254

HP-UX Security patch : PHCO\_15205

HP-UX Security patch : PHCO\_15206

HP-UX Security patch : PHCO\_17389

HP-UX Security Patch : PHCO\_18103

HP-UX Security Patch : PHCO\_18227

HP-UX Security patch : PHCO\_18615

HP-UX Security Patch : PHCO\_19090

HP-UX Security patch : PHCO\_19120

HP-UX Security Patch : PHCO\_19391

HP-UX Security Patch : PHCO\_19491

HP-UX Security Patch : PHCO\_19691

HP-UX Security Patch : PHCO\_19945

HP-UX Security Patch : PHCO\_20078

HP-UX Security patch : PHCO\_20209

HP-UX Security Patch : PHCO\_20555

HP-UX Security Patch : PHCO\_20765

HP-UX Security patch : PHCO\_20871

HP-UX Security patch : PHCO\_20960

HP-UX Security Patch : PHCO\_21492

HP-UX Security patch : PHCO\_21566

HP-UX Security patch : PHCO\_21574

HP-UX Security patch : PHCO\_21990

HP-UX Security patch : PHCO\_21991

HP-UX Security patch : PHCO\_21992

HP-UX Security Patch : PHCO\_22076

HP-UX Security patch : PHCO\_22185

HP-UX Security patch : PHCO\_22228

HP-UX Security patch : PHCO\_22273

HP-UX Security patch : PHCO\_22275

HP-UX Security Patch : PHCO\_22314

HP-UX Security patch : PHCO\_22324

HP-UX Security patch : PHCO\_22325

HP-UX Security patch : PHCO\_22364

HP-UX Security patch : PHCO\_22410

HP-UX Security patch : PHCO\_22411

HP-UX Security patch : PHCO\_22501

HP-UX Security patch : PHCO\_22502

HP-UX Security patch : PHCO\_22503

HP-UX Security patch : PHCO\_22504

HP-UX Security patch : PHCO\_22556

HP-UX Security patch : PHCO\_22557

HP-UX Security patch : PHCO\_22558

HP-UX Security patch : PHCO\_22571

HP-UX Security patch : PHCO\_22572

HP-UX Security patch : PHCO\_22591

HP-UX Security patch : PHCO\_22634

HP-UX Security patch : PHCO\_22763

HP-UX Security patch : PHCO\_22764

HP-UX Security patch : PHCO\_22765

HP-UX Security patch : PHCO\_22768

HP-UX Security patch : PHCO\_22769

HP-UX Security patch : PHCO\_22770

HP-UX Security patch : PHCO\_22848

HP-UX Security patch : PHCO\_22849

HP-UX Security patch : PHCO\_22922

HP-UX Security Patch : PHCO\_22923

HP-UX Security Patch : PHCO\_22957

HP-UX Security patch : PHCO\_23089

HP-UX Security patch : PHCO\_23090

HP-UX Security patch : PHCO\_23091

HP-UX Security Patch : PHCO\_23117

HP-UX Security Patch : PHCO\_23118

HP-UX Security patch : PHCO\_23319

HP-UX Security patch : PHCO\_23320

HP-UX Security patch : PHCO\_23321

HP-UX Security patch : PHCO\_23353

HP-UX Security patch : PHCO\_23455

HP-UX Security Patch : PHCO\_23770

HP-UX Security Patch : PHCO\_23966

HP-UX Security Patch : PHCO\_24148

HP-UX Security patch : PHCO\_24267

HP-UX Security patch : PHCO\_24454

HP-UX Security patch : PHCO\_24697

HP-UX Security patch : PHCO\_24698

HP-UX Security patch : PHCO\_24699

HP-UX Security Patch : PHCO\_24702

HP-UX Security Patch : PHCO\_25064

HP-UX Security patch : PHCO\_25107

HP-UX Security patch : PHCO\_25108

HP-UX Security patch : PHCO\_25109

HP-UX Security Patch : PHCO\_25342

HP-UX Security Patch : PHCO\_25429

HP-UX Security Patch : PHCO\_25526

HP-UX Security Patch : PHCO\_25590

HP-UX Security Patch : PHCO\_25707

HP-UX Security Patch : PHCO\_25893

HP-UX Security Patch : PHCO\_25976

HP-UX Security Patch : PHCO\_26020

HP-UX Security Patch : PHCO\_26021

HP-UX Security Patch : PHCO\_26060

HP-UX Security Patch : PHCO\_26061

HP-UX Security Patch : PHCO\_26089

HP-UX Security patch : PHCO\_26158

HP-UX Security Patch : PHCO\_26235

HP-UX Security Patch : PHCO\_27004

HP-UX Security Patch : PHCO\_27037

HP-UX Security patch : PHCO\_27133

HP-UX Security Patch : PHCO\_27141

HP-UX Security patch : PHCO\_27560

HP-UX Security patch : PHCO\_27564

HP-UX Security Patch : PHCO\_27608

HP-UX Security Patch : PHCO\_27671

HP-UX Security Patch : PHCO\_27672

HP-UX Security Patch : PHCO\_27694

HP-UX Security Patch : PHCO\_27721

HP-UX Security Patch : PHCO\_27731

HP-UX Security Patch : PHCO\_27774

HP-UX Security patch : PHCO\_27803

HP-UX Security patch : PHCO\_27804

HP-UX Security patch : PHCO\_27819

HP-UX Security patch : PHCO\_27882

HP-UX Security patch : PHCO\_27940

HP-UX Security patch : PHCO\_28128

HP-UX Security patch : PHCO\_28142

HP-UX Security Patch : PHCO\_28259

HP-UX Security Patch : PHCO\_28320

HP-UX Security Patch : PHCO\_28329

HP-UX Security Patch : PHCO\_28346

HP-UX Security Patch : PHCO\_28419

HP-UX Security Patch : PHCO\_28630

HP-UX Security patch : PHCO\_28717

HP-UX Security Patch : PHCO\_28831

HP-UX Security Patch : PHCO\_28832

HP-UX Security Patch : PHCO\_29029

HP-UX Security Patch : PHCO\_29269

HP-UX Security Patch : PHCO\_29287

HP-UX Security Patch : PHCO\_29352

HP-UX Security Patch : PHCO\_29633

HP-UX Security Patch : PHCO\_29674

HP-UX Security Patch : PHCO\_29768

HP-UX Security Patch : PHCO\_29955

HP-UX Security Patch : PHCO\_29956

HP-UX Security Patch : PHCO\_30000

HP-UX Security Patch : PHCO\_30005

HP-UX Security Patch : PHCO\_30030

HP-UX Security patch : PHCO\_30063

HP-UX Security Patch : PHCO\_30269

HP-UX Security Patch : PHCO\_30275

HP-UX Security Patch : PHCO\_30316

HP-UX Security Patch : PHCO\_30431

HP-UX Security Patch : PHCO\_30530

HP-UX Security Patch : PHCO\_30533

HP-UX Security Patch : PHCO\_31016

HP-UX Security Patch : PHCO\_31061

HP-UX Security Patch : PHCO\_31106

HP-UX Security Patch : PHCO\_31160

HP-UX Security Patch : PHCO\_31815

HP-UX Security Patch : PHCO\_31879

HP-UX Security Patch : PHCO\_31903

HP-UX Security Patch : PHCO\_31921

HP-UX Security Patch : PHCO\_31922

HP-UX Security Patch : PHCO\_32116

HP-UX Security Patch : PHCO\_32181

HP-UX Security Patch : PHCO\_32222

HP-UX Security Patch : PHCO\_32448

HP-UX Security Patch : PHCO\_32565

HP-UX Security Patch : PHCO\_32719

HP-UX Security Patch : PHCO\_32761

HP-UX Security Patch : PHCO\_32773

HP-UX Security Patch : PHCO\_32873

HP-UX Security Patch : PHCO\_33021

HP-UX Security Patch : PHCO\_33169

HP-UX Security Patch : PHCO\_33360

HP-UX Security Patch : PHCO\_33375

HP-UX Security Patch : PHCO\_33401

HP-UX Security Patch : PHCO\_33488

HP-UX Security Patch : PHCO\_33533

HP-UX Security Patch : PHCO\_33609

HP-UX Security Patch : PHCO\_33711

HP-UX Security Patch : PHCO\_33758

HP-UX Security Patch : PHCO\_34240

HP-UX Security Patch : PHCO\_34275

HP-UX Security Patch : PHCO\_34295

HP-UX Security Patch : PHCO\_34509

HP-UX Security Patch : PHCO\_34562

HP-UX Security Patch : PHCO\_34714

HP-UX Security Patch : PHCO\_34765

HP-UX Security Patch : PHCO\_34822

HP-UX Security Patch : PHCO\_34993

HP-UX Security Patch : PHCO\_35250

HP-UX Security Patch : PHCO\_35251

HP-UX Security Patch : PHCO\_35732

HP-UX Security Patch : PHCO\_35743

HP-UX Security Patch : PHCO\_35849

HP-UX Security Patch : PHCO\_35850

HP-UX Security Patch : PHCO\_35874

HP-UX Security Patch : PHCO\_35929

HP-UX Security Patch : PHCO\_36131

HP-UX Security Patch : PHCO\_36145

HP-UX Security Patch : PHCO\_36239

HP-UX Security Patch : PHCO\_36426

HP-UX Security Patch : PHCO\_36465

HP-UX Security Patch : PHCO\_36759

HP-UX Security Patch : PHCO\_38481

HP-UX Security Patch : PHCO\_38482

HP-UX Security Patch : PHCO\_38490

HP-UX Security patch : PHCO\_6157

HP-UX Security patch : PHCO\_7798

HP-UX Security patch : PHCO\_8652

HP-UX Security patch : PHCO\_8653

HP-UX Security patch : PHCO\_8654

HP-UX Security patch : PHCO\_9596

HP-UX Security patch : PHCO\_9597

HP-UX Security patch : PHCO\_9601

HP-UX Security patch : PHCO\_9602

HP-UX Security patch : PHCO\_9604

HP-UX Security patch : PHCO\_9605

HP-UX Security patch : PHCO\_9640

HP-UX Security patch : PHCO\_9641

HP-UX Security patch : PHKL\_12007

HP-UX Security patch : PHKL\_12008

HP-UX Security patch : PHKL\_14242

HP-UX Security patch : PHKL\_14243

HP-UX Security patch : PHKL\_16750

HP-UX Security patch : PHKL\_16751

HP-UX Security patch : PHKL\_16957

HP-UX Security patch : PHKL\_16959

HP-UX Security patch : PHKL\_17012

HP-UX Security patch : PHKL\_17013

HP-UX Security patch : PHKL\_17253

HP-UX Security patch : PHKL\_17254

HP-UX Security Patch : PHKL\_20315

HP-UX Security Patch : PHKL\_21361

HP-UX Security Patch : PHKL\_21608

HP-UX Security Patch : PHKL\_22142

HP-UX Security Patch : PHKL\_22517

HP-UX Security Patch : PHKL\_22589

HP-UX Security patch : PHKL\_22701

HP-UX Security patch : PHKL\_22702

HP-UX Security patch : PHKL\_23477

HP-UX Security patch : PHKL\_23478

HP-UX Security patch : PHKL\_23512

HP-UX Security patch : PHKL\_23513

HP-UX Security Patch : PHKL\_23812

HP-UX Security Patch : PHKL\_23813

HP-UX Security Patch : PHKL\_23857

HP-UX Security Patch : PHKL\_24015

HP-UX Security Patch : PHKL\_24116

HP-UX Security patch : PHKL\_24249

HP-UX Security patch : PHKL\_24250

HP-UX Security Patch : PHKL\_24273

HP-UX Security Patch : PHKL\_24457

HP-UX Security patch : PHKL\_24517

HP-UX Security patch : PHKL\_24518

HP-UX Security Patch : PHKL\_24612

HP-UX Security Patch : PHKL\_24734

HP-UX Security Patch : PHKL\_24753

HP-UX Security Patch : PHKL\_24826

HP-UX Security Patch : PHKL\_24943

HP-UX Security Patch : PHKL\_24971

HP-UX Security Patch : PHKL\_25044

HP-UX Security Patch : PHKL\_25164

HP-UX Security Patch : PHKL\_25188

HP-UX Security Patch : PHKL\_25210

HP-UX Security patch : PHKL\_25243

HP-UX Security patch : PHKL\_25244

HP-UX Security Patch : PHKL\_25475

HP-UX Security Patch : PHKL\_25525

HP-UX Security Patch : PHKL\_25906

HP-UX Security Patch : PHKL\_25999

HP-UX Security Patch : PHKL\_26059

HP-UX Security Patch : PHKL\_26794

HP-UX Security Patch : PHKL\_26800

HP-UX Security Patch : PHKL\_26815

HP-UX Security Patch : PHKL\_27070

HP-UX Security Patch : PHKL\_27089

HP-UX Security Patch : PHKL\_27157

HP-UX Security Patch : PHKL\_27238

HP-UX Security Patch : PHKL\_27278

HP-UX Security Patch : PHKL\_27351

HP-UX Security Patch : PHKL\_27364

HP-UX Security Patch : PHKL\_27510

HP-UX Security Patch : PHKL\_27648

HP-UX Security Patch : PHKL\_27710

HP-UX Security Patch : PHKL\_27759

HP-UX Security Patch : PHKL\_27770

HP-UX Security Patch : PHKL\_27813

HP-UX Security patch : PHKL\_27832

HP-UX Security patch : PHKL\_27833

HP-UX Security Patch : PHKL\_27919

HP-UX Security Patch : PHKL\_27994

HP-UX Security Patch : PHKL\_28053

HP-UX Security Patch : PHKL\_28105

HP-UX Security Patch : PHKL\_28152

HP-UX Security Patch : PHKL\_28180

HP-UX Security Patch : PHKL\_28202

HP-UX Security Patch : PHKL\_28267

HP-UX Security Patch : PHKL\_28428

HP-UX Security Patch : PHKL\_28766

HP-UX Security Patch : PHKL\_28990

HP-UX Security Patch : PHKL\_29345

HP-UX Security Patch : PHKL\_29434

HP-UX Security Patch : PHKL\_29648

HP-UX Security Patch : PHKL\_29760

HP-UX Security Patch : PHKL\_29851

HP-UX Security Patch : PHKL\_29911

HP-UX Security Patch : PHKL\_30158

HP-UX Security Patch : PHKL\_30190

HP-UX Security Patch : PHKL\_30578

HP-UX Security Patch : PHKL\_30616

HP-UX Security Patch : PHKL\_30690

HP-UX Security Patch : PHKL\_30709

HP-UX Security Patch : PHKL\_31003

HP-UX Security Patch : PHKL\_31867

HP-UX Security Patch : PHKL\_31983

HP-UX Security Patch : PHKL\_32035

HP-UX Security Patch : PHKL\_32204

HP-UX Security Patch : PHKL\_32355

HP-UX Security Patch : PHKL\_32578

HP-UX Security Patch : PHKL\_32772

HP-UX Security Patch : PHKL\_32806

HP-UX Security Patch : PHKL\_33158

HP-UX Security Patch : PHKL\_33258

HP-UX Security Patch : PHKL\_33261

HP-UX Security Patch : PHKL\_33268

HP-UX Security Patch : PHKL\_33270

HP-UX Security Patch : PHKL\_33355

HP-UX Security Patch : PHKL\_33484

HP-UX Security Patch : PHKL\_33500

HP-UX Security Patch : PHKL\_33526

HP-UX Security Patch : PHKL\_33819

HP-UX Security Patch : PHKL\_33920

HP-UX Security Patch : PHKL\_33988

HP-UX Security Patch : PHKL\_34039

HP-UX Security Patch : PHKL\_34095

HP-UX Security Patch : PHKL\_34122

HP-UX Security Patch : PHKL\_34153

HP-UX Security Patch : PHKL\_34341

HP-UX Security Patch : PHKL\_34432

HP-UX Security Patch : PHKL\_34665

HP-UX Security Patch : PHKL\_34805

HP-UX Security Patch : PHKL\_35464

HP-UX Security Patch : PHKL\_35564

HP-UX Security Patch : PHKL\_35828

HP-UX Security Patch : PHKL\_35847

HP-UX Security Patch : PHKL\_41156

HP-UX Security Patch : PHKL\_41421

HP-UX Security Patch : PHKL\_42310

HP-UX Security patch : PHKL\_7059

HP-UX Security patch : PHKL\_7060

HP-UX Security patch : PHKL\_8292

HP-UX Security patch : PHKL\_8293

HP-UX Security patch : PHKL\_9155

HP-UX Security patch : PHKL\_9156

HP-UX Security patch : PHKL\_9579

HP-UX Security patch : PHKL\_9580

HP-UX Security patch : PHNE\_10009

HP-UX Security patch : PHNE\_10010

HP-UX Security patch : PHNE\_10011

HP-UX Security patch : PHNE\_10042

HP-UX Security patch : PHNE\_10043

HP-UX Security patch : PHNE\_10090

HP-UX Security patch : PHNE\_10341

HP-UX Security patch : PHNE\_10469

HP-UX Security patch : PHNE\_10470

HP-UX Security patch : PHNE\_10475

HP-UX Security patch : PHNE\_10476

HP-UX Security patch : PHNE\_11096

HP-UX Security patch : PHNE\_11097

HP-UX Security patch : PHNE\_11722

HP-UX Security patch : PHNE\_11723

HP-UX Security patch : PHNE\_11724

HP-UX Security patch : PHNE\_11727

HP-UX Security patch : PHNE\_11728

HP-UX Security patch : PHNE\_12499

HP-UX Security patch : PHNE\_12608

HP-UX Security patch : PHNE\_12836

HP-UX Security patch : PHNE\_12866

HP-UX Security patch : PHNE\_13180

HP-UX Security patch : PHNE\_13181

HP-UX Security patch : PHNE\_13182

HP-UX Security patch : PHNE\_13468

HP-UX Security patch : PHNE\_13469

HP-UX Security patch : PHNE\_13470

HP-UX Security patch : PHNE\_13471

HP-UX Security patch : PHNE\_13472

HP-UX Security patch : PHNE\_13473

HP-UX Security patch : PHNE\_13474

HP-UX Security patch : PHNE\_13475

HP-UX Security patch : PHNE\_13596

HP-UX Security patch : PHNE\_13597

HP-UX Security patch : PHNE\_13618

HP-UX Security patch : PHNE\_13619

HP-UX Security patch : PHNE\_13671

HP-UX Security patch : PHNE\_13888

HP-UX Security patch : PHNE\_13889

HP-UX Security patch : PHNE\_14042

HP-UX Security patch : PHNE\_14086

HP-UX Security patch : PHNE\_14087

HP-UX Security Patch : PHNE\_14279

HP-UX Security patch : PHNE\_14377

HP-UX Security patch : PHNE\_14617

HP-UX Security Patch : PHNE\_14618

HP-UX Security patch : PHNE\_14655

HP-UX Security Patch : PHNE\_14702

HP-UX Security Patch : PHNE\_15047

HP-UX Security Patch : PHNE\_15509

HP-UX Security patch : PHNE\_15544

HP-UX Security Patch : PHNE\_15583

HP-UX Security Patch : PHNE\_15692

HP-UX Security patch : PHNE\_15802

HP-UX Security Patch : PHNE\_15995

HP-UX Security patch : PHNE\_16006

HP-UX Security patch : PHNE\_16204

HP-UX Security patch : PHNE\_16237

HP-UX Security Patch : PHNE\_16283

HP-UX Security Patch : PHNE\_16645

HP-UX Security patch : PHNE\_16726

HP-UX Security Patch : PHNE\_16852

HP-UX Security patch : PHNE\_16955

HP-UX Security Patch : PHNE\_17017

HP-UX Security Patch : PHNE\_17028

HP-UX Security patch : PHNE\_17097

HP-UX Security patch : PHNE\_17098

HP-UX Security Patch : PHNE\_17101

HP-UX Security Patch : PHNE\_17106

HP-UX Security patch : PHNE\_17135

HP-UX Security Patch : PHNE\_17188

HP-UX Security Patch : PHNE\_17200

HP-UX Security patch : PHNE\_17248

HP-UX Security Patch : PHNE\_17446

HP-UX Security Patch : PHNE\_17662

HP-UX Security patch : PHNE\_17948

HP-UX Security Patch : PHNE\_18221

HP-UX Security Patch : PHNE\_18354

HP-UX Security Patch : PHNE\_18546

HP-UX Security Patch : PHNE\_18554

HP-UX Security Patch : PHNE\_18611

HP-UX Security Patch : PHNE\_18708

HP-UX Security Patch : PHNE\_19110

HP-UX Security Patch : PHNE\_19375

HP-UX Security Patch : PHNE\_19620

HP-UX Security Patch : PHNE\_19899

HP-UX Security Patch : PHNE\_20436

HP-UX Security patch : PHNE\_20618

HP-UX Security patch : PHNE\_20628

HP-UX Security Patch : PHNE\_20714

HP-UX Security Patch : PHNE\_20735

HP-UX Security patch : PHNE\_20747

HP-UX Security patch : PHNE\_21288

HP-UX Security Patch : PHNE\_21376

HP-UX Security Patch : PHNE\_21581

HP-UX Security patch : PHNE\_21699

HP-UX Security Patch : PHNE\_21731

HP-UX Security patch : PHNE\_22057

HP-UX Security patch : PHNE\_22058

HP-UX Security patch : PHNE\_22059

HP-UX Security Patch : PHNE\_22125

HP-UX Security Patch : PHNE\_22397

HP-UX Security Patch : PHNE\_22642

HP-UX Security Patch : PHNE\_23003

HP-UX Security Patch : PHNE\_23249

HP-UX Security Patch : PHNE\_23257

HP-UX Security patch : PHNE\_23277

HP-UX Security patch : PHNE\_23439

HP-UX Security Patch : PHNE\_23456

HP-UX Security patch : PHNE\_23717

HP-UX Security Patch : PHNE\_23833

HP-UX Security patch : PHNE\_23947

HP-UX Security patch : PHNE\_23948

HP-UX Security patch : PHNE\_24076

HP-UX Security Patch : PHNE\_24084

HP-UX Security patch : PHNE\_24394

HP-UX Security patch : PHNE\_24510

HP-UX Security patch : PHNE\_24820

HP-UX Security patch : PHNE\_24821

HP-UX Security patch : PHNE\_24822

HP-UX Security Patch : PHNE\_24909

HP-UX Security Patch : PHNE\_24910

HP-UX Security patch : PHNE\_25183

HP-UX Security patch : PHNE\_25217

HP-UX Security Patch : PHNE\_25423

HP-UX Security Patch : PHNE\_25484

HP-UX Security Patch : PHNE\_25625

HP-UX Security Patch : PHNE\_25626

HP-UX Security Patch : PHNE\_25627

HP-UX Security Patch : PHNE\_25900

HP-UX Security Patch : PHNE\_25937

HP-UX Security patch : PHNE\_26003

HP-UX Security Patch : PHNE\_26305

HP-UX Security Patch : PHNE\_26387

HP-UX Security Patch : PHNE\_26388

HP-UX Security Patch : PHNE\_27063

HP-UX Security Patch : PHNE\_27217

HP-UX Security Patch : PHNE\_27218

HP-UX Security Patch : PHNE\_27765

HP-UX Security Patch : PHNE\_27886

HP-UX Security patch : PHNE\_28002

HP-UX Security Patch : PHNE\_28089

HP-UX Security Patch : PHNE\_28312

HP-UX Security Patch : PHNE\_28476

HP-UX Security Patch : PHNE\_28525

HP-UX Security patch : PHNE\_28535

HP-UX Security patch : PHNE\_28536

HP-UX Security Patch : PHNE\_28567

HP-UX Security Patch : PHNE\_28568

HP-UX Security patch : PHNE\_28635

HP-UX Security patch : PHNE\_28760

HP-UX Security Patch : PHNE\_28786

HP-UX Security Patch : PHNE\_28809

HP-UX Security Patch : PHNE\_28810

HP-UX Security Patch : PHNE\_28882

HP-UX Security patch : PHNE\_28886

HP-UX Security Patch : PHNE\_29302

HP-UX Security Patch : PHNE\_29303

HP-UX Security Patch : PHNE\_29387

HP-UX Security Patch : PHNE\_29445

HP-UX Security Patch : PHNE\_29463

HP-UX Security Patch : PHNE\_29530

HP-UX Security Patch : PHNE\_29773

HP-UX Security Patch : PHNE\_29774

HP-UX Security Patch : PHNE\_29825

HP-UX Security Patch : PHNE\_29882

HP-UX Security Patch : PHNE\_29883

HP-UX Security Patch : PHNE\_29913

HP-UX Security Patch : PHNE\_30007

HP-UX Security Patch : PHNE\_30367

HP-UX Security Patch : PHNE\_30377

HP-UX Security Patch : PHNE\_30378

HP-UX Security Patch : PHNE\_30380

HP-UX Security Patch : PHNE\_30432

HP-UX Security Patch : PHNE\_30450

HP-UX Security Patch : PHNE\_30660

HP-UX Security Patch : PHNE\_30661

HP-UX Security Patch : PHNE\_31091

HP-UX Security Patch : PHNE\_31096

HP-UX Security Patch : PHNE\_31097

HP-UX Security Patch : PHNE\_31247

HP-UX Security Patch : PHNE\_31821

HP-UX Security Patch : PHNE\_31822

HP-UX Security Patch : PHNE\_31917

HP-UX Security Patch : PHNE\_31929

HP-UX Security Patch : PHNE\_31965

HP-UX Security Patch : PHNE\_32041

HP-UX Security Patch : PHNE\_32286

HP-UX Security Patch : PHNE\_32477

HP-UX Security Patch : PHNE\_32643

HP-UX Security Patch : PHNE\_32811

HP-UX Security Patch : PHNE\_32825

HP-UX Security Patch : PHNE\_33313

HP-UX Security Patch : PHNE\_33315

HP-UX Security Patch : PHNE\_33498

HP-UX Security Patch : PHNE\_33628

HP-UX Security Patch : PHNE\_33729

HP-UX Security Patch : PHNE\_33766

HP-UX Security Patch : PHNE\_33789

HP-UX Security Patch : PHNE\_33793

HP-UX Security Patch : PHNE\_33798

HP-UX Security Patch : PHNE\_33971

HP-UX Security Patch : PHNE\_34104

HP-UX Security Patch : PHNE\_34135

HP-UX Security Patch : PHNE\_34150

HP-UX Security Patch : PHNE\_34226

HP-UX Security Patch : PHNE\_34293

HP-UX Security Patch : PHNE\_34662

HP-UX Security Patch : PHNE\_34698

HP-UX Security Patch : PHNE\_34777

HP-UX Security Patch : PHNE\_34938

HP-UX Security Patch : PHNE\_35314

HP-UX Security Patch : PHNE\_35418

HP-UX Security Patch : PHNE\_35453

HP-UX Security Patch : PHNE\_35545

HP-UX Security Patch : PHNE\_35730

HP-UX Security Patch : PHNE\_35765

HP-UX Security Patch : PHNE\_35871

HP-UX Security Patch : PHNE\_35950

HP-UX Security Patch : PHNE\_35951

HP-UX Security Patch : PHNE\_36065

HP-UX Security Patch : PHNE\_36129

HP-UX Security Patch : PHNE\_36217

HP-UX Security Patch : PHNE\_36219

HP-UX Security Patch : PHNE\_41721

HP-UX Security patch : PHNE\_5965

HP-UX Security patch : PHNE\_6976

HP-UX Security patch : PHNE\_7343

HP-UX Security patch : PHNE\_7919

HP-UX Security patch : PHNE\_7920

HP-UX Security patch : PHNE\_8018

HP-UX Security patch : PHNE\_8019

HP-UX Security patch : PHNE\_8020

HP-UX Security patch : PHNE\_8063

HP-UX Security patch : PHNE\_8064

HP-UX Security patch : PHNE\_8107

HP-UX Security patch : PHNE\_8168

HP-UX Security patch : PHNE\_8169

HP-UX Security patch : PHNE\_8806

HP-UX Security patch : PHNE\_8807

HP-UX Security patch : PHNE\_9030

HP-UX Security patch : PHNE\_9031

HP-UX Security patch : PHNE\_9032

HP-UX Security patch : PHNE\_9033

HP-UX Security patch : PHNE\_9034

HP-UX Security patch : PHNE\_9035

HP-UX Security patch : PHNE\_9036

HP-UX Security patch : PHNE\_9037

HP-UX Security patch : PHNE\_9102

HP-UX Security patch : PHNE\_9103

HP-UX Security patch : PHNE\_9104

HP-UX Security patch : PHNE\_9105

HP-UX Security patch : PHNE\_9106

HP-UX Security patch : PHNE\_9107

HP-UX Security patch : PHNE\_9375

HP-UX Security patch : PHNE\_9376

HP-UX Security patch : PHNE\_9377

HP-UX Security patch : PHNE\_9504

HP-UX Security patch : PHNE\_9624

HP-UX Security patch : PHNE\_9771

HP-UX Security patch : PHSS\_10337

HP-UX Security patch : PHSS\_10613

HP-UX Security patch : PHSS\_10688

HP-UX Security patch : PHSS\_10786

HP-UX Security patch : PHSS\_10789

HP-UX Security patch : PHSS\_11021

HP-UX Security patch : PHSS\_11043

HP-UX Security patch : PHSS\_11044

HP-UX Security patch : PHSS\_11045

HP-UX Security patch : PHSS\_11628

HP-UX Security patch : PHSS\_11629

HP-UX Security patch : PHSS\_11630

HP-UX Security patch : PHSS\_12137

HP-UX Security patch : PHSS\_12138

HP-UX Security patch : PHSS\_12139

HP-UX Security patch : PHSS\_12151

HP-UX Security patch : PHSS\_12152

HP-UX Security patch : PHSS\_12865

HP-UX Security patch : PHSS\_12961

HP-UX Security Patch : PHSS\_13406

HP-UX Security patch : PHSS\_13723

HP-UX Security patch : PHSS\_13724

HP-UX Security patch : PHSS\_13725

HP-UX Security patch : PHSS\_13772

HP-UX Security Patch : PHSS\_13961

HP-UX Security Patch : PHSS\_14597

HP-UX Security patch : PHSS\_15423

HP-UX Security Patch : PHSS\_15424

HP-UX Security patch : PHSS\_15532

HP-UX Security patch : PHSS\_15533

HP-UX Security patch : PHSS\_15534

HP-UX Security patch : PHSS\_15535

HP-UX Security Patch : PHSS\_15536

HP-UX Security Patch : PHSS\_15797

HP-UX Security patch : PHSS\_15935

HP-UX Security patch : PHSS\_15936

HP-UX Security patch : PHSS\_15993

HP-UX Security patch : PHSS\_15994

HP-UX Security patch : PHSS\_16147

HP-UX Security patch : PHSS\_16150

HP-UX Security patch : PHSS\_16151

HP-UX Security patch : PHSS\_16197

HP-UX Security Patch : PHSS\_16359

HP-UX Security patch : PHSS\_16473

HP-UX Security patch : PHSS\_16478

HP-UX Security patch : PHSS\_16533

HP-UX Security patch : PHSS\_16646

HP-UX Security patch : PHSS\_16647

HP-UX Security patch : PHSS\_16648

HP-UX Security Patch : PHSS\_16706

HP-UX Security Patch : PHSS\_16756

HP-UX Security patch : PHSS\_16800

HP-UX Security patch : PHSS\_16845

HP-UX Security patch : PHSS\_17083

HP-UX Security patch : PHSS\_17168

HP-UX Security Patch : PHSS\_17310

HP-UX Security Patch : PHSS\_17387

HP-UX Security Patch : PHSS\_17419

HP-UX Security patch : PHSS\_17478

HP-UX Security patch : PHSS\_17479

HP-UX Security patch : PHSS\_17480

HP-UX Security patch : PHSS\_17482

HP-UX Security Patch : PHSS\_17496

HP-UX Security patch : PHSS\_17580

HP-UX Security patch : PHSS\_17598

HP-UX Security patch : PHSS\_17599

HP-UX Security patch : PHSS\_17830

HP-UX Security Patch : PHSS\_17945

HP-UX Security Patch : PHSS\_18428

HP-UX Security patch : PHSS\_19376

HP-UX Security patch : PHSS\_19387

HP-UX Security patch : PHSS\_19388

HP-UX Security patch : PHSS\_19389

HP-UX Security patch : PHSS\_19482

HP-UX Security patch : PHSS\_19702

HP-UX Security patch : PHSS\_19739

HP-UX Security patch : PHSS\_19747

HP-UX Security patch : PHSS\_19819

HP-UX Security Patch : PHSS\_20140

HP-UX Security Patch : PHSS\_20385

HP-UX Security Patch : PHSS\_20444

HP-UX Security patch : PHSS\_20476

HP-UX Security Patch : PHSS\_20544

HP-UX Security Patch : PHSS\_20716

HP-UX Security Patch : PHSS\_20864

HP-UX Security Patch : PHSS\_21046

HP-UX Security Patch : PHSS\_21326

HP-UX Security Patch : PHSS\_21614

HP-UX Security Patch : PHSS\_21637

HP-UX Security patch : PHSS\_21662

HP-UX Security patch : PHSS\_22061

HP-UX Security patch : PHSS\_22187

HP-UX Security patch : PHSS\_22319

HP-UX Security Patch : PHSS\_22341

HP-UX Security patch : PHSS\_22406

HP-UX Security Patch : PHSS\_22424

HP-UX Security patch : PHSS\_22546

HP-UX Security Patch : PHSS\_22683

HP-UX Security Patch : PHSS\_22876

HP-UX Security patch : PHSS\_22914

HP-UX Security Patch : PHSS\_22936

HP-UX Security patch : PHSS\_23064

HP-UX Security patch : PHSS\_23065

HP-UX Security patch : PHSS\_23095

HP-UX Security patch : PHSS\_23103

HP-UX Security patch : PHSS\_23264

HP-UX Security patch : PHSS\_23265

HP-UX Security patch : PHSS\_23267

HP-UX Security patch : PHSS\_23268

HP-UX Security Patch : PHSS\_23332

HP-UX Security patch : PHSS\_23355

HP-UX Security Patch : PHSS\_23511

HP-UX Security Patch : PHSS\_23517

HP-UX Security Patch : PHSS\_23526

HP-UX Security patch : PHSS\_23632

HP-UX Security Patch : PHSS\_23655

HP-UX Security Patch : PHSS\_23670

HP-UX Security Patch : PHSS\_23688

HP-UX Security patch : PHSS\_23779

HP-UX Security patch : PHSS\_23796

HP-UX Security Patch : PHSS\_23800

HP-UX Security Patch : PHSS\_23840

HP-UX Security Patch : PHSS\_23847

HP-UX Security Patch : PHSS\_23927

HP-UX Security Patch : PHSS\_23975

HP-UX Security Patch : PHSS\_24009

HP-UX Security Patch : PHSS\_24019

HP-UX Security Patch : PHSS\_24033

HP-UX Security Patch : PHSS\_24070

HP-UX Security patch : PHSS\_24097

HP-UX Security Patch : PHSS\_24203

HP-UX Security Patch : PHSS\_24298

HP-UX Security Patch : PHSS\_24363

HP-UX Security Patch : PHSS\_24424

HP-UX Security Patch : PHSS\_24430

HP-UX Security Patch : PHSS\_24443

HP-UX Security patch : PHSS\_24497

HP-UX Security Patch : PHSS\_24527

HP-UX Security patch : PHSS\_24534

HP-UX Security Patch : PHSS\_24536

HP-UX Security Patch : PHSS\_24604

HP-UX Security patch : PHSS\_24797

HP-UX Security Patch : PHSS\_24836

HP-UX Security patch : PHSS\_24842

HP-UX Security Patch : PHSS\_24850

HP-UX Security patch : PHSS\_24863

HP-UX Security Patch : PHSS\_24945

HP-UX Security patch : PHSS\_24946

HP-UX Security Patch : PHSS\_25088

HP-UX Security patch : PHSS\_25136

HP-UX Security patch : PHSS\_25137

HP-UX Security Patch : PHSS\_25194

HP-UX Security Patch : PHSS\_25196

HP-UX Security Patch : PHSS\_25197

HP-UX Security Patch : PHSS\_25208

HP-UX Security Patch : PHSS\_25225

HP-UX Security Patch : PHSS\_25344

HP-UX Security Patch : PHSS\_25350

HP-UX Security Patch : PHSS\_25365

HP-UX Security patch : PHSS\_25419

HP-UX Security Patch : PHSS\_25432

HP-UX Security Patch : PHSS\_25435

HP-UX Security Patch : PHSS\_25499

HP-UX Security Patch : PHSS\_25595

HP-UX Security Patch : PHSS\_25661

HP-UX Security Patch : PHSS\_25662

HP-UX Security Patch : PHSS\_25703

HP-UX Security Patch : PHSS\_25743

HP-UX Security patch : PHSS\_25785

HP-UX Security patch : PHSS\_25786

HP-UX Security Patch : PHSS\_25789

HP-UX Security Patch : PHSS\_25820

HP-UX Security Patch : PHSS\_25843

HP-UX Security Patch : PHSS\_25935

HP-UX Security Patch : PHSS\_25944

HP-UX Security patch : PHSS\_26029

HP-UX Security patch : PHSS\_26137

HP-UX Security Patch : PHSS\_26338

HP-UX Security patch : PHSS\_26367

HP-UX Security Patch : PHSS\_26490

HP-UX Security Patch : PHSS\_26492

HP-UX Security Patch : PHSS\_26493

HP-UX Security patch : PHSS\_26510

HP-UX Security Patch : PHSS\_26553

HP-UX Security Patch : PHSS\_26625

HP-UX Security Patch : PHSS\_26650

HP-UX Security Patch : PHSS\_26750

HP-UX Security patch : PHSS\_26777

HP-UX Security Patch : PHSS\_26802

HP-UX Security patch : PHSS\_26806

HP-UX Security patch : PHSS\_26908

HP-UX Security patch : PHSS\_26918

HP-UX Security patch : PHSS\_26932

HP-UX Security Patch : PHSS\_27002

HP-UX Security Patch : PHSS\_27014

HP-UX Security Patch : PHSS\_27069

HP-UX Security Patch : PHSS\_27125

HP-UX Security Patch : PHSS\_27158

HP-UX Security Patch : PHSS\_27174

HP-UX Security patch : PHSS\_27181

HP-UX Security Patch : PHSS\_27184

HP-UX Security Patch : PHSS\_27192

HP-UX Security Patch : PHSS\_27206

HP-UX Security Patch : PHSS\_27227

HP-UX Security Patch : PHSS\_27262

HP-UX Security patch : PHSS\_27273

HP-UX Security Patch : PHSS\_27300

HP-UX Security Patch : PHSS\_27323

HP-UX Security Patch : PHSS\_27333

HP-UX Security patch : PHSS\_27426

HP-UX Security patch : PHSS\_27437

HP-UX Security Patch : PHSS\_27440

HP-UX Security Patch : PHSS\_27479

HP-UX Security Patch : PHSS\_27570

HP-UX Security Patch : PHSS\_27590

HP-UX Security patch : PHSS\_27638

HP-UX Security Patch : PHSS\_27696

HP-UX Security Patch : PHSS\_27747

HP-UX Security patch : PHSS\_27783

HP-UX Security Patch : PHSS\_27834

HP-UX Security Patch : PHSS\_27836

HP-UX Security patch : PHSS\_27849

HP-UX Security Patch : PHSS\_27858

HP-UX Security Patch : PHSS\_27869

HP-UX Security Patch : PHSS\_27872

HP-UX Security Patch : PHSS\_27873

HP-UX Security Patch : PHSS\_27917

HP-UX Security patch : PHSS\_27935

HP-UX Security Patch : PHSS\_27962

HP-UX Security Patch : PHSS\_27988

HP-UX Security Patch : PHSS\_28092

HP-UX Security Patch : PHSS\_28095

HP-UX Security patch : PHSS\_28173

HP-UX Security Patch : PHSS\_28198

HP-UX Security Patch : PHSS\_28207

HP-UX Security Patch : PHSS\_28258

HP-UX Security Patch : PHSS\_28348

HP-UX Security Patch : PHSS\_28386

HP-UX Security Patch : PHSS\_28387

HP-UX Security Patch : PHSS\_28400

HP-UX Security patch : PHSS\_28468

HP-UX Security Patch : PHSS\_28473

HP-UX Security patch : PHSS\_28492

HP-UX Security Patch : PHSS\_28521

HP-UX Security Patch : PHSS\_28546

HP-UX Security Patch : PHSS\_28571

HP-UX Security Patch : PHSS\_28587

HP-UX Security Patch : PHSS\_28650

HP-UX Security Patch : PHSS\_28684

HP-UX Security patch : PHSS\_28704

HP-UX Security Patch : PHSS\_28803

HP-UX Security Patch : PHSS\_28836

HP-UX Security Patch : PHSS\_28878

HP-UX Security patch : PHSS\_29201

HP-UX Security patch : PHSS\_29202

HP-UX Security Patch : PHSS\_29206

HP-UX Security Patch : PHSS\_29230

HP-UX Security Patch : PHSS\_29429

HP-UX Security Patch : PHSS\_29516

HP-UX Security Patch : PHSS\_29643

HP-UX Security Patch : PHSS\_29714

HP-UX Security Patch : PHSS\_29738

HP-UX Security Patch : PHSS\_29739

HP-UX Security Patch : PHSS\_29740

HP-UX Security Patch : PHSS\_29741

HP-UX Security Patch : PHSS\_29749

HP-UX Security Patch : PHSS\_29754

HP-UX Security Patch : PHSS\_29767

HP-UX Security Patch : PHSS\_30104

HP-UX Security Patch : PHSS\_30188

HP-UX Security Patch : PHSS\_30189

HP-UX Security Patch : PHSS\_30204

HP-UX Security Patch : PHSS\_30205

HP-UX Security Patch : PHSS\_30253

HP-UX Security Patch : PHSS\_30260

HP-UX Security Patch : PHSS\_30262

HP-UX Security Patch : PHSS\_30264

HP-UX Security Patch : PHSS\_30419

HP-UX Security Patch : PHSS\_30500

HP-UX Security Patch : PHSS\_30501

HP-UX Security Patch : PHSS\_30502

HP-UX Security Patch : PHSS\_30504

HP-UX Security Patch : PHSS\_30505

HP-UX Security Patch : PHSS\_30548

HP-UX Security Patch : PHSS\_30555

HP-UX Security Patch : PHSS\_30673

HP-UX Security Patch : PHSS\_30742

HP-UX Security Patch : PHSS\_30743

HP-UX Security Patch : PHSS\_30783

HP-UX Security Patch : PHSS\_30787

HP-UX Security Patch : PHSS\_30788

HP-UX Security Patch : PHSS\_30789

HP-UX Security Patch : PHSS\_30790

HP-UX Security Patch : PHSS\_30826

HP-UX Security Patch : PHSS\_30870

HP-UX Security Patch : PHSS\_30871

HP-UX Security Patch : PHSS\_30872

HP-UX Security Patch : PHSS\_30926

HP-UX Security Patch : PHSS\_30945

HP-UX Security Patch : PHSS\_30947

HP-UX Security Patch : PHSS\_30979

HP-UX Security Patch : PHSS\_31000

HP-UX Security Patch : PHSS\_31005

HP-UX Security Patch : PHSS\_31006

HP-UX Security Patch : PHSS\_31075

HP-UX Security Patch : PHSS\_31076

HP-UX Security Patch : PHSS\_31077

HP-UX Security Patch : PHSS\_31078

HP-UX Security Patch : PHSS\_31185

HP-UX Security Patch : PHSS\_31252

HP-UX Security Patch : PHSS\_31254

HP-UX Security Patch : PHSS\_31255

HP-UX Security Patch : PHSS\_31280

HP-UX Security Patch : PHSS\_31281

HP-UX Security Patch : PHSS\_31292

HP-UX Security Patch : PHSS\_31293

HP-UX Security Patch : PHSS\_31831

HP-UX Security Patch : PHSS\_31832

HP-UX Security Patch : PHSS\_32097

HP-UX Security Patch : PHSS\_32099

HP-UX Security Patch : PHSS\_32107

HP-UX Security Patch : PHSS\_32108

HP-UX Security Patch : PHSS\_32110

HP-UX Security Patch : PHSS\_32111

HP-UX Security Patch : PHSS\_32112

HP-UX Security Patch : PHSS\_32113

HP-UX Security Patch : PHSS\_32114

HP-UX Security Patch : PHSS\_32139

HP-UX Security Patch : PHSS\_32174

HP-UX Security Patch : PHSS\_32243

HP-UX Security Patch : PHSS\_32244

HP-UX Security Patch : PHSS\_32245

HP-UX Security Patch : PHSS\_32246

HP-UX Security Patch : PHSS\_32260

HP-UX Security Patch : PHSS\_32261

HP-UX Security Patch : PHSS\_32364

HP-UX Security Patch : PHSS\_32365

HP-UX Security Patch : PHSS\_32403

HP-UX Security Patch : PHSS\_32442

HP-UX Security Patch : PHSS\_32455

HP-UX Security Patch : PHSS\_32539

HP-UX Security Patch : PHSS\_32540

HP-UX Security Patch : PHSS\_32656

HP-UX Security Patch : PHSS\_32660

HP-UX Security Patch : PHSS\_32661

HP-UX Security Patch : PHSS\_32674

HP-UX Security Patch : PHSS\_32727

HP-UX Security Patch : PHSS\_32728

HP-UX Security Patch : PHSS\_32731

HP-UX Security Patch : PHSS\_32732

HP-UX Security Patch : PHSS\_32733

HP-UX Security Patch : PHSS\_32734

HP-UX Security Patch : PHSS\_32740

HP-UX Security Patch : PHSS\_32741

HP-UX Security Patch : PHSS\_32816

HP-UX Security Patch : PHSS\_32817

HP-UX Security Patch : PHSS\_32893

HP-UX Security Patch : PHSS\_32938

HP-UX Security Patch : PHSS\_32939

HP-UX Security Patch : PHSS\_32950

HP-UX Security Patch : PHSS\_32951

HP-UX Security Patch : PHSS\_32953

HP-UX Security Patch : PHSS\_32955

HP-UX Security Patch : PHSS\_32958

HP-UX Security Patch : PHSS\_32959

HP-UX Security Patch : PHSS\_32970

HP-UX Security Patch : PHSS\_32971

HP-UX Security Patch : PHSS\_32976

HP-UX Security Patch : PHSS\_32977

HP-UX Security Patch : PHSS\_33039

HP-UX Security Patch : PHSS\_33040

HP-UX Security Patch : PHSS\_33072

HP-UX Security Patch : PHSS\_33073

HP-UX Security Patch : PHSS\_33074

HP-UX Security Patch : PHSS\_33143

HP-UX Security Patch : PHSS\_33222

HP-UX Security Patch : PHSS\_33223

HP-UX Security Patch : PHSS\_33287

HP-UX Security Patch : PHSS\_33321

HP-UX Security Patch : PHSS\_33325

HP-UX Security Patch : PHSS\_33326

HP-UX Security Patch : PHSS\_33344

HP-UX Security Patch : PHSS\_33345

HP-UX Security Patch : PHSS\_33392

HP-UX Security Patch : PHSS\_33396

HP-UX Security Patch : PHSS\_33397

HP-UX Security Patch : PHSS\_33398

HP-UX Security Patch : PHSS\_33459

HP-UX Security Patch : PHSS\_33460

HP-UX Security Patch : PHSS\_33550

HP-UX Security Patch : PHSS\_33556

HP-UX Security Patch : PHSS\_33580

HP-UX Security Patch : PHSS\_33585

HP-UX Security Patch : PHSS\_33587

HP-UX Security Patch : PHSS\_33588

HP-UX Security Patch : PHSS\_33662

HP-UX Security Patch : PHSS\_33663

HP-UX Security Patch : PHSS\_33666

HP-UX Security Patch : PHSS\_33692

HP-UX Security Patch : PHSS\_33788

HP-UX Security Patch : PHSS\_33834

HP-UX Security Patch : PHSS\_33835

HP-UX Security Patch : PHSS\_33836

HP-UX Security Patch : PHSS\_33837

HP-UX Security Patch : PHSS\_33864

HP-UX Security Patch : PHSS\_33865

HP-UX Security Patch : PHSS\_33875

HP-UX Security Patch : PHSS\_33876

HP-UX Security Patch : PHSS\_33949

HP-UX Security Patch : PHSS\_34101

HP-UX Security Patch : PHSS\_34164

HP-UX Security Patch : PHSS\_34165

HP-UX Security Patch : PHSS\_34294

HP-UX Security Patch : PHSS\_34363

HP-UX Security Patch : PHSS\_34381

HP-UX Security Patch : PHSS\_34383

HP-UX Security Patch : PHSS\_34385

HP-UX Security Patch : PHSS\_34390

HP-UX Security Patch : PHSS\_34391

HP-UX Security Patch : PHSS\_34503

HP-UX Security Patch : PHSS\_34504

HP-UX Security Patch : PHSS\_34505

HP-UX Security Patch : PHSS\_34506

HP-UX Security Patch : PHSS\_34594

HP-UX Security Patch : PHSS\_34634

HP-UX Security Patch : PHSS\_34635

HP-UX Security Patch : PHSS\_34733

HP-UX Security Patch : PHSS\_34736

HP-UX Security Patch : PHSS\_34759

HP-UX Security Patch : PHSS\_34760

HP-UX Security Patch : PHSS\_34761

HP-UX Security Patch : PHSS\_34835

HP-UX Security Patch : PHSS\_34932

HP-UX Security Patch : PHSS\_34990

HP-UX Security Patch : PHSS\_35046

HP-UX Security Patch : PHSS\_35072

HP-UX Security Patch : PHSS\_35104

HP-UX Security Patch : PHSS\_35105

HP-UX Security Patch : PHSS\_35106

HP-UX Security Patch : PHSS\_35107

HP-UX Security Patch : PHSS\_35108

HP-UX Security Patch : PHSS\_35109

HP-UX Security Patch : PHSS\_35228

HP-UX Security Patch : PHSS\_35249

HP-UX Security Patch : PHSS\_35253

HP-UX Security Patch : PHSS\_35302

HP-UX Security Patch : PHSS\_35303

HP-UX Security Patch : PHSS\_35306

HP-UX Security Patch : PHSS\_35307

HP-UX Security Patch : PHSS\_35308

HP-UX Security Patch : PHSS\_35466

HP-UX Security Patch : PHSS\_35467

HP-UX Security Patch : PHSS\_35534

HP-UX Security Patch : PHSS\_35535

HP-UX Security Patch : PHSS\_35553

HP-UX Security Patch : PHSS\_35554

HP-UX Security Patch : PHSS\_35555

HP-UX Security Patch : PHSS\_35556

HP-UX Security Patch : PHSS\_35557

HP-UX Security Patch : PHSS\_35558

HP-UX Security Patch : PHSS\_35559

HP-UX Security Patch : PHSS\_35560

HP-UX Security Patch : PHSS\_35711

HP-UX Security Patch : PHSS\_35791

HP-UX Security Patch : PHSS\_35830

HP-UX Security Patch : PHSS\_35836

HP-UX Security Patch : PHSS\_35837

HP-UX Security Patch : PHSS\_35862

HP-UX Security Patch : PHSS\_35863

HP-UX Security Patch : PHSS\_35884

HP-UX Security Patch : PHSS\_35885

HP-UX Security Patch : PHSS\_35886

HP-UX Security Patch : PHSS\_35966

HP-UX Security Patch : PHSS\_36273

HP-UX Security Patch : PHSS\_36394

HP-UX Security Patch : PHSS\_36407

HP-UX Security Patch : PHSS\_36431

HP-UX Security Patch : PHSS\_36466

HP-UX Security Patch : PHSS\_36602

HP-UX Security Patch : PHSS\_36603

HP-UX Security Patch : PHSS\_36772

HP-UX Security Patch : PHSS\_37019

HP-UX Security Patch : PHSS\_37281

HP-UX Security Patch : PHSS\_41032

HP-UX Security Patch : PHSS\_41033

HP-UX Security Patch : PHSS\_42234

HP-UX Security Patch : PHSS\_42235

HP-UX Security patch : PHSS\_7752

HP-UX Security patch : PHSS\_7753

HP-UX Security patch : PHSS\_8233

HP-UX Security patch : PHSS\_8665

HP-UX Security patch : PHSS\_8667

HP-UX Security patch : PHSS\_9117

HP-UX Security patch : PHSS\_9343

HP-UX Security patch : PHSS\_9524

HP-UX Security patch : PHSS\_9627

HP-UX Security patch : PHSS\_9669

HP-UX Security patch : PHSS\_9690

HP-UX Security patch : PHSS\_9773

HP-UX Security patch : PHSS\_9804

HP-UX Security patch : PHSS\_9805

HP-UX Security patch : PHSS\_9809

HP-UX Security patch : PHSS\_9810

HP-UX Security patch : PHSS\_9811

HP-UX Security patch : PHSS\_9813

HP-UX Security patch : PHSS\_9815

# Gentoo Local Security Checks

Gentoo is not up-to-date

GLSA-200401-01 : Linux kernel do\_mremap() local privilege escalation vulnerability

GLSA-200401-02 : Honeyd remote detection vulnerability via a probe packet

GLSA-200401-03 : Apache mod\_python Denial of Service vulnerability

GLSA-200401-04 : GAIM 0.75 Remote overflows

GLSA-200402-01 : PHP setting leaks from .htaccess files on virtual hosts

GLSA-200402-02 : XFree86 Font Information File Buffer Overflow

GLSA-200402-03 : Monkeyd Denial of Service vulnerability

GLSA-200402-04 : Gallery 1.4.1 and below remote exploit vulnerability

GLSA-200402-05 : phpMyAdmin < 2.5.6-rc1: possible attack against export.php

GLSA-200402-06 : Updated kernel packages fix the AMD64 ptrace vulnerability

GLSA-200402-07 : Clam Antivirus DoS vulnerability

GLSA-200403-01 : Libxml2 URI Parsing Buffer Overflow Vulnerabilities

GLSA-200403-02 : Linux kernel do\_mremap local privilege escalation vulnerability

GLSA-200403-03 : Multiple OpenSSL Vulnerabilities

GLSA-200403-04 : Multiple security vulnerabilities in Apache 2

GLSA-200403-05 : UUDeview MIME Buffer Overflow

GLSA-200403-06 : Multiple remote buffer overflow vulnerabilities in Courier

GLSA-200403-07 : Multiple remote overflows and vulnerabilities in Ethereal

GLSA-200403-08 : oftpd DoS vulnerability

GLSA-200403-09 : Buffer overflow in Midnight Commander

GLSA-200403-10 : Fetchmail 6.2.5 fixes a remote DoS

GLSA-200403-11 : Squid ACL [url\_regex] bypass vulnerability

GLSA-200403-12 : OpenLDAP DoS Vulnerability

GLSA-200403-13 : Remote buffer overflow in MPlayer

GLSA-200403-14 : Multiple Security Vulnerabilities in Monit

GLSA-200404-01 : Insecure sandbox temporary lockfile vulnerabilities in Portage

GLSA-200404-02 : KDE Personal Information Management Suite Remote Buffer Overflow Vulnerability

GLSA-200404-03 : Tcpdump Vulnerabilities in ISAKMP Parsing

GLSA-200404-04 : Multiple vulnerabilities in sysstat

GLSA-200404-05 : ipsec-tools contains an X.509 certificates vulnerability.

GLSA-200404-06 : Util-linux login may leak sensitive data

GLSA-200404-07 : ClamAV RAR Archive Remote Denial Of Service Vulnerability

GLSA-200404-08 : GNU Automake symbolic link vulnerability

GLSA-200404-09 : Cross-realm trust vulnerability in Heimdal

GLSA-200404-10 : iproute local Denial of Service vulnerability

GLSA-200404-11 : Multiple Vulnerabilities in pwlib

GLSA-200404-12 : Scorched 3D server chat box format string vulnerability

GLSA-200404-13 : CVS Server and Client Vulnerabilities

GLSA-200404-14 : Multiple format string vulnerabilities in cadaver

GLSA-200404-15 : XChat 2.0.x SOCKS5 Vulnerability

GLSA-200404-16 : Multiple new security vulnerabilities in monit

GLSA-200404-17 : ipsec-tools and iputils contain a remote DoS vulnerability

GLSA-200404-18 : Multiple Vulnerabilities in ssmtp

GLSA-200404-19 : Buffer overflows and format string vulnerabilities in LCDproc

GLSA-200404-20 : Multiple vulnerabilities in xine

GLSA-200404-21 : Multiple Vulnerabilities in Samba

GLSA-200405-01 : Multiple format string vulnerabilities in neon 0.24.4 and earlier

GLSA-200405-02 : Multiple vulnerabilities in LHa

GLSA-200405-03 : ClamAV VirusEvent parameter vulnerability

GLSA-200405-04 : OpenOffice.org vulnerability when using DAV servers

GLSA-200405-05 : Utempter symlink vulnerability

GLSA-200405-06 : libpng denial of service vulnerability

GLSA-200405-07 : Exim verify=header\_syntax buffer overflow

GLSA-200405-08 : Pound format string vulnerability

GLSA-200405-09 : ProFTPD Access Control List bypass vulnerability

GLSA-200405-10 : Icecast denial of service vulnerability

GLSA-200405-11 : KDE URI Handler Vulnerabilities

GLSA-200405-12 : CVS heap overflow vulnerability

GLSA-200405-13 : neon heap-based buffer overflow

GLSA-200405-14 : Buffer overflow in Subversion

GLSA-200405-15 : cadaver heap-based buffer overflow

GLSA-200405-16 : Multiple XSS Vulnerabilities in SquirrelMail

GLSA-200405-17 : Multiple vulnerabilities in metamail

GLSA-200405-18 : Buffer Overflow in Firebird

GLSA-200405-19 : Opera telnet URI handler file creation/truncation vulnerability

GLSA-200405-20 : Insecure Temporary File Creation In MySQL

GLSA-200405-21 : Midnight Commander: Multiple vulnerabilities

GLSA-200405-22 : Apache 1.3: Multiple vulnerabilities

GLSA-200405-23 : Heimdal: Kerberos 4 buffer overflow in kadmin

GLSA-200405-24 : MPlayer, xine-lib: vulnerabilities in RTSP stream handling

GLSA-200405-25 : tla: Multiple vulnerabilities in included libneon

GLSA-200406-01 : Ethereal: Multiple security problems

GLSA-200406-02 : tripwire: Format string vulnerability

GLSA-200406-03 : sitecopy: Multiple vulnerabilities in included libneon

GLSA-200406-04 : Mailman: Member password disclosure vulnerability

GLSA-200406-05 : Apache: Buffer overflow in mod\_ssl

GLSA-200406-06 : CVS: additional DoS and arbitrary code execution vulnerabilities

GLSA-200406-07 : Subversion: Remote heap overflow

GLSA-200406-08 : Squirrelmail: Another XSS vulnerability

GLSA-200406-09 : Horde-Chora: Remote code execution

GLSA-200406-10 : Gallery: Privilege escalation vulnerability

GLSA-200406-11 : Horde-IMP: Input validation vulnerability

GLSA-200406-12 : Webmin: Multiple vulnerabilities

GLSA-200406-13 : Squid: NTLM authentication helper buffer overflow

GLSA-200406-14 : aspell: Buffer overflow in word-list-compress

GLSA-200406-15 : Usermin: Multiple vulnerabilities

GLSA-200406-16 : Apache 1.3: Buffer overflow in mod\_proxy

GLSA-200406-17 : IPsec-Tools: authentication bug in racoon

GLSA-200406-18 : gzip: Insecure creation of temporary files

GLSA-200406-19 : giFT-FastTrack: remote denial of service attack

GLSA-200406-20 : FreeS/WAN, Openswan, strongSwan: Vulnerabilities in certificate handling

GLSA-200406-21 : mit-krb5: Multiple buffer overflows in krb5\_aname\_to\_localname

GLSA-200406-22 : Pavuk: Remote buffer overflow

GLSA-200407-01 : Esearch: Insecure temp file handling

GLSA-200407-02 : Linux Kernel: Multiple vulnerabilities

GLSA-200407-03 : Apache 2: Remote denial of service attack

GLSA-200407-04 : Pure-FTPd: Potential DoS when maximum connections is reached

GLSA-200407-05 : XFree86, X.org: XDM ignores requestPort setting

GLSA-200407-06 : libpng: Buffer overflow on row buffers

GLSA-200407-07 : Shorewall : Insecure temp file handling

GLSA-200407-08 : Ethereal: Multiple security problems

GLSA-200407-09 : MoinMoin: Group ACL bypass

GLSA-200407-10 : rsync: Directory traversal in rsync daemon

GLSA-200407-11 : wv: Buffer overflow vulnerability

GLSA-200407-12 : Linux Kernel: Remote DoS vulnerability with IPTables TCP Handling

GLSA-200407-13 : PHP: Multiple security vulnerabilities

GLSA-200407-14 : Unreal Tournament 2003/2004: Buffer overflow in 'secure' queries

GLSA-200407-15 : Opera: Multiple spoofing vulnerabilities

GLSA-200407-16 : Linux Kernel: Multiple DoS and permission vulnerabilities

GLSA-200407-17 : l2tpd: Buffer overflow

GLSA-200407-18 : mod\_ssl: Format string vulnerability

GLSA-200407-19 : Pavuk: Digest authentication helper buffer overflow

GLSA-200407-20 : Subversion: Vulnerability in mod\_authz\_svn

GLSA-200407-21 : Samba: Multiple buffer overflows

GLSA-200407-22 : phpMyAdmin: Multiple vulnerabilities

GLSA-200407-23 : SoX: Multiple buffer overflows

GLSA-200408-01 : MPlayer: GUI filename handling overflow

GLSA-200408-02 : Courier: XSS vulnerability in SqWebMail

GLSA-200408-03 : libpng: Numerous vulnerabilities

GLSA-200408-04 : PuTTY: Pre-authentication arbitrary code execution

GLSA-200408-05 : Opera: Multiple new vulnerabilities

GLSA-200408-06 : SpamAssassin: Denial of Service vulnerability

GLSA-200408-07 : Horde-IMP: Input validation vulnerability for Internet Explorer users

GLSA-200408-08 : Cfengine: RSA Authentication Heap Corruption

GLSA-200408-09 : Roundup: Filesystem access vulnerability

GLSA-200408-10 : gv: Exploitable Buffer Overflow

GLSA-200408-11 : Nessus: 'adduser' race condition vulnerability

GLSA-200408-12 : Gaim: MSN protocol parsing function buffer overflow

GLSA-200408-13 : kdebase, kdelibs: Multiple security issues

GLSA-200408-14 : acroread: UUDecode filename buffer overflow

GLSA-200408-15 : Tomcat: Insecure installation

GLSA-200408-16 : glibc: Information leak with LD\_DEBUG

GLSA-200408-17 : rsync: Potential information leakage

GLSA-200408-18 : xine-lib: VCD MRL buffer overflow

GLSA-200408-19 : courier-imap: Remote Format String Vulnerability

GLSA-200408-20 : Qt: Image loader overflows

GLSA-200408-21 : Cacti: SQL injection vulnerability

GLSA-200408-22 : Mozilla, Firefox, Thunderbird, Galeon, Epiphany: New releases fix vulnerabilities

GLSA-200408-23 : kdelibs: Cross-domain cookie injection vulnerability

GLSA-200408-24 : Linux Kernel: Multiple information leaks

GLSA-200408-25 : MoinMoin: Group ACL bypass

GLSA-200408-26 : zlib: Denial of service vulnerability

GLSA-200408-27 : Gaim: New vulnerabilities

GLSA-200409-01 : vpopmail: Multiple vulnerabilities

GLSA-200409-02 : MySQL: Insecure temporary file creation in mysqlhotcopy

GLSA-200409-03 : Python 2.2: Buffer overflow in getaddrinfo()

GLSA-200409-04 : Squid: Denial of service when using NTLM authentication

GLSA-200409-05 : Gallery: Arbitrary command execution

GLSA-200409-06 : eGroupWare: Multiple XSS vulnerabilities

GLSA-200409-07 : xv: Buffer overflows in image handling

GLSA-200409-08 : Ruby: CGI::Session creates files insecurely

GLSA-200409-09 : MIT krb5: Multiple vulnerabilities

GLSA-200409-10 : multi-gnome-terminal: Information leak

GLSA-200409-11 : star: Suid root vulnerability

GLSA-200409-12 : ImageMagick, imlib, imlib2: BMP decoding buffer overflows

GLSA-200409-13 : LHa: Multiple vulnerabilities

GLSA-200409-15 : Webmin, Usermin: Multiple vulnerabilities in Usermin

GLSA-200409-16 : Samba: Denial of Service vulnerabilities

GLSA-200409-17 : SUS: Local root vulnerability

GLSA-200409-18 : cdrtools: Local root vulnerability in cdrecord if set SUID root

GLSA-200409-19 : Heimdal: ftpd root escalation

GLSA-200409-20 : mpg123: Buffer overflow vulnerability

GLSA-200409-21 : Apache 2, mod\_dav: Multiple vulnerabilities

GLSA-200409-22 : phpGroupWare: XSS vulnerability in wiki module

GLSA-200409-23 : SnipSnap: HTTP response splitting

GLSA-200409-24 : Foomatic: Arbitrary command execution in foomatic-rip filter

GLSA-200409-25 : CUPS: Denial of service vulnerability

GLSA-200409-26 : Mozilla, Firefox, Thunderbird, Epiphany: New releases fix vulnerabilities

GLSA-200409-27 : glFTPd: Local buffer overflow vulnerability

GLSA-200409-28 : GTK+ 2, gdk-pixbuf: Multiple image decoding vulnerabilities

GLSA-200409-29 : FreeRADIUS: Multiple Denial of Service vulnerabilities

GLSA-200409-30 : xine-lib: Multiple vulnerabilities

GLSA-200409-31 : jabberd 1.x: Denial of Service vulnerability

GLSA-200409-32 : getmail: Filesystem overwrite vulnerability

GLSA-200409-33 : Apache: Exposure of protected directories

GLSA-200409-34 : X.org, XFree86: Integer and stack overflows in libXpm

GLSA-200409-35 : Subversion: Metadata information leak

GLSA-200410-01 : sharutils: Buffer overflows in shar.c and unshar.c

GLSA-200410-02 : Netpbm: Multiple temporary file issues

GLSA-200410-03 : NetKit-telnetd: buffer overflows in telnet and telnetd

GLSA-200410-04 : PHP: Memory disclosure and arbitrary location file upload

GLSA-200410-05 : Cyrus-SASL: Buffer overflow and SASL\_PATH vulnerabilities

GLSA-200410-06 : CUPS: Leakage of sensitive information

GLSA-200410-07 : ed: Insecure temporary file handling

GLSA-200410-08 : ncompress: Buffer overflow

GLSA-200410-09 : LessTif: Integer and stack overflows in libXpm

GLSA-200410-10 : gettext: Insecure temporary file handling

GLSA-200410-11 : tiff: Buffer overflows in image decoding

GLSA-200410-12 : WordPress: HTTP response splitting and XSS vulnerabilities

GLSA-200410-13 : BNC: Input validation flaw

GLSA-200410-14 : phpMyAdmin: Vulnerability in MIME-based transformation system

GLSA-200410-15 : Squid: Remote DoS vulnerability

GLSA-200410-16 : PostgreSQL: Insecure temporary file use in make\_oidjoins\_check

GLSA-200410-17 : OpenOffice.org: Temporary files disclosure

GLSA-200410-18 : Ghostscript: Insecure temporary file use in multiple scripts

GLSA-200410-19 : glibc: Insecure tempfile handling in catchsegv script

GLSA-200410-20 : Xpdf, CUPS: Multiple integer overflows

GLSA-200410-21 : Apache 2, mod\_ssl: Bypass of SSLCipherSuite directive

GLSA-200410-22 : MySQL: Multiple vulnerabilities

GLSA-200410-23 : Gaim: Multiple vulnerabilities

GLSA-200410-24 : MIT krb5: Insecure temporary file use in send-pr.sh

GLSA-200410-25 : Netatalk: Insecure tempfile handling in etc2ps.sh

GLSA-200410-26 : socat: Format string vulnerability

GLSA-200410-27 : mpg123: Buffer overflow vulnerabilities

GLSA-200410-28 : rssh: Format string vulnerability

GLSA-200410-29 : PuTTY: Pre-authentication buffer overflow

GLSA-200410-30 : GPdf, KPDF, KOffice: Vulnerabilities in included xpdf

GLSA-200410-31 : Archive::Zip: Virus detection evasion

GLSA-200411-02 : Cherokee: Format string vulnerability

GLSA-200411-03 : Apache 1.3: Buffer overflow vulnerability in mod\_include

GLSA-200411-04 : Speedtouch USB driver: Privilege escalation vulnerability

GLSA-200411-05 : libxml2: Remotely exploitable buffer overflow

GLSA-200411-06 : MIME-tools: Virus detection evasion

GLSA-200411-07 : Proxytunnel: Format string vulnerability

GLSA-200411-08 : GD: Integer overflow

GLSA-200411-09 : shadow: Unauthorized modification of account information

GLSA-200411-10 : Gallery: XSS vulnerability

GLSA-200411-11 : ImageMagick: EXIF buffer overflow

GLSA-200411-12 : zgv: Multiple buffer overflows

GLSA-200411-13 : Portage, Gentoolkit: Temporary file vulnerabilities

GLSA-200411-14 : Kaffeine, gxine: Remotely exploitable buffer overflow

GLSA-200411-15 : OpenSSL, Groff: Insecure tempfile handling

GLSA-200411-16 : zip: Path name buffer overflow

GLSA-200411-17 : mtink: Insecure tempfile handling

GLSA-200411-18 : Apache 2.0: Denial of Service by memory consumption

GLSA-200411-19 : Pavuk: Multiple buffer overflows

GLSA-200411-20 : ez-ipupdate: Format string vulnerability

GLSA-200411-21 : Samba: Multiple vulnerabilities

GLSA-200411-22 : Davfs2, lvm-user: Insecure tempfile handling

GLSA-200411-23 : Ruby: Denial of Service issue

GLSA-200411-24 : BNC: Buffer overflow vulnerability

GLSA-200411-25 : SquirrelMail: Encoded text XSS vulnerability

GLSA-200411-26 : GIMPS, SETI@home, ChessBrain: Insecure installation

GLSA-200411-27 : Fcron: Multiple vulnerabilities

GLSA-200411-28 : X.Org, XFree86: libXpm vulnerabilities

GLSA-200411-29 : unarj: Long filenames buffer overflow and a path traversal vulnerability

GLSA-200411-30 : pdftohtml: Vulnerabilities in included Xpdf

GLSA-200411-31 : ProZilla: Multiple vulnerabilities

GLSA-200411-32 : phpBB: Remote command execution

GLSA-200411-33 : TWiki: Arbitrary command execution

GLSA-200411-34 : Cyrus IMAP Server: Multiple remote vulnerabilities

GLSA-200411-35 : phpWebSite: HTTP response splitting vulnerability

GLSA-200411-36 : phpMyAdmin: Multiple XSS vulnerabilities

GLSA-200411-37 : Open DC Hub: Remote code execution

GLSA-200411-38 : Sun and Blackdown Java: Applet privilege escalation

GLSA-200412-01 : rssh, scponly: Unrestricted command execution

GLSA-200412-02 : PDFlib: Multiple overflows in the included TIFF library

GLSA-200412-03 : imlib: Buffer overflows in image decoding

GLSA-200412-04 : Perl: Insecure temporary file creation

GLSA-200412-05 : mirrorselect: Insecure temporary file creation

GLSA-200412-06 : PHProjekt: setup.php vulnerability

GLSA-200412-07 : file: Arbitrary code execution

GLSA-200412-08 : nfs-utils: Multiple remote vulnerabilities

GLSA-200412-09 : ncpfs: Buffer overflow in ncplogin and ncpmap

GLSA-200412-10 : Vim, gVim: Vulnerable options in modelines

GLSA-200412-11 : Cscope: Insecure creation of temporary files

GLSA-200412-12 : Adobe Acrobat Reader: Buffer overflow vulnerability

GLSA-200412-13 : Samba: Integer overflow

GLSA-200412-14 : PHP: Multiple vulnerabilities

GLSA-200412-15 : Ethereal: Multiple vulnerabilities

GLSA-200412-16 : kdelibs, kdebase: Multiple vulnerabilities

GLSA-200412-17 : kfax: Multiple overflows in the included TIFF library

GLSA-200412-18 : abcm2ps: Buffer overflow vulnerability

GLSA-200412-19 : phpMyAdmin: Multiple vulnerabilities

GLSA-200412-20 : NASM: Buffer overflow vulnerability

GLSA-200412-21 : MPlayer: Multiple overflows

GLSA-200412-22 : mpg123: Playlist buffer overflow

GLSA-200412-23 : Zwiki: XSS vulnerability

GLSA-200412-24 : Xpdf, GPdf: New integer overflows

GLSA-200412-25 : CUPS: Multiple vulnerabilities

GLSA-200412-26 : ViewCVS: Information leak and XSS vulnerabilities

GLSA-200412-27 : PHProjekt: Remote code execution vulnerability

GLSA-200501-01 : LinPopUp: Buffer overflow in message reply

GLSA-200501-02 : a2ps: Multiple vulnerabilities

GLSA-200501-03 : Mozilla, Firefox, Thunderbird: Various vulnerabilities

GLSA-200501-04 : Shoutcast Server: Remote code execution

GLSA-200501-05 : mit-krb5: Heap overflow in libkadm5srv

GLSA-200501-06 : tiff: New overflows in image decoding

GLSA-200501-07 : xine-lib: Multiple overflows

GLSA-200501-08 : phpGroupWare: Various vulnerabilities

GLSA-200501-09 : xzgv: Multiple overflows

GLSA-200501-10 : Vilistextum: Buffer overflow vulnerability

GLSA-200501-11 : Dillo: Format string vulnerability

GLSA-200501-12 : TikiWiki: Arbitrary command execution

GLSA-200501-13 : pdftohtml: Vulnerabilities in included Xpdf

GLSA-200501-14 : mpg123: Buffer overflow

GLSA-200501-15 : UnRTF: Buffer overflow

GLSA-200501-16 : Konqueror: Java sandbox vulnerabilities

GLSA-200501-17 : KPdf, KOffice: More vulnerabilities in included Xpdf

GLSA-200501-18 : KDE FTP KIOslave: Command injection

GLSA-200501-19 : imlib2: Buffer overflows in image decoding

GLSA-200501-20 : o3read: Buffer overflow during file conversion

GLSA-200501-21 : HylaFAX: hfaxd unauthorized login vulnerability

GLSA-200501-22 : poppassd\_pam: Unauthorized password changing

GLSA-200501-23 : Exim: Two buffer overflows

GLSA-200501-24 : tnftp: Arbitrary file overwriting

GLSA-200501-25 : Squid: Multiple vulnerabilities

GLSA-200501-26 : ImageMagick: PSD decoding heap overflow

GLSA-200501-27 : Ethereal: Multiple vulnerabilities

GLSA-200501-28 : Xpdf, GPdf: Stack overflow in Decrypt::makeFileKey2

GLSA-200501-29 : Mailman: XSS vulnerability

GLSA-200501-30 : CUPS: Stack overflow in included Xpdf code

GLSA-200501-31 : teTeX, pTeX, CSTeX: Multiple vulnerabilities

GLSA-200501-32 : KPdf, KOffice: Stack overflow in included Xpdf code

GLSA-200501-33 : MySQL: Insecure temporary file creation

GLSA-200501-34 : Konversation: Various vulnerabilities

GLSA-200501-35 : Evolution: Integer overflow in camel-lock-helper

GLSA-200501-36 : AWStats: Remote code execution

GLSA-200501-37 : GraphicsMagick: PSD decoding heap overflow

GLSA-200501-38 : Perl: rmtree and DBI tmpfile vulnerabilities

GLSA-200501-39 : SquirrelMail: Multiple vulnerabilities

GLSA-200501-40 : ngIRCd: Buffer overflow

GLSA-200501-41 : TikiWiki: Arbitrary command execution

GLSA-200501-42 : VDR: Arbitrary file overwriting issue

GLSA-200501-43 : f2c: Insecure temporary file creation

GLSA-200501-44 : ncpfs: Multiple vulnerabilities

GLSA-200501-45 : Gallery: XSS vulnerability

GLSA-200501-46 : ClamAV: Multiple issues

GLSA-200502-01 : FireHOL: Insecure temporary file creation

GLSA-200502-02 : UW IMAP: CRAM-MD5 authentication bypass

GLSA-200502-03 : enscript: Multiple vulnerabilities

GLSA-200502-04 : Squid: Multiple vulnerabilities

GLSA-200502-05 : Newspost: Buffer overflow vulnerability

GLSA-200502-06 : LessTif: Multiple vulnerabilities in libXpm

GLSA-200502-07 : OpenMotif: Multiple vulnerabilities in libXpm

GLSA-200502-08 : PostgreSQL: Multiple vulnerabilities

GLSA-200502-09 : Python: Arbitrary code execution through SimpleXMLRPCServer

GLSA-200502-10 : pdftohtml: Vulnerabilities in included Xpdf

GLSA-200502-11 : Mailman: Directory traversal vulnerability

GLSA-200502-12 : Webmin: Information leak in Gentoo binary package

GLSA-200502-13 : Perl: Vulnerabilities in perl-suid wrapper

GLSA-200502-14 : mod\_python: Publisher Handler vulnerability

GLSA-200502-15 : PowerDNS: Denial of Service vulnerability

GLSA-200502-16 : ht://Dig: XSS vulnerability

GLSA-200502-17 : Opera: Multiple vulnerabilities

GLSA-200502-18 : VMware Workstation: Untrusted library search path

GLSA-200502-19 : PostgreSQL: Buffer overflows in PL/PgSQL parser

GLSA-200502-20 : Emacs, XEmacs: Format string vulnerabilities in movemail

GLSA-200502-21 : lighttpd: Script source disclosure

GLSA-200502-22 : wpa\_supplicant: Buffer overflow vulnerability

GLSA-200502-23 : KStars: Buffer overflow in fliccd

GLSA-200502-24 : Midnight Commander: Multiple vulnerabilities

GLSA-200502-25 : Squid: Denial of Service through DNS responses

GLSA-200502-26 : GProFTPD: gprostats format string vulnerability

GLSA-200502-27 : gFTP: Directory traversal vulnerability

GLSA-200502-28 : PuTTY: Remote code execution

GLSA-200502-29 : Cyrus IMAP Server: Multiple overflow vulnerabilities

GLSA-200502-30 : cmd5checkpw: Local password leak vulnerability

GLSA-200502-31 : uim: Privilege escalation vulnerability

GLSA-200502-32 : UnAce: Buffer overflow and directory traversal vulnerabilities

GLSA-200502-33 : MediaWiki: Multiple vulnerabilities

GLSA-200503-01 : Qt: Untrusted library search path

GLSA-200503-02 : phpBB: Multiple vulnerabilities

GLSA-200503-03 : Gaim: Multiple Denial of Service issues

GLSA-200503-04 : phpWebSite: Arbitrary PHP execution and path disclosure

GLSA-200503-05 : xli, xloadimage: Multiple vulnerabilities

GLSA-200503-06 : BidWatcher: Format string vulnerability

GLSA-200503-07 : phpMyAdmin: Multiple vulnerabilities

GLSA-200503-08 : OpenMotif, LessTif: New libXpm buffer overflows

GLSA-200503-09 : xv: Filename handling vulnerability

GLSA-200503-10 : Mozilla Firefox: Various vulnerabilities

GLSA-200503-11 : ImageMagick: Filename handling vulnerability

GLSA-200503-12 : Hashcash: Format string vulnerability

GLSA-200503-13 : mlterm: Integer overflow vulnerability

GLSA-200503-14 : KDE dcopidlng: Insecure temporary file creation

GLSA-200503-15 : X.org: libXpm vulnerability

GLSA-200503-16 : Ethereal: Multiple vulnerabilities

GLSA-200503-17 : libexif: Buffer overflow vulnerability

GLSA-200503-18 : Ringtone Tools: Buffer overflow vulnerability

GLSA-200503-19 : MySQL: Multiple vulnerabilities

GLSA-200503-20 : curl: NTLM response buffer overflow

GLSA-200503-21 : Grip: CDDB response overflow

GLSA-200503-22 : KDE: Local Denial of Service

GLSA-200503-23 : rxvt-unicode: Buffer overflow

GLSA-200503-24 : LTris: Buffer overflow

GLSA-200503-25 : OpenSLP: Multiple buffer overflows

GLSA-200503-26 : Sylpheed, Sylpheed-claws: Message reply overflow

GLSA-200503-27 : Xzabite dyndnsupdate: Multiple vulnerabilities

GLSA-200503-28 : Sun Java: Web Start argument injection vulnerability

GLSA-200503-29 : GnuPG: OpenPGP protocol attack

GLSA-200503-30 : Mozilla Suite: Multiple vulnerabilities

GLSA-200503-31 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200503-32 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200503-33 : IPsec-Tools: racoon Denial of Service

GLSA-200503-34 : mpg321: Format string vulnerability

GLSA-200503-35 : Smarty: Template vulnerability

GLSA-200503-36 : netkit-telnetd: Buffer overflow

GLSA-200503-37 : LimeWire: Disclosure of sensitive information

GLSA-200504-01 : telnet-bsd: Multiple buffer overflows

GLSA-200504-02 : Sylpheed, Sylpheed-claws: Buffer overflow on message display

GLSA-200504-03 : Dnsmasq: Poisoning and Denial of Service vulnerabilities

GLSA-200504-04 : mit-krb5: Multiple buffer overflows in telnet client

GLSA-200504-05 : Gaim: Denial of Service issues

GLSA-200504-06 : sharutils: Insecure temporary file creation

GLSA-200504-07 : GnomeVFS, libcdaudio: CDDB response overflow

GLSA-200504-08 : phpMyAdmin: XSS vulnerability

GLSA-200504-09 : Axel: Vulnerability in HTTP redirection handling

GLSA-200504-10 : Gld: Remote execution of arbitrary code

GLSA-200504-11 : JunkBuster: Multiple vulnerabilities

GLSA-200504-12 : rsnapshot: Local privilege escalation

GLSA-200504-13 : OpenOffice.Org: DOC document Heap Overflow

GLSA-200504-14 : monkeyd: Multiple vulnerabilities

GLSA-200504-15 : PHP: Multiple vulnerabilities

GLSA-200504-16 : CVS: Multiple vulnerabilities

GLSA-200504-17 : XV: Multiple vulnerabilities

GLSA-200504-18 : Mozilla Firefox, Mozilla Suite: Multiple vulnerabilities

GLSA-200504-19 : MPlayer: Two heap overflow vulnerabilities

GLSA-200504-20 : openMosixview: Insecure temporary file creation

GLSA-200504-21 : RealPlayer, Helix Player: Buffer overflow vulnerability

GLSA-200504-22 : KDE kimgio: PCX handling buffer overflow

GLSA-200504-23 : Kommander: Insecure remote script execution

GLSA-200504-24 : eGroupWare: XSS and SQL injection vulnerabilities

GLSA-200504-25 : Rootkit Hunter: Insecure temporary file creation

GLSA-200504-26 : Convert-UUlib: Buffer overflow

GLSA-200504-27 : xine-lib: Two heap overflow vulnerabilities

GLSA-200504-28 : Heimdal: Buffer overflow vulnerabilities

GLSA-200504-29 : Pound: Buffer overflow vulnerability

GLSA-200504-30 : phpMyAdmin: Insecure SQL script installation

GLSA-200505-01 : Horde Framework: Multiple XSS vulnerabilities

GLSA-200505-02 : Oops!: Remote code execution

GLSA-200505-03 : Ethereal: Numerous vulnerabilities

GLSA-200505-04 : GnuTLS: Denial of Service vulnerability

GLSA-200505-05 : gzip: Multiple vulnerabilities

GLSA-200505-06 : TCPDump: Decoding routines Denial of Service vulnerability

GLSA-200505-07 : libTIFF: Buffer overflow

GLSA-200505-08 : HT Editor: Multiple buffer overflows

GLSA-200505-09 : Gaim: Denial of Service and buffer overflow vulnerabilties

GLSA-200505-10 : phpBB: XSS Vulnerability

GLSA-200505-11 : Mozilla Suite, Mozilla Firefox: Remote compromise

GLSA-200505-12 : PostgreSQL: Multiple vulnerabilities

GLSA-200505-13 : FreeRADIUS: SQL injection and Denial of Service vulnerability

GLSA-200505-14 : Cheetah: Untrusted module search path

GLSA-200505-15 : gdb: Multiple vulnerabilities

GLSA-200505-16 : ImageMagick, GraphicsMagick: Denial of Service vulnerability

GLSA-200505-17 : Qpopper: Multiple Vulnerabilities

GLSA-200505-18 : Net-SNMP: fixproc insecure temporary file creation

GLSA-200505-19 : gxine: Format string vulnerability

GLSA-200505-20 : Mailutils: Multiple vulnerabilities in imap4d and mail

GLSA-200506-01 : Binutils, elfutils: Buffer overflow

GLSA-200506-02 : Mailutils: SQL Injection

GLSA-200506-03 : Dzip: Directory traversal vulnerability

GLSA-200506-04 : Wordpress: Multiple vulnerabilities

GLSA-200506-05 : SilverCity: Insecure file permissions

GLSA-200506-06 : libextractor: Multiple overflow vulnerabilities

GLSA-200506-07 : Ettercap: Format string vulnerability

GLSA-200506-08 : GNU shtool, ocaml-mysql: Insecure temporary file creation

GLSA-200506-09 : gedit: Format string vulnerability

GLSA-200506-10 : LutelWall: Insecure temporary file creation

GLSA-200506-11 : Gaim: Denial of Service vulnerabilities

GLSA-200506-12 : MediaWiki: XSS vulnerability

GLSA-200506-13 : webapp-config: Insecure temporary file handling

GLSA-200506-14 : Sun and Blackdown Java: Applet privilege escalation

GLSA-200506-15 : PeerCast: Format string vulnerability

GLSA-200506-16 : cpio: Directory traversal vulnerability

GLSA-200506-17 : SpamAssassin 3, Vipul's Razor: Denial of Service vulnerability

GLSA-200506-18 : Tor: Information disclosure

GLSA-200506-19 : SquirrelMail: Several XSS vulnerabilities

GLSA-200506-20 : Cacti: Several vulnerabilities

GLSA-200506-21 : Trac: File upload vulnerability

GLSA-200506-22 : sudo: Arbitrary command execution

GLSA-200506-23 : Clam AntiVirus: Denial of Service vulnerability

GLSA-200506-24 : Heimdal: Buffer overflow vulnerabilities

GLSA-200507-01 : PEAR XML-RPC, phpxmlrpc: PHP script injection vulnerability

GLSA-200507-02 : WordPress: Multiple vulnerabilities

GLSA-200507-03 : phpBB: Arbitrary command execution

GLSA-200507-04 : RealPlayer: Heap overflow vulnerability

GLSA-200507-05 : zlib: Buffer overflow

GLSA-200507-06 : TikiWiki: Arbitrary command execution through XML-RPC

GLSA-200507-07 : phpWebSite: Multiple vulnerabilities

GLSA-200507-08 : phpGroupWare, eGroupWare: PHP script injection vulnerability

GLSA-200507-09 : Adobe Acrobat Reader: Buffer overflow vulnerability

GLSA-200507-10 : Ruby: Arbitrary command execution through XML-RPC

GLSA-200507-11 : MIT Kerberos 5: Multiple vulnerabilities

GLSA-200507-12 : Bugzilla: Unauthorized access and information disclosure

GLSA-200507-13 : pam\_ldap and nss\_ldap: Plain text authentication leak

GLSA-200507-14 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200507-15 : PHP: Script injection through XML-RPC

GLSA-200507-16 : dhcpcd: Denial of Service vulnerability

GLSA-200507-17 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200507-18 : MediaWiki: XSS vulnerability

GLSA-200507-19 : zlib: Buffer overflow

GLSA-200507-20 : Shorewall: Security policy bypass

GLSA-200507-21 : fetchmail: Buffer Overflow

GLSA-200507-22 : sandbox: Insecure temporary file handling

GLSA-200507-23 : Kopete: Vulnerability in included Gadu library

GLSA-200507-24 : Mozilla Suite: Multiple vulnerabilities

GLSA-200507-25 : Clam AntiVirus: Integer overflows

GLSA-200507-26 : GNU Gadu, CenterICQ, Kadu, EKG, libgadu: Remote code execution in Gadu library

GLSA-200507-27 : Ethereal: Multiple vulnerabilities

GLSA-200507-28 : AMD64 x86 emulation base libraries: Buffer overflow

GLSA-200507-29 : pstotext: Remote execution of arbitrary code

GLSA-200508-01 : Compress::Zlib: Buffer overflow

GLSA-200508-02 : ProFTPD: Format string vulnerabilities

GLSA-200508-03 : nbSMTP: Format string vulnerability

GLSA-200508-04 : Netpbm: Arbitrary code execution in pstopnm

GLSA-200508-05 : Heartbeat: Insecure temporary file creation

GLSA-200508-06 : Gaim: Remote execution of arbitrary code

GLSA-200508-07 : AWStats: Arbitrary code execution using malicious Referrer information

GLSA-200508-08 : Xpdf, Kpdf, GPdf: Denial of Service vulnerability

GLSA-200508-09 : bluez-utils: Bluetooth device name validation vulnerability

GLSA-200508-10 : Kismet: Multiple vulnerabilities

GLSA-200508-11 : Adobe Reader: Buffer Overflow

GLSA-200508-12 : Evolution: Format string vulnerabilities

GLSA-200508-13 : PEAR XML-RPC, phpxmlrpc: New PHP script injection vulnerability

GLSA-200508-14 : TikiWiki, eGroupWare: Arbitrary command execution through XML-RPC

GLSA-200508-15 : Apache 2.0: Denial of Service vulnerability

GLSA-200508-16 : Tor: Information disclosure

GLSA-200508-17 : libpcre: Heap integer overflow

GLSA-200508-18 : PhpWiki: Arbitrary command execution through XML-RPC

GLSA-200508-19 : lm\_sensors: Insecure temporary file creation

GLSA-200508-20 : phpGroupWare: Multiple vulnerabilities

GLSA-200508-21 : phpWebSite: Arbitrary command execution through XML-RPC and SQL injection

GLSA-200508-22 : pam\_ldap: Authentication bypass vulnerability

GLSA-200509-01 : MPlayer: Heap overflow in ad\_pcm.c

GLSA-200509-02 : Gnumeric: Heap overflow in the included PCRE library

GLSA-200509-03 : OpenTTD: Format string vulnerabilities

GLSA-200509-04 : phpLDAPadmin: Authentication bypass

GLSA-200509-05 : Net-SNMP: Insecure RPATH

GLSA-200509-06 : Squid: Denial of Service vulnerabilities

GLSA-200509-07 : X.Org: Heap overflow in pixmap allocation

GLSA-200509-08 : Python: Heap overflow in the included PCRE library

GLSA-200509-09 : Py2Play: Remote execution of arbitrary Python code

GLSA-200509-10 : Mailutils: Format string vulnerability in imap4d

GLSA-200509-11 : Mozilla Suite, Mozilla Firefox: Multiple vulnerabilities

GLSA-200509-12 : Apache, mod\_ssl: Multiple vulnerabilities

GLSA-200509-13 : Clam AntiVirus: Multiple vulnerabilities

GLSA-200509-14 : Zebedee: Denial of Service vulnerability

GLSA-200509-15 : util-linux: umount command validation error

GLSA-200509-16 : Mantis: XSS and SQL injection vulnerabilities

GLSA-200509-17 : Webmin, Usermin: Remote code execution through PAM authentication

GLSA-200509-18 : Qt: Buffer overflow in the included zlib library

GLSA-200509-19 : PHP: Vulnerabilities in included PCRE and XML-RPC libraries

GLSA-200509-20 : AbiWord: RTF import stack-based buffer overflow

GLSA-200509-21 : Hylafax: Insecure temporary file creation in xferfaxstats script

GLSA-200510-01 : gtkdiskfree: Insecure temporary file creation

GLSA-200510-02 : Berkeley MPEG Tools: Multiple insecure temporary files

GLSA-200510-03 : Uim: Privilege escalation vulnerability

GLSA-200510-04 : Texinfo: Insecure temporary file creation

GLSA-200510-05 : Ruby: Security bypass vulnerability

GLSA-200510-06 : Dia: Arbitrary code execution through SVG import

GLSA-200510-07 : RealPlayer, Helix Player: Format string vulnerability

GLSA-200510-08 : xine-lib: Format string vulnerability

GLSA-200510-09 : Weex: Format string vulnerability

GLSA-200510-10 : uw-imap: Remote buffer overflow

GLSA-200510-11 : OpenSSL: SSL 2.0 protocol rollback

GLSA-200510-12 : KOffice, KWord: RTF import buffer overflow

GLSA-200510-13 : SPE: Insecure file permissions

GLSA-200510-14 : Perl, Qt-UnixODBC, CMake: RUNPATH issues

GLSA-200510-15 : Lynx: Buffer overflow in NNTP processing

GLSA-200510-16 : phpMyAdmin: Local file inclusion vulnerability

GLSA-200510-17 : AbiWord: New RTF import buffer overflows

GLSA-200510-18 : Netpbm: Buffer overflow in pnmtopng

GLSA-200510-19 : cURL: NTLM username stack overflow

GLSA-200510-20 : Zope: File inclusion through RestructuredText

GLSA-200510-21 : phpMyAdmin: Local file inclusion and XSS vulnerabilities

GLSA-200510-22 : SELinux PAM: Local password guessing attack

GLSA-200510-23 : TikiWiki: XSS vulnerability

GLSA-200510-24 : Mantis: Multiple vulnerabilities

GLSA-200510-25 : Ethereal: Multiple vulnerabilities in protocol dissectors

GLSA-200510-26 : XLI, Xloadimage: Buffer overflow

GLSA-200511-01 : libgda: Format string vulnerabilities

GLSA-200511-02 : QDBM, ImageMagick, GDAL: RUNPATH issues

GLSA-200511-03 : giflib: Multiple vulnerabilities

GLSA-200511-04 : ClamAV: Multiple vulnerabilities

GLSA-200511-05 : GNUMP3d: Directory traversal and XSS vulnerabilities

GLSA-200511-06 : fetchmail: Password exposure in fetchmailconf

GLSA-200511-07 : OpenVPN: Multiple vulnerabilities

GLSA-200511-08 : PHP: Multiple vulnerabilities

GLSA-200511-09 : Lynx: Arbitrary command execution

GLSA-200511-10 : RAR: Format string and buffer overflow vulnerabilities

GLSA-200511-11 : linux-ftpd-ssl: Remote buffer overflow

GLSA-200511-12 : Scorched 3D: Multiple vulnerabilities

GLSA-200511-13 : Sylpheed, Sylpheed-Claws: Buffer overflow in LDIF importer

GLSA-200511-14 : GTK+ 2, GdkPixbuf: Multiple XPM decoding vulnerabilities

GLSA-200511-15 : Smb4k: Local unauthorized file access

GLSA-200511-16 : GNUMP3d: Directory traversal and insecure temporary file creation

GLSA-200511-17 : FUSE: mtab corruption through fusermount

GLSA-200511-18 : phpSysInfo: Multiple vulnerabilities

GLSA-200511-19 : eix: Insecure temporary file creation

GLSA-200511-20 : Horde Application Framework: XSS vulnerability

GLSA-200511-21 : Macromedia Flash Player: Remote arbitrary code execution

GLSA-200511-22 : Inkscape: Buffer overflow

GLSA-200511-23 : chmlib, KchmViewer: Stack-based buffer overflow

GLSA-200512-01 : Perl: Format string errors can lead to code execution

GLSA-200512-02 : Webmin, Usermin: Format string vulnerability

GLSA-200512-03 : phpMyAdmin: Multiple vulnerabilities

GLSA-200512-04 : Openswan, IPsec-Tools: Vulnerabilities in ISAKMP Protocol implementation

GLSA-200512-05 : Xmail: Privilege escalation through sendmail

GLSA-200512-06 : Ethereal: Buffer overflow in OSPF protocol dissector

GLSA-200512-07 : OpenLDAP, Gauche: RUNPATH issues

GLSA-200512-08 : Xpdf, GPdf, CUPS, Poppler: Multiple vulnerabilities

GLSA-200512-09 : cURL: Off-by-one errors in URL handling

GLSA-200512-10 : Opera: Command-line URL shell command injection

GLSA-200512-11 : CenterICQ: Multiple vulnerabilities

GLSA-200512-12 : Mantis: Multiple vulnerabilities

GLSA-200512-13 : Dropbear: Privilege escalation

GLSA-200512-14 : NBD Tools: Buffer overflow in NBD server

GLSA-200512-15 : rssh: Privilege escalation

GLSA-200512-16 : OpenMotif, AMD64 x86 emulation X libraries: Buffer overflows in libUil library

GLSA-200512-17 : scponly: Multiple privilege escalation issues

GLSA-200512-18 : XnView: Privilege escalation

GLSA-200601-01 : pinentry: Local privilege escalation

GLSA-200601-02 : KPdf, KWord: Multiple overflows in included Xpdf code

GLSA-200601-03 : HylaFAX: Multiple vulnerabilities

GLSA-200601-04 : VMware Workstation: Vulnerability in NAT networking

GLSA-200601-05 : mod\_auth\_pgsql: Multiple format string vulnerabilities

GLSA-200601-06 : xine-lib, FFmpeg: Heap-based buffer overflow

GLSA-200601-07 : ClamAV: Remote execution of arbitrary code

GLSA-200601-08 : Blender: Heap-based buffer overflow

GLSA-200601-09 : Wine: Windows Metafile SETABORTPROC vulnerability

GLSA-200601-10 : Sun and Blackdown Java: Applet privilege escalation

GLSA-200601-11 : KDE kjs: URI heap overflow vulnerability

GLSA-200601-12 : Trac: XSS vulnerability

GLSA-200601-13 : Gallery: XSS vulnerability

GLSA-200601-14 : LibAST: Privilege escalation

GLSA-200601-15 : Paros: Default administrator password

GLSA-200601-16 : MyDNS: Denial of Service

GLSA-200601-17 : Xpdf, Poppler, GPdf, libextractor, pdftohtml: Heap overflows

GLSA-200602-01 : GStreamer FFmpeg plugin: Heap-based buffer overflow

GLSA-200602-02 : ADOdb: PostgreSQL command injection

GLSA-200602-03 : Apache: Multiple vulnerabilities

GLSA-200602-04 : Xpdf, Poppler: Heap overflow

GLSA-200602-05 : KPdf: Heap based overflow

GLSA-200602-06 : ImageMagick: Format string vulnerability

GLSA-200602-07 : Sun JDK/JRE: Applet privilege escalation

GLSA-200602-08 : libtasn1, GNU TLS: Security flaw in DER decoding

GLSA-200602-09 : BomberClone: Remote execution of arbitrary code

GLSA-200602-10 : GnuPG: Incorrect signature verification

GLSA-200602-11 : OpenSSH, Dropbear: Insecure use of system() call

GLSA-200602-12 : GPdf: heap overflows in included Xpdf code

GLSA-200602-13 : GraphicsMagick: Format string vulnerability

GLSA-200602-14 : noweb: Insecure temporary file creation

GLSA-200603-01 : WordPress: SQL injection vulnerability

GLSA-200603-02 : teTeX, pTeX, CSTeX: Multiple overflows in included XPdf code

GLSA-200603-03 : MPlayer: Multiple integer overflows

GLSA-200603-04 : IMAP Proxy: Format string vulnerabilities

GLSA-200603-05 : zoo: Stack-based buffer overflow

GLSA-200603-06 : GNU tar: Buffer overflow

GLSA-200603-07 : flex: Potential insecure code generation

GLSA-200603-08 : GnuPG: Incorrect signature verification

GLSA-200603-09 : SquirrelMail: XSS and IMAP command injection

GLSA-200603-10 : Cube: Multiple vulnerabilities

GLSA-200603-11 : Freeciv: Denial of Service

GLSA-200603-12 : zoo: Buffer overflow

GLSA-200603-13 : PEAR-Auth: Potential authentication bypass

GLSA-200603-14 : Heimdal: rshd privilege escalation

GLSA-200603-15 : Crypt::CBC: Insecure initialization vector

GLSA-200603-16 : Metamail: Buffer overflow

GLSA-200603-17 : PeerCast: Buffer overflow

GLSA-200603-18 : Pngcrush: Buffer overflow

GLSA-200603-19 : cURL/libcurl: Buffer overflow in the handling of TFTP URLs

GLSA-200603-20 : Macromedia Flash Player: Arbitrary code execution

GLSA-200603-21 : Sendmail: Race condition in the handling of asynchronous signals

GLSA-200603-22 : PHP: Format string and XSS vulnerabilities

GLSA-200603-23 : NetHack, Slash'EM, Falcon's Eye: Local privilege escalation

GLSA-200603-24 : RealPlayer: Buffer overflow vulnerability

GLSA-200603-25 : OpenOffice.org: Heap overflow in included libcurl

GLSA-200603-26 : bsd-games: Local privilege escalation in tetris-bsd

GLSA-200604-01 : MediaWiki: XSS vulnerability

GLSA-200604-02 : Horde Application Framework: Remote code execution

GLSA-200604-03 : FreeRADIUS: Authentication bypass in EAP-MSCHAPv2 module

GLSA-200604-04 : Kaffeine: Buffer overflow

GLSA-200604-05 : Doomsday: Format string vulnerability

GLSA-200604-06 : ClamAV: Multiple vulnerabilities

GLSA-200604-07 : Cacti: Multiple vulnerabilities in included ADOdb

GLSA-200604-08 : libapreq2: Denial of Service vulnerability

GLSA-200604-09 : Cyrus-SASL: DIGEST-MD5 Pre-Authentication Denial of Service

GLSA-200604-10 : zgv, xzgv: Heap overflow

GLSA-200604-11 : Crossfire server: Denial of Service and potential arbitrary code execution

GLSA-200604-12 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200604-13 : fbida: Insecure temporary file creation

GLSA-200604-14 : Dia: Arbitrary code execution through XFig import

GLSA-200604-15 : xine-ui: Format string vulnerabilities

GLSA-200604-16 : xine-lib: Buffer overflow vulnerability

GLSA-200604-17 : Ethereal: Multiple vulnerabilities in protocol dissectors

GLSA-200604-18 : Mozilla Suite: Multiple vulnerabilities

GLSA-200605-01 : MPlayer: Heap-based buffer overflow

GLSA-200605-02 : X.Org: Buffer overflow in XRender extension

GLSA-200605-03 : ClamAV: Buffer overflow in Freshclam

GLSA-200605-04 : phpWebSite: Local file inclusion

GLSA-200605-05 : rsync: Potential integer overflow

GLSA-200605-06 : Mozilla Firefox: Potential remote code execution

GLSA-200605-07 : Nagios: Buffer overflow

GLSA-200605-08 : PHP: Multiple vulnerabilities

GLSA-200605-09 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200605-10 : pdnsd: Denial of Service and potential arbitrary code execution

GLSA-200605-11 : Ruby: Denial of Service

GLSA-200605-12 : Quake 3 engine based games: Buffer Overflow

GLSA-200605-13 : MySQL: Information leakage

GLSA-200605-14 : libextractor: Two heap-based buffer overflows

GLSA-200605-15 : Quagga Routing Suite: Multiple vulnerabilities

GLSA-200605-16 : CherryPy: Directory traversal vulnerability

GLSA-200605-17 : libTIFF: Multiple vulnerabilities

GLSA-200606-01 : Opera: Buffer overflow

GLSA-200606-02 : shadow: Privilege escalation

GLSA-200606-03 : Dia: Format string vulnerabilities

GLSA-200606-04 : Tor: Several vulnerabilities

GLSA-200606-05 : Pound: HTTP request smuggling

GLSA-200606-06 : AWStats: Remote execution of arbitrary code

GLSA-200606-07 : Vixie Cron: Privilege Escalation

GLSA-200606-08 : WordPress: Arbitrary command execution

GLSA-200606-09 : SpamAssassin: Execution of arbitrary code

GLSA-200606-10 : Cscope: Many buffer overflows

GLSA-200606-11 : JPEG library: Denial of Service

GLSA-200606-12 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200606-13 : MySQL: SQL Injection

GLSA-200606-14 : GDM: Privilege escalation

GLSA-200606-15 : Asterisk: IAX2 video frame buffer overflow

GLSA-200606-16 : DokuWiki: PHP code injection

GLSA-200606-17 : OpenLDAP: Buffer overflow

GLSA-200606-18 : PAM-MySQL: Multiple vulnerabilities

GLSA-200606-19 : Sendmail: Denial of Service

GLSA-200606-20 : Typespeed: Remote execution of arbitrary code

GLSA-200606-21 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200606-22 : aRts: Privilege escalation

GLSA-200606-23 : KDM: Symlink vulnerability

GLSA-200606-24 : wv2: Integer overflow

GLSA-200606-25 : Hashcash: Possible heap overflow

GLSA-200606-26 : EnergyMech: Denial of Service

GLSA-200606-27 : Mutt: Buffer overflow

GLSA-200606-28 : Horde Web Application Framework: XSS vulnerability

GLSA-200606-29 : Tikiwiki: SQL injection and multiple XSS vulnerabilities

GLSA-200606-30 : Kiax: Arbitrary code execution

GLSA-200607-01 : mpg123: Heap overflow

GLSA-200607-02 : FreeType: Multiple integer overflows

GLSA-200607-03 : libTIFF: Multiple buffer overflows

GLSA-200607-04 : PostgreSQL: SQL injection

GLSA-200607-05 : SHOUTcast server: Multiple vulnerabilities

GLSA-200607-06 : libpng: Buffer overflow

GLSA-200607-07 : xine-lib: Buffer overflow

GLSA-200607-08 : GIMP: Buffer overflow

GLSA-200607-09 : Wireshark: Multiple vulnerabilities

GLSA-200607-10 : Samba: Denial of Service vulnerability

GLSA-200607-11 : TunePimp: Buffer overflow

GLSA-200607-12 : OpenOffice.org: Multiple vulnerabilities

GLSA-200607-13 : Audacious: Multiple heap and buffer overflows

GLSA-200608-01 : Apache: Off-by-one flaw in mod\_rewrite

GLSA-200608-02 : Mozilla SeaMonkey: Multiple vulnerabilities

GLSA-200608-03 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200608-04 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200608-05 : LibVNCServer: Authentication bypass

GLSA-200608-06 : Courier MTA: Denial of Service vulnerability

GLSA-200608-07 : libTIFF: Multiple vulnerabilities

GLSA-200608-08 : GnuPG: Integer overflow vulnerability

GLSA-200608-09 : MySQL: Denial of Service

GLSA-200608-10 : pike: SQL injection vulnerability

GLSA-200608-11 : Webmin, Usermin: File Disclosure

GLSA-200608-12 : x11vnc: Authentication bypass in included LibVNCServer code

GLSA-200608-13 : ClamAV: Heap buffer overflow

GLSA-200608-14 : DUMB: Heap buffer overflow

GLSA-200608-15 : MIT Kerberos 5: Multiple local privilege escalation vulnerabilities

GLSA-200608-16 : Warzone 2100 Resurrection: Multiple buffer overflows

GLSA-200608-17 : libwmf: Buffer overflow vulnerability

GLSA-200608-18 : Net::Server: Format string vulnerability

GLSA-200608-19 : WordPress: Privilege escalation

GLSA-200608-20 : Ruby on Rails: Several vulnerabilities

GLSA-200608-21 : Heimdal: Multiple local privilege escalation vulnerabilities

GLSA-200608-22 : fbida: Arbitrary command execution

GLSA-200608-23 : Heartbeat: Denial of Service

GLSA-200608-24 : AlsaPlayer: Multiple buffer overflows

GLSA-200608-25 : X.org and some X.org libraries: Local privilege escalations

GLSA-200608-26 : Wireshark: Multiple vulnerabilities

GLSA-200608-27 : Motor: Execution of arbitrary code

GLSA-200608-28 : PHP: Arbitary code execution

GLSA-200609-01 : Streamripper: Multiple remote buffer overflows

GLSA-200609-02 : GTetrinet: Remote code execution

GLSA-200609-03 : OpenTTD: Remote Denial of Service

GLSA-200609-04 : LibXfont: Multiple integer overflows

GLSA-200609-05 : OpenSSL, AMD64 x86 emulation base libraries: RSA signature forgery

GLSA-200609-06 : AdPlug: Multiple vulnerabilities

GLSA-200609-07 : LibXfont, monolithic X.org: Multiple integer overflows

GLSA-200609-08 : xine-lib: Buffer overflows

GLSA-200609-09 : FFmpeg: Buffer overflows

GLSA-200609-10 : DokuWiki: Arbitrary command execution

GLSA-200609-11 : BIND: Denial of Service

GLSA-200609-12 : Mailman: Multiple vulnerabilities

GLSA-200609-13 : gzip: Multiple vulnerabilities

GLSA-200609-14 : ImageMagick: Multiple Vulnerabilities

GLSA-200609-15 : GnuTLS: RSA Signature Forgery

GLSA-200609-16 : Tikiwiki: Arbitrary command execution

GLSA-200609-17 : OpenSSH: Denial of Service

GLSA-200609-18 : Opera: RSA signature forgery

GLSA-200609-19 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200609-20 : DokuWiki: Shell command injection and Denial of Service

GLSA-200610-01 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200610-02 : Adobe Flash Player: Arbitrary code execution

GLSA-200610-03 : ncompress: Buffer Underflow

GLSA-200610-04 : SeaMonkey: Multiple vulnerabilities

GLSA-200610-05 : CAPI4Hylafax fax receiver: Execution of arbitrary code

GLSA-200610-06 : Mozilla Network Security Service (NSS): RSA signature forgery

GLSA-200610-07 : Python: Buffer Overflow

GLSA-200610-08 : Cscope: Multiple buffer overflows

GLSA-200610-09 : libmusicbrainz: Multiple buffer overflows

GLSA-200610-10 : ClamAV: Multiple Vulnerabilities

GLSA-200610-11 : OpenSSL: Multiple vulnerabilities

GLSA-200610-12 : Apache mod\_tcl: Format string vulnerability

GLSA-200610-13 : Cheese Tracker: Buffer Overflow

GLSA-200610-14 : PHP: Integer overflow

GLSA-200610-15 : Asterisk: Multiple vulnerabilities

GLSA-200611-01 : Screen: UTF-8 character handling vulnerability

GLSA-200611-02 : Qt: Integer overflow

GLSA-200611-03 : NVIDIA binary graphics driver: Privilege escalation vulnerability

GLSA-200611-04 : Bugzilla: Multiple Vulnerabilities

GLSA-200611-05 : Netkit FTP Server: Privilege escalation

GLSA-200611-06 : OpenSSH: Multiple Denial of Service vulnerabilities

GLSA-200611-07 : GraphicsMagick: PALM and DCM buffer overflows

GLSA-200611-08 : RPM: Buffer overflow

GLSA-200611-09 : libpng: Denial of Service

GLSA-200611-10 : WordPress: Multiple vulnerabilities

GLSA-200611-11 : TikiWiki: Multiple vulnerabilities

GLSA-200611-12 : Ruby: Denial of Service vulnerability

GLSA-200611-13 : Avahi: 'netlink' message vulnerability

GLSA-200611-14 : TORQUE: Insecure temporary file creation

GLSA-200611-15 : qmailAdmin: Buffer overflow

GLSA-200611-16 : Texinfo: Buffer overflow

GLSA-200611-17 : fvwm: fvwm-menu-directory fvwm command injection

GLSA-200611-18 : TIN: Multiple buffer overflows

GLSA-200611-19 : ImageMagick: PALM and DCM buffer overflows

GLSA-200611-20 : GNU gv: Stack overflow

GLSA-200611-21 : Kile: Incorrect backup file permission

GLSA-200611-22 : Ingo H3: Folder name shell command injection

GLSA-200611-23 : Mono: Insecure temporary file creation

GLSA-200611-24 : LHa: Multiple vulnerabilities

GLSA-200611-25 : OpenLDAP: Denial of Service vulnerability

GLSA-200611-26 : ProFTPD: Remote execution of arbitrary code

GLSA-200612-01 : wv library: Multiple integer overflows

GLSA-200612-02 : xine-lib: Buffer overflow

GLSA-200612-03 : GnuPG: Multiple vulnerabilities

GLSA-200612-04 : ModPlug: Multiple buffer overflows

GLSA-200612-05 : KOffice shared libraries: Heap corruption

GLSA-200612-06 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200612-07 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200612-08 : SeaMonkey: Multiple vulnerabilities

GLSA-200612-09 : MadWifi: Kernel driver buffer overflow

GLSA-200612-10 : Tar: Directory traversal vulnerability

GLSA-200612-11 : AMD64 x86 emulation base libraries: OpenSSL multiple vulnerabilities

GLSA-200612-12 : F-PROT Antivirus: Multiple vulnerabilities

GLSA-200612-13 : libgsf: Buffer overflow

GLSA-200612-14 : Trac: Cross-site request forgery

GLSA-200612-15 : McAfee VirusScan: Insecure DT\_RPATH

GLSA-200612-16 : Links: Arbitrary Samba command execution

GLSA-200612-17 : GNU Radius: Format string vulnerability

GLSA-200612-18 : ClamAV: Denial of Service

GLSA-200612-19 : pam\_ldap: Authentication bypass vulnerability

GLSA-200612-20 : imlib2: Multiple vulnerabilities

GLSA-200612-21 : Ruby: Denial of Service vulnerability

GLSA-200701-01 : DenyHosts: Denial of Service

GLSA-200701-02 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200701-03 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200701-04 : SeaMonkey: Multiple vulnerabilities

GLSA-200701-05 : KDE kfile JPEG info plugin: Denial of Service

GLSA-200701-06 : w3m: Format string vulnerability

GLSA-200701-07 : OpenOffice.org: EMF/WMF file handling vulnerabilities

GLSA-200701-08 : Opera: Two remote code execution vulnerabilities

GLSA-200701-09 : oftpd: Denial of Service

GLSA-200701-10 : WordPress: Multiple vulnerabilities

GLSA-200701-11 : Kronolith: Local file inclusion

GLSA-200701-12 : Mono: Information disclosure

GLSA-200701-13 : Fetchmail: Denial of Service and password disclosure

GLSA-200701-14 : Mod\_auth\_kerb: Denial of Service

GLSA-200701-15 : Sun JDK/JRE: Multiple vulnerabilities

GLSA-200701-16 : Adobe Acrobat Reader: Multiple vulnerabilities

GLSA-200701-17 : libgtop: Privilege escalation

GLSA-200701-18 : xine-ui: Format string vulnerabilities

GLSA-200701-19 : OpenLDAP: Insecure usage of /tmp during installation

GLSA-200701-20 : Centericq: Remote buffer overflow in LiveJournal handling

GLSA-200701-21 : MIT Kerberos 5: Arbitrary Remote Code Execution

GLSA-200701-22 : Squid: Multiple Denial of Service vulnerabilities

GLSA-200701-23 : Cacti: Command execution and SQL injection

GLSA-200701-24 : VLC media player: Format string vulnerability

GLSA-200701-25 : X.Org X server: Multiple vulnerabilities

GLSA-200701-26 : KSirc: Denial of Service vulnerability

GLSA-200701-27 : ELinks: Arbitrary Samba command execution

GLSA-200701-28 : thttpd: Unauthenticated remote file access

GLSA-200702-01 : Samba: Multiple vulnerabilities

GLSA-200702-02 : ProFTPD: Local privilege escalation

GLSA-200702-03 : Snort: Denial of Service

GLSA-200702-04 : RAR, UnRAR: Buffer overflow

GLSA-200702-05 : Fail2ban: Denial of Service

GLSA-200702-06 : BIND: Denial of Service

GLSA-200702-07 : Sun JDK/JRE: Execution of arbitrary code

GLSA-200702-08 : AMD64 x86 emulation Sun's J2SE Development Kit: Multiple vulnerabilities

GLSA-200702-09 : Nexuiz: Multiple vulnerabilities

GLSA-200702-10 : UFO2000: Multiple vulnerabilities

GLSA-200702-11 : MPlayer: Buffer overflow

GLSA-200702-12 : CHMlib: User-assisted remote execution of arbitrary code

GLSA-200703-01 : Snort: Remote execution of arbitrary code

GLSA-200703-02 : SpamAssassin: Long URI Denial of Service

GLSA-200703-03 : ClamAV: Denial of Service

GLSA-200703-04 : Mozilla Firefox: Multiple vulnerabilities

GLSA-200703-05 : Mozilla Suite: Multiple vulnerabilities

GLSA-200703-06 : AMD64 x86 emulation Qt library: Integer overflow

GLSA-200703-07 : STLport: Possible remote execution of arbitrary code

GLSA-200703-08 : SeaMonkey: Multiple vulnerabilities

GLSA-200703-09 : Smb4K: Multiple vulnerabilities

GLSA-200703-10 : KHTML: XSS (XSS) vulnerability

GLSA-200703-11 : Amarok: User-assisted remote execution of arbitrary code

GLSA-200703-12 : SILC Server: Denial of Service

GLSA-200703-13 : SSH Communications Security's Secure Shell Server: SFTP privilege escalation

GLSA-200703-14 : Asterisk: SIP Denial of Service

GLSA-200703-15 : PostgreSQL: Multiple vulnerabilities

GLSA-200703-16 : Apache JK Tomcat Connector: Remote execution of arbitrary code

GLSA-200703-17 : ulogd: Remote execution of arbitrary code

GLSA-200703-18 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200703-19 : LTSP: Authentication bypass in included LibVNCServer code

GLSA-200703-20 : LSAT: Insecure temporary file creation

GLSA-200703-21 : PHP: Multiple vulnerabilities

GLSA-200703-22 : Mozilla Network Security Service: Remote execution of arbitrary code

GLSA-200703-23 : WordPress: Multiple vulnerabilities

GLSA-200703-24 : mgv: Stack overflow in included gv code

GLSA-200703-25 : Ekiga: Format string vulnerability

GLSA-200703-26 : file: Integer underflow

GLSA-200703-27 : Squid: Denial of Service

GLSA-200703-28 : CUPS: Denial of Service

GLSA-200704-01 : Asterisk: Two SIP Denial of Service vulnerabilities

GLSA-200704-02 : MIT Kerberos 5: Arbitrary remote code execution

GLSA-200704-03 : OpenAFS: Privilege escalation

GLSA-200704-04 : OpenPBS: Multiple vulnerabilities

GLSA-200704-05 : zziplib: Buffer Overflow

GLSA-200704-06 : Evince: Stack overflow in included gv code

GLSA-200704-07 : libwpd: Multiple vulnerabilities

GLSA-200704-08 : DokuWiki: XSS vulnerability

GLSA-200704-09 : xine-lib: Heap-based buffer overflow

GLSA-200704-10 : Inkscape: Two format string vulnerabilities

GLSA-200704-11 : Vixie Cron: Denial of Service

GLSA-200704-12 : OpenOffice.org: Multiple vulnerabilities

GLSA-200704-13 : File: Denial of Service

GLSA-200704-14 : FreeRADIUS: Denial of Service

GLSA-200704-15 : MadWifi: Multiple vulnerabilities

GLSA-200704-16 : Aircrack-ng: Remote execution of arbitrary code

GLSA-200704-17 : 3proxy: Buffer overflow

GLSA-200704-18 : Courier-IMAP: Remote execution of arbitrary code

GLSA-200704-19 : Blender: User-assisted remote execution of arbitrary code

GLSA-200704-20 : NAS: Multiple vulnerabilities

GLSA-200704-21 : ClamAV: Multiple vulnerabilities

GLSA-200704-22 : BEAST: Denial of Service

GLSA-200704-23 : capi4k-utils: Buffer overflow

GLSA-200705-01 : Ktorrent: Multiple vulnerabilities

GLSA-200705-02 : FreeType: User-assisted execution of arbitrary code

GLSA-200705-03 : Tomcat: Information disclosure

GLSA-200705-04 : Apache mod\_perl: Denial of Service

GLSA-200705-05 : Quagga: Denial of Service

GLSA-200705-06 : X.Org X11 library: Multiple integer overflows

GLSA-200705-07 : Lighttpd: Two Denials of Service

GLSA-200705-08 : GIMP: Buffer overflow

GLSA-200705-09 : IPsec-Tools: Denial of Service

GLSA-200705-10 : LibXfont, TightVNC: Multiple vulnerabilities

GLSA-200705-11 : MySQL: Two Denial of Service vulnerabilities

GLSA-200705-12 : PostgreSQL: Privilege escalation

GLSA-200705-13 : ImageMagick: Multiple buffer overflows

GLSA-200705-14 : XScreenSaver: Privilege escalation

GLSA-200705-15 : Samba: Multiple vulnerabilities

GLSA-200705-16 : PhpWiki: Remote execution of arbitrary code

GLSA-200705-17 : Apache mod\_security: Rule bypass

GLSA-200705-18 : PPTPD: Denial of Service attack

GLSA-200705-19 : PHP: Multiple vulnerabilities

GLSA-200705-20 : Blackdown Java: Applet privilege escalation

GLSA-200705-21 : MPlayer: Two buffer overflows

GLSA-200705-22 : FreeType: Buffer overflow

GLSA-200705-23 : Sun JDK/JRE: Multiple vulnerabilities

GLSA-200705-24 : libpng: Denial of Service

GLSA-200705-25 : file: Integer overflow

GLSA-200706-01 : libexif: Integer overflow vulnerability

GLSA-200706-02 : Evolution: User-assisted execution of arbitrary code

GLSA-200706-03 : ELinks: User-assisted execution of arbitrary code

GLSA-200706-04 : MadWifi: Multiple vulnerabilities

GLSA-200706-05 : ClamAV: Multiple Denials of Service

GLSA-200706-06 : Mozilla products: Multiple vulnerabilities

GLSA-200706-07 : PHProjekt: Multiple vulnerabilities

GLSA-200706-08 : emul-linux-x86-java: Multiple vulnerabilities

GLSA-200706-09 : libexif: Buffer overflow

GLSA-200707-01 : Firebird: Buffer overflow

GLSA-200707-02 : OpenOffice.org: Two buffer overflows

GLSA-200707-03 : Evolution: User-assisted remote execution of arbitrary code

GLSA-200707-04 : GNU C Library: Integer overflow

GLSA-200707-05 : Webmin, Usermin: XSS vulnerabilities

GLSA-200707-06 : XnView: Stack-based buffer overflow

GLSA-200707-07 : MPlayer: Multiple buffer overflows

GLSA-200707-08 : NVClock: Insecure file usage

GLSA-200707-09 : GIMP: Multiple integer overflows

GLSA-200707-10 : Festival: Privilege elevation

GLSA-200707-11 : MIT Kerberos 5: Arbitrary remote code execution

GLSA-200707-12 : VLC media player: Format string vulnerabilities

GLSA-200707-13 : Fail2ban: Denial of Service

GLSA-200707-14 : tcpdump: Integer overflow

GLSA-200708-01 : Macromedia Flash Player: Remote arbitrary code execution

GLSA-200708-02 : Xvid: Array indexing vulnerabilities

GLSA-200708-03 : libarchive (formerly named as bsdtar): Multiple PaX Extension Header Vulnerabilities

GLSA-200708-04 : ClamAV: Denial of Service

GLSA-200708-05 : GD: Multiple vulnerabilities

GLSA-200708-06 : Net::DNS: Multiple vulnerabilities

GLSA-200708-07 : Xfce Terminal: Remote arbitrary code execution

GLSA-200708-08 : SquirrelMail G/PGP plugin: Arbitrary code execution

GLSA-200708-09 : Mozilla products: Multiple vulnerabilities

GLSA-200708-10 : MySQL: Denial of Service and information leakage

GLSA-200708-11 : Lighttpd: Multiple vulnerabilities

GLSA-200708-12 : Wireshark: Multiple vulnerabilities

GLSA-200708-13 : BIND: Weak random number generation

GLSA-200708-14 : NVIDIA drivers: Denial of Service

GLSA-200708-15 : Apache mod\_jk: Directory traversal

GLSA-200708-16 : Qt: Multiple format string vulnerabilities

GLSA-200708-17 : Opera: Multiple vulnerabilities

GLSA-200709-01 : MIT Kerberos 5: Multiple vulnerabilities

GLSA-200709-02 : KVIrc: Remote arbitrary code execution

GLSA-200709-03 : Streamripper: Buffer overflow

GLSA-200709-04 : po4a: Insecure temporary file creation

GLSA-200709-05 : RealPlayer: Buffer overflow

GLSA-200709-06 : flac123: Buffer overflow

GLSA-200709-07 : Eggdrop: Buffer overflow

GLSA-200709-08 : id3lib: Insecure temporary file creation

GLSA-200709-09 : GNU Tar: Directory traversal vulnerability

GLSA-200709-10 : PhpWiki: Authentication bypass

GLSA-200709-11 : GDM: Local Denial of Service

GLSA-200709-12 : Poppler: Two buffer overflow vulnerabilities

GLSA-200709-13 : rsync: Two buffer overflows

GLSA-200709-14 : ClamAV: Multiple vulnerabilities

GLSA-200709-15 : BEA JRockit: Multiple vulnerabilities

GLSA-200709-16 : Lighttpd: Buffer overflow

GLSA-200709-17 : teTeX: Multiple buffer overflows

GLSA-200709-18 : Bugzilla: Multiple vulnerabilities

GLSA-200710-01 : RPCSEC\_GSS library: Buffer overflow

GLSA-200710-02 : PHP: Multiple vulnerabilities

GLSA-200710-03 : libvorbis: Multiple vulnerabilities

GLSA-200710-04 : libsndfile: Buffer overflow

GLSA-200710-05 : QGit: Insecure temporary file creation

GLSA-200710-06 : OpenSSL: Multiple vulnerabilities

GLSA-200710-07 : Tk: Buffer overflow

GLSA-200710-08 : KOffice, KWord, KPDF, KDE Graphics Libraries: Stack-based buffer overflow

GLSA-200710-09 : NX 2.1: User-assisted execution of arbitrary code

GLSA-200710-10 : SKK Tools: Insecure temporary file creation

GLSA-200710-11 : X Font Server: Multiple Vulnerabilities

GLSA-200710-12 : T1Lib: Buffer overflow

GLSA-200710-13 : Ampache: Multiple vulnerabilities

GLSA-200710-14 : DenyHosts: Denial of Service

GLSA-200710-15 : KDM: Local privilege escalation

GLSA-200710-16 : X.Org X server: Composite local privilege escalation

GLSA-200710-17 : Balsa: Buffer overflow

GLSA-200710-18 : util-linux: Local privilege escalation

GLSA-200710-19 : The Sleuth Kit: Integer underflow

GLSA-200710-20 : PDFKit, ImageKits: Buffer overflow

GLSA-200710-21 : TikiWiki: Arbitrary command execution

GLSA-200710-22 : TRAMP: Insecure temporary file creation

GLSA-200710-23 : Star: Directory traversal vulnerability

GLSA-200710-24 : OpenOffice.org: Heap-based buffer overflow

GLSA-200710-25 : MLDonkey: Privilege escalation

GLSA-200710-26 : HPLIP: Privilege escalation

GLSA-200710-27 : ImageMagick: Multiple vulnerabilities

GLSA-200710-28 : Qt: Buffer overflow

GLSA-200710-29 : Sylpheed, Claws Mail: User-assisted remote execution of arbitrary code

GLSA-200710-30 : OpenSSL: Remote execution of arbitrary code

GLSA-200710-31 : Opera: Multiple vulnerabilities

GLSA-200711-01 : gFTP: Multiple vulnerabilities

GLSA-200711-02 : OpenSSH: Security bypass

GLSA-200711-03 : Gallery: Multiple vulnerabilities

GLSA-200711-04 : Evolution: User-assisted remote execution of arbitrary code

GLSA-200711-05 : SiteBar: Multiple issues

GLSA-200711-06 : Apache: Multiple vulnerabilities

GLSA-200711-07 : Python: User-assisted execution of arbitrary code

GLSA-200711-08 : libpng: Multiple Denials of Service

GLSA-200711-09 : MadWifi: Denial of Service

GLSA-200711-10 : Mono: Buffer overflow

GLSA-200711-11 : Nagios Plugins: Two buffer overflows

GLSA-200711-12 : Tomboy: User-assisted execution of arbitrary code

GLSA-200711-13 : 3proxy: Denial of Service

GLSA-200711-14 : Mozilla Firefox, SeaMonkey, XULRunner: Multiple vulnerabilities

GLSA-200711-15 : FLAC: Buffer overflow

GLSA-200711-16 : CUPS: Memory corruption

GLSA-200711-17 : Ruby on Rails: Multiple vulnerabilities

GLSA-200711-18 : Cpio: Buffer overflow

GLSA-200711-19 : TikiWiki: Multiple vulnerabilities

GLSA-200711-20 : Pioneers: Multiple Denials of Service

GLSA-200711-21 : Bochs: Multiple vulnerabilities

GLSA-200711-22 : Poppler, KDE: User-assisted execution of arbitrary code

GLSA-200711-23 : VMware Workstation and Player: Multiple vulnerabilities

GLSA-200711-24 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-200711-25 : MySQL: Denial of Service

GLSA-200711-26 : teTeX: Multiple vulnerabilities

GLSA-200711-27 : Link Grammar: User-assisted execution of arbitrary code

GLSA-200711-28 : Perl: Buffer overflow

GLSA-200711-29 : Samba: Execution of arbitrary code

GLSA-200711-30 : PCRE: Multiple vulnerabilities

GLSA-200711-31 : Net-SNMP: Denial of Service

GLSA-200711-32 : Feynmf: Insecure temporary file creation

GLSA-200711-33 : nss\_ldap: Information disclosure

GLSA-200711-34 : CSTeX: Multiple vulnerabilities

GLSA-200712-01 : Hugin: Insecure temporary file creation

GLSA-200712-02 : Cacti: SQL injection

GLSA-200712-03 : GNU Emacs: Multiple vulnerabilities

GLSA-200712-04 : Cairo: User-assisted execution of arbitrary code

GLSA-200712-05 : PEAR::MDB2: Information disclosure

GLSA-200712-06 : Firebird: Multiple buffer overflows

GLSA-200712-07 : Lookup: Insecure temporary file creation

GLSA-200712-08 : AMD64 x86 emulation Qt library: Multiple vulnerabilities

GLSA-200712-09 : Ruby-GNOME2: Format string error

GLSA-200712-10 : Samba: Execution of arbitrary code

GLSA-200712-11 : Portage: Information disclosure

GLSA-200712-12 : IRC Services: Denial of Service

GLSA-200712-13 : E2fsprogs: Multiple buffer overflows

GLSA-200712-14 : CUPS: Multiple vulnerabilities

GLSA-200712-15 : libexif: Multiple vulnerabilities

GLSA-200712-16 : Exiv2: Integer overflow

GLSA-200712-17 : exiftags: Multiple vulnerabilities

GLSA-200712-18 : Multi-Threaded DAAP Daemon: Multiple vulnerabilities

GLSA-200712-19 : Syslog-ng: Denial of Service

GLSA-200712-20 : ClamAV: Multiple vulnerabilities

GLSA-200712-21 : Mozilla Firefox, SeaMonkey: Multiple vulnerabilities

GLSA-200712-22 : Opera: Multiple vulnerabilities

GLSA-200712-23 : Wireshark: Multiple vulnerabilities

GLSA-200712-24 : AMD64 x86 emulation GTK+ library: User-assisted execution of arbitrary code

GLSA-200712-25 : OpenOffice.org: User-assisted arbitrary code execution

GLSA-200801-01 : unp: Arbitrary command execution

GLSA-200801-02 : R: Multiple vulnerabilities

GLSA-200801-03 : Claws Mail: Insecure temporary file creation

GLSA-200801-04 : OpenAFS: Denial of Service

GLSA-200801-05 : Squid: Denial of Service

GLSA-200801-06 : Xfce: Multiple vulnerabilities

GLSA-200801-07 : Adobe Flash Player: Multiple vulnerabilities

GLSA-200801-08 : libcdio: User-assisted execution of arbitrary code

GLSA-200801-09 : X.Org X server and Xfont library: Multiple vulnerabilities

GLSA-200801-10 : TikiWiki: Multiple vulnerabilities

GLSA-200801-11 : CherryPy: Directory traversal vulnerability

GLSA-200801-12 : xine-lib: User-assisted execution of arbitrary code

GLSA-200801-13 : ngIRCd: Denial of Service

GLSA-200801-14 : Blam: User-assisted execution of arbitrary code

GLSA-200801-15 : PostgreSQL: Multiple vulnerabilities

GLSA-200801-16 : MaraDNS: CNAME Denial of Service

GLSA-200801-17 : Netkit FTP Server: Denial of Service

GLSA-200801-18 : Kazehakase: Multiple vulnerabilities

GLSA-200801-19 : GOffice: Multiple vulnerabilities

GLSA-200801-20 : libxml2: Denial of Service

GLSA-200801-21 : Xdg-Utils: Arbitrary command execution

GLSA-200801-22 : PeerCast: Buffer overflow

GLSA-200802-01 : SDL\_image: Two buffer overflow vulnerabilities

GLSA-200802-02 : Doomsday: Multiple vulnerabilities

GLSA-200802-03 : Horde IMP: Security bypass

GLSA-200802-04 : Gallery: Multiple vulnerabilities

GLSA-200802-05 : Gnumeric: User-assisted execution of arbitrary code

GLSA-200802-06 : scponly: Multiple vulnerabilities

GLSA-200802-07 : Pulseaudio: Privilege escalation

GLSA-200802-08 : Boost: Denial of Service

GLSA-200802-09 : ClamAV: Multiple vulnerabilities

GLSA-200802-10 : Python: PCRE Integer overflow

GLSA-200802-11 : Asterisk: Multiple vulnerabilities

GLSA-200802-12 : xine-lib: User-assisted execution of arbitrary code

GLSA-200803-01 : Adobe Acrobat Reader: Multiple vulnerabilities

GLSA-200803-02 : Firebird: Multiple vulnerabilities

GLSA-200803-03 : Audacity: Insecure temporary file creation

GLSA-200803-04 : Mantis: XSS

GLSA-200803-05 : SplitVT: Privilege escalation

GLSA-200803-06 : SWORD: Shell command injection

GLSA-200803-07 : Paramiko: Information disclosure

GLSA-200803-08 : Win32 binary codecs: Multiple vulnerabilities

GLSA-200803-09 : Opera: Multiple vulnerabilities

GLSA-200803-10 : lighttpd: Multiple vulnerabilities

GLSA-200803-11 : Vobcopy: Insecure temporary file creation

GLSA-200803-12 : Evolution: Format string vulnerability

GLSA-200803-13 : VLC: Multiple vulnerabilities

GLSA-200803-14 : Ghostscript: Buffer overflow

GLSA-200803-15 : phpMyAdmin: SQL injection vulnerability

GLSA-200803-16 : MPlayer: Multiple buffer overflows

GLSA-200803-17 : PDFlib: Multiple buffer overflows

GLSA-200803-18 : Cacti: Multiple vulnerabilities

GLSA-200803-19 : Apache: Multiple vulnerabilities

GLSA-200803-20 : International Components for Unicode: Multiple vulnerabilities

GLSA-200803-21 : Sarg: Remote execution of arbitrary code

GLSA-200803-22 : LIVE555 Media Server: Denial of Service

GLSA-200803-23 : Website META Language: Insecure temporary file usage

GLSA-200803-24 : PCRE: Buffer overflow

GLSA-200803-25 : Dovecot: Multiple vulnerabilities

GLSA-200803-26 : Adobe Acrobat Reader: Insecure temporary file creation

GLSA-200803-27 : MoinMoin: Multiple vulnerabilities

GLSA-200803-28 : OpenLDAP: Denial of Service vulnerabilities

GLSA-200803-29 : ViewVC: Multiple vulnerabilities

GLSA-200803-30 : ssl-cert eclass: Certificate disclosure

GLSA-200803-31 : MIT Kerberos 5: Multiple vulnerabilities

GLSA-200803-32 : Wireshark: Denial of Service

GLSA-200804-01 : CUPS: Multiple vulnerabilities

GLSA-200804-02 : bzip2: Denial of Service

GLSA-200804-03 : OpenSSH: Privilege escalation

GLSA-200804-04 : MySQL: Multiple vulnerabilities

GLSA-200804-05 : NX: User-assisted execution of arbitrary code

GLSA-200804-06 : UnZip: User-assisted execution of arbitrary code

GLSA-200804-07 : PECL APC: Buffer Overflow

GLSA-200804-08 : lighttpd: Multiple vulnerabilities

GLSA-200804-09 : am-utils: Insecure temporary file creation

GLSA-200804-10 : Tomcat: Multiple vulnerabilities

GLSA-200804-11 : policyd-weight: Insecure temporary file creation

GLSA-200804-12 : gnome-screensaver: Privilege escalation

GLSA-200804-13 : Asterisk: Multiple vulnerabilities

GLSA-200804-14 : Opera: Multiple vulnerabilities

GLSA-200804-15 : libpng: Execution of arbitrary code

GLSA-200804-16 : rsync: Execution of arbitrary code

GLSA-200804-17 : Speex: User-assisted execution of arbitrary code

GLSA-200804-18 : Poppler: User-assisted execution of arbitrary code

GLSA-200804-19 : PHP Toolkit: Data disclosure and Denial of Service

GLSA-200804-20 : Sun JDK/JRE: Multiple vulnerabilities

GLSA-200804-21 : Adobe Flash Player: Multiple vulnerabilities

GLSA-200804-22 : PowerDNS Recursor: DNS Cache Poisoning

GLSA-200804-23 : CUPS: Integer overflow vulnerability

GLSA-200804-24 : DBmail: Data disclosure

GLSA-200804-25 : VLC: User-assisted execution of arbitrary code

GLSA-200804-26 : Openfire: Denial of Service

GLSA-200804-27 : SILC: Multiple vulnerabilities

GLSA-200804-28 : JRockit: Multiple vulnerabilities

GLSA-200804-29 : Comix: Multiple vulnerabilities

GLSA-200804-30 : KDE start\_kdeinit: Multiple vulnerabilities

GLSA-200805-01 : Horde Application Framework: Multiple vulnerabilities

GLSA-200805-02 : phpMyAdmin: Information disclosure

GLSA-200805-03 : Multiple X11 terminals: Local privilege escalation

GLSA-200805-04 : eGroupWare: Multiple vulnerabilities

GLSA-200805-05 : Wireshark: Denial of Service

GLSA-200805-06 : Firebird: Data disclosure

GLSA-200805-07 : Linux Terminal Server Project: Multiple vulnerabilities

GLSA-200805-08 : InspIRCd: Denial of Service

GLSA-200805-09 : MoinMoin: Privilege escalation

GLSA-200805-10 : Pngcrush: User-assisted execution of arbitrary code

GLSA-200805-11 : Chicken: Multiple vulnerabilities

GLSA-200805-12 : Blender: Multiple vulnerabilities

GLSA-200805-13 : PTeX: Multiple vulnerabilities

GLSA-200805-14 : Common Data Format library: User-assisted execution of arbitrary code

GLSA-200805-15 : libid3tag: Denial of Service

GLSA-200805-16 : OpenOffice.org: Multiple vulnerabilities

GLSA-200805-17 : Perl: Execution of arbitrary code

GLSA-200805-18 : Mozilla products: Multiple vulnerabilities

GLSA-200805-19 : ClamAV: Multiple vulnerabilities

GLSA-200805-20 : GnuTLS: Execution of arbitrary code

GLSA-200805-21 : Roundup: Permission bypass

GLSA-200805-22 : MPlayer: User-assisted execution of arbitrary code

GLSA-200805-23 : Samba: Heap-based buffer overflow

GLSA-200806-01 : mtr: Stack-based buffer overflow

GLSA-200806-02 : libxslt: Execution of arbitrary code

GLSA-200806-03 : Imlib 2: User-assisted execution of arbitrary code

GLSA-200806-04 : rdesktop: Multiple vulnerabilities

GLSA-200806-05 : cbrPager: User-assisted execution of arbitrary code

GLSA-200806-06 : Evolution: User-assisted execution of arbitrary code

GLSA-200806-07 : X.Org X server: Multiple vulnerabilities

GLSA-200806-08 : OpenSSL: Denial of Service

GLSA-200806-09 : libvorbis: Multiple vulnerabilities

GLSA-200806-10 : FreeType: User-assisted execution of arbitrary code

GLSA-200806-11 : IBM JDK/JRE: Multiple vulnerabilities

GLSA-200807-01 : Python: Multiple integer overflows

GLSA-200807-02 : Motion: Execution of arbitrary code

GLSA-200807-03 : PCRE: Buffer overflow

GLSA-200807-04 : Poppler: User-assisted execution of arbitrary code

GLSA-200807-05 : OpenOffice.org: User-assisted execution of arbitrary code

GLSA-200807-06 : Apache: Denial of Service

GLSA-200807-07 : NX: User-assisted execution of arbitrary code

GLSA-200807-08 : BIND: Cache poisoning

GLSA-200807-09 : Mercurial: Directory traversal

GLSA-200807-10 : Bacula: Information disclosure

GLSA-200807-11 : PeerCast: Buffer overflow

GLSA-200807-12 : BitchX: Multiple vulnerabilities

GLSA-200807-13 : VLC: Multiple vulnerabilities

GLSA-200807-14 : Linux Audit: Buffer overflow

GLSA-200807-15 : Pan: User-assisted execution of arbitrary code

GLSA-200807-16 : Python: Multiple vulnerabilities

GLSA-200808-01 : xine-lib: User-assisted execution of arbitrary code

GLSA-200808-02 : Net-SNMP: Multiple vulnerabilities

GLSA-200808-03 : Mozilla products: Multiple vulnerabilities

GLSA-200808-04 : Wireshark: Denial of Service

GLSA-200808-05 : ISC DHCP: Denial of Service

GLSA-200808-06 : libxslt: Execution of arbitrary code

GLSA-200808-07 : ClamAV: Multiple Denials of Service

GLSA-200808-08 : stunnel: Security bypass

GLSA-200808-09 : OpenLDAP: Denial of Service vulnerability

GLSA-200808-10 : Adobe Reader: User-assisted execution of arbitrary code

GLSA-200808-11 : UUDeview: Insecure temporary file creation

GLSA-200808-12 : Postfix: Local privilege escalation vulnerability

GLSA-200809-01 : yelp: User-assisted execution of arbitrary code

GLSA-200809-02 : dnsmasq: Denial of Service and DNS spoofing

GLSA-200809-03 : RealPlayer: Buffer overflow

GLSA-200809-04 : MySQL: Privilege bypass

GLSA-200809-05 : Courier Authentication Library: SQL injection vulnerability

GLSA-200809-06 : VLC: Multiple vulnerabilities

GLSA-200809-07 : libTIFF: User-assisted execution of arbitrary code

GLSA-200809-08 : Amarok: Insecure temporary file creation

GLSA-200809-09 : Postfix: Denial of Service

GLSA-200809-10 : Mantis: Multiple vulnerabilities

GLSA-200809-11 : HAVP: Denial of Service

GLSA-200809-12 : Newsbeuter: User-assisted execution of arbitrary code

GLSA-200809-13 : R: Insecure temporary file creation

GLSA-200809-14 : BitlBee: Security bypass

GLSA-200809-15 : GNU ed: User-assisted execution of arbitrary code

GLSA-200809-16 : Git: User-assisted execution of arbitrary code

GLSA-200809-17 : Wireshark: Multiple Denials of Service

GLSA-200809-18 : ClamAV: Multiple Denials of Service

GLSA-200810-01 : WordNet: Execution of arbitrary code

GLSA-200810-02 : Portage: Untrusted search path local root vulnerability

GLSA-200810-03 : libspf2: DNS response buffer overflow

GLSA-200811-01 : Opera: Multiple vulnerabilities

GLSA-200811-02 : Gallery: Multiple vulnerabilities

GLSA-200811-03 : FAAD2: User-assisted execution of arbitrary code

GLSA-200811-04 : Graphviz: User-assisted execution of arbitrary code

GLSA-200811-05 : PHP: Multiple vulnerabilities

GLSA-200812-01 : OptiPNG: User-assisted execution of arbitrary code

GLSA-200812-02 : enscript: User-assisted execution of arbitrary code

GLSA-200812-03 : IPsec-Tools: racoon Denial of Service

GLSA-200812-04 : lighttpd: Multiple vulnerabilities

GLSA-200812-05 : libsamplerate: User-assisted execution of arbitrary code

GLSA-200812-06 : libxml2: Multiple vulnerabilities

GLSA-200812-07 : Mantis: Multiple vulnerabilities

GLSA-200812-08 : Mgetty: Insecure temporary file usage

GLSA-200812-09 : OpenSC: Insufficient protection of smart card PIN

GLSA-200812-10 : Archive::Tar: Directory traversal vulnerability

GLSA-200812-11 : CUPS: Multiple vulnerabilities

GLSA-200812-12 : Honeyd: Insecure temporary file creation

GLSA-200812-13 : OpenOffice.org: Multiple vulnerabilities

GLSA-200812-14 : aview: Insecure temporary file usage

GLSA-200812-15 : POV-Ray: User-assisted execution of arbitrary code

GLSA-200812-16 : Dovecot: Multiple vulnerabilities

GLSA-200812-17 : Ruby: Multiple vulnerabilities

GLSA-200812-18 : JasPer: User-assisted execution of arbitrary code

GLSA-200812-19 : PowerDNS: Multiple vulnerabilities

GLSA-200812-20 : phpCollab: Multiple vulnerabilities

GLSA-200812-21 : ClamAV: Multiple vulnerabilities

GLSA-200812-22 : Ampache: Insecure temporary file usage

GLSA-200812-23 : Imlib2: User-assisted execution of arbitrary code

GLSA-200812-24 : VLC: Multiple vulnerabilities

GLSA-200901-01 : NDISwrapper: Arbitrary remote code execution

GLSA-200901-02 : JHead: Multiple vulnerabilities

GLSA-200901-03 : pdnsd: Denial of Service and cache poisoning

GLSA-200901-04 : D-Bus: Denial of Service

GLSA-200901-05 : Streamripper: Multiple vulnerabilities

GLSA-200901-06 : Tremulous: User-assisted execution of arbitrary code

GLSA-200901-07 : MPlayer: Multiple vulnerabilities

GLSA-200901-08 : Online-Bookmarks: Multiple vulnerabilities

GLSA-200901-09 : Adobe Reader: User-assisted execution of arbitrary code

GLSA-200901-10 : GnuTLS: Certificate validation error

GLSA-200901-11 : Avahi: Denial of Service

GLSA-200901-12 : noip-updater: Execution of arbitrary code

GLSA-200901-13 : Pidgin: Multiple vulnerabilities

GLSA-200901-14 : Scilab: Insecure temporary file usage

GLSA-200901-15 : Net-SNMP: Denial of Service

GLSA-200902-01 : sudo: Privilege escalation

GLSA-200902-02 : OpenSSL: Certificate validation error

GLSA-200902-03 : Valgrind: Untrusted search path

GLSA-200902-04 : xterm: User-assisted arbitrary commands execution

GLSA-200902-05 : KTorrent: Multiple vulnerabilitites

GLSA-200902-06 : GNU Emacs, XEmacs: Multiple vulnerabilities

GLSA-200903-01 : Vinagre: User-assisted execution of arbitrary code

GLSA-200903-02 : ZNC: Privilege escalation

GLSA-200903-03 : Audacity: User-assisted execution of arbitrary code

GLSA-200903-04 : DevIL: User-assisted execution of arbitrary code

GLSA-200903-05 : PDFjam: Multiple vulnerabilities

GLSA-200903-06 : nfs-utils: Access restriction bypass

GLSA-200903-07 : Samba: Data disclosure

GLSA-200903-08 : gEDA: Insecure temporary file creation

GLSA-200903-09 : OpenTTD: Execution of arbitrary code

GLSA-200903-10 : Irrlicht: User-assisted execution of arbitrary code

GLSA-200903-11 : PyCrypto: Execution of arbitrary code

GLSA-200903-12 : OptiPNG: User-assisted execution of arbitrary code

GLSA-200903-13 : MPFR: Denial of Service

GLSA-200903-14 : BIND: Incorrect signature verification

GLSA-200903-15 : git: Multiple vulnerabilties

GLSA-200903-16 : Epiphany: Untrusted search path

GLSA-200903-17 : Real VNC: User-assisted execution of arbitrary code

GLSA-200903-18 : Openswan: Insecure temporary file creation

GLSA-200903-19 : Xerces-C++: Denial of Service

GLSA-200903-20 : WebSVN: Multiple vulnerabilities

GLSA-200903-21 : cURL: Arbitrary file access

GLSA-200903-22 : Ganglia: Execution of arbitrary code

GLSA-200903-23 : Adobe Flash Player: Multiple vulnerabilities

GLSA-200903-24 : Shadow: Privilege escalation

GLSA-200903-25 : Courier Authentication Library: SQL Injection vulnerability

GLSA-200903-26 : TMSNC: Execution of arbitrary code

GLSA-200903-27 : ProFTPD: Multiple vulnerabilities

GLSA-200903-28 : libpng: Multiple vulnerabilities

GLSA-200903-29 : BlueZ: Arbitrary code execution

GLSA-200903-30 : Opera: Multiple vulnerabilities

GLSA-200903-31 : libcdaudio: User-assisted execution of arbitrary code

GLSA-200903-32 : phpMyAdmin: Multiple vulnerabilities

GLSA-200903-33 : FFmpeg: Multiple vulnerabilities

GLSA-200903-34 : Amarok: User-assisted execution of arbitrary code

GLSA-200903-35 : Muttprint: Insecure temporary file usage

GLSA-200903-36 : MLDonkey: Information disclosure

GLSA-200903-37 : Ghostscript: User-assisted execution of arbitrary code

GLSA-200903-38 : Squid: Multiple Denial of Service vulnerabilities

GLSA-200903-39 : pam\_krb5: Privilege escalation

GLSA-200903-40 : Analog: Denial of Service

GLSA-200903-41 : gedit: Untrusted search path

GLSA-200904-01 : Openfire: Multiple vulnerabilities

GLSA-200904-02 : GLib: Execution of arbitrary code

GLSA-200904-03 : Gnumeric: Untrusted search path

GLSA-200904-04 : WeeChat: Denial of Service

GLSA-200904-05 : ntp: Certificate validation error

GLSA-200904-06 : Eye of GNOME: Untrusted search path

GLSA-200904-07 : Xpdf: Untrusted search path

GLSA-200904-08 : OpenSSL: Denial of Service

GLSA-200904-09 : MIT Kerberos 5: Multiple vulnerabilities

GLSA-200904-10 : Avahi: Denial of Service

GLSA-200904-11 : Tor: Multiple vulnerabilities

GLSA-200904-12 : Wicd: Information disclosure

GLSA-200904-13 : Ventrilo: Denial of Service

GLSA-200904-14 : F-PROT Antivirus: Multiple Denial of Service vulnerabilities

GLSA-200904-15 : mpg123: User-assisted execution of arbitrary code

GLSA-200904-16 : libsndfile: User-assisted execution of arbitrary code

GLSA-200904-17 : Adobe Reader: User-assisted execution of arbitrary code

GLSA-200904-18 : udev: Multiple vulnerabilities

GLSA-200904-19 : LittleCMS: Multiple vulnerabilities

GLSA-200904-20 : CUPS: Multiple vulnerabilities

GLSA-200905-01 : Asterisk: Multiple vulnerabilities

GLSA-200905-02 : Cscope: User-assisted execution of arbitrary code

GLSA-200905-03 : IPSec Tools: Denial of Service

GLSA-200905-04 : GnuTLS: Multiple vulnerabilities

GLSA-200905-05 : FreeType: Multiple vulnerabilities

GLSA-200905-06 : acpid: Denial of Service

GLSA-200905-07 : Pidgin: Multiple vulnerabilities

GLSA-200905-08 : NTP: Remote execution of arbitrary code

GLSA-200905-09 : libsndfile: User-assisted execution of arbitrary code

GLSA-200906-01 : libpng: Information disclosure

GLSA-200906-02 : Ruby: Denial of Service

GLSA-200906-03 : phpMyAdmin: Multiple vulnerabilities

GLSA-200906-04 : Apache Tomcat JK Connector: Information disclosure

GLSA-200906-05 : Wireshark: Multiple vulnerabilities

GLSA-200907-01 : libwmf: User-assisted execution of arbitrary code

GLSA-200907-02 : ModSecurity: Denial of Service

GLSA-200907-03 : APR Utility Library: Multiple vulnerabilities

GLSA-200907-04 : Apache: Multiple vulnerabilities

GLSA-200907-05 : git: git-daemon Denial of Service

GLSA-200907-06 : Adobe Reader: User-assisted execution of arbitrary code

GLSA-200907-07 : ModPlug: User-assisted execution of arbitrary code

GLSA-200907-08 : Multiple Ralink wireless drivers: Execution of arbitrary code

GLSA-200907-09 : Cyrus-SASL: Execution of arbitrary code

GLSA-200907-10 : Syslog-ng: Chroot escape

GLSA-200907-11 : GStreamer plug-ins: User-assisted execution of arbitrary code

GLSA-200907-12 : ISC DHCP: dhcpclient Remote execution of arbitrary code

GLSA-200907-13 : PulseAudio: Local privilege escalation

GLSA-200907-14 : Rasterbar libtorrent: Directory traversal

GLSA-200907-15 : Nagios: Execution of arbitrary code

GLSA-200907-16 : Python: Integer overflows

GLSA-200908-01 : OpenSC: Multiple vulnerabilities

GLSA-200908-02 : BIND: Denial of Service

GLSA-200908-03 : libTIFF: User-assisted execution of arbitrary code

GLSA-200908-04 : Adobe products: Multiple vulnerabilities

GLSA-200908-05 : Subversion: Remote execution of arbitrary code

GLSA-200908-06 : CDF: User-assisted execution of arbitrary code

GLSA-200908-07 : Perl Compress::Raw modules: Denial of Service

GLSA-200908-08 : ISC DHCP: dhcpd Denial of Service

GLSA-200908-09 : DokuWiki: Local file inclusion

GLSA-200908-10 : Dillo: User-assisted execution of arbitrary code

GLSA-200909-01 : Linux-PAM: Privilege escalation

GLSA-200909-02 : libvorbis: User-assisted execution of arbitrary code

GLSA-200909-03 : Apache Portable Runtime, APR Utility Library: Execution of arbitrary code

GLSA-200909-04 : Clam AntiVirus: Multiple vulnerabilities

GLSA-200909-05 : Openswan: Denial of Service

GLSA-200909-06 : aMule: Parameter injection

GLSA-200909-07 : TkMan: Insecure temporary file usage

GLSA-200909-08 : C\* music player: Insecure temporary file usage

GLSA-200909-09 : Screenie: Insecure temporary file usage

GLSA-200909-10 : LMBench: Insecure temporary file usage

GLSA-200909-11 : GCC-XML: Insecure temporary file usage

GLSA-200909-12 : HTMLDOC: User-assisted execution of arbitrary code

GLSA-200909-13 : irssi: Execution of arbitrary code

GLSA-200909-14 : Horde: Multiple vulnerabilities

GLSA-200909-15 : Lynx: Arbitrary command execution

GLSA-200909-16 : Wireshark: Denial of Service

GLSA-200909-17 : ZNC: Directory traversal

GLSA-200909-18 : nginx: Remote execution of arbitrary code

GLSA-200909-19 : Dnsmasq: Multiple vulnerabilities

GLSA-200909-20 : cURL: Certificate validation error

GLSA-200910-01 : Wget: Certificate validation error

GLSA-200910-02 : Pidgin: Multiple vulnerabilities

GLSA-200910-03 : Adobe Reader: Multiple vulnerabilities

GLSA-200911-01 : Horde: Multiple vulnerabilities

GLSA-200911-02 : Sun JDK/JRE: Multiple vulnerabilities

GLSA-200911-03 : UW IMAP toolkit: Multiple vulnerabilities

GLSA-200911-04 : dstat: Untrusted search path

GLSA-200911-05 : Wireshark: Multiple vulnerabilities

GLSA-200911-06 : PEAR Net\_Traceroute: Command injection

GLSA-200912-01 : OpenSSL: Multiple vulnerabilities

GLSA-200912-02 : Ruby on Rails: Multiple vulnerabilities

GLSA-201001-01 : NTP: Denial of Service

GLSA-201001-02 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201001-03 : PHP: Multiple vulnerabilities

GLSA-201001-04 : VirtualBox: Multiple vulnerabilities

GLSA-201001-05 : net-snmp: Authorization bypass

GLSA-201001-06 : aria2: Multiple vulnerabilities

GLSA-201001-07 : Blender: Untrusted search path

GLSA-201001-08 : SquirrelMail: Multiple vulnerabilities

GLSA-201001-09 : Ruby: Terminal Control Character Injection

GLSA-201003-01 : sudo: Privilege escalation

GLSA-201006-01 : FreeType 1: User-assisted execution of arbitrary code

GLSA-201006-02 : CamlImages: User-assisted execution of arbitrary code

GLSA-201006-03 : ImageMagick: User-assisted execution of arbitrary code

GLSA-201006-04 : xine-lib: User-assisted execution of arbitrary code

GLSA-201006-05 : Wireshark: Multiple vulnerabilities

GLSA-201006-06 : Transmission: Multiple vulnerabilities

GLSA-201006-07 : SILC: Multiple vulnerabilities

GLSA-201006-08 : nano: Multiple vulnerabilities

GLSA-201006-09 : sudo: Privilege escalation

GLSA-201006-10 : multipath-tools: World-writeable socket

GLSA-201006-11 : BIND: Multiple vulnerabilities

GLSA-201006-12 : Fetchmail: Multiple vulnerabilities

GLSA-201006-13 : Smarty: Multiple vulnerabilities

GLSA-201006-14 : Newt: User-assisted execution of arbitrary code

GLSA-201006-15 : XEmacs: User-assisted execution of arbitrary code

GLSA-201006-16 : GD: User-assisted execution of arbitrary code

GLSA-201006-17 : lighttpd: Denial of Service

GLSA-201006-18 : Oracle JRE/JDK: Multiple vulnerabilities

GLSA-201006-19 : Bugzilla: Multiple vulnerabilities

GLSA-201006-20 : Asterisk: Multiple vulnerabilities

GLSA-201006-21 : UnrealIRCd: Multiple vulnerabilities

GLSA-201009-01 : wxGTK: User-assisted execution of arbitrary code

GLSA-201009-02 : Maildrop: privilege escalation

GLSA-201009-03 : sudo: Privilege Escalation

GLSA-201009-04 : SARG: User-assisted execution of arbitrary code

GLSA-201009-05 : Adobe Reader: Multiple vulnerabilities

GLSA-201009-06 : Clam AntiVirus: Multiple vulnerabilities

GLSA-201009-07 : libxml2: Denial of Service

GLSA-201009-08 : python-updater: Untrusted search path

GLSA-201009-09 : fence: Multiple symlink vulnerabilities

GLSA-201010-01 : Libpng: Multiple vulnerabilities

GLSA-201011-01 : GNU C library: Multiple vulnerabilities

GLSA-201012-01 : Chromium: Multiple vulnerabilities

GLSA-201101-01 : gif2png: User-assisted execution of arbitrary code

GLSA-201101-02 : Tor: Remote heap-based buffer overflow

GLSA-201101-03 : libvpx: User-assisted execution of arbitrary code

GLSA-201101-04 : aria2: Directory traversal

GLSA-201101-05 : OpenAFS: Arbitrary code execution

GLSA-201101-06 : IO::Socket::SSL: Certificate validation error

GLSA-201101-07 : Prewikka: password disclosure

GLSA-201101-08 : Adobe Reader: Multiple vulnerabilities

GLSA-201101-09 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201110-01 : OpenSSL: Multiple vulnerabilities

GLSA-201110-02 : Wireshark: Multiple vulnerabilities

GLSA-201110-03 : Bugzilla: Multiple vulnerabilities

GLSA-201110-04 : Dovecot: Multiple vulnerabilities

GLSA-201110-05 : GnuTLS: Multiple vulnerabilities

GLSA-201110-06 : PHP: Multiple vulnerabilities

GLSA-201110-07 : vsftpd: Denial of Service

GLSA-201110-08 : feh: Multiple vulnerabilities

GLSA-201110-09 : Conky: Privilege escalation

GLSA-201110-10 : Wget: User-assisted file creation or overwrite

GLSA-201110-11 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201110-12 : Unbound: Denial of Service

GLSA-201110-13 : Tor: Multiple vulnerabilities

GLSA-201110-14 : D-Bus: Multiple vulnerabilities

GLSA-201110-15 : GnuPG: User-assisted execution of arbitrary code

GLSA-201110-16 : Cyrus IMAP Server: Multiple vulnerabilities

GLSA-201110-17 : Avahi: Denial of Service

GLSA-201110-18 : rgmanager: Privilege escalation

GLSA-201110-19 : X.Org X Server: Multiple vulnerabilities

GLSA-201110-20 : Clam AntiVirus: Multiple vulnerabilities

GLSA-201110-21 : Asterisk: Multiple vulnerabilities

GLSA-201110-22 : PostgreSQL: Multiple vulnerabilities

GLSA-201110-23 : Apache mod\_authnz\_external: SQL injection

GLSA-201110-24 : Squid: Multiple vulnerabilities

GLSA-201110-25 : Pure-FTPd: Multiple vulnerabilities

GLSA-201110-26 : libxml2: Multiple vulnerabilities

GLSA-201111-01 : Chromium, V8: Multiple vulnerabilities

GLSA-201111-02 : Oracle JRE/JDK: Multiple vulnerabilities (BEAST)

GLSA-201111-03 : OpenTTD: Multiple vulnerabilities

GLSA-201111-04 : phpDocumentor: Function call injection

GLSA-201111-05 : Chromium, V8: Multiple vulnerabilities

GLSA-201111-06 : MaraDNS: Arbitrary code execution

GLSA-201111-07 : TinTin++: Multiple vulnerabilities

GLSA-201111-08 : radvd: Multiple vulnerabilities

GLSA-201111-09 : Perl Safe module: Arbitrary Perl code injection

GLSA-201111-10 : Evince: Multiple vulnerabilities

GLSA-201111-11 : GNU Tar: User-assisted execution of arbitrary code

GLSA-201111-12 : abcm2ps: Multiple vulnerabilities

GLSA-201201-01 : phpMyAdmin: Multiple vulnerabilities

GLSA-201201-02 : MySQL: Multiple vulnerabilities

GLSA-201201-03 : Chromium, V8: Multiple vulnerabilities

GLSA-201201-04 : Logsurfer: Arbitrary code execution

GLSA-201201-05 : mDNSResponder: Multiple vulnerabilities

GLSA-201201-06 : iSCSI Enterprise Target: Arbitrary code execution

GLSA-201201-07 : NX Server Free Edition, NX Node: Privilege escalation

GLSA-201201-08 : FontForge: User-assisted execution of arbitrary code

GLSA-201201-09 : FreeType: Multiple vulnerabilities

GLSA-201201-10 : JasPer: User-assisted execution of arbitrary code

GLSA-201201-11 : Firewall Builder: Privilege escalation

GLSA-201201-12 : Tor: Multiple vulnerabilities

GLSA-201201-13 : MIT Kerberos 5: Multiple vulnerabilities

GLSA-201201-14 : MIT Kerberos 5 Applications: Multiple vulnerabilities

GLSA-201201-15 : ktsuss: Privilege escalation

GLSA-201201-16 : X.Org X Server/X Keyboard Configuration Database: Screen lock bypass

GLSA-201201-17 : Chromium: Multiple vulnerabilities

GLSA-201201-18 : bip: Multiple vulnerabilities

GLSA-201201-19 : Adobe Reader: Multiple vulnerabilities

GLSA-201202-01 : Chromium: Multiple vulnerabilities

GLSA-201202-02 : Quagga: Multiple vulnerabilities

GLSA-201202-03 : MaraDNS: Denial of Service

GLSA-201202-04 : PowerDNS: Denial of Service

GLSA-201202-05 : Heimdal: Arbitrary code execution

GLSA-201202-06 : Asterisk: Denial of Service

GLSA-201202-07 : libvirt: Multiple vulnerabilities

GLSA-201202-08 : stunnel: Arbitrary code execution

GLSA-201202-09 : libxml2: User-assisted execution of arbitrary code

GLSA-201203-01 : spamdyke: Arbitrary code execution

GLSA-201203-02 : cURL: Multiple vulnerabilities (BEAST)

GLSA-201203-03 : Puppet: Multiple vulnerabilities

GLSA-201203-04 : libxml2: Denial of Service

GLSA-201203-05 : Rack: Denial of Service

GLSA-201203-06 : sudo: Privilege escalation

GLSA-201203-07 : foomatic-filters: User-assisted execution of arbitrary code

GLSA-201203-08 : libxslt: Denial of Service

GLSA-201203-09 : ImageMagick: User-assisted execution of arbitrary code

GLSA-201203-10 : libmikmod: User-assisted execution of arbitrary code

GLSA-201203-11 : usbmuxd: User-assisted execution of arbitrary code

GLSA-201203-12 : OpenSSL: Multiple vulnerabilities

GLSA-201203-13 : Openswan: Denial of Service

GLSA-201203-14 : Audacious Plugins: User-assisted execution of arbitrary code

GLSA-201203-15 : gif2png: Multiple vulnerabilities

GLSA-201203-16 : ModPlug: User-assisted execution of arbitrary code

GLSA-201203-17 : HPLIP: Multiple vulnerabilities

GLSA-201203-18 : Minitube: Insecure temporary file usage

GLSA-201203-19 : Chromium: Multiple vulnerabilities

GLSA-201203-20 : Logwatch: Arbitrary code execution

GLSA-201203-21 : Asterisk: Multiple vulnerabilities

GLSA-201203-22 : nginx: Multiple vulnerabilities

GLSA-201203-23 : libzip: Multiple vulnerabilities

GLSA-201203-24 : Chromium, V8: Multiple vulnerabilities

GLSA-201204-01 : VirtualBox: Multiple vulnerabilities

GLSA-201204-02 : InspIRCd: Arbitrary code execution

GLSA-201204-03 : Chromium: Multiple vulnerabilities

GLSA-201204-04 : FreeType: Multiple vulnerabilities

GLSA-201204-05 : SWFTools: User-assisted execution of arbitrary code

GLSA-201204-06 : PolicyKit: Multiple vulnerabilities

GLSA-201204-07 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201204-08 : Perl DBD-Pg Module: Arbitrary code execution

GLSA-201205-01 : Chromium: Multiple vulnerabilities

GLSA-201205-02 : ConnMan: Multiple vulnerabilities

GLSA-201205-03 : Chromium, V8: Multiple vulnerabilities

GLSA-201205-04 : Chromium, V8: Multiple vulnerabilities

GLSA-201206-01 : BIND: Multiple vulnerabilities

GLSA-201206-02 : QtGui: User-assisted execution of arbitrary code

GLSA-201206-03 : Opera: Multiple vulnerabilities

GLSA-201206-04 : ArgyllCMS: User-assisted execution of arbitrary code

GLSA-201206-05 : Asterisk: Multiple vulnerabilities

GLSA-201206-06 : OpenJPEG: User-assisted execution of arbitrary code

GLSA-201206-07 : nginx: User-assisted execution of arbitrary code

GLSA-201206-08 : Wicd: Multiple vulnerabilities

GLSA-201206-09 : MediaWiki: Multiple vulnerabilities

GLSA-201206-10 : ejabberd: Multiple Denial of Service vulnerabilities

GLSA-201206-11 : Pidgin: Multiple vulnerabilities

GLSA-201206-12 : tftp-hpa: Remote buffer overflow

GLSA-201206-13 : Mono: Multiple vulnerabilities

GLSA-201206-14 : Adobe Reader: Multiple vulnerabilities

GLSA-201206-15 : libpng: Multiple vulnerabilities

GLSA-201206-16 : TagLib: Multiple vulnerabilities

GLSA-201206-17 : virtualenv: Insecure temporary file usage

GLSA-201206-18 : GnuTLS: Multiple vulnerabilities

GLSA-201206-19 : NVIDIA Drivers: Privilege escalation

GLSA-201206-20 : gdk-pixbuf: Denial of Service

GLSA-201206-21 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201206-22 : Samba: Multiple vulnerabilities

GLSA-201206-23 : PyCrypto: Weak key generation

GLSA-201206-24 : Apache Tomcat: Multiple vulnerabilities

GLSA-201206-25 : Apache HTTP Server: Multiple vulnerabilities

GLSA-201206-26 : RPM: Multiple vulnerabilities

GLSA-201206-27 : mini\_httpd: Arbitrary code execution

GLSA-201206-28 : TeX Live: Multiple vulnerabilities

GLSA-201206-29 : mount-cifs: Multiple vulnerabilites

GLSA-201206-30 : sendmail: X.509 NULL spoofing vulnerability

GLSA-201206-31 : Linux-PAM: Multiple vulnerabilities

GLSA-201206-32 : Links: SSL verification vulnerability

GLSA-201206-33 : Postfix: Multiple vulnerabilities

GLSA-201206-34 : msmtp: X.509 NULL spoofing vulnerability

GLSA-201206-35 : nbd: Multiple vulnerabilities

GLSA-201206-36 : logrotate: Multiple vulnerabilities

GLSA-201207-01 : sudo: Privilege escalation

GLSA-201207-02 : libxml2: User-assisted execution of arbitrary code

GLSA-201207-03 : ChaSen: User-assisted execution of arbitrary code

GLSA-201207-04 : X.Org X Server: Privilege escalation

GLSA-201207-05 : pidgin-otr: Arbitrary code execution

GLSA-201207-06 : JRuby: Denial of Service

GLSA-201207-07 : Keepalived: Denial of Service

GLSA-201207-08 : Gnash: Multiple vulnerabilities

GLSA-201207-09 : mod\_fcgid: Multiple vulnerabilities

GLSA-201207-10 : CUPS: Multiple vulnerabilities

GLSA-201208-01 : socat: Arbitrary code execution

GLSA-201208-02 : Puppet: Multiple vulnerabilities

GLSA-201208-03 : Chromium: Multiple vulnerabilities

GLSA-201208-04 : Gajim: Multiple vulnerabilities

GLSA-201208-05 : Perl Config-IniFiles Module: Insecure temporary file usage

GLSA-201208-06 : libgdata: Man-in-the-Middle attack

GLSA-201209-01 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201209-02 : libTIFF: Multiple vulnerabilities

GLSA-201209-03 : PHP: Multiple vulnerabilities

GLSA-201209-04 : BIND: Multiple vulnerabilities

GLSA-201209-05 : LibreOffice: Multiple vulnerabilities

GLSA-201209-06 : Expat: Multiple vulnerabilities

GLSA-201209-07 : International Components for Unicode: User-assisted execution of arbitrary code

GLSA-201209-08 : SquidClamav: Denial of Service

GLSA-201209-09 : Atheme IRC Services: Denial of Service

GLSA-201209-10 : Calligra: User-assisted execution of arbitrary code

GLSA-201209-11 : Opera: Multiple vulnerabilities

GLSA-201209-12 : Libtasn1: Denial of Service

GLSA-201209-13 : libjpeg-turbo: User-assisted execution of arbitrary code

GLSA-201209-14 : file: Denial of Service

GLSA-201209-15 : Asterisk: Multiple vulnerabilities

GLSA-201209-16 : SQLAlchemy: SQL injection

GLSA-201209-17 : Pidgin: Arbitrary code execution

GLSA-201209-18 : Postfixadmin: Multiple vulnerabilities

GLSA-201209-19 : NUT: Arbitrary code execution

GLSA-201209-20 : mod\_rpaf: Denial of Service

GLSA-201209-21 : fastjar: Directory traversal

GLSA-201209-22 : libgssglue: Privilege escalation

GLSA-201209-23 : GIMP: Multiple vulnerabilities

GLSA-201209-24 : PostgreSQL: Multiple vulnerabilities

GLSA-201209-25 : VMware Player, Server, Workstation: Multiple vulnerabilities

GLSA-201210-01 : w3m: SSL spoofing vulnerability

GLSA-201210-02 : MoinMoin: Multiple vulnerabilities

GLSA-201210-03 : rdesktop: Directory Traversal

GLSA-201210-04 : qemu-kvm: Multiple vulnerabilities

GLSA-201210-05 : Bash: Multiple vulnerabilities

GLSA-201210-06 : Libav: Multiple vulnerabilities

GLSA-201210-07 : Chromium: Multiple vulnerabilities

GLSA-201211-01 : MantisBT: Multiple vulnerabilities

GLSA-201301-01 : Mozilla Products: Multiple vulnerabilities (BEAST)

GLSA-201301-02 : HAProxy: Arbitrary code execution

GLSA-201301-03 : Tor: Multiple vulnerabilities

GLSA-201301-04 : dhcpcd: Arbitrary code execution

GLSA-201301-05 : bzip2: User-assisted execution of arbitrary code

GLSA-201301-06 : ISC DHCP: Denial of Service

GLSA-201301-07 : DokuWiki: Multiple vulnerabilities

GLSA-201304-01 : NVIDIA Drivers: Privilege escalation

GLSA-201307-01 : HAProxy: Multiple vulnerabilities

GLSA-201308-01 : PuTTY: Multiple Vulnerabilities

GLSA-201308-02 : D-Bus: Denial of Service

GLSA-201308-03 : Adobe Reader: Multiple vulnerabilities

GLSA-201308-04 : Puppet: Multiple vulnerabilities

GLSA-201308-05 : Wireshark: Multiple vulnerabilities

GLSA-201308-06 : MySQL: Multiple vulnerabilities

GLSA-201309-01 : Cyrus-SASL: Denial of Service

GLSA-201309-02 : strongSwan: Multiple vulnerabilities

GLSA-201309-03 : Xlockmore: Denial of Service

GLSA-201309-04 : Snack: User-assisted execution of arbitrary code

GLSA-201309-05 : pip: Multiple vulnerabilities

GLSA-201309-06 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201309-07 : libotr: Arbitrary code execution

GLSA-201309-08 : FileZilla: Multiple vulnerabilities

GLSA-201309-09 : LibRaw, libkdcraw: Multiple vulnerabilities

GLSA-201309-10 : Adobe Reader: Arbitrary Code Execution

GLSA-201309-11 : Subversion: Multiple vulnerabilities

GLSA-201309-12 : Apache HTTP Server: Multiple vulnerabilities

GLSA-201309-13 : GNU ZRTP: Multiple vulnerabilities

GLSA-201309-14 : MoinMoin: Multiple vulnerabilities

GLSA-201309-15 : ProFTPD: Multiple vulnerabilities

GLSA-201309-16 : Chromium, V8: Multiple vulnerabilities

GLSA-201309-17 : Monkey HTTP Daemon: Multiple vulnerabilities

GLSA-201309-18 : libvirt: Multiple vulnerabilities

GLSA-201309-19 : TPP: User-assisted execution of arbitrary code

GLSA-201309-20 : Dropbear: Multiple vulnerabilities

GLSA-201309-21 : klibc: Command Injection

GLSA-201309-22 : Squid: Multiple vulnerabilities

GLSA-201309-23 : Mozilla Products: Multiple vulnerabilities

GLSA-201309-24 : Xen: Multiple vulnerabilities

GLSA-201310-01 : Perl Module-Signature module: Arbitrary code execution

GLSA-201310-02 : isync: Man-in-the-Middle attack

GLSA-201310-03 : Poppler: Multiple vulnerabilities

GLSA-201310-04 : nginx: Multiple vulnerabilities

GLSA-201310-05 : GEGL: User-assisted execution of arbitrary code

GLSA-201310-06 : Aircrack-ng: User-assisted execution of arbitrary code

GLSA-201310-07 : OpenJPEG: User-assisted execution of arbitrary code

GLSA-201310-08 : Quagga: Multiple vulnerabilities

GLSA-201310-09 : Setuptools: Man-in-the-Middle attack

GLSA-201310-10 : PolarSSL: Multiple vulnerabilities

GLSA-201310-11 : Perl Parallel-ForkManager Module: Insecure temporary file usage

GLSA-201310-12 : FFmpeg: Multiple vulnerabilities

GLSA-201310-13 : MPlayer: Multiple vulnerabilities

GLSA-201310-14 : Groff: Multiple Vulnerabilities

GLSA-201310-15 : GNU Automake: Multiple vulnerabilities

GLSA-201310-16 : TPTEST: Arbitrary code execution

GLSA-201310-17 : pmake: Insecure temporary file usage

GLSA-201310-18 : GnuTLS: Multiple vulnerabilities

GLSA-201310-19 : X2Go Server: Arbitrary code execution

GLSA-201310-20 : acpid2: Privilege escalation

GLSA-201310-21 : MediaWiki: Multiple vulnerabilities

GLSA-201311-01 : Mednafen: Arbitrary code execution

GLSA-201311-02 : phpMyAdmin: Multiple vulnerabilities

GLSA-201311-03 : Quassel: Multiple Vulnerabilities

GLSA-201311-04 : Vixie cron: Denial of Service

GLSA-201311-05 : GIMP: Multiple vulnerabilities

GLSA-201311-06 : libxml2: Multiple vulnerabilities

GLSA-201311-07 : Blender: Multiple vulnerabilities

GLSA-201311-08 : Netpbm: User-assisted arbitrary code execution

GLSA-201311-09 : FreeRADIUS: Multiple vulnerabilities

GLSA-201311-10 : GraphicsMagick: Multiple vulnerabilities

GLSA-201311-11 : CTorrent: User-assisted arbitrary code execution

GLSA-201311-12 : Open DC Hub: Arbitrary code execution

GLSA-201311-13 : OpenVPN: Multiple vulnerabilities

GLSA-201311-14 : QtCore, QtGui: Multiple vulnerabilities

GLSA-201311-15 : Zabbix: Multiple vulnerabilities

GLSA-201311-16 : fcron: Information disclosure

GLSA-201311-17 : Perl: Multiple vulnerabilities

GLSA-201311-18 : Unbound: Denial of Service

GLSA-201311-19 : rssh: Access restriction bypass

GLSA-201311-20 : Okular: Arbitrary code execution

GLSA-201311-21 : cpio: Arbitrary code execution

GLSA-201311-22 : Namazu: Multiple vulnerabilities

GLSA-201312-01 : GNU C Library: Multiple vulnerabilities

GLSA-201312-02 : BusyBox: Multiple vulnerabilities

GLSA-201312-03 : OpenSSL: Multiple Vulnerabilities

GLSA-201312-04 : libtheora: Arbitrary code execution

GLSA-201312-05 : SWI-Prolog : Multiple vulnerabilities

GLSA-201312-06 : Festival: Arbitrary code execution

GLSA-201312-07 : OpenEXR: Multiple Vulnerabilities

GLSA-201312-08 : WebP: User-assisted execution of arbitrary code

GLSA-201312-09 : cabextract: Multiple vulnerabilities

GLSA-201312-10 : libsmi: Arbitrary code execution

GLSA-201312-11 : Win32 Codecs: User-assisted execution of arbitrary code

GLSA-201312-12 : MIT Kerberos 5: Multiple vulnerabilities

GLSA-201312-13 : Wireshark: Multiple vulnerabilities

GLSA-201312-14 : libsndfile: Arbitrary code execution

GLSA-201312-15 : Tinyproxy: Denial of Service

GLSA-201312-16 : Xfig: Arbitrary code execution

GLSA-201401-01 : Libgdiplus: Arbitrary code execution

GLSA-201401-02 : Gajim: Information disclosure

GLSA-201401-03 : Nagstamon: Information disclosure

GLSA-201401-04 : Python: Multiple vulnerabilities

GLSA-201401-05 : ISC DHCP: Denial of Service

GLSA-201401-06 : Git: Privilege escalation

GLSA-201401-07 : libxslt: Denial of Service

GLSA-201401-08 : NTP: Traffic amplification

GLSA-201401-09 : Openswan: User-assisted execution of arbitrary code

GLSA-201401-10 : libexif, exif: Multiple vulnerabilities

GLSA-201401-11 : Perl, Locale Maketext Perl module: Multiple vulnerabilities

GLSA-201401-12 : GNUstep Base library: Multiple vulnerabilities

GLSA-201401-13 : VirtualBox: Multiple Vulnerabilities

GLSA-201401-14 : cURL: Multiple vulnerabilities

GLSA-201401-15 : Asterisk: Multiple vulnerabilities

GLSA-201401-16 : CCID: Arbitrary code execution

GLSA-201401-17 : PCSC-Lite: Arbitrary code execution

GLSA-201401-18 : OpenSC: Arbitrary code execution

GLSA-201401-19 : GMime: Arbitrary code execution

GLSA-201401-20 : Cacti: Multiple vulnerabilities

GLSA-201401-21 : Poppler: Multiple vulnerabilities

GLSA-201401-22 : Active Record: SQL injection

GLSA-201401-23 : sudo: Privilege escalation

GLSA-201401-24 : INN: Man-in-the-middle attack

GLSA-201401-25 : ldns: Arbitrary code execution

GLSA-201401-26 : Zabbix: Shell command injection

GLSA-201401-27 : GNU TeXmacs: Privilege escalation

GLSA-201401-28 : Tomboy: Privilege escalation

GLSA-201401-29 : VIPS: Privilege Escalation

GLSA-201401-30 : Oracle JRE/JDK: Multiple vulnerabilities (ROBOT)

GLSA-201401-31 : CEDET: Privilege escalation

GLSA-201401-32 : Exim: Multiple vulnerabilities

GLSA-201401-33 : Perl Digest-Base module: Arbitrary code execution

GLSA-201401-34 : BIND: Denial of Service

GLSA-201402-01 : GNU libmicrohttpd: Multiple vulnerabilities

GLSA-201402-02 : NVIDIA Drivers: Privilege Escalation

GLSA-201402-03 : Pixman: User-assisted execution of arbitrary code

GLSA-201402-04 : libwww-perl: Multiple vulnerabilities

GLSA-201402-05 : Banshee: Arbitrary code execution

GLSA-201402-06 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201402-07 : Freeciv: User-assisted execution of arbitrary code

GLSA-201402-08 : stunnel: Arbitrary code execution

GLSA-201402-09 : Apache mod\_fcgid: Arbitrary code execution

GLSA-201402-10 : PulseAudio: Insecure temporary file usage

GLSA-201402-11 : Links: Denial of Service

GLSA-201402-12 : PAM S/Key: Information disclosure

GLSA-201402-13 : DjVu: User-assisted execution of arbitrary code

GLSA-201402-14 : International Components for Unicode: Denial of Service

GLSA-201402-15 : Roundcube: Arbitrary code execution

GLSA-201402-16 : FreeType: Multiple vulnerabilities

GLSA-201402-17 : Xpdf: User-assisted execution of arbitrary code

GLSA-201402-18 : GNU Midnight Commander: User-assisted execution of arbitrary code

GLSA-201402-19 : libtar: Arbitraty code execution

GLSA-201402-20 : KVIrc: Multiple vulnerabilities

GLSA-201402-21 : libTIFF: Multiple vulnerabilities

GLSA-201402-22 : TCPTrack: Arbitrary code execution

GLSA-201402-23 : libXfont: Multiple vulnerabilities

GLSA-201402-24 : GnuPG, Libgcrypt: Multiple vulnerabilities

GLSA-201402-25 : OpenSSL: Denial of Service

GLSA-201402-26 : libssh: Arbitrary code execution

GLSA-201402-27 : pidgin-knotify: Arbitrary code execution

GLSA-201402-28 : Chrony: Multiple vulnerabilities

GLSA-201402-29 : ArgyllCMS: User-assisted execution of arbitrary code

GLSA-201403-01 : Chromium, V8: Multiple vulnerabilities

GLSA-201403-02 : LibYAML: Arbitrary code execution

GLSA-201403-03 : file: Denial of Service

GLSA-201403-04 : QtCore: Denial of Service

GLSA-201403-05 : GNU Emacs: Multiple vulnerabilities

GLSA-201403-06 : libupnp: Arbitrary code execution

GLSA-201403-07 : grep: User-assisted execution of arbitrary code

GLSA-201404-01 : CUPS: Arbitrary file read/write

GLSA-201404-02 : libproxy: User-assisted execution of arbitrary code

GLSA-201404-03 : OptiPNG: User-assisted execution of arbitrary code

GLSA-201404-04 : Crack: Arbitrary code execution

GLSA-201404-05 : OpenAFS: Multiple vulnerabilities

GLSA-201404-06 : Mesa: Multiple vulnerabilities

GLSA-201404-07 : OpenSSL: Information Disclosure

GLSA-201405-01 : udisks: Arbitrary code execution

GLSA-201405-02 : libSRTP: Denial of Service

GLSA-201405-03 : WeeChat: Multiple vulnerabilities

GLSA-201405-04 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201405-05 : Asterisk: Denial of Service

GLSA-201405-06 : OpenSSH: Multiple vulnerabilities

GLSA-201405-07 : X.Org X Server: Multiple vulnerabilities

GLSA-201405-08 : ClamAV: Multiple vulnerabilities

GLSA-201405-09 : ImageMagick: Multiple vulnerabilities

GLSA-201405-10 : Rack: Multiple vulnerabilities

GLSA-201405-11 : Bacula: Information disclosure

GLSA-201405-12 : Ettercap: Multiple vulnerabilities

GLSA-201405-13 : Pango: Multiple vulnerabilities

GLSA-201405-14 : Ruby OpenID: Denial of Service

GLSA-201405-15 : util-linux: Multiple vulnerabilities

GLSA-201405-16 : Mono: Denial of Service

GLSA-201405-17 : Munin: Multiple vulnerabilities

GLSA-201405-18 : OpenConnect: User-assisted execution of arbitrary code

GLSA-201405-19 : MCrypt: User-assisted execution of arbitrary code

GLSA-201405-20 : JBIG-KIT: Denial of Service

GLSA-201405-21 : Charybdis, ShadowIRCd: Denial of Service

GLSA-201405-22 : Pidgin: Multiple vulnerabilities

GLSA-201405-23 : lib3ds: User-assisted execution of arbitrary code

GLSA-201405-24 : Apache Portable Runtime, APR Utility Library: Denial of Service

GLSA-201405-25 : Symfony: Information disclosure

GLSA-201405-26 : X2Go Server: Privilege Escalation

GLSA-201405-27 : LibYAML: Arbitrary code execution

GLSA-201405-28 : xmonad-contrib: Arbitrary code execution

GLSA-201406-01 : D-Bus, GLib: Privilege escalation

GLSA-201406-02 : libarchive: Multiple vulnerabilities

GLSA-201406-03 : Fail2ban: Multiple vulnerabilities

GLSA-201406-04 : SystemTap: Denial of Service

GLSA-201406-05 : Mutt: Arbitrary code execution

GLSA-201406-06 : Mumble: Multiple vulnerabilities

GLSA-201406-07 : Echoping: Buffer Overflow Vulnerabilities

GLSA-201406-08 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201406-09 : GnuTLS: Multiple vulnerabilities

GLSA-201406-10 : lighttpd: Multiple vulnerabilities

GLSA-201406-11 : libXfont: Multiple vulnerabilities

GLSA-201406-12 : FreeRADIUS: Arbitrary code execution

GLSA-201406-13 : memcached: Multiple vulnerabilities

GLSA-201406-14 : Opera: Multiple vulnerabilities

GLSA-201406-15 : KDirStat: Arbitrary command execution

GLSA-201406-16 : cups-filters: Multiple vulnerabilities

GLSA-201406-17 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201406-18 : rxvt-unicode: User-assisted execution of arbitrary code

GLSA-201406-19 : Mozilla Network Security Service: Multiple vulnerabilities

GLSA-201406-20 : nginx: Arbitrary code execution

GLSA-201406-21 : cURL: Multiple vulnerabilities

GLSA-201406-22 : Network Audio System: Multiple vulnerabilities

GLSA-201406-23 : DenyHosts: Denial of Service

GLSA-201406-24 : Dnsmasq: Denial of Service

GLSA-201406-25 : Asterisk: Multiple vulnerabilities

GLSA-201406-26 : Django: Multiple vulnerabilities

GLSA-201406-27 : polkit, Spice-Gtk, systemd, HPLIP, libvirt: Privilege escalation

GLSA-201406-28 : Libav: Multiple vulnerabilities

GLSA-201406-29 : spice-gtk: Privilege escalation

GLSA-201406-30 : sudo: Privilege escalation

GLSA-201406-31 : Konqueror: Multiple vulnerabilities

GLSA-201406-32 : IcedTea JDK: Multiple vulnerabilities (BEAST) (ROBOT)

GLSA-201406-33 : Wireshark: Multiple vulnerabilities

GLSA-201406-34 : KDE Libraries: Multiple vulnerabilities

GLSA-201406-35 : Openfire: Multiple vulnerabilities

GLSA-201406-36 : OpenLDAP: Multiple vulnerabilities

GLSA-201407-01 : OpenTTD: Denial of Service

GLSA-201407-02 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201407-03 : Xen: Multiple Vunlerabilities

GLSA-201407-04 : GnuPG: Denial of Service

GLSA-201407-05 : OpenSSL: Multiple vulnerabilities

GLSA-201408-01 : Zend Framework: SQL injection

GLSA-201408-02 : FreeType: Arbitrary code execution

GLSA-201408-03 : LibSSH: Information disclosure

GLSA-201408-04 : Catfish: Multiple Vulnerabilities

GLSA-201408-05 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201408-06 : libpng: Multiple vulnerabilities

GLSA-201408-07 : ModPlug XMMS Plugin: Multiple vulnerabilities

GLSA-201408-08 : file: Denial of Service

GLSA-201408-09 : GNU Libtasn1: Multiple vulnerabilities

GLSA-201408-10 : Libgcrypt: Side-channel attack

GLSA-201408-11 : PHP: Multiple vulnerabilities

GLSA-201408-12 : Apache HTTP Server: Multiple vulnerabilities

GLSA-201408-13 : Jinja2: Multiple vulnerabilities

GLSA-201408-14 : stunnel: Information disclosure

GLSA-201408-15 : PostgreSQL: Multiple vulnerabilities

GLSA-201408-16 : Chromium: Multiple vulnerabilities

GLSA-201408-17 : QEMU: Multiple vulnerabilities

GLSA-201408-18 : NRPE: Multiple Vulnerabilities

GLSA-201408-19 : OpenOffice, LibreOffice: Multiple vulnerabilities

GLSA-201409-01 : Wireshark: Multiple vulnerabilities

GLSA-201409-02 : Net-SNMP: Denial of Service

GLSA-201409-03 : dhcpcd: Denial of service

GLSA-201409-04 : MySQL: Multiple vulnerabilities

GLSA-201409-05 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201409-06 : Chromium: Multiple vulnerabilities

GLSA-201409-07 : c-icap: Denial of Service

GLSA-201409-08 : libxml2: Denial of Service

GLSA-201409-09 : Bash: Code Injection (Shellshock)

GLSA-201409-10 : Bash: Code Injection (Updated fix for GLSA 201409-09)

GLSA-201410-01 : Bash: Multiple vulnerabilities (Shellshock)

GLSA-201410-02 : Perl, Perl Locale-Maketext module: Multiple vulnerabilities

GLSA-201411-01 : VLC: Multiple vulnerabilities

GLSA-201411-02 : MySQL, MariaDB: Multiple vulnerabilities

GLSA-201411-03 : TigerVNC: User-assisted execution of arbitrary code

GLSA-201411-04 : PHP: Multiple vulnerabilities

GLSA-201411-05 : GNU Wget: Arbitrary code execution

GLSA-201411-06 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201411-07 : Openswan: Denial of Service

GLSA-201411-08 : Aircrack-ng: User-assisted execution of arbitrary code

GLSA-201411-09 : Ansible: Privilege escalation

GLSA-201411-10 : Asterisk: Multiple Vulnerabilities (POODLE)

GLSA-201411-11 : Squid: Multiple vulnerabilities

GLSA-201412-01 : QEMU: Multiple Vulnerabilities

GLSA-201412-02 : nfs-utils: Information disclosure

GLSA-201412-03 : Dovecot: Denial of Service

GLSA-201412-04 : libvirt: Multiple vulnerabilities

GLSA-201412-05 : Clam AntiVirus: Denial of service

GLSA-201412-06 : libxml2: Denial of Service

GLSA-201412-07 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201412-08 : Multiple packages, Multiple vulnerabilities fixed in 2010

GLSA-201412-09 : Multiple packages, Multiple vulnerabilities fixed in 2011

GLSA-201412-10 : Multiple packages, Multiple vulnerabilities fixed in 2012

GLSA-201412-11 : AMD64 x86 emulation base libraries: Multiple vulnerabilities (Heartbleed)

GLSA-201412-12 : D-Bus: Multiple Vulnerabilities

GLSA-201412-13 : Chromium: Multiple vulnerabilities

GLSA-201412-14 : Xfig: User-assisted execution of arbitrary code

GLSA-201412-15 : MCollective: Privilege escalation

GLSA-201412-16 : CouchDB: Denial of Service

GLSA-201412-17 : GPL Ghostscript: Multiple vulnerabilities

GLSA-201412-18 : FreeRDP: User-assisted execution of arbitrary code

GLSA-201412-19 : PPP: Information disclosure

GLSA-201412-20 : GNUstep Base library: Denial of Service

GLSA-201412-21 : mod\_wsgi: Privilege escalation

GLSA-201412-22 : Django: Multiple vulnerabilities

GLSA-201412-23 : Nagios: Multiple vulnerabilities

GLSA-201412-24 : OpenJPEG: Multiple vulnerabilities

GLSA-201412-25 : QtGui: Denial of Service

GLSA-201412-26 : strongSwan: Multiple Vulnerabilities

GLSA-201412-27 : Ruby: Denial of Service

GLSA-201412-28 : Ruby on Rails: Multiple vulnerabilities

GLSA-201412-29 : Apache Tomcat: Multiple vulnerabilities

GLSA-201412-30 : Varnish: Multiple vulnerabilities

GLSA-201412-31 : ZNC: Denial of Service

GLSA-201412-32 : sendmail: Information disclosure

GLSA-201412-33 : PowerDNS Recursor: Multiple vulnerabilities

GLSA-201412-34 : NTP: Multiple vulnerabilities

GLSA-201412-35 : RSYSLOG: Denial of Service

GLSA-201412-36 : libvirt: Denial of Service

GLSA-201412-37 : QEMU: Multiple Vulnerabilities

GLSA-201412-38 : Icecast: Multiple Vulnerabilities

GLSA-201412-39 : OpenSSL: Multiple vulnerabilities

GLSA-201412-40 : FLAC: User-assisted execution of arbitrary code

GLSA-201412-41 : OpenVPN: Denial of Service

GLSA-201412-42 : Xen: Denial of Service

GLSA-201412-43 : MuPDF: User-assisted execution of arbitrary code

GLSA-201412-44 : policycoreutils: Privilege escalation

GLSA-201412-45 : Facter: Privilege escalation

GLSA-201412-46 : LittleCMS: Denial of Service

GLSA-201412-47 : TORQUE Resource Manager: Multiple vulnerabilities

GLSA-201412-48 : file: Denial of Service

GLSA-201412-49 : fish: Multiple vulnerabilities

GLSA-201412-50 : getmail: Information disclosure

GLSA-201412-51 : Asterisk: Multiple vulnerabilities

GLSA-201412-52 : Wireshark: Multiple vulnerabilities

GLSA-201412-53 : MIT Kerberos 5: User-assisted execution of arbitrary code

GLSA-201502-01 : mpg123: User-assisted execution of arbitrary code

GLSA-201502-02 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201502-03 : BIND: Multiple Vulnerabilities

GLSA-201502-04 : MediaWiki: Multiple vulnerabilities

GLSA-201502-05 : tcpdump: Multiple vulnerabilities

GLSA-201502-06 : nginx: Information disclosure

GLSA-201502-07 : libevent: User-assisted execution of arbitrary code

GLSA-201502-08 : Libav: Multiple vulnerabilities

GLSA-201502-09 : Antiword: User-assisted execution of arbitrary code

GLSA-201502-10 : libpng: User-assisted execution of arbitrary code

GLSA-201502-11 : GNU cpio: Multiple vulnerabilities

GLSA-201502-12 : Oracle JRE/JDK: Multiple vulnerabilities

GLSA-201502-13 : Chromium: Multiple vulnerabilities

GLSA-201502-14 : grep: Denial of Service

GLSA-201502-15 : Samba: Multiple vulnerabilities

GLSA-201503-01 : JasPer: Multiple Vulnerabilities

GLSA-201503-02 : D-Bus: Denial of Service

GLSA-201503-03 : PHP: Multiple vulnerabilities

GLSA-201503-04 : GNU C Library: Multiple vulnerabilities (GHOST)

GLSA-201503-05 : FreeType: Multiple vulnerabilities

GLSA-201503-06 : ICU: Multiple Vulnerabilities

GLSA-201503-07 : hivex: User-assisted execution of arbitrary code

GLSA-201503-08 : file: Denial of Service

GLSA-201503-09 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201503-10 : Python: Multiple vulnerabilities

GLSA-201503-11 : OpenSSL: Multiple vulnerabilities (FREAK)

GLSA-201503-12 : Chromium: Multiple vulnerabilities

GLSA-201503-13 : BusyBox: Multiple vulnerabilities

GLSA-201504-01 : Mozilla Products: Multiple vulnerabilities

GLSA-201504-02 : sudo: Information disclosure

GLSA-201504-03 : Apache: Multiple vulnerabilities

GLSA-201504-04 : Xen: Multiple vulnerabilities

GLSA-201504-05 : MySQL and MariaDB: Multiple vulnerabilities

GLSA-201504-06 : X.Org X Server: Multiple vulnerabilities

GLSA-201504-07 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201505-01 : Ettercap: Multiple vulnerabilities

GLSA-201505-02 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201505-03 : phpMyAdmin: Multiple vulnerabilities

GLSA-201506-01 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201506-02 : OpenSSL: Multiple vulnerabilities (Logjam)

GLSA-201506-03 : GnuTLS: Multiple vulnerabilities

GLSA-201506-04 : Chromium: Multiple vulnerabilities

GLSA-201507-01 : chrony: Multiple vulnerabilities

GLSA-201507-02 : Tor: Denial of Service

GLSA-201507-03 : Exiv2: Denial of Service

GLSA-201507-04 : International Components for Unicode: Multiple vulnerabilities

GLSA-201507-05 : SQLite: Multiple vulnerabilities

GLSA-201507-06 : UnRTF: Multiple vulnerabilities

GLSA-201507-07 : LibVNCServer: Multiple vulnerabilities

GLSA-201507-08 : libxml2: Denial of Service

GLSA-201507-09 : PyPAM: Arbitrary code execution

GLSA-201507-10 : t1utils: Arbitrary code execution

GLSA-201507-11 : Perl: Denial of Service

GLSA-201507-12 : libCapsiNetwork: Denial of Service

GLSA-201507-13 : Adobe Flash Player: Multiple vulnerabilities (Underminer)

GLSA-201507-14 : Oracle JRE/JDK: Multiple vulnerabilities (POODLE)

GLSA-201507-15 : OpenSSL: Alternate chains certificate forgery

GLSA-201507-16 : Portage: Man-in-the-middle attack

GLSA-201507-17 : SNMP: Denial of Service

GLSA-201507-18 : Chromium: Multiple vulnerabilities

GLSA-201507-19 : MySQL: Multiple vulnerabilities

GLSA-201507-20 : PostgreSQL: Multiple vulnerabilities

GLSA-201507-21 : libXfont: Multiple vulnerabilities

GLSA-201507-22 : e2fsprogs: Arbitrary code execution

GLSA-201508-01 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201508-02 : libgadu: Multiple vulnerabilities

GLSA-201508-03 : Icecast: Denial of Service

GLSA-201509-01 : NTP: Multiple vulnerablities

GLSA-201509-02 : cURL: Multiple vulnerabilities

GLSA-201509-03 : Cacti: Multiple vulnerabilities

GLSA-201509-04 : libtasn1: Multiple vulnerabilities

GLSA-201509-05 : NetworkManager: Denial of Service

GLSA-201509-06 : Git: Arbitrary command execution

GLSA-201509-07 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201510-01 : BIND: Denial of Service

GLSA-201510-02 : QEMU: Arbitrary code execution

GLSA-201510-03 : Wireshark: Multiple vulnerabilities

GLSA-201510-04 : tcpdump: Multiple vulnerabilities

GLSA-201510-05 : MediaWiki: Multiple vulnerabilities

GLSA-201510-06 : Django: Multiple vulnerabilities

GLSA-201510-07 : CUPS: Multiple vulnerabilities

GLSA-201510-08 : cups-filters: Multiple vulnerabilities

GLSA-201511-01 : MirBSD Korn Shell: Arbitrary code execution

GLSA-201511-02 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201512-01 : Dnsmasq: Denial of Service

GLSA-201512-02 : IPython: User-assisted execution of arbitrary code

GLSA-201512-03 : GRUB: Authentication bypass

GLSA-201512-04 : OpenSSH: Multiple vulnerabilities

GLSA-201512-05 : gdk-pixbuf: Multiple Vulnerabilities

GLSA-201512-06 : MPFR: User-assisted execution of arbitrary code

GLSA-201512-07 : GStreamer: User-assisted execution of arbitrary code

GLSA-201512-08 : ClamAV: Multiple vulnerabilities

GLSA-201512-09 : encfs: Multiple vulnerabilities

GLSA-201512-10 : Mozilla Products: Multiple vulnerabilities (Bar Mitzvah) (Logjam)

GLSA-201512-11 : Firebird: Buffer Overflow

GLSA-201512-12 : KDE Systemsettings: Privilege escalation

GLSA-201512-13 : InspIRCd: Multiple vulnerabilities

GLSA-201601-01 : OpenSSH: Multiple vulnerabilities

GLSA-201601-02 : WebKitGTK+: Multiple vulnerabilities

GLSA-201601-03 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201601-04 : OpenSMTPD: Multiple vulnerabilities

GLSA-201601-05 : OpenSSL: Multiple vulnerabilities

GLSA-201602-01 : QEMU: Multiple vulnerabilities (Venom)

GLSA-201602-02 : GNU C Library: Multiple vulnerabilities

GLSA-201602-03 : libwmf: Multiple vulnerabilities

GLSA-201603-01 : GIMP: Multiple vulnerabilities

GLSA-201603-02 : OSC: Shell command injection

GLSA-201603-03 : Roundcube: Multiple Vulnerabilities

GLSA-201603-04 : FUSE: incorrect filtering of environment variables leading to privilege escalation

GLSA-201603-05 : LibreOffice, OpenOffice: Multiple vulnerabilities

GLSA-201603-06 : FFmpeg: Multiple vulnerabilities

GLSA-201603-07 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201603-08 : VLC: Multiple vulnerabilities

GLSA-201603-09 : Chromium: Multiple vulnerabilities

GLSA-201603-10 : QtGui: Multiple vulnerabilities

GLSA-201603-11 : Oracle JRE/JDK: Multiple vulnerabilities (Logjam)

GLSA-201603-12 : FlightGear, SimGear: Multiple vulnerabilities

GLSA-201603-13 : Libreswan: Multiple Vulnerabilities

GLSA-201603-14 : IcedTea: Multiple vulnerabilities

GLSA-201603-15 : OpenSSL: Multiple vulnerabilities (DROWN)

GLSA-201604-01 : QEMU: Multiple vulnerabilities

GLSA-201604-02 : Xalan-Java: Arbitrary code execution

GLSA-201604-03 : Xen: Multiple vulnerabilities (Venom)

GLSA-201604-04 : libksba: Multiple vulnerabilities

GLSA-201604-05 : Wireshark: Multiple vulnerabilities

GLSA-201605-01 : Git: Multiple vulnerabilities

GLSA-201605-02 : Chromium: Multiple vulnerabilities

GLSA-201605-03 : libfpx: Denial of Service

GLSA-201605-04 : rsync: Multiple vulnerabilities

GLSA-201605-05 : Linux-PAM: Multiple vulnerabilities

GLSA-201605-06 : Mozilla Products: Multiple vulnerabilities (Logjam) (SLOTH)

GLSA-201606-01 : PuTTY: Multiple vulnerabilities

GLSA-201606-02 : Puppet Server and Agent: Multiple vulnerabilities

GLSA-201606-03 : libjpeg-turbo: Multiple vulnerabilities

GLSA-201606-04 : GnuPG: Multiple vulnerabilities

GLSA-201606-05 : spice: Multiple vulnerabilities

GLSA-201606-06 : nginx: Multiple vulnerabilities

GLSA-201606-07 : dhcpcd: Multiple vulnerabilities

GLSA-201606-08 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201606-09 : FFmpeg: Multiple vulnerabilities

GLSA-201606-10 : PHP: Multiple vulnerabilities

GLSA-201606-11 : claws-mail: Multiple Vulnerabilities (POODLE)

GLSA-201606-12 : libssh and libssh2: Multiple vulnerabilities

GLSA-201606-13 : sudo: Unauthorized privilege escalation in sudoedit

GLSA-201606-14 : ImageMagick: Multiple vulnerabilities

GLSA-201606-15 : FreeXL: Multiple vulnerabilities

GLSA-201606-16 : PLIB: Buffer overflow vulnerability

GLSA-201606-17 : hostapd and wpa\_supplicant: Multiple vulnerabilities

GLSA-201606-18 : IcedTea: Multiple vulnerabilities

GLSA-201606-19 : kwalletd: Information disclosure

GLSA-201607-01 : Squid: Multiple vulnerabilities

GLSA-201607-02 : libpcre: Multiple Vulnerabilities

GLSA-201607-03 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201607-04 : GD: Multiple vulnerabilities

GLSA-201607-05 : Cacti: Multiple vulnerabilities

GLSA-201607-06 : CUPS: Buffer overflow

GLSA-201607-07 : Chromium: Multiple vulnerabilities

GLSA-201607-08 : Dropbear: Privilege escalation

GLSA-201607-09 : Commons-BeanUtils: Arbitrary code execution

GLSA-201607-10 : Varnish: Multiple vulnerabilities

GLSA-201607-11 : Bugzilla: Multiple vulnerabilities

GLSA-201607-12 : Exim: Arbitrary code execution

GLSA-201607-13 : libbsd: Arbitrary code execution

GLSA-201607-14 : Ansible: Privilege escalation

GLSA-201607-15 : NTP: Multiple vulnerabilities

GLSA-201607-16 : arpwatch: Privilege escalation

GLSA-201607-17 : BeanShell: Arbitrary code execution

GLSA-201608-01 : OptiPNG: Multiple vulnerabilities

GLSA-201609-01 : QEMU: Multiple vulnerabilities

GLSA-201609-02 : Bundler: Insecure installation

GLSA-201610-01 : Groovy: Arbitrary code execution

GLSA-201610-02 : Apache: Multiple vulnerabilities

GLSA-201610-03 : Quagga: Arbitrary code execution

GLSA-201610-04 : libgcrypt: Multiple vulnerabilities

GLSA-201610-05 : Subversion, Serf: Multiple Vulnerabilities

GLSA-201610-06 : MySQL and MariaDB: Multiple vulnerabilities

GLSA-201610-07 : BIND: Multiple vulnerabilities

GLSA-201610-08 : Oracle JRE/JDK: Multiple vulnerabilities

GLSA-201610-09 : Chromium: Multiple vulnerabilities

GLSA-201610-10 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201610-11 : GNU Wget: Multiple vulnerabilities

GLSA-201611-01 : UnZip: Multiple vulnerabilities

GLSA-201611-02 : OpenVPN: Multiple vulnerabilities (SWEET32)

GLSA-201611-03 : LibreOffice, OpenOffice: Multiple vulnerabilities

GLSA-201611-04 : Oracle JRE/JDK: Multiple vulnerabilities

GLSA-201611-05 : tnftp: Arbitrary code execution

GLSA-201611-06 : xinetd: Privilege escalation

GLSA-201611-07 : polkit: Heap-corruption on duplicate IDs

GLSA-201611-08 : libpng: Multiple vulnerabilities

GLSA-201611-09 : Xen: Multiple vulnerabilities (Bunker Buster)

GLSA-201611-10 : libuv: Privilege escalation

GLSA-201611-11 : QEMU: Multiple vulnerabilities

GLSA-201611-12 : imlib2: Multiple vulnerabilities

GLSA-201611-13 : MongoDB: Denial of Service

GLSA-201611-14 : MIT Kerberos 5: Multiple vulnerabilities

GLSA-201611-15 : Poppler: Multiple vulnerabilities

GLSA-201611-16 : Chromium: Multiple vulnerabilities

GLSA-201611-17 : RPCBind: Denial of Service

GLSA-201611-18 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201611-19 : Tar: Extract pathname bypass

GLSA-201611-20 : TestDisk: User-assisted execution of arbitrary code

GLSA-201611-21 : ImageMagick: Multiple vulnerabilities (ImageTragick)

GLSA-201611-22 : PHP: Multiple vulnerabilities (httpoxy)

GLSA-201612-01 : GnuPG: RNG output is predictable

GLSA-201612-02 : DavFS2: Local privilege escalation

GLSA-201612-03 : libsndfile: Multiple vulnerabilities

GLSA-201612-04 : BusyBox: Multiple vulnerabilities

GLSA-201612-05 : Pygments: Arbitrary code execution

GLSA-201612-06 : nghttp2: Heap-use-after-free

GLSA-201612-07 : dpkg: Arbitrary code execution

GLSA-201612-08 : LinuxCIFS utils: Buffer overflow

GLSA-201612-09 : GD: Multiple vulnerabilities

GLSA-201612-10 : libvirt: Directory traversal

GLSA-201612-11 : Chromium: Multiple vulnerabilities

GLSA-201612-12 : Patch: Denial of Service

GLSA-201612-13 : nghttp2: Denial of Service

GLSA-201612-14 : util-linux: Arbitrary code execution

GLSA-201612-15 : ARJ: Multiple vulnerabilities

GLSA-201612-16 : OpenSSL: Multiple vulnerabilities

GLSA-201612-17 : PECL HTTP: Remote execution of arbitrary code

GLSA-201612-18 : OpenSSH: Multiple vulnerabilities

GLSA-201612-19 : Mercurial: Multiple vulnerabilities

GLSA-201612-20 : jq: Buffer overflow

GLSA-201612-21 : SQLite: Multiple vulnerabilities

GLSA-201612-22 : Coreutils: Arbitrary code execution

GLSA-201612-23 : socat: Multiple vulnerabilities

GLSA-201612-24 : Binutils: Multiple vulnerabilities

GLSA-201612-25 : CrackLib: Buffer overflow

GLSA-201612-26 : OpenJPEG: Multiple vulnerabilities

GLSA-201612-27 : VirtualBox: Multiple vulnerabilities (Venom)

GLSA-201612-28 : Docker: Privilege escalation

GLSA-201612-29 : libmms: Remote execution of arbitrary code

GLSA-201612-30 : SoX: User-assisted execution of arbitrary code

GLSA-201612-31 : exFAT: Multiple vulnerabilities

GLSA-201612-32 : elfutils: Heap-based buffer overflow

GLSA-201612-33 : GPL Ghostscript: User-assisted execution of arbitrary code

GLSA-201612-34 : systemd: Multiple vulnerabilities

GLSA-201612-35 : XStream: Remote execution of arbitrary code

GLSA-201612-36 : TigerVNC: Integer overflow

GLSA-201612-37 : Pixman: Buffer overflow

GLSA-201612-38 : Botan: Multiple vulnerabilities

GLSA-201612-39 : Bash: Arbitrary code execution

GLSA-201612-40 : SQUASHFS: Multiple vulnerabilities

GLSA-201612-41 : WebKitGTK+: Multiple vulnerabilities

GLSA-201612-42 : Zabbix: Multiple vulnerabilities

GLSA-201612-43 : Node.js: Multiple vulnerabilities

GLSA-201612-44 : Roundcube: Arbitrary code execution

GLSA-201612-45 : Tor: Multiple vulnerabilities

GLSA-201612-46 : Xerces-C++: Multiple vulnerabilities

GLSA-201612-47 : Samba: Multiple vulnerabilities (Badlock)

GLSA-201612-48 : Firejail: Multiple vulnerabilities

GLSA-201612-49 : mod\_wsgi: Privilege escalation

GLSA-201612-50 : Openfire: Multiple vulnerabilities

GLSA-201612-51 : Icinga: Privilege escalation

GLSA-201612-52 : Pillow: Multiple vulnerabilities

GLSA-201612-53 : CyaSSL: Multiple vulnerabilities

GLSA-201612-54 : Chicken: Multiple vulnerabilities

GLSA-201612-55 : libjpeg-turbo: User-assisted execution of arbitrary code

GLSA-201612-56 : Xen: Multiple vulnerabilities

GLSA-201701-01 : MariaDB and MySQL: Multiple vulnerabilities

GLSA-201701-02 : Bash: Multiple vulnerabilities

GLSA-201701-03 : libarchive: Multiple vulnerabilities

GLSA-201701-04 : Mutt: Heap-based buffer overflow

GLSA-201701-05 : BusyBox: Denial of Service

GLSA-201701-06 : e2fsprogs: Heap-based buffer overflow

GLSA-201701-07 : Open vSwitch: Remote execution of arbitrary code

GLSA-201701-08 : w3m: Multiple vulnerabilities

GLSA-201701-09 : Xdg-Utils: Command injection

GLSA-201701-10 : libotr, Pidgin OTR: Remote execution of arbitrary code

GLSA-201701-11 : musl: Integer overflow

GLSA-201701-12 : memcached: Multiple vulnerabilities

GLSA-201701-13 : HDF5: Multiple vulnerabilities

GLSA-201701-14 : LZO: Multiple vulnerabilities

GLSA-201701-15 : Mozilla Firefox, Thunderbird: Multiple vulnerabilities (SWEET32)

GLSA-201701-16 : libTIFF: Multiple vulnerabilities

GLSA-201701-17 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201701-18 : Python: Multiple vulnerabilities

GLSA-201701-19 : NTFS-3G: Privilege escalation

GLSA-201701-20 : D-Bus: Format string vulnerability

GLSA-201701-21 : Expat: Multiple vulnerabilities

GLSA-201701-22 : NGINX: Privilege escalation

GLSA-201701-23 : Botan: Multiple vulnerabilities

GLSA-201701-24 : PgBouncer: Multiple vulnerabilities

GLSA-201701-25 : phpBB: Multiple vulnerabilities

GLSA-201701-26 : BIND: Denial of Service

GLSA-201701-27 : 7-Zip: Multiple vulnerabilities

GLSA-201701-28 : c-ares: Heap-based buffer overflow

GLSA-201701-29 : Vim, gVim: Remote execution of arbitrary code

GLSA-201701-30 : vzctl: Security bypass

GLSA-201701-31 : flex: Potential insecure code generation

GLSA-201701-32 : phpMyAdmin: Multiple vulnerabilities

GLSA-201701-33 : PostgreSQL: Multiple vulnerabilities

GLSA-201701-34 : runC: Privilege escalation

GLSA-201701-35 : Mozilla SeaMonkey: Multiple vulnerabilities

GLSA-201701-36 : Apache: Multiple vulnerabilities (httpoxy)

GLSA-201701-37 : libxml2: Multiple vulnerabilities

GLSA-201701-38 : Pidgin: Multiple vulnerabilities

GLSA-201701-39 : VLC: Buffer overflow

GLSA-201701-40 : xdelta: User-assisted execution of arbitrary code

GLSA-201701-41 : MiniUPnPc: Buffer overflow

GLSA-201701-42 : file: Multiple vulnerabilities

GLSA-201701-43 : IcedTea: Multiple vulnerabilities

GLSA-201701-44 : CVS: Heap-based overflow

GLSA-201701-45 : irssi: Multiple vulnerabilities

GLSA-201701-46 : Mozilla Network Security Service (NSS): Multiple vulnerabilities (Logjam) (SLOTH)

GLSA-201701-47 : cURL: Multiple vulnerabilities

GLSA-201701-48 : Quagga: Multiple vulnerabilities

GLSA-201701-49 : QEMU: Multiple vulnerabilities

GLSA-201701-50 : PPP: Buffer overflow

GLSA-201701-51 : DBD::mysql: Multiple vulnerabilities

GLSA-201701-52 : libupnp: Multiple vulnerabilities

GLSA-201701-53 : Lua: Buffer overflow

GLSA-201701-54 : DCRaw: Buffer overflow

GLSA-201701-55 : DirectFB: Multiple vulnerabilities

GLSA-201701-56 : zlib: Multiple vulnerabilities

GLSA-201701-57 : T1Lib: : Multiple vulnerabilities

GLSA-201701-58 : ICU: Multiple vulnerabilities

GLSA-201701-59 : ADOdb: Multiple vulnerabilities

GLSA-201701-60 : LibRaw: Multiple vulnerabilities

GLSA-201701-61 : WebP: Multiple vulnerabilities

GLSA-201701-62 : Firejail: Multiple vulnerabilities

GLSA-201701-63 : Graphite: Multiple vulnerabilities

GLSA-201701-64 : X.Org X Server: Multiple vulnerabilities

GLSA-201701-65 : Oracle JRE/JDK: Multiple vulnerabilities

GLSA-201701-66 : Chromium: Multiple vulnerabilities

GLSA-201701-67 : a2ps: Arbitrary code execution

GLSA-201701-68 : FreeImage: Multiple vulnerabilities

GLSA-201701-69 : Ark: Unintended execution of scripts and executable files

GLSA-201701-70 : Firewalld: Improper authentication methods

GLSA-201701-71 : FFmpeg: Multiple vulnerabilities

GLSA-201701-72 : libXpm: Remote execution of arbitrary code

GLSA-201701-73 : SQUASHFS: Multiple vulnerabilities

GLSA-201701-74 : libpng: Remote execution of arbitrary code

GLSA-201701-75 : Perl: Multiple vulnerabilities

GLSA-201701-76 : HarfBuzz: Multiple vulnerabilities

GLSA-201701-77 : Ansible: Remote execution of arbitrary code

GLSA-201702-01 : PCSC-Lite: Multiple vulnerabilities

GLSA-201702-02 : RTMPDump: Multiple vulnerabilities

GLSA-201702-03 : Firejail: Privilege escalation

GLSA-201702-04 : GnuTLS: Multiple vulnerabilities

GLSA-201702-05 : Lsyncd: Remote execution of arbitrary code

GLSA-201702-06 : Graphviz: Multiple vulnerabilities

GLSA-201702-07 : OpenSSL: Multiple vulnerabilities

GLSA-201702-08 : VirtualBox: Multiple vulnerabilities

GLSA-201702-09 : ImageMagick: Multiple vulnerabilities

GLSA-201702-10 : NTFS-3G: Privilege escalation

GLSA-201702-11 : GNU C Library: Multiple vulnerabilities

GLSA-201702-12 : MuPDF: Multiple vulnerabilities

GLSA-201702-13 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-201702-14 : PyCrypto: Remote execution of arbitrary code

GLSA-201702-15 : OCaml: Buffer overflow and information disclosure

GLSA-201702-16 : Redis: Multiple vulnerabilities

GLSA-201702-17 : MySQL: Multiple vulnerabilities

GLSA-201702-18 : MariaDB: Multiple vulnerabilities

GLSA-201702-19 : TigerVNC: Buffer overflow

GLSA-201702-20 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201702-21 : Opus: User-assisted execution of arbitrary code

GLSA-201702-22 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201702-23 : Dropbear: Multiple vulnerabilities

GLSA-201702-24 : LibVNCServer/LibVNCClient: Multiple vulnerabilities

GLSA-201702-25 : libass: Multiple vulnerabilities

GLSA-201702-26 : Nagios: Multiple vulnerabilities

GLSA-201702-27 : Xen: Multiple vulnerabilities

GLSA-201702-28 : QEMU: Multiple vulnerabilities

GLSA-201702-29 : PHP: Multiple vulnerabilities

GLSA-201702-30 : tcpdump: Multiple vulnerabilities

GLSA-201702-31 : GPL Ghostscript: Multiple vulnerabilities

GLSA-201702-32 : Ruby Archive::Tar::Minitar: Directory traversal

GLSA-201703-01 : OpenOffice: User-assisted execution of arbitrary code

GLSA-201703-02 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201703-03 : PuTTY: Buffer overflow

GLSA-201703-04 : cURL: Certificate validation error

GLSA-201703-05 : GNU Libtasn1: Denial of Service

GLSA-201703-06 : Deluge: Remote execution of arbitrary code

GLSA-201703-07 : Xen: Privilege Escalation

GLSA-201704-01 : QEMU: Multiple vulnerabilities

GLSA-201704-02 : Chromium: Multiple vulnerabilities

GLSA-201704-03 : X.Org: Multiple vulnerabilities

GLSA-201704-04 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201705-01 : libevent: Multiple vulnerabilities

GLSA-201705-02 : Chromium: Multiple vulnerabilities

GLSA-201705-03 : Oracle JDK/JRE: Multiple vulnerabilities

GLSA-201705-04 : Mozilla Network Security Service (NSS): Multiple vulnerabilities

GLSA-201705-05 : FFmpeg: Multiple vulnerabilities

GLSA-201705-06 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201705-07 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-201705-08 : libav: Multiple vulnerabilities

GLSA-201705-09 : Apache Tomcat: Multiple vulnerabilities

GLSA-201705-10 : GStreamer plug-ins: User-assisted execution of arbitrary code

GLSA-201705-11 : Xen: Multiple vulnerabilities

GLSA-201705-12 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201705-13 : Teeworlds: Remote execution of arbitrary code on client

GLSA-201705-14 : Smb4K: Arbitrary command execution as root

GLSA-201705-15 : sudo: Privilege escalation

GLSA-201706-01 : MUNGE: Privilege escalation

GLSA-201706-02 : Shadow: Multiple vulnerabilities

GLSA-201706-03 : QEMU: Multiple vulnerabilities

GLSA-201706-04 : Git: Security bypass

GLSA-201706-05 : D-Bus: Multiple vulnerabilities

GLSA-201706-06 : ImageWorsener: Multiple vulnerabilities

GLSA-201706-07 : Libtirpc and RPCBind: Denial of Service

GLSA-201706-08 : MuPDF: Multiple vulnerabilities

GLSA-201706-09 : FileZilla: Buffer overflow

GLSA-201706-10 : Pidgin: Arbitrary code execution

GLSA-201706-11 : PCRE library: Denial of Service

GLSA-201706-12 : Wireshark: Multiple vulnerabilities

GLSA-201706-13 : minicom: Remote execution of arbitrary code

GLSA-201706-14 : FreeType: Multiple vulnerabilities

GLSA-201706-15 : WebKitGTK+: Multiple vulnerabilities

GLSA-201706-16 : GNU Wget: Header injection

GLSA-201706-17 : Kodi: Multiple vulnerabilities

GLSA-201706-18 : mbed TLS: Multiple vulnerabilities (SLOTH)

GLSA-201706-19 : GNU C Library: Multiple vulnerabilities (Stack Clash)

GLSA-201706-20 : Chromium: Multiple vulnerabilities

GLSA-201706-21 : nettle: Information disclosure

GLSA-201706-22 : libksba: Denial of Service and information disclosure

GLSA-201706-23 : Urban Terror: Multiple vulnerabilities

GLSA-201706-24 : jbig2dec: Multiple vulnerabilities

GLSA-201706-25 : Graphite: User-assisted execution of arbitrary code

GLSA-201706-26 : Vim, gVim: Remote execution of arbitrary code

GLSA-201706-27 : FreeRADIUS: Security bypass

GLSA-201706-28 : LibreOffice: Multiple vulnerabilities

GLSA-201706-29 : KAuth and KDELibs: Privilege escalation

GLSA-201707-01 : IcedTea: Multiple vulnerabilities

GLSA-201707-02 : Game Music Emu: Multiple vulnerabilities

GLSA-201707-03 : phpMyAdmin: Security bypass

GLSA-201707-04 : libsndfile: Multiple vulnerabilities

GLSA-201707-05 : OpenSLP: Multiple vulnerabilities

GLSA-201707-06 : virglrenderer: Multiple vulnerabilities

GLSA-201707-07 : JasPer: Multiple vulnerabilities

GLSA-201707-08 : feh: Arbitrary remote code execution

GLSA-201707-09 : GNOME applet for NetworkManager: Arbitrary file read/write

GLSA-201707-10 : VLC: Multiple vulnerabilities

GLSA-201707-11 : RoundCube: Security bypass

GLSA-201707-12 : MAN DB: Privilege escalation

GLSA-201707-13 : libcroco: Multiple vulnerabilities

GLSA-201707-14 : Gajim: Information disclosure

GLSA-201707-15 : Adobe Flash Player: Multiple Vulnerabilities

GLSA-201708-01 : BIND: Multiple vulnerabilities

GLSA-201708-02 : TNEF: Multiple vulnerabilities

GLSA-201708-04 : Ked Password Manager: Information leak

GLSA-201708-05 : RAR and UnRAR: User-assisted execution of arbitrary code

GLSA-201708-06 : GPL Ghostscript: Multiple vulnerabilities

GLSA-201708-07 : evilvte: User-assisted execution of arbitrary code

GLSA-201708-08 : bzip2: Denial of Service

GLSA-201708-09 : AutoTrace: Multiple vulnerabilities

GLSA-201708-10 : jbig2dec: User-assisted execution of arbitrary code

GLSA-201709-01 : MCollective: Remote Code Execution

GLSA-201709-02 : Binutils: Multiple vulnerabilities

GLSA-201709-03 : WebKitGTK+: Multiple vulnerabilities

GLSA-201709-04 : mod\_gnutls: Certificate validation error

GLSA-201709-05 : chkrootkit: Local privilege escalation

GLSA-201709-06 : Supervisor: command injection vulnerability

GLSA-201709-07 : Kpathsea: User-assisted execution of arbitrary code

GLSA-201709-08 : GDK-PixBuf: Multiple vulnerabilities

GLSA-201709-09 : Subversion: Arbitrary code execution

GLSA-201709-10 : Git: Command injection

GLSA-201709-11 : GIMPS: Root privilege escalation

GLSA-201709-12 : Perl: Race condition vulnerability

GLSA-201709-13 : SquirrelMail: Remote Code Execution

GLSA-201709-14 : cURL: Multiple vulnerabilities

GLSA-201709-15 : Chromium: Multiple vulnerabilities

GLSA-201709-16 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201709-17 : CVS: Command injection

GLSA-201709-18 : Mercurial: Multiple vulnerabilities

GLSA-201709-19 : Exim: Local privilege escalation (Stack Clash)

GLSA-201709-20 : Postfix: Privilege escalation

GLSA-201709-21 : PHP: Multiple vulnerabilities

GLSA-201709-22 : Oracle JDK/JRE, IcedTea: Multiple vulnerabilities

GLSA-201709-23 : Tcpdump: Multiple vulnerabilities

GLSA-201709-24 : RAR, UnRAR: Multiple vulnerabilities

GLSA-201709-25 : Chromium: Multiple vulnerabilities

GLSA-201709-26 : libsoup: Arbitrary remote code execution

GLSA-201709-27 : libTIFF: Multiple vulnerabilities

GLSA-201710-01 : RubyGems: Multiple vulnerabilities

GLSA-201710-02 : file: Stack-based buffer overflow

GLSA-201710-03 : ICU: Multiple vulnerabilities

GLSA-201710-04 : sudo: Privilege escalation

GLSA-201710-05 : Munin: Arbitrary file write

GLSA-201710-06 : PostgreSQL: Multiple vulnerabilities

GLSA-201710-07 : OCaml: Privilege escalation

GLSA-201710-08 : Pacemaker: Multiple vulnerabilities

GLSA-201710-09 : PCRE2: Multiple vulnerabilities

GLSA-201710-10 : elfutils: Multiple vulnerabilities

GLSA-201710-11 : GNU Libtasn1: Multiple vulnerabilities

GLSA-201710-12 : Puppet Agent: Multiple vulnerabilities

GLSA-201710-13 : Graphite: Multiple vulnerabilities

GLSA-201710-14 : WebKitGTK+: Multiple Vulnerabilities

GLSA-201710-15 : GnuTLS: Denial of Service

GLSA-201710-16 : Shadow: Buffer overflow

GLSA-201710-17 : Xen: Multiple vulnerabilities

GLSA-201710-18 : Ruby: Multiple vulnerabilities

GLSA-201710-19 : libarchive: Multiple vulnerabilities

GLSA-201710-20 : Nagios: Multiple vulnerabilities

GLSA-201710-21 : Kodi: Arbitrary code execution

GLSA-201710-22 : Adobe Flash Player: Remote execution of arbitrary code

GLSA-201710-23 : Go: Multiple vulnerabilities

GLSA-201710-24 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201710-25 : PCRE: Multiple vulnerabilities

GLSA-201710-26 : OpenJPEG: Multiple vulnerabilities

GLSA-201710-27 : Dnsmasq: Multiple vulnerabilities

GLSA-201710-28 : Jython: Arbitrary code execution

GLSA-201710-29 : Asterisk: Multiple vulnerabilities

GLSA-201710-30 : X.Org Server: Multiple vulnerabilities

GLSA-201710-31 : Oracle JDK/JRE: Multiple vulnerabilities

GLSA-201710-32 : Apache: Multiple vulnerabilities (Optionsbleed)

GLSA-201711-01 : libxml2: Multiple vulnerabilities

GLSA-201711-02 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201711-03 : hostapd and wpa\_supplicant: Key Reinstallation (KRACK) attacks (KRACK)

GLSA-201711-04 : MariaDB, MySQL: Root privilege escalation

GLSA-201711-05 : X.Org Server: Multiple vulnerabilities

GLSA-201711-06 : GNU Wget: Multiple vulnerabilities

GLSA-201711-07 : ImageMagick: Multiple vulnerabilities

GLSA-201711-08 : LibXfont, LibXfont2: Multiple vulnerabilities

GLSA-201711-09 : LXC: Remote security bypass

GLSA-201711-10 : Cacti: Multiple vulnerabilities

GLSA-201711-11 : VDE: Privilege escalation

GLSA-201711-12 : eGroupWare: Remote code execution

GLSA-201711-13 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201711-14 : IcedTea: Multiple vulnerabilities

GLSA-201711-15 : PHPUnit: Remote code execution

GLSA-201711-16 : CouchDB: Multiple vulnerabilities

GLSA-201712-01 : WebKitGTK+: Multiple vulnerabilities

GLSA-201712-02 : OpenCV: Multiple vulnerabilities

GLSA-201712-03 : OpenSSL: Multiple vulnerabilities

GLSA-201712-04 : cURL: Multiple vulnerabilities

GLSA-201801-01 : Binutils: Multiple vulnerabilities

GLSA-201801-02 : OptiPNG: Multiple vulnerabilities

GLSA-201801-03 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201801-04 : LibXcursor: User-assisted execution of arbitrary code

GLSA-201801-05 : OpenSSH: Permission issue

GLSA-201801-06 : Back In Time: Command injection

GLSA-201801-07 : GNU Emacs: Command injection

GLSA-201801-08 : MiniUPnPc: Arbitrary code execution

GLSA-201801-09 : WebkitGTK+: Multiple vulnerabilities

GLSA-201801-10 : LibXfont, LibXfont2: Arbitrary file access

GLSA-201801-11 : PySAML2: Security bypass

GLSA-201801-12 : icoutils: Multiple vulnerabilities

GLSA-201801-13 : TigerVNC: Multiple vulnerabilities

GLSA-201801-14 : Xen: Multiple vulnerabilities

GLSA-201801-15 : PolarSSL: Multiple vulnerabilities (SLOTH)

GLSA-201801-16 : rsync: Multiple vulnerabilities

GLSA-201801-17 : Poppler: Multiple vulnerabilities

GLSA-201801-18 : Newsbeuter: User-assisted execution of arbitrary code

GLSA-201801-19 : ClamAV: Multiple vulnerabilities

GLSA-201801-20 : Fossil: User-assisted execution of arbitrary code

GLSA-201802-01 : VirtualBox: Multiple vulnerabilities

GLSA-201802-02 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201802-03 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201802-04 : MySQL: Multiple vulnerabilities

GLSA-201802-05 : Ruby: Command injection

GLSA-201802-06 : LibreOffice: Information disclosure

GLSA-201803-01 : Exim: Multiple vulnerabilities

GLSA-201803-02 : util-linux: User-assisted execution of arbitrary code

GLSA-201803-03 : Go: User-assisted execution of arbitrary code

GLSA-201803-04 : Newsbeuter: User-assisted execution of arbitrary code

GLSA-201803-05 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201803-06 : Oracle JDK/JRE: Multiple vulnerabilities

GLSA-201803-07 : JabberD 2.x: Multiple vulnerabilities

GLSA-201803-08 : Adobe Flash Player: Multiple vulnerabilities (Underminer)

GLSA-201803-09 : KDE Plasma Workspaces: Multiple vulnerabilities

GLSA-201803-10 : collectd: Multiple vulnerabilities

GLSA-201803-11 : WebKitGTK+: Multiple Vulnerabilities

GLSA-201803-12 : BusyBox: Multiple vulnerabilities

GLSA-201803-13 : PLIB: User-assisted execution of arbitrary code

GLSA-201803-14 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-201804-01 : libxslt: Multiple vulnerabilities

GLSA-201804-02 : glibc: Multiple vulnerabilities

GLSA-201804-03 : Poppler: Multiple vulnerabilities

GLSA-201804-04 : cURL: Multiple vulnerabilities

GLSA-201804-05 : ISC DHCP: Multiple vulnerabilities

GLSA-201804-06 : mailx: Multiple vulnerabilities

GLSA-201804-07 : libvirt: Multiple vulnerabilities

GLSA-201804-08 : QEMU: Multiple vulnerabilities (Spectre)

GLSA-201804-09 : SPICE VDAgent: Arbitrary command injection

GLSA-201804-10 : Zend Framework: Multiple vulnerabilities

GLSA-201804-11 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201804-12 : Go: Arbitrary code execution

GLSA-201804-13 : ncurses: Multiple vulnerabilities

GLSA-201804-14 : GDK-PixBuf: Remote code execution

GLSA-201804-15 : Evince: Command injection

GLSA-201804-16 : ClamAV: Multiple vulnerabilities

GLSA-201804-17 : Quagga: Multiple vulnerabilities

GLSA-201804-18 : tenshi: Privilege escalation

GLSA-201804-19 : mbed TLS: Multiple vulnerabilites

GLSA-201804-20 : unADF: Remote code execution

GLSA-201804-21 : librelp: Remote code execution

GLSA-201804-22 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201805-01 : hesiod: Root privilege escalation

GLSA-201805-02 : Python: Buffer overflow

GLSA-201805-03 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201805-04 : rsync: Arbitrary command execution

GLSA-201805-05 : mpv: Remote code execution

GLSA-201805-06 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201805-07 : Samba: Multiple vulnerabilities (SambaCry)

GLSA-201805-08 : VirtualBox: Multiple vulnerabilities

GLSA-201805-09 : Shadow: security bypass

GLSA-201805-10 : Zsh: Multiple vulnerabilities

GLSA-201805-11 : Rootkit Hunter: User-assisted execution of arbitrary code

GLSA-201805-12 : NTP: Multiple vulnerabilities

GLSA-201805-13 : Git: Multiple vulnerabilities

GLSA-201805-14 : procps: Multiple vulnerabilities

GLSA-201805-15 : beep: Local privilege escalation

GLSA-201806-01 : GNU Wget: Cookie injection

GLSA-201806-02 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201806-03 : BURP: Multiple vulnerabilities

GLSA-201806-04 : Quassel: Multiple vulnerabilities

GLSA-201806-05 : cURL: Multiple vulnerabilities

GLSA-201806-06 : Chromium, Google Chrome: User-assisted execution of arbitrary code

GLSA-201806-07 : Transmission: Remote code execution

GLSA-201806-08 : file: Denial of service

GLSA-201806-09 : PNP4Nagios: Root privilege escalation

GLSA-201807-01 : tqdm: Arbitrary code execution

GLSA-201807-02 : Passenger: Multiple Vulnerabilities

GLSA-201807-03 : ZNC:Multiple Vulnerabilities

GLSA-201807-04 : cURL: Heap-based buffer overflow

GLSA-201808-01 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201808-02 : LinuX Containers user space utilities: Arbitrary file read

GLSA-201808-03 : NetworkManager VPNC plugin: Privilege escalation

GLSA-201808-04 : WebkitGTK+: Multiple vulnerabilities

GLSA-201810-01 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201810-02 : SoX: Multiple vulnerabilities

GLSA-201810-03 : OpenSSH: User enumeration vulnerability

GLSA-201810-04 : ImageMagick: Security hardening

GLSA-201810-05 : xkbcommon: Multiple vulnerabilities

GLSA-201810-06 : Xen: Multiple vulnerabilities (Foreshadow) (Meltdown) (Spectre)

GLSA-201810-07 : Mutt, NeoMutt: Multiple vulnerabilities

GLSA-201810-08 : PostgreSQL: Multiple vulnerabilities

GLSA-201810-09 : X.Org X Server: Privilege escalation

GLSA-201810-10 : systemd: Multiple vulnerabilities

GLSA-201811-01 : X.Org X11 library: Multiple vulnerabilities

GLSA-201811-02 : Python: Buffer overflow

GLSA-201811-03 : OpenSSL: Denial of Service

GLSA-201811-04 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201811-05 : PHProjekt: Multiple vulnerabilities

GLSA-201811-06 : libde265: Multiple vulnerabilities

GLSA-201811-07 : Pango: Denial of Service

GLSA-201811-08 : Okular: Directory traversal

GLSA-201811-09 : Icecast: Arbitrary code execution

GLSA-201811-10 : Chromium: Multiple vulnerabilities

GLSA-201811-11 : Asterisk: Multiple vulnerabilities

GLSA-201811-12 : GPL Ghostscript: Multiple vulnerabilities

GLSA-201811-13 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-201811-14 : Exiv2: Multiple vulnerabilities

GLSA-201811-15 : MuPDF: Multiple vulnerabilities

GLSA-201811-16 : strongSwan: Multiple vulnerabilities

GLSA-201811-17 : Binutils: Multiple vulnerabilities

GLSA-201811-18 : Tablib: Arbitrary command execution

GLSA-201811-19 : Libav: Multiple vulnerabilities

GLSA-201811-20 : spice-gtk: Remote code execution

GLSA-201811-21 : OpenSSL: Multiple vulnerabilities

GLSA-201811-22 : RPM: Multiple vulnerabilities

GLSA-201811-23 : libsndfile: Multiple vulnerabilities

GLSA-201811-24 : PostgreSQL: SQL injection

GLSA-201812-01 : PHP: Multiple vulnerabilities

GLSA-201812-02 : ConnMan: Multiple vulnerabilities

GLSA-201812-03 : Nagios: Privilege escalation

GLSA-201812-04 : WebkitGTK+: Multiple vulnerabilities

GLSA-201812-05 : EDE: Privilege escalation

GLSA-201812-06 : CouchDB: Multiple vulnerabilities

GLSA-201812-07 : SpamAssassin: Multiple vulnerabilities

GLSA-201812-08 : Scala: Privilege escalation

GLSA-201812-09 : Go: Multiple vulnerabilities

GLSA-201812-10 : GKSu: Arbitrary command execution

GLSA-201812-11 : Rust: Multiple vulnerabilities

GLSA-201903-01 : Keepalived: Multiple vulnerabilities

GLSA-201903-02 : Zsh: User-assisted execution of arbitrary code

GLSA-201903-03 : cURL: Multiple vulnerabilities

GLSA-201903-04 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201903-05 : Tar: Denial of Service

GLSA-201903-06 : rdesktop: Multiple vulnerabilities

GLSA-201903-07 : systemd: Multiple vulnerabilities

GLSA-201903-08 : GNU Wget: Password and metadata leak

GLSA-201903-09 : GNU C Library: Arbitrary descriptor allocation

GLSA-201903-10 : OpenSSL: Multiple vulnerabilities

GLSA-201903-11 : XRootD: Remote code execution

GLSA-201903-12 : WebkitGTK+: Multiple vulnerabilities

GLSA-201903-13 : BIND: Multiple vulnerabilities

GLSA-201903-14 : Oracle JDK/JRE: Multiple vulnerabilities

GLSA-201903-15 : NTP: Multiple vulnerabilities

GLSA-201903-16 : OpenSSH: Multiple vulnerabilities

GLSA-201903-17 : SDL2\_Image: Multiple vulnerabilities

GLSA-201903-18 : GD: Multiple vulnerabilities

GLSA-201903-19 : NASM: Multiple vulnerabilities

GLSA-201903-20 : cabextract, libmspack: Multiple vulnerabilities

GLSA-201903-21 : Apache: Multiple vulnerabilities

GLSA-201903-22 : ZeroMQ: Code execution

GLSA-201903-23 : Chromium: Multiple vulnerabilities

GLSA-201904-01 : Cairo: Denial of Service

GLSA-201904-02 : Libical: Multiple vulnerabilities

GLSA-201904-03 : Unbound: Multiple vulnerabilities

GLSA-201904-04 : Poppler: Multiple vulnerabilities

GLSA-201904-05 : BURP: Root privilege escalation

GLSA-201904-06 : GlusterFS: Multiple Vulnerabilities

GLSA-201904-07 : Mozilla Thunderbird and Firefox: Multiple vulnerabilities

GLSA-201904-08 : Subversion: Denial of Service

GLSA-201904-09 : Xen: Multiple Vulnerabilities

GLSA-201904-10 : Mailman: Multiple vulnerabilities

GLSA-201904-11 : Portage: Man-in-the-middle

GLSA-201904-12 : ClamAV: Multiple vulnerabilities

GLSA-201904-13 : Git: Multiple vulnerabilities

GLSA-201904-14 : GnuTLS: Multiple vulnerabilities

GLSA-201904-15 : libTIFF: Denial of Service

GLSA-201904-16 : phpMyAdmin: Multiple vulnerabilities

GLSA-201904-17 : Patch: Multiple vulnerabilities

GLSA-201904-18 : libseccomp: Privilege escalation

GLSA-201904-19 : Dovecot: Multiple vulnerabilities

GLSA-201904-20 : Apache: Privilege escalation

GLSA-201904-21 : SQLite: Remote code execution

GLSA-201904-22 : OpenDKIM: Root privilege escalation

GLSA-201904-23 : GLib: Multiple vulnerabilities

GLSA-201904-24 : Ming: Multiple vulnerabilities

GLSA-201904-25 : QEMU: Multiple vulnerabilities

GLSA-201906-01 : Exim: Remote command execution

GLSA-201908-01 : Binutils: Multiple vulnerabilities

GLSA-201908-02 : libpng: Multiple vulnerabilities

GLSA-201908-03 : JasPer: Multiple vulnerabilities

GLSA-201908-04 : Redis: Multiple vulnerabilities

GLSA-201908-05 : LibVNCServer: Multiple vulnerabilities

GLSA-201908-06 : glibc: Multiple vulnerabilities

GLSA-201908-07 : KDE KConfig: User-assisted execution of arbitrary code

GLSA-201908-08 : CUPS: Multiple vulnerabilities

GLSA-201908-09 : SQLite: Multiple vulnerabilities

GLSA-201908-10 : Oracle JDK/JRE: Multiple vulnerabilities

GLSA-201908-11 : libarchive: Multiple vulnerabilities

GLSA-201908-12 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201908-13 : LibreOffice: Multiple vulnerabilities

GLSA-201908-14 : polkit: Multiple vulnerabilities

GLSA-201908-15 : ZNC: Privilege escalation

GLSA-201908-16 : ProFTPD: Remote code execution

GLSA-201908-17 : ZeroMQ: Arbitrary code execution

GLSA-201908-18 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201908-19 : GNU Wget: Arbitrary code execution

GLSA-201908-20 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-201908-21 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201908-22 : Patch: Multiple vulnerabilities

GLSA-201908-23 : VLC: Multiple vulnerabilities

GLSA-201908-24 : MariaDB, MySQL: Multiple vulnerabilities

GLSA-201908-25 : hostapd and wpa\_supplicant: Denial of Service

GLSA-201908-26 : libofx: Multiple vulnerabilities

GLSA-201908-27 : Nautilus: Security bypass

GLSA-201908-28 : GNOME desktop library: Security bypass

GLSA-201908-29 : Dovecot: Multiple vulnerabilities

GLSA-201909-01 : Perl: Multiple vulnerabilities

GLSA-201909-02 : VLC: Multiple vulnerabilities

GLSA-201909-03 : Pango: Buffer overflow

GLSA-201909-04 : Apache: Multiple vulnerabilities (Internal Data Buffering)

GLSA-201909-05 : WebkitGTK+: Multiple vulnerabilities

GLSA-201909-06 : Exim: Multiple vulnerabilities

GLSA-201909-07 : Simple DirectMedia Layer: Multiple vulnerabilities

GLSA-201909-08 : D-Bus: Authentication bypass

GLSA-201910-01 : PHP: Arbitrary code execution

GLSA-201911-01 : OpenSSH: Integer overflow

GLSA-201911-02 : pump: User-assisted execution of arbitrary code

GLSA-201911-03 : Oniguruma: Multiple vulnerabilities

GLSA-201911-04 : OpenSSL: Multiple vulnerabilities

GLSA-201911-05 : Adobe Flash Player: Multiple vulnerabilities

GLSA-201911-06 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-201911-07 : Mozilla Firefox: Multiple vulnerabilities

GLSA-201911-08 : Expat: Multiple vulnerabilities

GLSA-202003-01 : Groovy: Arbitrary code execution

GLSA-202003-02 : Mozilla Firefox: Multiple vulnerabilities

GLSA-202003-03 : PostgreSQL: Multiple vulnerabilities

GLSA-202003-04 : Vim, gVim: Remote execution of arbitrary code

GLSA-202003-05 : e2fsprogs: Arbitrary code execution

GLSA-202003-06 : Ruby: Multiple vulnerabilities

GLSA-202003-07 : RabbitMQ C client: Arbitrary code execution

GLSA-202003-08 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-202003-09 : OpenID library for Ruby: Server-Side Request Forgery

GLSA-202003-10 : Mozilla Thunderbird: Multiple vulnerabilities

GLSA-202003-11 : SVG Salamander: Server-Side Request Forgery

GLSA-202003-12 : sudo: Multiple vulnerabilities

GLSA-202003-13 : musl: x87 floating-point stack adjustment imbalance

GLSA-202003-14 : atftp: Multiple vulnerabilities

GLSA-202003-15 : ICU: Integer overflow

GLSA-202003-16 : SQLite: Multiple vulnerabilities

GLSA-202003-17 : nfdump: Multiple vulnerabilities

GLSA-202003-18 : libvirt: Multiple vulnerabilities

GLSA-202003-19 : PPP: Buffer overflow

GLSA-202003-20 : systemd: Heap use-after-free

GLSA-202003-21 : runC: Multiple vulnerabilities

GLSA-202003-22 : WebkitGTK+: Multiple vulnerabilities

GLSA-202003-23 : libjpeg-turbo: User-assisted execution of arbitrary code

GLSA-202003-24 : file: Heap-based buffer overflow

GLSA-202003-25 : libTIFF: Multiple vulnerabilities

GLSA-202003-26 : Python: Multiple vulnerabilities

GLSA-202003-27 : libssh: Arbitrary command execution

GLSA-202003-28 : libarchive: Multiple vulnerabilities

GLSA-202003-29 : cURL: Multiple vulnerabilities

GLSA-202003-30 : Git: Multiple vulnerabilities

GLSA-202003-31 : gdb: Buffer overflow

GLSA-202003-32 : Libgcrypt: Side-channel attack

GLSA-202003-33 : GStreamer Base Plugins: Heap-based buffer overflow

GLSA-202003-34 : Squid: Multiple vulnerabilities

GLSA-202003-35 : ProFTPd: Multiple vulnerabilities

GLSA-202003-36 : libvorbis: Multiple vulnerabilities

GLSA-202003-37 : Mozilla Network Security Service: Multiple vulnerabilities

GLSA-202003-38 : PECL Imagick: Arbitrary code execution

GLSA-202003-39 : phpMyAdmin: SQL injection

GLSA-202003-40 : Cacti: Multiple vulnerabilities

GLSA-202003-41 : GNU FriBidi: Heap-based buffer overflow

GLSA-202003-42 : libgit2: Multiple vulnerabilities

GLSA-202003-43 : Apache Tomcat: Multiple vulnerabilities

GLSA-202003-44 : Binary diff: Heap-based buffer overflow

GLSA-202003-45 : PyYAML: Arbitrary code execution

GLSA-202003-46 : ClamAV: Multiple vulnerabilities

GLSA-202003-47 : Exim: Heap-based buffer overflow

GLSA-202003-48 : Node.js: Multiple vulnerabilities

GLSA-202003-49 : BlueZ: Security bypass

GLSA-202003-50 : Tor: Multiple vulnerabilities

GLSA-202003-51 : WeeChat: Multiple vulnerabilities

GLSA-202003-52 : Samba: Multiple vulnerabilities

GLSA-202003-53 : Chromium, Google Chrome: Multiple vulnerabilities

GLSA-202003-54 : Pure-FTPd: Multiple vulnerabilities

GLSA-202003-55 : Zsh: Privilege escalation

GLSA-202003-56 : Xen: Multiple vulnerabilities (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

GLSA-202003-57 : PHP: Multiple vulnerabilities

GLSA-202003-58 : UnZip: User-assisted execution of arbitrary code

GLSA-202003-59 : libvpx: User-assisted execution of arbitrary code

GLSA-202003-60 : QtCore: Multiple vulnerabilities

GLSA-202003-61 : Adobe Flash Player: Remote execution of arbitrary code

GLSA-202003-62 : GNU Screen: Buffer overflow

GLSA-202003-63 : GNU IDN Library 2: Multiple vulnerabilities

GLSA-202003-64 : libxls: Multiple vulnerabilities

GLSA-202003-65 : FFmpeg: Multiple vulnerabilities

GLSA-202003-66 : QEMU: Multiple vulnerabilities

GLSA-202004-01 : HAProxy: Remote execution of arbitrary code

GLSA-202004-02 : VirtualBox: Multiple vulnerabilities

GLSA-202004-03 : GPL Ghostscript: Multiple vulnerabilities

GLSA-202004-04 : Qt WebEngine: Arbitrary code execution

GLSA-202004-05 : ledger: Multiple vulnerabilities

GLSA-202004-06 : GnuTLS: DTLS protocol regression

GLSA-202004-07 : Mozilla Firefox: Multiple vulnerabilities

GLSA-202004-08 : libssh: Denial of Service

GLSA-202004-09 : Chromium, Google Chrome: Multiple vulnerabilities

Unmaintainted Gentoo Packages

# General

ACAP Service STARTTLS Command Support

Active Inbound Connection From Host Listed in Custom Netstat IP Threat List

Active Inbound Connection From Host Listed in Known Bot Database

Active Outbound Connection From Host Listed in Custom Netstat IP Threat List

Active Outbound Connection to Host Listed in Known Bot Database

Additional DNS Hostnames

Alcatel OmniSwitch Default Credentials (telnet)

Alcatel-Lucent OmniSwitch Series Agranat-Embweb Management Server Session Cookie Handling Remote Overflow

Amazon Web Services EC2 Instance Metadata Enumeration (Unix)

Anonymous Key Exchanges Supported (PCI DSS)

Anonymous SFTP Enabled

APT1-Related SSL Certificate Detected

Backported Security Patch Detection (FTP)

Backported Security Patch Detection (SMTP)

Backported Security Patch Detection (SSH)

Backported Security Patch Detection (WWW)

BIOS Info (SSH)

Blacklisted SSL Certificate

Certificate Revocation List Expiry

Command Builder Initialization

Common Platform Enumeration (CPE)

Cyrus IMAPd NNTP AUTHINFO USER Command Parsing Authentication Bypass

Deprecated SSLv2 Connection Attempts

Device Hostname

Device Type

DNS Server Listed in Known Bot Database

Dropbox Software Detection (listener)

Dropbox Software Detection (uncredentialed check)

EMC AutoStart ftAgent Version Detection

Enumerate IPv4 Interfaces via SSH

Enumerate IPv6 Interfaces via SSH

Enumerate MAC Addresses via SSH

Errors in nessusd.dump

Ethernet MAC Addresses

External Scanner Service Identification

F5 TLS Session Ticket Implementation Remote Memory Disclosure (Ticketbleed) (uncredentialed check)

Firebird SQL Server for Linux 2.5.x < 2.5.7 / 3.0.x < 3.0.2 UDF Libraries RCE

Generic Overflow Detection

Google Cloud Platform Compute Engine Instance Metadata Enumeration (Unix)

Host Fully Qualified Domain Name (FQDN) Resolution

Host is Listed in Known Bot Database

HP B-series SAN Network Advisor < 12.1.1 Remote Code Execution (Linux)

HP B-series SAN Network Advisor Installed (Linux)

HP LaserJet PJL Interface Directory Traversal (HPSBPI02575)

HP OfficeJet Pro and PageWide Pro PJL Interface Directory Traversal RCE

HPE LoadRunner Virtual Table Server import\_csv Remote File Deletion DoS

Hyper-V Virtual Machine Detection

IBM AIX TCP Large Send Denial of Service Vulnerability

IBM Global Security Kit 7 < 7.0.4.47 / 8 < 8.0.50.13 DoS

IBM Global Security Kit 7 < 7.0.4.50 / 8.0.14.x < 8.0.14.43 / 8.0.50.x < 8.0.50.20 Multiple Vulnerabilities (Linux)

IBM GSKit 7.x < 7.0.4.45 / 8.0.14.x < 8.0.14.27 TLS Side-Channel Timing Information Disclosure

IBM GSKit Installed (Linux)

IBM Netezza Analytics Open Source James Clark Expat Multiple Vulnerabilities (swg22012645)

IBM Spectrum Protect 7.1.x < 7.1.9.300 / 8.1.x < 8.1.8 Multiple Vulnerabilities

IBM Spectrum Protect Client 7.1.x < 7.1.8.4 / 8.1.x < 8.1.6.1 Denial of Service Vulnerability (CVE-2018-1786)

IBM Spectrum Protect Server 7.1.1.0 - 7.1.7.0 SELECT Command RCE

IBM Spectrum Protect Server 7.1.x < 7.1.9.100 / 8.1.x < 8.1.6 Information Disclosure Vulnerability

IBM Spectrum Protect Server and Storage Agent RCE

IBM Tivoli Directory Server TLS NULL Cipher (uncredentialed check)

IBM Tivoli Storage Manager FastBack 5.5.x / 6.1.x < 6.1.12.2 Multiple Vulnerabilities

IBM Tivoli Storage Manager FastBack 5.5.x Multiple Vulnerabilities

IBM Tivoli Storage Manager FastBack 6.1.x < 6.1.12 Multiple Vulnerabilities

IBM Tivoli Storage Manager FastBack 6.1.x < 6.1.12.1 Multiple Vulnerabilities

IBM Tivoli Storage Manager FastBack Mount 6.1.x < 6.1.11.1 Multiple Vulnerabilities

IBM Tivoli Storage Manager FastBack Mount CMountDismount::GetVaultDump RCE

IBM Tivoli Storage Manager FastBack Server Opcode 1329 Information Disclosure

IBM Tivoli Storage Manager Server 5.5.x Multiple Vulnerabilities

IBM Tivoli Storage Manager Server 6.1.x Multiple Vulnerabilities

IBM Tivoli Storage Manager Server 6.2 < 6.2.7 / 6.3 < 6.3.5 / 7.1 < 7.1.1 GSKit X.509 Certificate Chain DoS

IBM Tivoli Storage Manager Server 6.2.x < 6.2.6.0 Multiple Vulnerabilities

IBM Tivoli Storage Manager Server 6.3.x < 6.3.4.0 DoS

IBM Tivoli Storage Manager Server 6.3.x < 6.3.4.200 Information Disclosure

ICAP Server Type and Version

ICMP Domain Name Request

ICMP Netmask Request Information Disclosure

ICMP Node Information Query Information Disclosure

ICMP Timestamp Request Remote Date Disclosure

identd Service UID Association

Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

IP Protocols Scan

IPMI Cipher Suite Zero Authentication Bypass

IPMI Cipher Suites Supported

IPMI v2.0 Password Hash Disclosure

IPMI Versions Supported

Jenkins < 1.638 / 1.625.2 Java Object Deserialization RCE

Jenkins < 1.642.2 / 1.650 Java Object Deserialization RCE

Jenkins < 1.642.2 / 1.650 Java Object Deserialization RCE

KSplice : Installed Patches

LaBrea Tarpitted Host Detection

Link Layer Topology Discovery (LLTD) Detection

Linux Alternate Patch Detection

Linux Kernel TCP Sequence Number Generation Security Weakness

Linux Kernel UDP Implementation IP Identification Field Remote OS Disclosure

Linux User List Enumeration

memcached < 1.4.17 Multiple Vulnerabilities

Memory Information (via DMI)

Microsoft Azure Instance Metadata Enumeration (Unix)

Microsoft Visual Studio Code for Installed (Linux)

MIT Kerberos 5 setup\_server\_realm() Remote DoS

Netstat Connection Information

Network UPS Tools Detection

News Server (NNTP) Anonymous Read / Write Access

News Server (NNTP) Anonymous Read Access

News Server (NNTP) Information Disclosure

NNTP Service STARTTLS Command Support

Open Port Re-check

OpenSSL AES-NI Padding Oracle MitM Information Disclosure

OpenSSL SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG Ciphersuite Disabled Cipher Issue

OpenSSL SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG Session Resume Ciphersuite Downgrade Issue

Oracle Java Runtime Environment (JRE) Detection (Unix)

OS Identification

OS Identification : Apple AirPlay

OS Identification : Apple Filing Protocol

OS Identification : FTP

OS Identification : HNAP

OS Identification : HTML

OS Identification : HTTP

OS Identification : ICMP

OS Identification : LDAP

OS Identification : Linux Distribution

OS Identification : mDNS

OS Identification : Miscellaneous Methods

OS Identification : MSRPC

OS Identification : NativeLanManager

OS Identification : NETCONF Over SSH

OS Identification : NTP

OS Identification : OUI

OS Identification : RDP

OS Identification : SinFP

OS Identification : SIP

OS Identification : SMB

OS Identification : SMTP

OS Identification : SNMP

OS Identification : SNMP hrSWInstalledName

OS Identification : SNMP sysObjectID

OS Identification : SSH

OS Identification : SSL Certificates

OS Identification : Telnet

OS Identification : Unix uname

OS Identification : UPnP

OS Identification Failed

OS Identification: iPhone or iPad

OS Identification: Probabilistic SinFP

Palo Alto Networks PAN-OS GlobalProtect Web Portal RCE (PAN-SA-2016-0005)

Patch Data Finalization

Patch Management Auditing Satisfied

Patch Management Windows Auditing Conflicts

Patch Report

PCI DSS Compliance : Scan Interference

Persistent Systems Radia Client Automation Agent Command Injection

Point-of-Sale (POS) OUI Detection

PolarSSL 'asn1\_get\_sequence\_of' Function Uninitialized Pointer RCE

PolarSSL Weak Signature Algorithm Negotiation

Post-scan OS Identification

Processor Information (via DMI)

RDP Screenshot

Reachable IPv6 address

Record Route

Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure

Riverbed SteelHead CX WAN Traffic Manager Web UI Detection

RuggedCom RuggedOS Known Hardcoded SSL RSA Private Key

Samba Badlock Vulnerability

SAP Gateway 10Kblaze Remote Code Execution Vulnerability.

SAProuter Remote Authentication Bypass (Note 1853140)

SELinux Status Check

SFTP Supported

SIP Script Remote Command Execution via Shellshock

Small SSH RSA Key

Software Enumeration (SSH)

Solaris Installed Package Enumeration (credentialed check)

SSH Protocol Version 1 Session Key Retrieval

SSH Protocol Versions Supported

SSHD libkeyutils Backdoor

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

SSL / TLS Versions Supported

SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

SSL Certificate 'commonName' Mismatch

SSL Certificate Cannot Be Trusted

SSL Certificate Chain Analysis

SSL Certificate Chain Contains Illegitimate TURKTRUST Intermediate CA

SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

SSL Certificate Chain Contains RSA Keys Less Than 2048 bits (PCI DSS)

SSL Certificate Chain Contains Unnecessary Certificates

SSL Certificate Chain Contains Weak RSA Keys

SSL Certificate Chain Not Sorted

SSL Certificate Contains Weak RSA Key (Infineon TPM / ROCA)

SSL Certificate Expiry

SSL Certificate Expiry - Future Expiry

SSL Certificate Expiry - Future Validity

SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions

SSL Certificate Information

SSL Certificate Null Character Spoofing Weakness

SSL Certificate Signed Using SHA-1 Algorithm

SSL Certificate Signed Using Weak Hashing Algorithm

SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

SSL Certificate Signed with the Compromised FortiGate Key

SSL Certificate Signed with the Publicly Known Cyberoam Key

SSL Certificate Signed with the Revoked DigiNotar Certificate Authority

SSL Certificate Validity - Duration

SSL Certificate with Wrong Hostname

SSL Cipher Block Chaining Cipher Suites Supported

SSL Cipher Suites Supported

SSL Compression Methods Supported

SSL Medium Strength Cipher Suites Supported (SWEET32)

SSL Null Cipher Suites Supported

SSL Perfect Forward Secrecy Cipher Suites Supported

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

SSL Resume With Different Cipher Issue

SSL Root Certification Authority Certificate Information

SSL Root Certification Authority Distrusted

SSL Self-Signed Certificate

SSL Server Accepts Weak Diffie-Hellman Keys

SSL Session Resume Supported

SSL Weak Cipher Suites Supported

SSL/TLS Deprecated Ciphers

SSL/TLS Deprecated Ciphers Unsupported

SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

SSL/TLS Services Support RC4 (PCI DSS)

SSLv2-Only Open Ports

SSLv2-Only Open Ports Unsupported

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Super Micro detection (dmidecode)

SuperMicro Device Uses Default SSH Host Key

SuperMicro Device Uses Default SSL Certificate

Symantec Encryption Desktop Multiple Vulnerabilities (SYMSA1485)

Symantec Endpoint Encryption < 11.3.0 Multiple Vulnerabilities (SYMSA1485)

System Information Enumeration (via DMI)

TCP/IP Initial Sequence Number (ISN) Reuse Weakness

TCP/IP Predictable ISN (Initial Sequence Number) Generation Weakness

TCP/IP Timestamps Supported

Time of Last System Startup

TLS Next Protocols Supported

TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)

Traceroute Information

Transport Layer Security (TLS) Protocol CRIME Vulnerability

Unix / Linux Running Processes Information

Unix Operating System on Extended Support

Unix Operating System Unsupported Version Detection

Unprotected memcached

VirtualBox Virtual Machine detection (dmidecode)

VirtualPC Virtual Machine detection (dmidecode)

VMware Player 12.1.x < 12.1.1 Shared Folders (HGFS) Guest DLL Hijacking Arbitrary Code Execution (VMSA-2016-0010) (Linux)

VMware Player 12.x < 12.5.2 Drag-and-Drop Feature Arbitrary Code Execution (VMSA-2016-0019) (Linux)

VMware Player 12.x < 12.5.4 Drag-and-Drop Feature Guest-to-Host Code Execution (VMSA-2017-0005) (Linux)

VMware Player 14.x < 14.1.3 Out-of-Bounds Write (VMSA-2018-022) (Linux)

VMware Player 5.x < 5.0.1 VMX Process DoS (VMSA-2014-0001) (Linux)

VMware Player 5.x < 5.0.3 Host Privilege Escalation (VMSA-2013-0013)

VMware Player 6.x < 6.0.2 OpenSSL Library Multiple Vulnerabilities (VMSA-2014-0004) (Linux) (Heartbleed)

VMware Player 6.x < 6.0.2 Windows 8.1 Guest Privilege Escalation (VMSA-2014-0005) (Linux)

VMware Player 6.x < 6.0.5 Multiple Vulnerabilities (VMSA-2015-0001) (Linux)

VMware Player 6.x < 6.0.6 RPC Command DoS (VMSA-2015-0004) (Linux)

VMware Player 7.x < 7.1.2 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (Linux)

VMware Player < 5.0.4 / 6.0.3 OpenSSL Library Multiple Vulnerabilities (Linux)

VMware Player for Linux Installed

VMware Virtual Machine Detection

VMware Virtual Machine detection (dmidecode)

VMware vRealize Log Insight Detection (Linux)

VMware Workstation (Linux) 15.0.x < 15.1.0 Use After Free Vulnerability (VMSA-2019-0009)

VMware Workstation 10.x < 10.0.2 OpenSSL Library Multiple Vulnerabilities (VMSA-2014-0004) (Linux) (Heartbleed)

VMware Workstation 10.x < 10.0.2 Windows 8.1 Guest Privilege Escalation (VMSA-2014-0005) (Linux)

VMware Workstation 10.x < 10.0.5 Multiple Vulnerabilities (VMSA-2015-0001) (Linux)

VMware Workstation 10.x < 10.0.6 RPC Command DoS (VMSA-2015-0004) (Linux)

VMware Workstation 11.x < 11.1.2 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (Linux)

VMware Workstation 12.1.x < 12.1.1 Shared Folders (HGFS) Guest DLL Hijacking Arbitrary Code Execution (VMSA-2016-0010) (Linux)

VMware Workstation 12.x < 12.5.2 Drag-and-Drop Feature Arbitrary Code Execution (VMSA-2016-0019) (Linux)

VMware Workstation 12.x < 12.5.4 Drag-and-Drop Feature Guest-to-Host Code Execution (VMSA-2017-0005) (Linux)

VMware Workstation 12.x < 12.5.5 Multiple Vulnerabilities (VMSA-2017-0006) (Linux)

VMware Workstation 12.x < 12.5.6 Insecure Library Loading Privilege Escalation (VMSA-2017-0009) (Linux)

VMware Workstation 12.x < 12.5.7 Multiple Vulnerabilities (VMSA-2017-0015) (Linux)

VMware Workstation 14.x < 14.1.1 Denial of Service Vulnerability (VMSA-2018-0008)

VMware Workstation 14.x < 14.1.3 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Linux)

VMware Workstation 14.x < 14.1.3 Out-of-Bounds Write (VMSA-2018-0022) (Linux)

VMware Workstation 14.x < 14.1.3 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (Linux)

VMware Workstation 14.x < 14.1.4 / 15.x < 15.0.1 vmxnet3 Guest-to-Host Code Execution Vulnerability (VMSA-2018-0027)

VMware Workstation 14.x < 14.1.5 / 15.x < 15.0.2 Virtual Network Integer Overflow Vulnerability (VMSA-2018-0030)

VMware Workstation 14.x < 14.1.6 / 15.x < 15.0.3 Elevation of Privilege Vulnerability (VMSA-2019-0002)

VMware Workstation 14.x < 14.1.6 / 15.x < 15.0.3 Multiple Vulnerabilities (VMSA-2019-0006)

VMware Workstation 14.x < 14.1.7 / 15.x < 15.0.4 Multiple Vulnerabilities (VMSA-2019-0005)

VMware Workstation 15.0.x < 15.5.0 Multiple Vulnerabilities (VMSA-2019-0014)

VMware Workstation 15.0.x < 15.5.1 Vulnerability (VMSA-2019-0023)

VMware Workstation 15.0.x < 15.5.2 Multiple Vulnerabilities (VMSA-2020-0005)

VMware Workstation 15.x < 15.5.2 Multiple Vulnerabilities (VMSA-2020-0004) (Linux)

VMware Workstation 9.x < 9.0.1 VMX Process DoS (VMSA-2014-0001) (Linux)

VMware Workstation 9.x < 9.0.3 Multiple Privilege Escalation Vulnerabilities (VMSA-2013-0013 / VMSA-2013-0014)

VMware Workstation < 15.5.0 Vulnerability (VMSA-2019-0019)

VMware Workstation < 9.0.4 / 10.0.3 OpenSSL Library Multiple Vulnerabilities (Linux)

VMware Workstation for Linux Installed

Vulnerability in TLS Could Allow Information Disclosure (2655992) (uncredentialed check)

Weak DH Key Exchange Supported (PCI DSS)

Web Site Links to Malicious Content (disabled)

Well-Known Ruby on Rails Secret Token Used on Remote Application

Well-known SSL Certificate Used in Remote Device

Wireless Access Controller Detection

Wireless Access Point Detection

# Gain a shell remotely

Adobe Flash Media Server < 2.0.5 Multiple Remote Vulnerabilities

AIX lpd Multiple Functions Remote Overflow

APC < 3.8.0 apcupsd Multiple Vulnerabilities

Apple TV < 5.1 Multiple Vulnerabilities

Asterisk main/udptl.c Buffer Overflows (AST-2011-002)

Asterisk main/utils.c ast\_uri\_encode() CallerID Information Overflow (AST-2011-001)

Asterisk SIP Channel T.38 SDP Parsing Multiple Buffer Overflows

Asterisk Skinny Channel Driver (chan\_skinny) get\_input Function Remote Overflow

AT-TFTP Server Filename Handling Remote Overflow

Avirt Gateway Suite Telnet Proxy Arbitrary Command Execution

AXIGEN Mail Server < 2.0.0 Multiple Remote Vulnerabilities

AXIGEN Mail Server AXIMilter CNHO Command Remote Format String

BakBone NetVault < 7.1.2 / 7.3.1 Multiple Remote Overflows

Barracuda Appliances Default Credentials

Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)

Bash Remote Code Execution (CVE-2014-6277 / CVE-2014-6278) (Shellshock)

Bash Remote Code Execution (Shellshock)

Batalla Naval gbnserver Remote Overflow

BayTech RPC-3 Telnet Daemon Remote Authentication Bypass

BeanShell Remote Server Mode Arbitrary Code Execution

Berlios gpsd gpsd\_report() Function Format String

BitKeeper Daemon Mode diff Shell Command Injection

BlackBerry Enterprise Server Attachment Handling Buffer Overflows

BlackBerry Enterprise Server PNG Attachment Buffer Overflow

Brightmail AntiSpam bmagent Multiple Remote Vulnerabilities (DoS, Traversal)

BSD Based telnetd telrcv Function Remote Command Execution

BSD in.lpd File Name Handling Remote Overflow

CA ARCserve Backup Remote Code Execution (CA20121018) (uncredentialed check)

CA BrightStor ARCserve/Enterprise Backup Persistent Default Administrator Account

CA Multiple Products Message Queuing Multiple Remote Vulnerabilities

CA Multiple Products Message Queuing Server (Cam.exe) Remote Overflow

Canna SR\_INIT Command Remote Overflow

Cfengine AuthenticationDialogue() Function Remote Overflow

Cfengine CAUTH Command Remote Format String

Cfengine cfservd ReceiveTransaction Function Remote Overflow (intrusive check)

Cfengine cfservd ReceiveTransaction Function Remote Overflow (version check)

Cisco Prime Data Center Network Manager RMI Remote Code Execution (credentialed check)

Cisco Prime Data Center Network Manager RMI Remote Code Execution (uncredentialed check)

Citadel/UX lprintf() Function Remote Format String

Citadel/UX select() Bitmap Array Index Remote Oerflow

Citadel/UX USER Command Remote Overflow

ClamAV < 0.94 Multiple Vulnerabilities

ClamAV < 0.94.1 get\_unicode\_name() Off-by-One Buffer Overflow

ClamAV < 0.94.2 cli\_check\_jpeg\_exploit() Malformed JPEG File DoS

Cyrus IMAP Server < 2.2.10 Multiple Remote Overflows

Cyrus IMAP Server < 2.2.11 Multiple Remote Overflows

Cyrus IMAP Server login Command Remote Overflow

Darwin Streaming Server < 5.5.5 Multiple RCE Vulnerabilities

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Dell NetVault Backup 10.0.x < 10.0.5 RCE

Digital Mappings Systems POP3 Server (pop3svr.exe) Multiple Field Remote Overflow

Dropbear SSH Server DSS Verification Failure Remote Privilege Escalation

Ebola AV Daemon < 0.1.5 Authentication Sequence Remote Overflow

EMC AlphaStor Device Manager robotd RCE

EMC AlphaStor Library Manager Remote Code Execution

EMC AutoStart ftAgent Multiple Remote Code Execution Vulnerabilities (ESA-2012-020)

EMC Legato Networker Remote Exec Service Stack Overflow RCE

EMC Replication Manager irccd.exe RunProgram Message Handling Arbitrary Command Execution

EMC RepliStor < 6.2 SP5/6.3 SP2 Multiple Heap Overflows

EMC RepliStor Multiple Remote Heap Based Buffer Overflows

EMC Retrospect Client Packet Handling Remote Overflow

Eudora Internet Mail Server for Mac OS USER Overflow

F-Secure SSH Password Authentication Policy Evasion

F5 Multiple Products Root Authentication Bypass

fake identd (fakeidentd) Fragmented Packet Request Remote Overflow

FakeBO NetBus Handling Code Remote Overflow

Fenice <= 1.10 Multiple Remote Vulnerabilities

Firefly Media Server webserver.c ws\_addarg Function /xml-rpc Authorization Header Remote Format String

Firefly Media Server ws\_getpostvars Function Content-Length Header HTTP Request Handling Overflow

FreeBSD 'telnetd' Daemon Remote Buffer Overflow

FreeBSD 2.x lpd Long DNS Hostname Overflow

FreeBSD telnetd sys\_term.c Environment Variable Handling Privilege Escalation (FreeBSD-SA-09:05)

freeFTPd / freeSSHd SFTP Authentication Bypass

freeSSHd Key Exchange Algorithm String Remote Overflow

FTGate4 IMAP EXAMINE Command Remote Overflow

Gauntlet CyberPatrol Content Monitoring System Overflow

gnocatan Multiple Buffer Overflows

GNOME libgtop Daemon Remote Format String

GNU Bash Local Environment Variable Handling Command Injection via Telnet (CVE-2014-7169) (Shellshock)

GNU Mailutils <= 0.6 Multiple Vulnerabilities

GNU Mailutils imap4d Search Command Remote Format String

GpsDrive friendsd2 dir Field Remote Format String

Helix Servers View Source Plug-in RTSP Parser Overflow

Hobbit Monitor < 4.1.0 hobbitd Malformed Message Remote Overflow

HP Data Protector <= A.06.20 Multiple Vulnerabilities (uncredentialed check)

HP Data Protector Backup Agent RCE

HP Data Protector OmniInet.exe MSG\_PROTOCOL Command RCE

HP Data Protector Remote Command Execution

HP iNode Management Center Buffer Overflow (HPSB3C02687) (remote check)

HP Intelligent Management Center < 5.2 E401 Multiple Vulnerabilities

HP Intelligent Management Center Multiple Vulnerabilities

HP Intelligent Management Center TFTP Multiple Vulnerabilities

HP Intelligent Management Center User Access Manager Datagram Parsing Code Execution

HP Intelligent Management Center User Access Manager Unspecified Information Disclosure

HP LeftHand Virtual SAN Appliance < 10.0 hydra Service Multiple RCE

HP Linux Imaging and Printing Project (hplip) hpssd from Address Command Injection

HP LoadRunner 11.52 Buffer Overflow RCE (uncredentialed check)

HP LoadRunner < 11.00 Patch 4 Code Execution (intrusive check)

HP LoadRunner < 11.52 SSL Connection Handling Stack Buffer Overflow RCE

HP OpenView Network Node Manager Multiple Code Execution Vulnerabilities (HPSBMU02712 SSRT100649)

HP OpenView Network Node Manager Multiple Services Remote Overflow

HP Remote Watch showdisk Remote Privilege Escalation

HP SAN/iQ < 9.5 Root Shell Command Injection

HP SAN/iQ <= 10.0 Root Shell Command Injection

HP StorageWorks MSA P2000 Default Credentials

HP StorageWorks MSA P2000 Hidden 'admin' User Default Credentials

HP System Management Homepage SetSMHData admin-group Parameter Handling RCE

HP Virtual Table Server (VTS) Database Import RCE

HPE LoadRunner Shared Memory Name Construction RCE

Hummingbird InetD LPD Component (Lpdw.exe) Data Overflow

IAXClient Open Source Library iax\_net\_read Function Packet Handling Remote Overflow

IBM Lotus Domino < 5.0.12 / 6.0.1 Multiple Vulnerabilities

IBM Lotus Domino < 6.5.6 FP2 Multiple Vulnerabilities

IBM Lotus Domino < 7.0.2 FP2 Multiple Vulnerabilities

IBM Lotus Domino IMAP Server (nimap.exe) CRAM-MD5 Authentication Remote Overflow

IBM Lotus Domino IMAP Service Mailbox Name Overflow

IBM Tivoli Directory Server SASL Bind Request Buffer Overflow (uncredentialed check)

IBM Tivoli Storage Manager Client Multiple Vulnerabilities (swg21405562)

IBM Tivoli Storage Manager Multiple Remote Overflows

IMail IMAP Server Login Functions Remote Overflow

IMail IMonitor Service Remote Overflow

IMAP pop-2d POP Daemon FOLD Command Remote Overflow

Informix Dynamic Server Multiple Remote Vulnerabilities

INN < 1.6 Multiple Vulnerabilities

INN < 2.2.3 verifycancels Option Cancel Request Message Overflow

INN < 2.4.1 Control Message Handling Code Overflow

Intel PXE Server Remote Overflow

Ipswitch IMail IMAP EXAMINE Argument Buffer Overflow

Kerberos klogind Remote Overflow

Kerberos telnet Crafted Username Remote Authentication Bypass

Kerio MailServer < 6.5.0 Multiple Vulnerabilities

Knox Arkeia Backup Client Type 77 Request Processing Buffer Remote Overflow

l2tpd < 0.68 Multiple Vulnerabilities

l2tpd < 0.69 control.c write\_packet Function Remote Overflow

LCDproc < 0.4.1 screen\_add Command Remote Overflow

Linux lpd DVI Print Filter (dvips) Remote Command Execution

Lotus Notes < 6.5.5 / 7.0.1 Attachment Handling Vulnerabilities

LPRng use\_syslog() Remote Format String Arbitrary Command Execution

MailMax < 5.0.10.8 Multiple Remote Overflows

MailMax IMAP Server SELECT Command Remote Overflow

MBDMS Database Server Long String Remote Overflow

McAfee LinuxShield <= 1.5.1 nailsd Daemon Remote Privilege Escalation

MDaemon IMAP Server Multiple AUTHENTICATE Commands Remote Overflow

Medal of Honor Multiple Remote Overflows

MERCUR Messaging IMAP Server NTLM Authentication NTLMSSP Argument Remote Overflow

MERCUR Messaging IMAP Service Multiple Command Remote Overflow

Mercury IMAP Server LOGIN Command Remote Overflow

Mercury IMAP Server SEARCH Command Remote Buffer Overflow

Mercury LoadRunner Agent server\_ip\_name Field Remote Buffer Overflow

Mercury Mail ph Server Remote Overflow

Mercury Mail Remote IMAP Server Remote Overflow

MiniUPnP < 1.4 Multiple Vulnerabilities

Multiple Cisco Products brstart sm\_read\_string\_length Remote Code Execution

Multiple Linux rpc.mountd Remote Overflow

Multiple OS /bin/login Remote Overflow

Multiple Switch Vendors '\_\_super' Account Backdoor

Multiple Vendor IRC Daemon Debug Format String

Multiple Vendor POP3 Remote Overflows

NAI WebShield SMTP Management Agent SET\_CONFIG Overflow

Netatalk OpenSession Remote Code Execution

NetCPlus SmartServer3 POP3 (NCPOPSERV.EXE) USER Command Remote Overflow

Netscape Messaging Server IMAP LIST Command Remote Overflow

Netscape NSS Library SSLv2 Challenge Overflow

NetWin DMail Server Multiple Remote Vulnerabilities

Network Solutions Rwhoisd -soa Command Remote Format String

Network Solutions Rwhoisd Syslog Remote Format String

Network Time Protocol Daemon (ntpd) readvar Variable Overflow RCE

ngIRCd < 0.8.2 Lists\_MakeMask() Remote Overflow DoS

ngIRCd < 0.8.3 Log\_Resolver() Format String

NNTP Server Message Header Handling Remote Overflow

NNTP Server Password Handling Remote Overflow

Novell eDirectory < 8.8.2 FTF2 / 8.7.3 SP10b Multiple Remote Overflows

Novell eDirectory Server iMonitor Multiple Remote Overflows

Novell File Reporter Agent VOL Tag Remote Code Execution (uncredentialed check)

Novell File Reporter Agent XML Parsing Remote Code Execution

Novell File Reporter Engine RECORD Element Tag Parsing Overflow (uncredentialed check)

Novell GroupWise Internet Agent Request Content-Length Header Parsing Remote Overflow

Novell GroupWise Messenger Accept Language Remote Overflow

Novell Groupwise WebAccess GWINTER.EXE Base64 Decoding Remote Overflow

Novell NetMail < 3.52C IMAP Agent Multiple Remote Overflows

Novell NetMail IMAP Agent Long Verb Arguments Remote Overflow

Novell PlateSpin Orchestrate Remote Code Execution

Novell ZENworks Asset Management Collection Client Remote Overflow

Novell ZENworks Multiple Remote Pre-Authentication Overflows

Omron WorldView Wnn Multiple Command Remote Overflow

OpenLink Web Configurator GET Request Remote Overflow

OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation

OpenSSH < 3.2.3 YP Netgroups Authentication Bypass

OpenSSH < 3.4 Multiple Remote Overflows

OpenSSH < 3.7.1 Multiple Vulnerabilities

OpenSSH < 3.7.1p2 Multiple Remote Vulnerabilities

OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow

OpenSSL < 0.9.6e / 0.9.7b3 Multiple Remote Vulnerabilities

OpenVMPS Logging Function Format String

pam\_smb / pam\_ntdom User Name Remote Overflow

Perdition IMAPD IMAP Tag Remote Format String Arbitrary Code Execution

Persistent Systems Radia Client Automation Agent Stack Overflow Remote Code Execution (destructive check)

PoPToP PPTP ctrlpacket.c Negative Read Remote Overflow

Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE

Qualcomm WorldMail Multiple IMAP Command Remote Overflow

Random password for 'root' account

RealNetworks Helix DNA Server RTSP Service Crafted Require Header Remote Overflow

RealNetworks Helix Server < 11.1.8/12.0.1 Multiple Vulnerabilities

RealNetworks Helix Servers DESCRIBE Request LoadTestPassword Field Remote Overflow

RealServer G2 Malformed Telnet Data Remote Overflow

Rendezvous < 7.5.1 HTTP Admin Interface Remote Overflow

rlogin -froot Remote Root Access

Rockliffe MailSite Management Agent wconsole.dll GET Request Overflow

Rover POP3 Server Username Remote Overflow

rsh NULL Login Remote Privilege Escalation

rsh Unauthenticated Access (via finger Information)

rsync < 2.5.7 Unspecified Remote Heap Overflow

rsync I/O Functions Multiple Signedness Errors RCE

rsync sanitize\_path() Function Arbitrary File Disclosure

Samba < 2.2.8 Multiple Vulnerabilities

Samba < 2.2.8a / 3.0.0 Multiple Remote Overflows

Samba Encrypted Password String Conversion Decryption Overflow

Samba enum\_csc\_policy Data Structure Termination Remote Overflow

Samba Mangling Method Hash Overflow

Samba NETBIOS Name Traversal Arbitrary Remote File Creation

Samba smbd Security Descriptor Parsing Remote Overflow

Samba TNG < 0.3.1 Multiple Remote Vulnerabilities

SCO UnixWare i2odialogd daemon Username Authorization String Overflow

Sentinel License Manager lservnt Service Remote Buffer Overflow

SIDVault < 2.0f LDAP Server Malformed Search Request Buffer Overflow

Solaris 10 Forced Login Telnet Authentication Bypass

Solaris cachefsd Multiple Vulnerabilities (ESCROWUPGRADE)

Solaris in.lpd Crafted Job Request Arbitrary Remote Command Execution

Solaris in.lpd Transfer Job Routine Remote Buffer Overflow

Solaris rpc.yppasswdd username Remote Overflow

Solaris sadmind AUTH\_SYS Credential Remote Command Execution

Solaris snmpXdmid Long Indication Event Overflow (ELVISCICADA)

Solsoft NSM Format Strings RCE

SpamAssassin spamd Crafted Message Arbitrary Command Execution

SSH Static Key Accepted

SSH1 SSH Daemon Logging Failure

sshd scp Traversal Arbitrary File Overwrite

Sun Java System Directory Server Multiple Vulnerabilities

Sun SPARC Enterprise T5120 and T5220 Default Configuration Root Command Execution

SuperMicro IPMI PSBlock File Plaintext Password Disclosure

Sybase M-Business Anywhere (AvantGo) gsoap Module password Tag Handling Overflow

Symantec pcAnywhere awhost32 Remote Code Execution

Symantec Veritas Enterprise Administrator Service (vxsvc) Multiple Integer Overflows

Symantec Veritas Storage Foundation Scheduler Service (VxSchedService.exe) Remote Code Execution

SysV /bin/login Environment Remote Overflow (rlogin)

SysV /bin/login Environment Remote Overflow (telnet check)

TANDBERG Video Communication Server Static SSH Host Keys

Tanne netzio.c logger Function Remote Format String

TCL Shell (tclsh) Arbitrary Command Execution

Tectia SSH Server Authentication Bypass

TFTPD Server Filename Handling Remote Overflow

TFTPD small overflow

Tftpd32 Error Message Format String

Trend Micro Control Manager CmdProcessor.exe Remote Buffer Overflow (uncredentialed check)

Trend Micro ServerProtect TmRpcSrv.dll RPC Request Multiple Overflows

TrueType Font Server for X11 (xfstt) Malformed Packet Remote Overflow

UMN Gopherd < 3.0.6 Multiple Remote Vulnerabilities

University of Washington imap Server (uw-imapd) BODY Request Remote Overflow

Unprotected Telnet Service

Unreal Engine Multiple Remote Vulnerabilities

Unreal Engine Secure Query Remote Overflow

UoW IMAP/POP server\_login() Function Remote Overflow

UoW imapd (UW-IMAP) Multiple Command Remote Overflows

UoW imapd (UW-IMAP) Multiple Command Remote Overflows (2)

UoW imapd AUTHENTICATE Command Remote Overflow

UW-IMAP Mailbox Name Buffer Overflow

VERITAS Backup Exec Agent Browser Registration Request Remote Overflow

VERITAS Backup Exec Agent Unauthenticated Remote Registry Access

Versant Connection Services Daemon Arbitrary Command Execution

VLC Media Player network/httpd.c httpd\_FileCallBack Function Connection Parameter Format String

VMSA-2012-0009 : ESXi and ESX patches address critical security issues (uncredentialed check)

VNC Server 'password' Password

vpopmail vchkpw USER/PASS Command Format String

Weak Debian OpenSSH Keys in ~/.ssh/authorized\_keys

Wyse Thin Client hagent.exe Unspecified Buffer Overflow

X Font Service Crafted XFS Query Remote Overflow

XMail APOP / USER Command Remote Overflow

XtraMail POP3 PASS Command Remote Overflow

YardRadius process\_menu Function Remote Buffer Overflow

Zend Session Clustering Daemon PHP Session Identifier Remote Overflow

# FTP

3Com 3CServer/3CDaemon FTP Server Multiple Vulnerabilities (OF, FS, PD, DoS)

3Com NBX ftpd CEL Command Remote Overflow (1)

3Com NBX ftpd CEL Command Remote Overflow (2)

4D WebStar Pre-authentication FTP Overflow

4D WebSTAR Symlink Privilege Escalation

Ability FTP Server Multiple Command Remote Buffer Overflows

AIX FTPd libc Library Remote Buffer Overflow

Alcatel OmniSwitch Default Credentials (ftp)

Anonymous FTP Enabled

Anonymous FTP Writable root Directory

ArGoSoft FTP Server .lnk Shortcut Upload Arbitrary File Manipulation

ArGoSoft FTP Server < 1.4.2.8 Multiple .LNK File Handling Vulnerabilities

ArGoSoft FTP Server DELE Command Remote Buffer Overrun

ArGoSoft FTP Server RNTO Command Remote Buffer Overflow

ArGoSoft FTP Server USER Command Account Enumeration

ArGoSoft FTP Server XCWD Remote Overflow

Ariel FTP Server Default 'document' Account

bftpd Multiple Command Remote Overflow

bftpd NLST Command Output Format String

BlackJumboDog FTP Server Multiple Command Overflow

BlackMoon FTP Login Error Message User Enumeration

BlackMoon FTP Server Denial of Service

Broker FTP Multiple Command Arbitrary File/Directory Manipulation

BSD Based FTP Server Multiple glob Function Remote Overflow

BSD ftpd Single Byte Buffer Overflow

Cerberus FTP Server 6.x < 6.0.10.0 / 7.x < 7.0.0.3 Multiple OpenSSL Vulnerabilities

Cerberus FTP Server 6.x < 6.0.9.0 / 7.x < 7.0.0.2 SSH FTP Account Enumeration

Cerberus FTP Server < 5.0.4.0 SSH DES Cipher Weakness

Cerberus FTP Server < 5.0.5.0 Cross-Site Request Forgery

Cerberus FTP Server < 5.0.6.0 Multiple XSS

Cerberus FTP Server < 5.0.8.0 / 6.x < 6.0.7.0 Web Client Security Bypass

Cerberus FTP Server Command Processing DoS

Cerberus FTP Server Detection

Cerberus FTP Server MLSD and MLST Command Hidden Files Security Bypass

CesarFTP Multiple Vulnerabilities (OF, File Access, more)

Core FTP Server < 1.2 Build 508 lstrcpy Overflow Code Execution

Core FTP Server < 1.2 Build 515 Multiple Vulnerabilities

Core FTP Server < 1.2 Build 588 32-bit Unspecified Overflow Vulnerability

Core FTP Server Detection

Crob FTP Server < 3.6.1 build 263 Multiple Vulnerabilities

Crob FTP Server Connection Saturation Remote DoS

Crob FTP Server user Field Remote Format String

DataWizard FTPXQ Default Accounts

Default FTP Credentials (ntpupdate / ntpupdate)

Default Password for FTP 'admin' Account

Dragon FTP USER Command Remote Overflow

DreamFTP Server username Remote Format String

Easy File Sharing FTP Server PASS Command Overflow

EFTP .lnk File Handling Remote Overflow

EFTP Multiple Command Traversal Arbitrary Directory Listing

EFTP Newline String Handling Remote DoS

EFTP Nonexistent File Request Installation Directory Disclosure

eScan Server Management Console (eserv.exe) FTP Server Arbitrary File Download

Farmers WIFE FTP Server Multiple Command Traversal Arbitrary File Creation

FileZilla FTP Server Multiple DoS

Foscam C1 IP Camera FTP Hard Coded Password

freeFTPd Multiple Command Malformed Argument Remote DoS

FTP 'CWD ~root' Command Privilege Escalation

FTP Daemon Long Command XSRF

FTP Privileged Port Bounce Scan

FTP Server Any Command Accepted (possible backdoor/proxy)

FTP Server Bad Command Sequence Accepted (possible backdoor/proxy)

FTP Server Copyrighted Material Present

FTP Server No Command Accepted (possible backdoor/proxy)

FTP Server root Directory .forward File Present

FTP Server root Directory .rhosts File Present

FTP Server Traversal Arbitrary File Access

FTP Server Traversal Arbitrary File Access (RETR)

FTP Service AUTH TLS Command Support

FTP Service AUTH TLS Plaintext Command Injection

FTP Supports Cleartext Authentication

FTP Writable Directories

FTPd CWD Command Account Enumeration

FTPS Cleartext Fallback Security Bypass

FTPshell Server 3.38 Malformed PORT/QUIT DoS

Gene6 FTP Server Multiple Command Remote Overflows

glFTPd Multiple Script ZIP File Handling Arbitrary File / Directory Access

GlobalSCAPE Secure FTP Server (gsftps) Custom Command Long Parameter DoS

GlobalSCAPE Secure FTP Server User Input Overflow

Globus Toolkit GridFTP Server < 3.42 / 6.11 'getpwnam\_r()' Authentication Bypass Vulnerability

Globus Toolkit GridFTP Server Detection

GNU Bash Environment Variable Handling Code Injection via ProFTPD (Shellshock)

Golden FTP Server <= 2.60 LS Command Traversal Information Disclosure

Golden FTP Server APPE Command Remote Overflow

Golden FTP Server Pro GET Traversal Arbitrary File Access

Golden FTP Server Pro Multiple Command Remote Overflow DoS

GoodTech FTP Server Connection Saturation DoS

GuildFTPd Long SITE Command Overflow

GuildFTPd Traversal Arbitrary File Enumeration

Home FTP Server Multiple Vulnerabilities

HP-UX FTP Daemon PASS Command Remote Format String

HP-UX ftpd glob() Expansion STAT Buffer Overflow

HP-UX ftpd PAM Authentication Configuration Weakness Authentication Bypass

HP-UX FTPD REST Command Remote Arbitrary Memory Disclosure

Hummingbird Connectivity FTP Service XCWD Command Overflow

Hummingbird InetD FTP Component (ftpdw.exe) Command Overflow

Inframail FTP Server NLST Command Remote Overflow

Intersoft NetTerm Netftpd USER Command Remote Overflow

Ipswitch WS\_FTP Server < 6.1.1 Multiple Vulnerabilities

Ipswitch WS\_FTP Server < 6.1.1 Multiple Vulnerabilities (uncredentialed check)

Ipswitch WS\_FTP Server Version Detection (credentialed check)

Janitza Hard-Coded FTP Password

Mac OS X FTP Server Directory Traversal

Microsoft IIS FTP Server NLST Command Overflow DoS

MPEi/X Default FTP Accounts

MS02-018: Microsoft IIS FTP Status Request DoS (uncredentialed check)

MS09-053: Microsoft IIS FTPd NLST Command Remote Buffer Overflow (975191) (uncredentialed check)

Multiple FTP Server Command Handling Overflow

Multiple FTP Server QUOTE CWD Command Home Path Disclosure

Multiple FTP Server quote stat Command Traversal Arbitrary Directory Access

Multiple FTP Server setproctitle Function Arbitrary Command Execution

Multiple FTP Server Traversal Arbitrary File/Directory Access

Multiple FTPD glob Command Arbitrary Command Execution

Multiple Vendor Embedded FTP Service Any Username Authentication Bypass

Multiple Vendor FTP Multiple PASV Command Port Exhaustion DoS

Multiple Vendor FTPD on Windows Floppy Request CPU Consumption DoS

NETFile FTP/Web Server FTP Bounce Attack

NGC Active FTPServer 2002 Multiple Command Remote DoS

oftpd PORT Command Remote DoS

OpenFTPD SITE MSG FTP Command Format String

PFTP Default Unpassworded Account

PlanetFileServer mshftp.dll Data Processing Remote Overflow

PlatinumFTPServer Multiple Vulnerabilities

PlatinumFTPServer username Multiple Connection Handling Remote Format String

PostgreSQL Authentication Module (mod\_sql) for ProFTPD USER Name Parameter SQL Injection

ProFTPD 'mod\_copy' Arbitrary File Copy Vulnerability (Remote)

ProFTPD 1.2.0pre4 mkdir Command Directory Name Handling Remote Overflow

ProFTPD 1.2.0rc2 Malformed cwd Command Format String

ProFTPD 1.3.1 SQL injection protection bypass

ProFTPD 1.3.4d / 1.3.5rc3 Denial of Service

ProFTPD < 1.3.0a Multiple Vulnerabilities

ProFTPD < 1.3.0rc2 Multiple Remote Format Strings

ProFTPD < 1.3.1rc1 mod\_ctrls Module pr\_ctrls\_recv\_request Function Local Overflow

ProFTPD < 1.3.2b / 1.3.3x < 1.3.3rc2 client-hostname restriction bypass

ProFTPD < 1.3.2rc3 ABOR Denial of Service

ProFTPD < 1.3.3c Multiple Vulnerabilities

ProFTPD < 1.3.3d 'mod\_sql' Buffer Overflow

ProFTPD < 1.3.3g / 1.3.4 Response Pool Use-After-Free Code Execution

ProFTPD < 1.3.4rc2 client-hostname restriction bypass

ProFTPD < 1.3.5b / 1.3.6x < 1.3.6rc2 weak Diffie-Hellman key

ProFTPD < 1.3.5e / 1.3.6x < 1.3.6rc5 AllowChrootSymlinks bypass

ProFTPD Auth API Multiple Auth Module Authentication Bypass

ProFTPD Command Truncation Cross-Site Request Forgery

ProFTPD Compromised Source Packages Trojaned Distribution

ProFTPD File Transfer Newline Character Overflow

ProFTPD FTP Command Handling Symlink Arbitrary File Overwrite

ProFTPD Login Timing Account Name Enumeration

ProFTPD mkdir Buffer Overflow

ProFTPD mod\_copy Information Disclosure

ProFTPD Multiple Remote Overflows (palmetto)

ProFTPD NLST Command Argument Handling Remote Overflow

ProFTPD on Debian Linux postinst Installation Privilege Escalation

ProFTPD STAT Command Remote DoS

ProFTPD TELNET IAC Escape Sequence Remote Buffer Overflow

ProFTPD Username Variable Substitution SQL Injection

QNX RTP FTP stat Command strtok() Function Overflow

RaidenFTPD Multiple Command Traversal Arbitrary File Access

RaidenFTPD urlget Command Traversal Arbitrary File Access

Robo-FTP Pre-authentication Command Execution DoS

Ruby ftpd Gem 'filename' Parameter Remote Command Execution

Sambar FTP Server Malformed SIZE Command DoS

Sami FTP Server Multiple DoS

Serv-U 2.5e Null Byte Saturation DoS

Serv-U 4.x-5.x STOU Command MS-DOS Argument Remote DoS

Serv-U 7.x < 7.2.0.1 SFTP Directory Creation Logging DoS

Serv-U 7.x < 7.3.0.1 Multiple Remote Vulnerabilities (DoS, Traversal)

Serv-U 7.x < 7.4.0.0 Multiple Command Remote DoS

Serv-U < 10.2.0.0

Serv-U < 14.0.2.0 FTP Server SSL Renegotiation DoS

Serv-U < 2.5e Multiple Vulnerabilities (OF, Path Disc)

Serv-U < 8.0.0.1 Multiple Vulnerabilities (DoS, Traversal)

Serv-U < 9.0.0.1

Serv-U < 9.1.0.0

Serv-U < 9.2.0.1

Serv-U < 9.4.0.0

Serv-U CD Command Encoded Traversal Arbitrary File/Directory Access

Serv-U CWD Command Overflow

Serv-U FTP Server < 15.0.0.0 Multiple Security Vulnerabilities

Serv-U FTP Server < 15.0.1.20 DoS

Serv-U FTP Server < 15.1.0.458 Multiple Vulnerabilities

Serv-U MDTM Command Overflow

Serv-U SITE CHMOD Command Multiple Vulnerabilities

Serv-U Version Detection

SlimFTPd Multiple Command Handling Overflow

SlimFTPd Username/Password Overflow Remote DoS

smallftpd 1.0.3 Multiple DoS

smallftpd Multiple Vulnerabilities (Traversal, DoS)

Solaris FTP Daemon CWD Command Account Enumeration

ST FTP Service Arbitrary File/Directory Access

SunFTP GET Request Remote Overflow

SunFTP Multiple Command Traversal Arbitrary File Creation/Deletion

SurgeFTP LEAK Command Remote DoS

Titan FTP Server Multiple Command Remote Overflow

Titan FTP Server quote stat Command Traversal Arbitrary Directory Listing

Titan FTP Server SITE WHO Command Resource Consumption DoS

TurboFTP Server < 1.00.720 DoS

TYPSoft FTP Server 1.10 Invalid Path Request DoS

TYPSoft FTP Server <= 1.10 Multiple DoS

TYPSoft FTP Server Crafted RETR Command Sequence Remote DoS

TYPSoft FTP Server Empty Username DoS

TYPSoft FTP Server LIST Command Traversal Arbitrary Directory Listing

TYPSoft FTP Server Malformed STOR / RETR Command DoS

Vermillion FTPD Long CWD Commands DoS

vsftpd Detection

vsftpd Smiley Face Backdoor

vsftpd vsf\_filename\_passes\_filter Function Denial of Service

War FTP Daemon 1.82 Denial of Service

WarFTPd CWD Command Remote DoS

WarFTPd CWD/MKD Command Overflow

WarFTPd dir Command Traversal Arbitrary Directory Listing

WarFTPd USER/PASS Command Remote Overflow

WebWeaver FTP Aborted RETR Command Remote DoS

WFTP 3.21 Multiple Vulnerabilities (OF, DoS)

WFTP Unpassworded Guest Account

WFTPD APPE Command Buffer Overflow

WFTPD Out-of-Sequence RNTO Command DoS

WFTPD Unauthenticated MLST Command DoS

Windows 98 FTP MS/DOS Device Name Request DoS

Windows FTP Server NULL Administrator Password

Windows NT FTP 'guest' Account Present

Wing FTP Server < 3.2.0 PORT Command DoS

Wing FTP Server < 3.6.6 DoS

Wing FTP Server Detection

Wing FTP Server LDAP Authentication Bypass

Wing FTP Server Multiple ZIP Commands Parsing Remote DoS

Wing FTP Server SFTP Connection Unspecified DoS

Wing FTP Server SSH Public Key Authentication Bypass

WS\_FTP Multiple Command Long Argument Overflow

WS\_FTP Server CWD Command Remote DoS

WS\_FTP Server Multiple Command Remote Overflow DoS

WS\_FTP Server Multiple Vulnerabilities (Bounce, PASV Hijacking)

WS\_FTP Server Multiple Vulnerabilities (OF, DoS, Cmd Exec)

WS\_FTP Server Path Parsing Remote DoS

WS\_FTP Server SITE CPWD Command Remote Overflow

WS\_FTP Server STAT Command Remote Overflow

WU-FTPD ABOR Command Arbitrary File Access

WU-FTPD Debug Mode Client Hostname Remote Format String

WU-FTPD fb\_realpath() Function Off-by-one Overflow

WU-FTPD fileutils/coreutils ls -w Argument Memory Consumption DoS

WU-FTPD MAIL\_ADMIN Function Remote Overflow

WU-FTPD Multiple Vulnerabilities (OF, Priv Esc)

WU-FTPD QUOTE PASV Forced Core Dump Information Disclosure

WU-FTPD restricted-gid Directory Access Restriction Bypass

WU-FTPD rnfr File Overwrite

WU-FTPD S/KEY Authentication ftpd.c skey\_challenge Function Remote Overflow

WU-FTPD SITE EXEC Arbitrary Local Command Execution

WU-FTPD SITE NEWER Command Memory Exhaustion DoS

WU-FTPD site\_exec() Function Remote Format String

WU-FTPD Unspecified Security Issue

WU-FTPD wu\_fnmatch() Function File Globbing Remote DoS

Wyse Device Manager Default FTP Account

XAMPP Default FTP Account

Xlight FTP Server Authentication SQL Injection

Xlight FTP Server Multiple Remote Overflows

XM Easy FTP Server USER Command Buffer Overflow

Zaurus PDA FTP Server Unpassworded root Account

# FreeBSD Local Security Checks

FreeBSD 10.3 / 10.4 / 11.0 / 11.1 : ptrace / kldstat Information Disclosure Vulnerabilities (FreeBSD-SA-17:08.ptrace) (FreeBSD-SA-17:10.kldstat)

FreeBSD 10.3 / 10.4 : shm Insecure Memory Vulnerability (FreeBSD-SA-17:09.shm)

FreeBSD 11.x < 11.2-RELEASE-p10 / 12.x < 12.0-RELEASE-p4 Multiple vulnerabilities in pf

FreeBSD 11.x < 11.2-RELEASE-p12 / 12.x < 12.0-RELEASE-p7 Privilege escalation in cd(4) driver

FreeBSD 11.x < 11.2-RELEASE-p13 / 11.x < 11.3-RELEASE-p2 / 12.x < 12.0-RELEASE-p9 MLDv2 Out-of-Bounds Memory Access DoS

FreeBSD 11.x < 11.2-RELEASE-p14 / 11.x < 11.3-RELEASE-p3 / 12.x < 12.0-RELEASE-p10 midistat Race Condition

FreeBSD 11.x < 11.2-RELEASE-p7 / 12.x < 12.0-RELEASE-p1 bootpd stack buffer overflow

FreeBSD 7.3 to 9.0-RC1 privilege escalation/denial of service

FreeBSD : 'Content-Type' XSS vulnerability affecting other webmail systems (c5519420-cec2-11d8-8898-000d6111a684)

FreeBSD : a2ps -- format string vulnerability (e359051d-90bd-11e5-bd18-002590263bf5)

FreeBSD : a2ps -- insecure command line argument handling (8091fcea-f35e-11d8-81b0-000347a4fa7d)

FreeBSD : a2ps -- insecure temporary file creation (9168253c-5a6d-11d9-a9e7-0001020eed82)

FreeBSD : aacplusenc -- denial of service (7801b1e1-99b4-42ac-ab22-7646235e7c16)

FreeBSD : abiword, koffice -- stack based buffer overflow vulnerabilities (9cd52bc6-a213-11da-b410-000e0c2e438a)

FreeBSD : acroread (2130)

FreeBSD : acroread -- buffer overflow vulnerability (70c59485-ee5a-11d9-8310-0001020eed82)

FreeBSD : acroread -- insecure temporary file creation (107692a1-ee6c-11d9-8310-0001020eed82)

FreeBSD : acroread -- plug-in buffer overflow vulnerability (f74dc01b-0e83-11da-bc08-0001020eed82)

FreeBSD : acroread -- XML External Entity vulnerability (02bc9b7c-e019-11d9-a8bd-000cf18bbe54)

FreeBSD : acroread uudecoder input validation error (78348ea2-ec91-11d8-b913-000c41e2cdad)

FreeBSD : acroread5 -- mailListIsPdf() buffer overflow vulnerability (28e93883-539f-11d9-a9e7-0001020eed82)

FreeBSD : acroread9 -- Multiple Vulnerabilities (fa2f386f-4814-11e1-89b4-001ec9578670)

FreeBSD : activemq -- Unsafe deserialization (a258604d-f2aa-11e5-b4a9-ac220bdcec59)

FreeBSD : activemq -- Web Console Clickjacking (950b2d60-f2a9-11e5-b4a9-ac220bdcec59)

FreeBSD : activemq -- Web Console XSS (a6cc5753-f29e-11e5-b4a9-ac220bdcec59)

FreeBSD : adminer -- remote code execution (dd563930-d59a-11e5-8fa8-14dae9d210b8)

FreeBSD : adminer -- XSS vulnerability (18201a1c-d59a-11e5-8fa8-14dae9d210b8)

FreeBSD : adminer -- XSS vulnerability (8cf54d73-d591-11e5-8fa8-14dae9d210b8)

FreeBSD : adminer -- XSS vulnerability (ad91ee9b-d599-11e5-8fa8-14dae9d210b8)

FreeBSD : Adobe Flash Player -- critical vulnerabilities (1e63db88-1050-11e5-a4df-c485083ca99c)

FreeBSD : Adobe Flash Player -- critical vulnerabilities (3364d497-e4e6-11e4-a265-c485083ca99c)

FreeBSD : Adobe Flash Player -- critical vulnerabilities (348bfa69-25a2-11e5-ade1-0011d823eebd) (Underminer)

FreeBSD : Adobe Flash Player -- critical vulnerabilities (8b3ecff5-c9b2-11e4-b71f-00bd5af88c00)

FreeBSD : Adobe Flash Player -- critical vulnerabilities (d02f6b01-1a3f-11e5-8bd6-c485083ca99c)

FreeBSD : Adobe Flash Player -- critical vulnerabilities (e206df57-f97b-11e4-b799-c485083ca99c)

FreeBSD : Adobe Flash Player -- critical vulnerabilities (f3778328-d288-4b39-86a4-65877331eaf7)

FreeBSD : Adobe Flash Player -- critical vulnerability (37a87ade-a59f-11e4-958e-0011d823eebd)

FreeBSD : Adobe Flash Player -- multiple vulnerabilities (cc294a2c-a232-11e4-8e9f-0011d823eebd)

FreeBSD : alsaplayer -- multiple vulnerabilities (9855ac8e-2aec-11db-a6e2-000e0c2e438a)

FreeBSD : amarok -- multiple vulnerabilities (6bb6188c-17b2-11de-ae4d-0030843d3802)

FreeBSD : amaya -- Attribute Value Buffer Overflow Vulnerabilities (dc930435-d59f-11da-8098-00123ffe8333)

FreeBSD : amaya -- multiple buffer overflow vulnerabilities (a89b76a7-f6bd-11dd-94d9-0030843d3802)

FreeBSD : ampache -- insecure temporary file usage (0ac68e68-d32b-11dd-b540-d1288664c17e)

FreeBSD : ansible -- code execution from compromised remote host data or untrusted local data (9dae9d62-205f-11e5-a4a5-002590263bf5)

FreeBSD : Ansible -- Command execution on Ansible controller from host (a93c3287-d8fd-11e6-be5c-001fbc0f280f)

FreeBSD : ansible -- enable host key checking in paramiko connection type (a478421e-2059-11e5-a4a5-002590263bf5)

FreeBSD : ansible -- information disclosure flaw (478d4102-2319-4026-b3b2-a57c48f159ac)

FreeBSD : ansible -- Input validation flaw in jinja2 templating system (15a04b9f-47cb-11e7-a853-001fbc0f280f)

FreeBSD : ansible -- local symlink exploits (a6a9f9d5-205c-11e5-a4a5-002590263bf5)

FreeBSD : ansible -- multiple vulnerabilities (72fccfdf-2061-11e5-a4a5-002590263bf5)

FreeBSD : ansible -- multiple vulnerabilities (e308c61a-2060-11e5-a4a5-002590263bf5)

FreeBSD : ansible -- remote code execution vulnerability (2c493ac8-205e-11e5-a4a5-002590263bf5)

FreeBSD : ansible -- use of predictable paths in lxc\_container (253c6889-06f0-11e6-925f-6805ca0b3d42)

FreeBSD : apache (1342)

FreeBSD : apache (1925)

FreeBSD : apache -- ap\_resolve\_env buffer overflow (4d49f4ba-071f-11d9-b45d-000c41e2cdad)

FreeBSD : apache -- apr\_uri\_parse IPv6 address handling vulnerability (762d1c6d-0722-11d9-b45d-000c41e2cdad)

FreeBSD : apache -- Certificate Revocation List (CRL) off-by-one vulnerability (e936d612-253f-11da-bc01-000e0c2e438a)

FreeBSD : Apache -- Denial of service vulnerability in HTTP/2 (e182c076-c189-11e8-a6d2-b499baebfeaf)

FreeBSD : apache -- heap overflow in mod\_proxy (ca6c8f35-0a5f-11d9-ad6f-00061bc2ad93)

FreeBSD : Apache -- HTTP OPTIONS method can leak server memory (76b085e2-9d33-11e7-9260-000c292ee6b8) (Optionsbleed)

FreeBSD : apache -- http request smuggling (651996e0-fe07-11d9-8329-000e0c2e438a)

FreeBSD : Apache -- Insecure LD\_LIBRARY\_PATH handling (de2bc01f-dc44-11e1-9f4d-002354ed89bc)

FreeBSD : apache -- mod\_imap XSS flaw (9fff8dc8-7aa7-11da-bf72-00123f589060)

FreeBSD : apache -- mod\_rewrite buffer overflow vulnerability (dc8c08c7-1e7c-11db-88cf-000c6ec775d9)

FreeBSD : apache -- multiple vulnerabilities (4b7dbfab-4c6b-11e1-bc16-0023ae8e59f0)

FreeBSD : Apache -- Multiple vulnerabilities (b360b120-74b1-11ea-a84a-4c72b94353b5)

FreeBSD : apache -- multiple vulnerabilities (c115271d-602b-11dc-898c-001921ab2fa4)

FreeBSD : apache -- multiple vulnerabilities (c84dc9ad-41f7-11dd-a4f9-00163e000016)

FreeBSD : Apache -- Multiple vulnerabilities (caf545f2-c0d9-11e9-9051-4c72b94353b5) (Internal Data Buffering)

FreeBSD : Apache -- Multiple vulnerabilities (cf2105c6-551b-11e9-b95c-b499baebfeaf)

FreeBSD : apache -- multiple vulnerabilities (f38187e7-2f6e-11e8-8f07-b499baebfeaf)

FreeBSD : apache -- Prevent chunk-size integer overflow on platforms where sizeof(int) < sizeof(long) (cae01d7b-110d-11df-955a-00219b0fc4d8)

FreeBSD : apache -- Range header DoS vulnerability (7f6108d2-cea8-11e0-9d58-0800279895ea)

FreeBSD : apache -- Remote DoS bug in mod\_cache and mod\_dav (28a7310f-9855-11df-8d36-001aa0166822)

FreeBSD : apache -- several vulnerabilities (91ecb546-b1e6-11e3-980f-20cf30e32f6d)

FreeBSD : Apache -- vulnerability (eb888ce5-1f19-11e9-be05-4c72b94353b5)

FreeBSD : apache -- XSS vulnerability (f1892066-0e74-11de-92de-000bcdc1757a)

FreeBSD : Apache 1.3 -- mod\_proxy reverse proxy exposure (d8c901ff-0f0f-11e1-902b-20cf30e32f6d)

FreeBSD : Apache 1.3 IP address access control failure on some 64-bit platforms (09d418db-70fd-11d8-873f-0020ed76ef5a)

FreeBSD : Apache 2 mod\_ssl denial-of-service (492f8896-70fa-11d8-873f-0020ed76ef5a)

FreeBSD : Apache APR -- DoS vulnerabilities (00b296b6-7db1-11e0-96b7-00300582f9fc)

FreeBSD : Apache APR -- DoS vulnerabilities (38560d79-0e42-11e1-902b-20cf30e32f6d)

FreeBSD : Apache APR -- DoS vulnerabilities (99a5590c-857e-11e0-96b7-00300582f9fc)

FreeBSD : Apache Commons FileUpload -- denial of service (61b8c359-4aab-11e6-a7bd-14dae9d210b8)

FreeBSD : Apache Commons FileUpload -- denial of service (DoS) vulnerability (cbceeb49-3bc7-11e6-8e82-002590263bf5)

FreeBSD : Apache httpd -- denial of service in HTTP/2 (cb0bf1ec-bb92-11e6-a9a5-b499baebfeaf)

FreeBSD : Apache httpd -- multiple vulnerabilities (457ce015-67fa-11e7-867f-b499baebfeaf)

FreeBSD : Apache httpd -- multiple vulnerabilities (8b1a50ab-8a8e-11e8-add2-b499baebfeaf)

FreeBSD : Apache httpd -- several vulnerabilities (0c2db2aa-5584-11e7-9a7d-b499baebfeaf)

FreeBSD : Apache httpd -- several vulnerabilities (862d6ab3-c75e-11e6-9f98-20cf30e32f6d) (httpoxy)

FreeBSD : apache mod\_include buffer overflow vulnerability (6e6a6b8a-2fde-11d9-b3a2-0050fc56d258)

FreeBSD : Apache OpenOffice -- multiple vulnerabilities (27229c67-b8ff-11e7-9f79-ac9e174be3af)

FreeBSD : Apache OpenOffice 4.1.2 -- Memory Corruption Vulnerability (Impress Presentations) (72f71e26-4f69-11e6-ac37-ac9e174be3af)

FreeBSD : Apache Traffic Server -- heap overflow vulnerability (acab2f88-7490-11e1-865f-00e0814cab4e)

FreeBSD : apache+mod\_ssl\* (1721)

FreeBSD : apache+mod\_ssl\* (1778)

FreeBSD : apache+mod\_ssl\* (2092)

FreeBSD : Apache-SSL optional client certificate vulnerability (7557a2b1-5d63-11d8-80e3-0020ed76ef5a)

FreeBSD : apache-xml-security-c -- heap overflow (279e5f4b-d823-11e2-928e-08002798f6ff)

FreeBSD : apache-xml-security-c -- heap overflow during XPointer evaluation (81da673e-dfe1-11e2-9389-08002798f6ff)

FreeBSD : apache13-modssl -- format string vulnerability in proxy support (18974c8a-1fbd-11d9-814e-0001020eed82)

FreeBSD : apache2 -- SSL remote DoS (7b81fc47-239f-11d9-814e-0001020eed82)

FreeBSD : apache2 multiple space header denial-of-service vulnerability (282dfea0-3378-11d9-b404-000c6e8f12ef)

FreeBSD : apache22 -- chunk header parsing defect (29083f8e-2ca8-11e5-86ff-14dae9d210b8)

FreeBSD : apache22 -- several vulnerabilities (65539c54-2517-11e2-b9d6-20cf30e32f6d)

FreeBSD : apache22 -- several vulnerabilities (9c88d8a8-8372-11e2-a010-20cf30e32f6d)

FreeBSD : apache22 -- several vulnerabilities (e15f2356-9139-11de-8f42-001aa0166822)

FreeBSD : apache22 -- several vulnerabilities (f3d24aee-e5ad-11e2-b183-20cf30e32f6d)

FreeBSD : apache22 -- several vulnerabilities (f927e06c-1109-11e4-b090-20cf30e32f6d)

FreeBSD : apache24 -- multiple vulnerabilities (a12494c1-2af4-11e5-86ff-14dae9d210b8)

FreeBSD : apache24 -- several vulnerabilities (4364e1f1-0f44-11e4-b090-20cf30e32f6d)

FreeBSD : apache24 -- several vulnerabilities (5804b9d4-a959-11e4-9363-20cf30e32f6d)

FreeBSD : apache24 -- several vulnerabilities (ca4d63fb-f15c-11e2-b183-20cf30e32f6d)

FreeBSD : apache24 -- X509 Client certificate based authentication can be bypassed when HTTP/2 is used (e9d1e040-42c9-11e6-9608-20cf30e32f6d)

FreeBSD : apr -- multiple vulnerabilities (eb9212f7-526b-11de-bbf2-001b77d09812)

FreeBSD : apr -- multiple vunerabilities (dd943fbb-d0fe-11df-95a8-00219b0fc4d8)

FreeBSD : Arbitrary code execution via a format string vulnerability in jftpgw (65a17a3f-ed6e-11d8-aff1-00061bc2ad93)

FreeBSD : arj -- multiple vulnerabilities (b95e5674-b4d6-11e7-b895-0cc47a494882)

FreeBSD : asterisk -- AMI user could execute system commands (49b61ab6-0d04-11ea-87ca-001999f8d30b)

FreeBSD : asterisk -- Asterisk Susceptibility to POODLE Vulnerability (76c7a0f5-5928-11e4-adc7-001999f8d30b) (POODLE)

FreeBSD : asterisk -- Authentication Bypass (c0b13887-be44-11e6-b04f-001999f8d30b)

FreeBSD : asterisk -- Buffer overflow in CDR's set user (356b02e9-1954-11e7-9608-001999f8d30b)

FreeBSD : asterisk -- Buffer overflow in CDR's set user (ab04cb0b-c533-11e7-8da5-001999f8d30b)

FreeBSD : asterisk -- Buffer overflow in pjproject header parsing can cause crash in Asterisk (19b052c9-c533-11e7-8da5-001999f8d30b)

FreeBSD : asterisk -- Buffer Overrun in PJSIP transaction layer (0537afa3-3ce0-11e7-bf9d-001999f8d30b)

FreeBSD : asterisk -- Crash in PJSIP resource when missing a contact header (2a3bc6ac-e7c6-11e7-a90b-001999f8d30b)

FreeBSD : asterisk -- Crash on ACK from unknown endpoint (7fda7920-7603-11e6-b362-001999f8d30b)

FreeBSD : asterisk -- Crash on SDP offer or answer from endpoint using Opus (9e6640fe-be3a-11e6-b04f-001999f8d30b)

FreeBSD : asterisk -- Crash when negotiating for T.38 with a declined stream (d94c08d2-d079-11e9-8f1a-001999f8d30b)

FreeBSD : asterisk -- denial of service vulnerability, local system access (8b683bea-d49c-11da-a672-000e0c2e438a)

FreeBSD : asterisk -- DOS Vulnerability in Asterisk chan\_skinny (e91cf90c-d6dd-11e7-9d10-001999f8d30b)

FreeBSD : asterisk -- Exploitable Stack and Heap Array Overflows (65d16342-3ec8-11e0-9df7-001c42d23634)

FreeBSD : asterisk -- Exploitable Stack Buffer Overflow (5ab9fb2a-23a5-11e0-a835-0003ba02bf30)

FreeBSD : asterisk -- File descriptor leak when incompatible codecs are offered (2eeb6652-a7a6-11e4-96ba-001999f8d30b)

FreeBSD : asterisk -- Infinite loop when reading iostreams (f14ce57f-6dc8-11e8-a671-001999f8d30b)

FreeBSD : asterisk -- Long Contact URIs in REGISTER requests can crash Asterisk (ee50726e-0319-11e6-aa86-001999f8d30b)

FreeBSD : asterisk -- Memory exhaustion on short SCCP packets (fab87bff-3ce5-11e7-bf9d-001999f8d30b)

FreeBSD : asterisk -- Memory/File Descriptor/RTP leak in pjsip session resource (be261737-c535-11e7-8da5-001999f8d30b)

FreeBSD : asterisk -- Mitigation for libcURL HTTP request injection vulnerability (7656fc62-a7a7-11e4-96ba-001999f8d30b)

FreeBSD : asterisk -- multiple vulnerabilities (03159886-a8a3-11e3-8f36-0025905a4771)

FreeBSD : asterisk -- multiple vulnerabilities (0c39bafc-6771-11e3-868f-0025905a4771)

FreeBSD : asterisk -- multiple vulnerabilities (0d530174-6eef-11e1-afd6-14dae9ebcf89)

FreeBSD : asterisk -- multiple vulnerabilities (1c5abbe2-8d7f-11e1-a374-14dae9ebcf89)

FreeBSD : asterisk -- multiple vulnerabilities (359f615d-a9e1-11e1-8a66-14dae9ebcf89)

FreeBSD : Asterisk -- multiple vulnerabilities (3c7d565a-6c64-11e0-813a-6c626dd55a41)

FreeBSD : Asterisk -- multiple vulnerabilities (40544e8c-9f7b-11e0-9bec-6c626dd55a41)

FreeBSD : asterisk -- multiple vulnerabilities (4c1ac2dd-c788-11e1-be25-14dae9ebcf89)

FreeBSD : asterisk -- multiple vulnerabilities (4c53f007-f2ed-11e1-a215-14dae9ebcf89)

FreeBSD : asterisk -- Multiple vulnerabilities (559f3d1b-cb1d-11e5-80a4-001999f8d30b) (BEAST)

FreeBSD : asterisk -- Multiple vulnerabilities (7bfd797c-716d-11e4-b008-001999f8d30b)

FreeBSD : asterisk -- multiple vulnerabilities (933654ce-17b8-11e8-90b8-001999f8d30b)

FreeBSD : asterisk -- Multiple vulnerabilities (a92ed304-716c-11e4-b008-001999f8d30b)

FreeBSD : asterisk -- Multiple Vulnerabilities (bb389137-21fb-11e1-89b4-001ec9578670)

FreeBSD : asterisk -- Multiple Vulnerabilities (bfe9c75e-5028-11e0-b2d2-00215c6a37bb)

FreeBSD : asterisk -- multiple vulnerabilities (daf0a339-9850-11e2-879e-d43d7e0c7c02)

FreeBSD : asterisk -- multiple vulnerabilities (f109b02f-f5a4-11e3-82e9-00a098b18457)

FreeBSD : asterisk -- multiple vulnerabilities (f7c87a8a-55d5-11e2-a255-c8600054b392)

FreeBSD : asterisk -- multiple vulnerabilities (fd2bf3b5-1001-11e3-ba94-0025905a4771)

FreeBSD : asterisk -- PJSIP endpoint presence disclosure when using ACL (0137167b-6dca-11e8-a671-001999f8d30b)

FreeBSD : asterisk -- Re-invite with T.38 and malformed SDP causes crash (94c6951a-0d04-11ea-87ca-001999f8d30b)

FreeBSD : asterisk -- Remote Crash Vulerability in res\_pjsip (ec1df2a1-8ee6-11e7-8be8-001999f8d30b)

FreeBSD : asterisk -- Remote crash vulnerability (34ce5817-8d56-11e0-b5a2-6c626dd55a41)

FreeBSD : asterisk -- remote crash vulnerability (3c8d1e5b-b673-11e1-be25-14dae9ebcf89)

FreeBSD : asterisk -- Remote crash vulnerability DNS SRV and NAPTR lookups (c6fb2734-e835-11e8-b14b-001999f8d30b)

FreeBSD : asterisk -- Remote Crash Vulnerability in audio transcoding (7d53d8da-d07a-11e9-8f1a-001999f8d30b)

FreeBSD : asterisk -- Remote Crash Vulnerability in chan\_sip channel driver (e9d2e981-a46d-11e9-bed9-001999f8d30b)

FreeBSD : asterisk -- Remote crash vulnerability in HTTP websocket upgrade (77f67b46-bd75-11e8-81b6-001999f8d30b)

FreeBSD : asterisk -- Remote Crash Vulnerability in RTCP Stack (4a67450a-e044-11e7-accc-001999f8d30b)

FreeBSD : asterisk -- remote crash vulnerability in SIP channel driver (a95092a6-f8f1-11e0-a7ea-00215c6a37bb)

FreeBSD : asterisk -- Remote Crash Vulnerability in WebSocket Server (94268da0-8118-11e4-a180-001999f8d30b)

FreeBSD : asterisk -- Remote crash vulnerability with MESSAGE messages (818b2bcb-a46f-11e9-bed9-001999f8d30b)

FreeBSD : asterisk -- Remote crash vulnerability with SDP protocol violation (be0e3817-3bfe-11e9-9cd6-001999f8d30b)

FreeBSD : asterisk -- remote heap overwrite vulnerability (1c0def84-5fb1-11db-b2e9-0008c79fa3d2)

FreeBSD : asterisk -- Remotely triggered crash (e60d9e65-3f6b-11e4-ad16-001999f8d30b)

FreeBSD : asterisk -- RTP Resource Exhaustion (5cb18881-7604-11e6-b362-001999f8d30b)

FreeBSD : asterisk -- RTP/RTCP information leak (c2ea3b31-9d75-11e7-bb13-001999f8d30b)

FreeBSD : asterisk -- SIP request can change address of a SIP peer (a8d94711-0d03-11ea-87ca-001999f8d30b)

FreeBSD : asterisk -- SRTP Video Remote Crash Vulnerability (dd698b76-42f7-11e1-a1b6-14dae9ebcf89)

FreeBSD : asterisk -- TLS Certificate Common name NULL byte exploit (5fee3f02-de37-11e4-b7c3-001999f8d30b)

FreeBSD : asterisk -- Unauthorized data disclosure and shell access command injection in app\_minivm (c599f95c-8ee5-11e7-8be8-001999f8d30b)

FreeBSD : asterisk and pjsip -- multiple vulnerabilities (f9f5c5a2-17b5-11e8-90b8-001999f8d30b)

FreeBSD : atheme-services -- multiple vulnerabilities (e47ab5db-c333-11e6-ae1b-002590263bf5)

FreeBSD : atutor -- multiple vulnerabilities (00cb1469-4afc-11e6-97ea-002590263bf5)

FreeBSD : atutor -- multiple vulnerabilities (ffa8ca79-4afb-11e6-97ea-002590263bf5)

FreeBSD : automake -- Insecure 'distcheck' recipe granted world-writable distdir (36235c38-e0a8-11e1-9f4d-002354ed89bc)

FreeBSD : avahi -- denial of service (8b986a05-4dbe-11e0-8b9a-02e0184b8d35)

FreeBSD : avidemux26 -- multiple vulnerabilities in bundled FFmpeg (022255be-0895-11e5-a242-5404a68ad561)

FreeBSD : awstats -- arbitrary code execution vulnerability (e86fbb5f-0d04-11da-bc08-0001020eed82)

FreeBSD : awstats -- arbitrary command execution (fdad8a87-7f94-11d9-a9e7-0001020eed82)

FreeBSD : awstats -- arbitrary command execution vulnerability (2df297a2-dc74-11da-a22b-000c6ec775d9)

FreeBSD : awstats -- arbitrary commands execution vulnerability (ce6ce2f8-34ac-11e0-8103-00215c6a37bb)

FreeBSD : awstats -- multiple XSS vulnerabilities (27d78386-d35f-11dd-b800-001b77d09812)

FreeBSD : awstats -- remote code execution (4055aee5-f4c6-11e7-95f2-005056925db4)

FreeBSD : awstats -- remote command execution vulnerability (0f5a2b4d-694b-11d9-a9e7-0001020eed82)

FreeBSD : axel -- remote buffer overflow (0163b498-af54-11d9-acd0-000854d03344)

FreeBSD : Axis2 -- Security vulnerabilities on dependency Apache HttpClient (ac18046c-9b08-11e6-8011-005056925db4)

FreeBSD : Axis2 -- Security vulnerability on dependency Apache Commons FileUpload (c1265e85-7c95-11e7-93af-005056925db4)

FreeBSD : Axis2 -- XSS (XSS) vulnerability (0baadc45-92d0-11e6-8011-005056925db4)

FreeBSD : bacula -- Console ACL Bypass (143f6932-fedb-11e1-ad4a-003067b2972c)

FreeBSD : base -- PHP SQL injection vulnerability (f38c87a5-4a3e-11da-8ba2-0004614cc33d)

FreeBSD : bash -- out-of-bounds memory access in parser (4a4e9f88-491c-11e4-ae2c-c80aa9043978)

FreeBSD : bash -- remote code execution (512d1301-49b9-11e4-ae2c-c80aa9043978) (Shellshock)

FreeBSD : bash -- remote code execution vulnerability (71ad81da-4414-11e4-a33e-3c970e169bc2) (Shellshock)

FreeBSD : bchunk -- access violation near NULL on destination operand and crash (279f682c-0e9e-11e8-83e7-485b3931c969)

FreeBSD : bchunk -- heap-based buffer overflow (with invalid free) and crash (8ba2819c-0e9d-11e8-83e7-485b3931c969)

FreeBSD : bchunk -- heap-based buffer overflow and crash (1ec1c59b-0e98-11e8-83e7-485b3931c969)

FreeBSD : bidwatcher -- format string vulnerability (74c86a29-81ef-11d9-a9e7-0001020eed82)

FreeBSD : bind -- buffer overrun vulnerability (947f4b14-1c89-11da-bc01-000e0c2e438a)

FreeBSD : bind -- denial of service vulnerability (2c5e7e23-5248-11e5-9ad8-14dae9d210b8)

FreeBSD : bind -- denial of service vulnerability (314830d8-bf91-11e5-96d6-14dae9d210b8)

FreeBSD : bind -- denial of service vulnerability (58033a95-bba8-11e4-88ae-d050992ecde8)

FreeBSD : bind -- denial of service vulnerability (731cdeaa-3564-11e5-9970-14dae9d210b8)

FreeBSD : bind -- denial of service vulnerability (7943e521-f648-11e2-8607-3c970e169bc2)

FreeBSD : bind -- denial of service vulnerability (7a31e0de-5b6d-11e6-b334-002590263bf5)

FreeBSD : bind -- denial of service vulnerability (ab3e98d9-8175-11e4-907d-d050992ecde8)

FreeBSD : bind -- denial of service vulnerability (b4578647-c12b-11e5-96d6-14dae9d210b8)

FreeBSD : bind -- denial of service vulnerability (c9075321-f483-11e5-92ce-002590263bf5)

FreeBSD : bind -- denial of service vulnerability (cb252f01-7c43-11e3-b0a6-005056a37f68)

FreeBSD : bind -- denial of service vulnerability (cba246d2-f483-11e5-92ce-002590263bf5)

FreeBSD : bind -- denial of service vulnerability (cd409df7-f483-11e5-92ce-002590263bf5)

FreeBSD : bind -- denial of service vulnerability (eaf3b255-5245-11e5-9ad8-14dae9d210b8)

FreeBSD : BIND -- Dynamic update message remote DoS (83725c91-7c7e-11de-9672-00e0815b8da8)

FreeBSD : BIND -- Large RRSIG RRsets and Negative Caching DoS (1e1421f0-8d6f-11e0-89b4-001ec9578670)

FreeBSD : bind -- Multiple Denial of Service vulnerabilities (3cb6f059-c69d-11db-9f82-000e0c2e438a)

FreeBSD : BIND -- multiple vulnerabilities (94599fe0-5ca3-11e8-8be1-d05099c0ae8c)

FreeBSD : bind -- multiple vulnerabilities (a8ec4db7-a398-11e5-85e9-14dae9d210b8)

FreeBSD : BIND -- multiple vulnerabilities (c6861494-1ffb-11e7-934d-d05099c0ae8c)

FreeBSD : BIND -- multiple vulnerabilities (d4c7e9a9-d893-11e6-9b4d-d050996490d0)

FreeBSD : BIND -- Remote Denial of Service vulnerability (0b8d01a4-a0d2-11e6-9ca2-d050996490d0)

FreeBSD : BIND -- Remote Denial of Service vulnerability (c8d902b1-8550-11e6-81e7-d050996490d0)

FreeBSD : BIND -- Remote DOS (90cc1494-10ac-11e1-b3ec-0024e830109b)

FreeBSD : BIND -- Remote DoS against authoritative and recursive servers (fd64188d-a71d-11e0-89b4-001ec9578670)

FreeBSD : BIND -- Remote DoS with certain RPZ configurations (4ccee784-a721-11e0-89b4-001ec9578670)

FreeBSD : BIND,Knot,NSD,PowerDNS -- denial over service via oversized zone transfers (7d08e608-5e95-11e6-b334-002590263bf5)

FreeBSD : bind8 negative cache poison attack (f04cc5cb-2d0b-11d8-beaf-000a95c4d922)

FreeBSD : bind9 -- denial of service (30e4ed7b-1ca6-11da-bc01-000e0c2e438a)

FreeBSD : bind9 -- Denial of Service in named(8) (ef3306fc-8f9b-11db-ab33-000e0c2e438a)

FreeBSD : bip -- buffer overflow (1c4cab30-5468-11e1-9fb7-003067b2972c)

FreeBSD : bitcoin -- denial of service (b50913ce-f4a7-11e1-b135-003067b2972c)

FreeBSD : bitcoin -- denial of service (d7b9a28d-238c-11e5-86ff-14dae9d210b8)

FreeBSD : bitcoin -- Denial of Service and Possible Mining Inflation (40a844bf-c430-11e8-96dc-000743165db0)

FreeBSD : bitlbee -- account recreation security issues (24ec781b-8c11-11dd-9923-0016d325a0ed)

FreeBSD : bitmessage -- remote code execution vulnerability (1a75c84a-11c8-11e8-83e7-485b3931c969)

FreeBSD : bmon -- unsafe set-user-ID application (938f357c-16dd-11d9-bc4a-000c41e2cdad)

FreeBSD : bnbt (1351)

FreeBSD : bnc -- remotely exploitable buffer overflow in getnickuserhost (9be819c6-4633-11d9-a9e7-0001020eed82)

FreeBSD : bogofilter -- heap corruption by invalid base64 input (f524d8e0-3d83-11e2-807a-080027ef73ec)

FreeBSD : bogofilter -- heap corruption through excessively long words (b747b2a9-7be0-11da-8ec4-0002b3b60e4c)

FreeBSD : bogofilter -- heap corruption through malformed input (92140bc9-7bde-11da-8ec4-0002b3b60e4c)

FreeBSD : bogofilter -- heap underrun on malformed base64 input (25ed4ff8-8940-11df-a339-0026189baca3)

FreeBSD : bogofilter -- RFC 2047 decoder denial-of-service vulnerability (f4428842-a583-4a4c-89b7-297c3459a1c3)

FreeBSD : borgbackup -- remote users can override repository restrictions (0d369972-d4ba-11e7-bfca-005056925db4)

FreeBSD : botan -- cryptographic vulnerability (f771880c-31cf-11e6-8e82-002590263bf5)

FreeBSD : botan -- multiple vulnerabilities (ac0900df-31d0-11e6-8e82-002590263bf5)

FreeBSD : Botan BER Decoder vulnerabilities (2004616d-f66c-11e5-b94c-001999f8d30b)

FreeBSD : botan2 -- ECDSA side channel (7762d7ad-2e38-41d2-9785-c51f653ba8bd)

FreeBSD : botan2 -- Side channel during ECC key generation (d8e7e854-17fa-11e9-bef6-6805ca2fa271)

FreeBSD : bro -- 'Magellan' remote code execution vulnerability in bundled sqlite (b80f039d-579e-4b82-95ad-b534a709f220)

FreeBSD : bro -- array bounds and potential DOS issues (d0be41fe-2a20-4633-b057-4e8b25c41780)

FreeBSD : bro -- integer overflow allows remote DOS (044cff62-ed8b-4e72-b102-18a7d58a669f)

FreeBSD : bro -- invalid memory access or heap buffer over-read (55571619-454e-4769-b1e5-28354659e152)

FreeBSD : bro -- multiple memory allocation issues (2f4fd3aa-32f8-4116-92f2-68f05398348e)

FreeBSD : bro -- NULL pointer dereference and Signed integer overflow (f56669f5-d799-4ff5-9174-64a6d571c451)

FreeBSD : bro -- out of bounds write allows remote DOS (746d04dc-507e-4450-911f-4c41e48bb07a)

FreeBSD : bro -- Unsafe integer conversions can cause unintentional code paths to be executed (177fa455-48fc-4ded-ba1b-9975caa7f62a)

FreeBSD : brotli -- buffer overflow (1bcfd963-e483-41b8-ab8e-bad5c3ce49c9)

FreeBSD : bsh -- remote code execution vulnerability (9e5bbffc-d8ac-11e5-b2bd-002590263bf5)

FreeBSD : Buffer overflow in INN control message handling (fd376b8b-41e1-11d8-b096-0020ed76ef5a)

FreeBSD : Buffer overflow in Mutt 1.4 (67c05283-5d62-11d8-80e3-0020ed76ef5a)

FreeBSD : Buffer overflow in pam\_smb password handling (2bcd2d24-24ca-11d8-82e5-0020ed76ef5a)

FreeBSD : Buffer overflow in Squid NTLM authentication helper (6f955451-ba54-11d8-b88c-000d610a3b12)

FreeBSD : Buffer overflows and format string bugs in Emil (ce46b93a-80f2-11d8-9645-0020ed76ef5a)

FreeBSD : Buffer overflows in libmcrypt (c4b7badf-24ca-11d8-82e5-0020ed76ef5a)

FreeBSD : Buffer overflows in XFree86 servers (3837f462-5d6b-11d8-80e3-0020ed76ef5a)

FreeBSD : bugzilla (1783)

FreeBSD : bugzilla -- 'createmailregexp' security bypass vulnerability (f8d3689e-6770-11dc-8be8-02e0185f8d72)

FreeBSD : bugzilla -- Cross Site Request Forgery (9defb2d6-1404-11e4-8cae-20cf30e32f6d)

FreeBSD : bugzilla -- Cross-Site Request Forgery (608ed765-c700-11e3-848c-20cf30e32f6d)

FreeBSD : Bugzilla -- Directory Traversal in importxml.pl (1d96305d-6ae6-11dd-91d5-000c29d47fd7)

FreeBSD : bugzilla -- information disclosure (f1331504-8849-11df-89b8-00151735203a)

FreeBSD : bugzilla -- information disclosure, denial of service (8cbf4d65-af9a-11df-89b8-00151735203a)

FreeBSD : bugzilla -- information leak (696053c6-0f50-11df-a628-001517351c22)

FreeBSD : bugzilla -- information leak (92ca92c1-d859-11de-89f9-001517351c22)

FreeBSD : bugzilla -- multiple serious vulnerabilities (c8c927e5-2891-11e0-8f26-00151735203a)

FreeBSD : bugzilla -- multiple vulnerabilities (09c87973-8b9d-11e1-b393-20cf30e32f6d)

FreeBSD : bugzilla -- multiple vulnerabilities (0c7a3ee2-3654-11e1-b404-20cf30e32f6d)

FreeBSD : bugzilla -- multiple vulnerabilities (1c8a039b-7b23-11e2-b17b-20cf30e32f6d)

FreeBSD : bugzilla -- multiple vulnerabilities (2b841f88-2e8d-11e2-ad21-20cf30e32f6d)

FreeBSD : bugzilla -- multiple vulnerabilities (309542b5-50b9-11e1-b0d8-00151735203a)

FreeBSD : bugzilla -- multiple vulnerabilities (46f7b598-a781-11da-906a-fde5cdde365e)

FreeBSD : bugzilla -- multiple vulnerabilities (58253655-d82c-11e1-907c-20cf30e32f6d)

FreeBSD : bugzilla -- multiple vulnerabilities (6ad18fe5-f469-11e1-920d-20cf30e32f6d)

FreeBSD : bugzilla -- multiple vulnerabilities (6d68618a-7199-11db-a2ad-000c6ec775d9)

FreeBSD : bugzilla -- multiple vulnerabilities (6e33f4ab-efed-11d9-8310-0001020eed82)

FreeBSD : bugzilla -- multiple vulnerabilities (75231c63-f6a2-499d-8e27-787773bda284)

FreeBSD : bugzilla -- multiple vulnerabilities (dc8741b9-c5d5-11e0-8a8e-00151735203a)

FreeBSD : bugzilla -- multiple vulnerabilities (e135f0c9-375f-11e3-80b7-20cf30e32f6d)

FreeBSD : bugzilla -- product name information leak (d67b517d-8214-11de-88ea-001a4d49522b)

FreeBSD : bugzilla -- Social Engineering (60bfa396-c702-11e3-848c-20cf30e32f6d)

FreeBSD : bugzilla -- two SQL injections, sensitive data exposure (b9ec7fe3-a38a-11de-9c6b-003048818f40)

FreeBSD : bugzilla -- XSS vulnerability (97c3a452-6e36-11d9-8324-000a95bc6fae)

FreeBSD : bugzilla Cross-Site Request Forgery (7f448dc1-82ca-11e1-b393-20cf30e32f6d)

FreeBSD : Bugzilla multiple security issues (b6587341-4d88-11e4-aef9-20cf30e32f6d)

FreeBSD : Bugzilla multiple security issues (dc2d76df-a595-11e4-9363-20cf30e32f6d)

FreeBSD : Bugzilla security issues (036d6c38-1c5b-11e6-b9e0-20cf30e32f6d)

FreeBSD : Bugzilla security issues (22283b8c-13c5-11e8-a861-20cf30e32f6d)

FreeBSD : Bugzilla security issues (54075861-a95a-11e5-8b40-20cf30e32f6d)

FreeBSD : Bugzilla security issues (ea893f06-5a92-11e5-98c0-20cf30e32f6d)

FreeBSD : buildbot -- CRLF injection in Buildbot login and logout redirect code (5536ea5f-6814-11e9-a8f7-0050562a4d7b)

FreeBSD : buildbot -- OAuth Authentication Vulnerability (ada8db8a-8471-11e9-8170-0050562a4d7b)

FreeBSD : bzip2 -- crash with certain malformed archive files (063399fc-f6d6-11dc-bcee-001c2514716c)

FreeBSD : bzip2 -- denial of service and permission race vulnerabilities (197f444f-e8ef-11d9-b875-0001020eed82)

FreeBSD : bzip2 -- integer overflow vulnerability (0ddb57a9-da20-4e99-b048-4366092f3d31)

FreeBSD : bzip2 -- multiple issues (4b6cb45d-881e-447a-a4e0-c97a954ea758)

FreeBSD : c-ares -- DNS Cache Poisoning Vulnerability (70ae62b0-16b0-11dc-b803-0016179b2dd5)

FreeBSD : ca\_root\_nss -- extraction of explicitly-untrusted certificates into trust bundle (1b27af46-d6f6-11e0-89a6-080027ef73ec)

FreeBSD : cabextract -- directory traversal with UTF-8 symbols in filenames (cfb12f02-06e1-11e5-8fda-002590263bf5)

FreeBSD : cabextract -- insecure directory handling (61480a9a-22b2-11d9-814e-0001020eed82)

FreeBSD : cacti -- ADOdb 'server.php' Insecure Test Script Security Issue (79c1154d-d5a5-11da-8098-00123ffe8333)

FreeBSD : cacti -- allow remote attackers to execute arbitrary SQL commands (b3b8d491-0fbb-11e3-8c50-1c6f65c11ee6)

FreeBSD : cacti -- Authenticated users may bypass authorization checks (ed18aa92-e4f4-11e9-b6fa-3085a9a95629)

FreeBSD : cacti -- multiple security vulnerabilities (a0e74731-181b-11e5-a1cf-002590263bf5)

FreeBSD : cacti -- Multiple security vulnerabilities have been discovered (dea7df85-d96c-11dc-9bfc-000e0c092e7a)

FreeBSD : cacti -- multiple vulnerabilities (1cf00643-ed8a-11d9-8310-0001020eed82)

FreeBSD : cacti -- Multiple vulnerabilities (41da2ba4-a24e-11db-bd24-000f3dcc6a5d)

FreeBSD : cacti -- multiple vulnerabilities (6167b341-250c-11e6-a6fb-003048f2e514)

FreeBSD : cacti -- multiple vulnerabilities (86224a04-26de-11ea-97f2-001a8c5c04b6)

FreeBSD : cacti -- multiple vulnerabilities (db3301be-e01c-11e5-b2bd-002590263bf5)

FreeBSD : cacti -- multiple vulnerabilities (db570002-ce06-11e7-804e-c85b763a2f96)

FreeBSD : cacti -- multiple vulnerabilities (e02e6a4e-6b26-11df-96b2-0015587e2cc1)

FreeBSD : cacti -- multiple vulnerabilities (e2b564fc-7462-11ea-af63-38d547003487)

FreeBSD : cacti -- Multiple vulnerabilities (f08e2c15-ffc9-11e0-b0f3-bcaec565249c)

FreeBSD : cacti -- Multiple XSS and SQL injection vulnerabilities (0bfda05f-2e6f-11e5-a4a5-002590263bf5)

FreeBSD : cacti -- Multiple XSS and SQL injection vulnerabilities (a3929112-181b-11e5-a1cf-002590263bf5)

FreeBSD : cacti -- potential SQL injection and XSS attacks (96948a6a-e239-11d9-83cf-0010dc5df42d)

FreeBSD : cacti -- SQL injection (ca543e06-207a-11d9-814e-0001020eed82)

FreeBSD : cacti -- SQL injection and command execution vulnerabilities (5198ef84-4fdc-11df-83fb-0015587e2cc1)

FreeBSD : cacti -- SQL injection vulnerabilities (bb961ff3-b3a4-11e5-8255-5453ed2e2b49)

FreeBSD : Cacti -- XSS (XSS) vulnerability in auth\_profile.php (f86d0e5d-7467-11e7-93af-005056925db4)

FreeBSD : Cacti -- XSS (XSS) vulnerability in link.php (dc3c66e8-6a18-11e7-93af-005056925db4)

FreeBSD : cacti -- XSS issue (e1cb9dc9-daa9-44db-adde-e94d900e2f7f)

FreeBSD : cacti -- XSS issues (04104985-d846-11de-84e4-00215af774f0)

FreeBSD : Calligra, KOffice -- input validation failure (aa4d3d73-ef17-11e1-b593-00269ef07d24)

FreeBSD : caml-light -- insecure use of temporary files (9dde9dac-08f4-11e1-af36-003067b2972c)

FreeBSD : cassandra -- remote execution of arbitrary code (607f4d44-0158-11e5-8fda-002590263bf5)

FreeBSD : CCE contains exploitable buffer overflows (a736deab-5d7d-11d8-80e3-0020ed76ef5a)

FreeBSD : cdf3 -- Buffer overflow vulnerability (c4f31e16-6e33-11dd-8eb7-0011098ad87f)

FreeBSD : cdrdao -- unspecified privilege escalation vulnerability (d51a7e6e-c546-11d9-9aed-000e0c2e438a)

FreeBSD : cdrtools-cjk (2513)

FreeBSD : cfengine -- arbitrary file overwriting vulnerability (8688d5cd-328c-11da-a263-0001020eed82)

FreeBSD : cfengine2 (2448)

FreeBSD : cgit -- directory traversal vulnerability (06c4a79b-981d-11e8-b460-9c5c8e75236a)

FreeBSD : cgit -- multiple vulnerabilities (62c0dbbd-bfce-11e5-b5fe-002590263bf5)

FreeBSD : cgiwrap -- XSS Vulnerability (bc6a7e79-e111-11dd-afcd-00e0815b8da8)

FreeBSD : ChaSen -- buffer overflow (972837fc-c304-11e3-8758-00262d5ed8ee)

FreeBSD : chicken -- buffer overrun in substring-index[-ci] (e7b7f2b5-177a-11e5-ad33-f8d111029e6a)

FreeBSD : chicken -- multiple vulnerabilities (5a771686-9e33-11e8-8b2d-9cf7a8059466)

FreeBSD : chicken -- multiple vulnerabilities (c6932dd4-eaff-11e6-9ac1-a4badb2f4699)

FreeBSD : chicken -- Potential buffer overrun in string-translate\* (0da404ad-1891-11e5-a1cf-002590263bf5)

FreeBSD : ChiTeX/ChiLaTeX unsafe set-user-id root (49ad1bf8-5d7e-11d8-80e3-0020ed76ef5a)

FreeBSD : chora (2069)

FreeBSD : chromium -- Errant plug-in load and GPU process memory corruption (ab1f515d-6b69-11e1-8288-00262d5ed8ee)

FreeBSD : chromium -- Incorrect handling of CSP header (4cb49a23-6c89-11e8-8b33-e8e0b747a45a)

FreeBSD : chromium -- multiple memory corruption issues (e62ab2af-4df4-11e3-b0cf-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (057130e6-7f61-11e1-8a43-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (09e83f7f-1326-11e2-afe3-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (0b0fb9b0-f0fb-11e3-9bcd-000c6e25e3e9)

FreeBSD : chromium -- multiple vulnerabilities (0e425bb7-64f2-11e5-b2fd-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (1449af37-9eba-11e1-b9c1-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (1a1aef8e-3894-11e1-8b5c-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (1a6bbb95-24b8-11e6-bd31-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (1d951e85-ffdb-11e7-8b91-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (209c068d-28be-11e2-9160-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (210f80b9-ede4-11e4-81c4-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (219d0bfd-a915-11e1-b519-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (2f5ff968-5829-11e1-8288-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (330106da-7406-11e1-a1d7-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (33d73d59-4677-11e1-88cd-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (358133b5-c2b9-11e2-a738-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (36034227-cf81-11e5-9c2b-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (3718833e-0d27-11e4-89db-000c6e25e3e9)

FreeBSD : chromium -- multiple vulnerabilities (371bbea9-3836-4832-9e70-e8e928727f8c)

FreeBSD : chromium -- multiple vulnerabilities (3b80104f-e96c-11e2-8bac-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (3bfc7016-4bcc-11e3-b0cf-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (40d5ab37-85f2-11e2-b528-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (427b0f58-644c-11e8-9e1b-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (46bd747b-5b84-11e2-b06d-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (4865d189-cd62-11e2-ae11-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (4b9ca994-e3d9-11e6-813d-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (4d64fc61-3878-11e2-a4eb-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (4dfafa16-24ba-11e6-bd31-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (51f84e28-444e-11e2-8306-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (52f4b48b-4ac3-11e7-99aa-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (546d4dd4-10ea-11e9-b407-080027ef1a23)

FreeBSD : chromium -- multiple vulnerabilities (548f74bd-993c-11e5-956b-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (5acf4638-7e2c-11e3-9fba-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (5af51ae9-3acd-11e2-a4eb-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (5bae2ab4-0820-11e2-be5f-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (5c288f68-c7ca-4c0d-b7dc-1ec6295200b3)

FreeBSD : chromium -- multiple vulnerabilities (603fe0a1-bb26-11e6-8e5a-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (60bbe12c-e2c1-11e1-a8ca-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (64f3872b-e05d-11e3-9dd4-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (653a8059-7c49-11e6-9242-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (6887828f-0229-11e0-b84d-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (68ac6266-25c3-11e1-b63a-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (69098c5c-fc4b-11e2-8ad0-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (6d8505f0-0614-11e6-b39c-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (6e3b700a-7ca3-11ea-b594-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (6fae9fe1-5048-11e6-8aa7-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (710cd5d5-35cb-11e3-85f9-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (72c145df-a1e0-11e5-8ad0-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (769ba449-79e1-11e6-bf75-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (79356040-5da4-11e3-829e-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (7cf058d8-158d-11e7-ba2c-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (7cf25a0c-d031-11e3-947b-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (7d138476-7710-11e7-88a1-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (7da1da96-24bb-11e6-bd31-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (8301c04d-71df-11e5-9fcb-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (8505e013-c2b3-11e4-875d-000c6e25e3e9)

FreeBSD : chromium -- multiple vulnerabilities (88d00176-058e-11ea-bd1c-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (8be8ca39-ae70-4422-bf1a-d8fae6911c5e)

FreeBSD : chromium -- multiple vulnerabilities (8d03202c-6559-11e2-a389-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (8e986b2b-1baa-11e8-a944-54ee754af08e)

FreeBSD : chromium -- multiple vulnerabilities (9118961b-9fa5-11e6-a265-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (917e5519-9fdd-11e7-8b58-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (94c0ac4f-9388-11e1-b242-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (958b9cee-79da-11e6-bf75-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (95a74a48-2691-11e7-9e2d-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (963413a5-bf50-11e3-a2d6-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (99aef698-66ed-11e1-8288-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (9c135c7e-9fa4-11e6-a265-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (9cb57a06-7517-11ea-b594-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (9d732078-32c7-11e5-b263-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (9dd47fa3-9d53-11e3-b20f-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (a3473f5a-a739-11e6-afaa-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (a505d397-0758-11e7-8d8b-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (a692bffe-b6ad-11e7-a1c2-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (a6eb239f-adbe-11e4-9fce-080027593b9a)

FreeBSD : chromium -- multiple vulnerabilities (a9350df8-5157-11e5-b5c1-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (a9d456b4-fe4c-11e4-ad15-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (ae651a4b-0a42-11e3-ba52-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (b4023753-a4ba-11e3-bec2-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (b57f690e-ecc9-11e4-876c-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (b8f0a391-7910-11e1-8a43-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (b9c525d9-9198-11e8-beba-080027ef1a23)

FreeBSD : chromium -- multiple vulnerabilities (bb7d4791-a5bf-11e5-a0e5-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (bdd48858-9656-11e2-a9a8-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (c039a761-2c29-11e6-8912-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (cdf450fc-db52-11e3-a9fc-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (ce84e136-e2f6-11e1-a8ca-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (d2bbcc01-4ec3-11e4-ab3f-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (d395e44f-6f4f-11e4-a444-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (d59ebed4-34be-11e6-be25-3065ec8fd3ec)

FreeBSD : chromium -- multiple vulnerabilities (df7754c0-2294-11e4-b505-000c6e25e3e9)

FreeBSD : chromium -- multiple vulnerabilities (dfd92cb2-7d48-11e2-ad48-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (e1100e63-92f7-11e7-bd95-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (e264e74e-ffe0-11e7-8b91-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (e30e0c99-a1b7-11e4-b85c-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (e457978b-5484-11e8-9b85-54ee754af08e)

FreeBSD : chromium -- multiple vulnerabilities (e5414d0c-2ade-11e3-821d-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (e6161b65-1187-11e2-afe3-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (ee68923d-f2f5-11e1-8014-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (f0b9049f-88c4-11e5-aed7-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (f53dd5cc-527f-11e7-a772-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (f85fa236-e2a6-412e-b5c7-c42120892de5)

FreeBSD : chromium -- multiple vulnerabilities (f8e72cd4-c66a-11e7-bb17-e8e0b747a45a)

FreeBSD : chromium -- multiple vulnerabilities (f9810c43-87a5-11e3-9214-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (fd5f305d-2d3d-11e4-aa3d-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (fe1976c2-5317-11e1-9e99-00262d5ed8ee)

FreeBSD : chromium -- multiple vulnerabilities (ff922811-c096-11e1-b0f4-00262d5ed8ee)

FreeBSD : chromium -- out of bounds read (82894193-ffd4-11e7-8b91-e8e0b747a45a)

FreeBSD : chromium -- out-of-bounds memory access (ae9cb9b8-a203-11e6-a265-3065ec8fd3ec)

FreeBSD : chromium -- race condition vulnerability (92e345d0-304d-11e7-8359-e8e0b747a45a)

FreeBSD : chromium -- RSA signature malleability in NSS (bd2ef267-4485-11e4-b0b7-00262d5ed8ee)

FreeBSD : chromium -- same origin bypass (368993bb-d685-11e5-8858-00262d5ed8ee)

FreeBSD : chromium -- Stack overflow in V8 (3cd46257-bbc5-11e7-a3bc-e8e0b747a45a)

FreeBSD : chromium -- use after free (25efe05c-7ffc-11ea-b594-3065ec8fd3ec)

FreeBSD : chromium -- use after free (d4fc4599-8f75-11e9-8d9f-3065ec8fd3ec)

FreeBSD : chromium -- Use after free in PDFium (720590df-10eb-11e9-b407-080027ef1a23)

FreeBSD : chromium -- vulnerability (006bee4e-4c49-11e8-9c32-54ee754af08e)

FreeBSD : chromium -- vulnerability (36ff7a74-47b1-11e8-a7d6-54e1ad544088)

FreeBSD : chromium -- vulnerability (3ae21918-31e3-11e8-927b-e8e0b747a45a)

FreeBSD : chromium -- vulnerability (555af074-22b9-11e8-9799-54ee754af08e)

FreeBSD : chromium -- vulnerability (abfc932e-1ba8-11e8-a944-54ee754af08e)

FreeBSD : chromium -- WebKit vulnerability (54bed676-87ce-11e2-b528-00262d5ed8ee)

FreeBSD : chromium -- XSS vulnerability (1015e1fe-69ce-11e1-8288-00262d5ed8ee)

FreeBSD : chrony -- multiple vulnerabilities (c4571ca8-053d-44c9-ab3c-89b1372ad0a5)

FreeBSD : clamav -- arbitrary code execution and DoS vulnerabilities (271498a9-2cd4-11da-a263-0001020eed82)

FreeBSD : clamav -- cabinet file handling DoS vulnerability (d8e1aadd-ee68-11d9-8310-0001020eed82)

FreeBSD : clamav -- CHM Processing Denial of Service (da5c4072-8082-11dd-9c8c-001c2514716c)

FreeBSD : clamav -- CHM unpacker and PE rebuilding vulnerabilities (8012a79d-5d21-11db-bb8d-00123ffe8333)

FreeBSD : clamav -- ClamAV libclamav PE File Integer Overflow Vulnerability (be4b0529-dbaf-11dc-9791-000ea6702141)

FreeBSD : clamav -- Denial-of-Service (DoS) vulnerability (6ade62d9-0f62-11ea-9673-4c72b94353b5)

FreeBSD : clamav -- Denial-of-Service (DoS) vulnerability (e7bc2b99-485a-11ea-bff9-9c5c8e75236a)

FreeBSD : clamav -- Freshclam HTTP Header Buffer Overflow Vulnerability (b088bf48-da3b-11da-93e0-00123ffe8333)

FreeBSD : clamav -- heap overflow vulnerability (342d2e48-26db-11db-9275-000475abc56f)

FreeBSD : clamav -- MS-Expand file handling DoS vulnerability (6d18fe19-ee67-11d9-8310-0001020eed82)

FreeBSD : clamav -- Multipart Nestings Denial of Service (eb5124a4-8a20-11db-b033-00123ffe8333)

FreeBSD : clamav -- multiple remote buffer overflows (1db7ecf5-fd24-11d9-b4d6-0007e900f87b)

FreeBSD : clamav -- multiple remote Denial of Service vulnerabilities (b6f6da57-680a-11dc-b350-001921ab2fa4)

FreeBSD : clamav -- multiple vulnerabilities (3d0428b2-fdfb-11e4-894f-d050996490d0)

FreeBSD : clamav -- Multiple Vulnerabilities (589d8053-0b03-11dd-b4ef-00e07dc4ec84)

FreeBSD : clamav -- Multiple Vulnerabilities (6a5174bd-c580-11da-9110-00123ffe8333)

FreeBSD : clamav -- multiple vulnerabilities (84ce26c3-5769-11e9-abd6-001b217b3468)

FreeBSD : clamav -- multiple vulnerabilities (8b812395-c739-11e8-ab5b-9c5c8e75236a)

FreeBSD : clamav -- multiple vulnerabilities (903654bd-1927-11dc-b8a0-02e0185f8d72)

FreeBSD : clamav -- multiple vulnerabilities (b464f61b-84c7-4e1c-8ad4-6cf9efffd025)

FreeBSD : clamav -- multiple vulnerabilities (d1e9d8c5-839b-11e8-9610-9c5c8e75236a)

FreeBSD : clamav -- multiple vulnerabilities (dbd1f627-c43b-11e9-a923-9c5c8e75236a)

FreeBSD : clamav -- multiple vulnerabilities (eb12ebee-b7af-11e1-b5e0-000c299b62e1)

FreeBSD : clamav -- off-by-one heap overflow in VBA project parser (24b64fb0-af1d-11dd-8a16-001b1116b350)

FreeBSD : clamav -- possible heap overflow in the UPX code (612a34ec-81dc-11da-a043-0002a5c3d308)

FreeBSD : clamav -- zip handling DoS vulnerability (70b62f5e-9e2e-11d9-a256-0001020eed82)

FreeBSD : clamav remote denial-of-service (74a9541d-5d6c-11d8-80e3-0020ed76ef5a)

FreeBSD : claws-mail -- APOP vulnerability (c389d06d-ee57-11db-bd51-0016179b2dd5)

FreeBSD : claws-mail -- insecure temporary file creation (a59afa47-c930-11dc-810c-0016179b2dd5)

FreeBSD : claws-mail -- no bounds checking on the output buffer in conv\_jistoeuc, conv\_euctojis, conv\_sjistoeuc (51358314-bec8-11e5-82cd-bcaec524bf84)

FreeBSD : claws-mail -- POP3 Format String Vulnerability (d9867f50-54d0-11dc-b80b-0016179b2dd5)

FreeBSD : codeigniter -- arbitrary script execution in the new Form Validation class (83574d5a-f828-11dd-9fdf-0050568452ac)

FreeBSD : codeigniter -- file upload class vulnerability (0502c1cb-8f81-11df-a0bb-0050568452ac)

FreeBSD : codeigniter -- input validation bypass (aaedf196-6436-11e7-8b49-002590263bf5)

FreeBSD : codeigniter -- input validation bypass (ef3423e4-d056-11e7-a52c-002590263bf5)

FreeBSD : codeigniter -- multiple vulnerabilities (496160d3-d3be-11e6-ae1b-002590263bf5)

FreeBSD : codeigniter -- multiple vulnerabilities (5e439ee7-d3bd-11e6-ae1b-002590263bf5)

FreeBSD : codeigniter -- multiple vulnerabilities (698403a7-803d-11e5-ab94-002590263bf5)

FreeBSD : codeigniter -- multiple vulnerabilities (71ebbc50-01c1-11e7-ae1b-002590263bf5)

FreeBSD : codeigniter -- multiple vulnerabilities (c21f4e61-6570-11e5-9909-002590263bf5)

FreeBSD : codeigniter -- multiple vulnerabilities (df0144fb-295e-11e7-970f-002590263bf5)

FreeBSD : codeigniter -- multiple vulnerabilities (f838dcb4-656f-11e5-9909-002590263bf5)

FreeBSD : codeigniter -- multiple XSS vulnerabilities (95602550-76cf-11e5-a2a1-002590263bf5)

FreeBSD : codeigniter -- mysql database driver vulnerability (01bce4c6-6571-11e5-9909-002590263bf5)

FreeBSD : codeigniter -- SQL injection vulnerability (5114cd11-6571-11e5-9909-002590263bf5)

FreeBSD : codeigniter -- SQL injection vulnerability (b7d785ea-656d-11e5-9909-002590263bf5)

FreeBSD : collectd -- Network plugin heap overflow (6da45e38-5b55-11e6-8859-000c292ee6b8)

FreeBSD : collectd5 -- Denial of service by sending a signed network packet to a server which is not set up to check signatures (08a2df48-6c6a-11e7-9b01-2047478f2f70)

FreeBSD : comms/hylafax -- Malformed fax sender remote code execution in JPEG support (3df5a920-6edc-11e9-a44b-0050562a4d7b)

FreeBSD : consul -- vulnerability in embedded DNS library (ad2eeab6-ca68-4f06-9325-1937b237df60)

FreeBSD : Containous Traefik -- exposes the configuration and secret (fe818607-b5ff-11e8-856b-485b3931c969)

FreeBSD : coppermine -- 'file' Local File Inclusion Vulnerability (6738977b-e9a5-11da-b9f4-00123ffe8333)

FreeBSD : coppermine -- File Inclusion Vulnerabilities (77cceaef-e9a4-11da-b9f4-00123ffe8333)

FreeBSD : coppermine -- IP spoofing and XSS vulnerability (756db070-b9d4-11d9-ae81-000ae42e9b93)

FreeBSD : coppermine -- Multiple File Extensions Vulnerability (0b628470-e9a6-11da-b9f4-00123ffe8333)

FreeBSD : coppermine -- multiple vulnerabilities (12488805-6773-11dc-8be8-02e0185f8d72)

FreeBSD : coppermine -- Multiple vulnerabilities (6dd5e45c-f084-11e1-8d0f-406186f3d89d)

FreeBSD : coppermine -- multiple vulnerabilities (9f581778-e3d4-11dc-bb89-000bcdc1757a)

FreeBSD : corkscrew -- buffer overflow vulnerability (67a1c3ae-ad69-11df-9be6-0015587e2cc1)

FreeBSD : couchdb -- administrator privilege escalation (1999a215-fc6b-11e8-8a95-ac1f6b67e138)

FreeBSD : couchdb -- administrator privilege escalation (9b19b6df-a4be-11e8-9366-0028f8d09152)

FreeBSD : couchdb -- DOM based XSS via Futon UI (4fb45a1c-c5d0-11e2-8400-001b216147b0)

FreeBSD : couchdb -- multiple vulnerabilities (1e54d140-8493-11e8-a795-0028f8d09152)

FreeBSD : Courier Authentication Library -- SQL Injection (022baf71-38e6-11dd-8d34-00e0815b8da8)

FreeBSD : Courier mail services: remotely exploitable buffer overflows (98bd69c3-834b-11d8-a41f-0020ed76ef5a)

FreeBSD : courier-imap -- format string vulnerability in debug mode (616cf823-f48b-11d8-9837-000c41e2cdad)

FreeBSD : cpio -- multiple vulnerabilities (72ee9707-d7b2-11e4-8d8e-f8b156b6dcc8)

FreeBSD : Critical SQL injection in phpBB (70f5b3c6-80f0-11d8-9645-0020ed76ef5a)

FreeBSD : crossfire-server -- denial of service and remote code execution vulnerability (86cc5c6f-d2b4-11da-a672-000e0c2e438a)

FreeBSD : cryptopp -- multiple vulnerabilities (eab68cff-bc0c-11e6-b2ca-001b3856973b)

FreeBSD : cscope -- buffer overflow (91a2066b-5ab6-11de-bc9b-0030843d3802)

FreeBSD : cscope -- buffer overflow vulnerabilities (72d8df84-ea6d-11da-8a53-00123ffe8333)

FreeBSD : cscope -- Buffer Overflow Vulnerabilities (74ff10f6-520f-11db-8f1a-000a48049292)

FreeBSD : cscope -- multiple buffer overflows (c14aa48c-5ab7-11de-bc9b-0030843d3802)

FreeBSD : cscope -- symlink attack vulnerability (a7bfd423-484f-11d9-a9e7-0001020eed82)

FreeBSD : cups -- Incomplete SSL Negotiation Denial of Service (39988ee8-1918-11dc-b6bd-0016179b2dd5)

FreeBSD : CUPS -- local information disclosure (30cea6be-1d0c-11d9-814e-0001020eed82)

FreeBSD : CUPS -- multiple vulnerabilities (60e991ac-c013-11e9-b662-001cc0382b2f)

FreeBSD : cups -- multiple vulnerabilities (a40ec970-0efa-11e5-90e4-d050996490d0)

FreeBSD : cups -- multiple vulnerabilities (ce29ce1d-971a-11dd-ab7e-001c2514716c)

FreeBSD : cups -- off-by-one buffer overflow (8dd9722c-8e97-11dc-b8f6-001c2514716c)

FreeBSD : cups -- potential buffer overflow in PNG reading code (87106b67-be13-11dd-a578-0030843d3802)

FreeBSD : cups -- print queue browser denial-of-service (05dcf751-0733-11d9-b45d-000c41e2cdad)

FreeBSD : cups -- remote code execution and DNS rebinding (736e55bc-39bb-11de-a493-001b77d09812)

FreeBSD : cups-base -- CUPS server remote DoS vulnerability (990cf07e-6988-11d9-a9e7-0001020eed82)

FreeBSD : cups-base -- HPGL buffer overflow vulnerability (40a3bca2-6809-11d9-a9e7-0001020eed82)

FreeBSD : cups-filters -- buffer overflow in texttopdf size allocation (b19da422-1e02-11e5-b43d-002590263bf5)

FreeBSD : cups-filters -- code execution (6dbae1a8-a4e6-11e5-b864-14dae9d210b8)

FreeBSD : cups-filters -- code execution (7329938b-a4e6-11e5-b864-14dae9d210b8)

FreeBSD : cups-filters -- texttopdf integer overflow (bf1d9331-21b6-11e5-86ff-14dae9d210b8)

FreeBSD : cups-lpr -- lppasswd multiple vulnerabilities (7850a238-680a-11d9-a9e7-0001020eed82)

FreeBSD : curl -- authentication buffer overflow vulnerability (96df5fd0-8900-11d9-aa18-0001020eed82)

FreeBSD : cURL -- buffer overflow (42880202-c81c-11e6-a9a5-b499baebfeaf)

FreeBSD : curl -- Credentials not checked (8b27f1bc-c509-11e5-a95f-b499baebfeaf)

FreeBSD : curl -- cURL/libcURL Location: Redirect URLs Security Bypass (5d433534-f41c-402e-ade5-e0a2259a7cb6)

FreeBSD : cURL -- Escape and unescape integer overflows (b018121b-7a4b-11e6-bf52-b499baebfeaf)

FreeBSD : cURL -- inappropriate GSSAPI delegation (9aecb94c-c1ad-11e3-a5ac-001b21614864)

FreeBSD : curl -- libcurl buffer overflow vulnerability (c8c31c41-49ed-11df-83fb-0015587e2cc1)

FreeBSD : cURL -- multiple vulnerabilities (04fe6c8d-2a34-4009-a81e-e7a7e759b5d2)

FreeBSD : cURL -- Multiple vulnerabilities (0cbf0fa6-dcb7-469c-b87a-f94cffd94583)

FreeBSD : cURL -- Multiple vulnerabilities (301a01b7-d50e-11e7-ac58-b499baebfeaf)

FreeBSD : cURL -- multiple vulnerabilities (6294f75f-03f2-11e5-aab1-d050996490d0)

FreeBSD : cURL -- multiple vulnerabilities (69cfa386-7cd0-11e7-867f-b499baebfeaf)

FreeBSD : curl -- multiple vulnerabilities (714b033a-2b09-11e9-8bc3-610fd6e6cd05)

FreeBSD : cURL -- multiple vulnerabilities (765feb7d-a0d1-11e6-a881-b499baebfeaf)

FreeBSD : curl -- multiple vulnerabilities (9fb4e57b-d65a-11e9-8a5f-e5c82b486287)

FreeBSD : curl -- multiple vulnerabilities (dd343a2b-7ee7-11e9-a290-8ddc52868fa9)

FreeBSD : curl -- multiple vulnerabilities (e0ab1773-07c1-46c6-9170-4c5e81c00927)

FreeBSD : cURL -- Multiple Vulnerability (2438d4af-1538-11e5-a106-3c970e169bc2)

FreeBSD : cURL -- ocsp status validation error (311e4b1c-f8ee-11e6-9940-b499baebfeaf)

FreeBSD : cURL -- out of bounds read (143ec3d6-b7cf-11e7-ac58-b499baebfeaf)

FreeBSD : cURL -- out of bounds read (ccace707-a8d8-11e7-ac58-b499baebfeaf)

FreeBSD : curl -- password overflow vulnerability (f4d638b9-e6e5-4dbe-8c70-571dbc116174)

FreeBSD : cURL -- potential memory disclosure (04f29189-1a05-11e7-bc6e-b499baebfeaf)

FreeBSD : cURL -- sensitive HTTP server headers also sent to proxies (27f742f6-03f4-11e5-aab1-d050996490d0)

FreeBSD : curl -- SMTP send heap buffer overflow (3849e28f-8693-11e8-9610-9c5c8e75236a)

FreeBSD : curl -- TFTP packet buffer overflow vulnerability (b8e361b8-b7ff-11da-8414-0013d4a4a40e)

FreeBSD : cURL -- TLS session resumption client cert bypass (again) (3e2e9b44-25ce-11e7-a175-939b30e0836d)

FreeBSD : cURL -- uninitialized random vulnerability (c40ca16c-4d9f-4d70-8b6c-4d53aeb8ead4)

FreeBSD : curl -- URL buffer overflow vulnerability (9b4facec-6761-11da-99f6-00123ffe8333)

FreeBSD : cURL -- URL file scheme drive letter buffer overflow (9314058e-5204-11e7-b712-b1a44a034d72)

FreeBSD : cURL -- URL request injection vulnerability (caa98ffd-0a92-40d0-b234-fd79b429157e)

FreeBSD : cURL library -- cert name check ignore with GnuTLS (4e1f4abc-6837-11e3-9cda-3c970e169bc2)

FreeBSD : cURL library -- heap corruption in curl\_easy\_unescape (01cf67b3-dc3b-11e2-a6cd-c48508086173)

FreeBSD : cvs -- numerous vulnerabilities (d2102505-f03d-11d8-81b0-000347a4fa7d)

FreeBSD : cvs -- Remote code execution via ssh command injection (d9fe59ea-1940-11e8-9eb8-5404a68ad561)

FreeBSD : CVS path validation errors (0792e7a7-8e37-11d8-90d1-0020ed76ef5a)

FreeBSD : cvsbug -- race condition (c5c17ead-8f23-11da-8c1d-000e0c2e438a)

FreeBSD : cvstrac (1276)

FreeBSD : Cyrus IMAP pre-authentication heap overflow vulnerability (35f6fdf8-a425-11d8-9c6d-0020ed76ef5a)

FreeBSD : Cyrus IMAPd -- APPEND command uses undefined programming construct (31952117-3d17-11d9-8818-008088034841)

FreeBSD : Cyrus IMAPd -- FETCH command out of bounds memory corruption (c0a269d5-3d16-11d9-8818-008088034841)

FreeBSD : Cyrus IMAPd -- IMAPMAGICPLUS preauthentification overflow (816fdd8b-3d14-11d9-8818-008088034841)

FreeBSD : Cyrus IMAPd -- PARTIAL command out of bounds memory corruption (114d70f3-3d16-11d9-8818-008088034841)

FreeBSD : Cyrus IMSPd multiple vulnerabilities (700d43b4-a42a-11d8-9c6d-0020ed76ef5a)

FreeBSD : cyrus-imapd -- broken 'other users' behaviour (f9f76a50-9642-11e7-ab09-080027b00c2e)

FreeBSD : cyrus-imapd -- buffer overrun in httpd (10fd731c-8088-11e9-b6ae-001871ec5271)

FreeBSD : cyrus-imapd -- integer overflow in the start\_octet addition (d62ec98e-97d8-11e5-8c0e-080027b00c2e)

FreeBSD : cyrus-imapd -- multiple buffer overflow vulnerabilities (b2d248ad-88f6-11d9-aa18-0001020eed82)

FreeBSD : cyrus-imapd -- Potential buffer overflow in Sieve (012b495c-9d51-11de-8d20-001bd3385381)

FreeBSD : cyrus-sasl -- buffer overflow vulnerability (14ab174c-40ef-11de-9fd5-001bd3385381)

FreeBSD : cyrus-sasl -- DIGEST-MD5 Pre-Authentication Denial of Service (408f6ebf-d152-11da-962f-000b972eb521)

FreeBSD : cyrus-sasl -- dynamic library loading and set-user-ID applications (92268205-1947-11d9-bc4a-000c41e2cdad)

FreeBSD : cyrus-sasl -- potential buffer overflow in DIGEST-MD5 plugin (0c592c4a-1bcc-11d9-a3ec-00061bd2d56f)

FreeBSD : dansguardian (2475)

FreeBSD : Darwin Streaming Server denial-of-service vulnerability (c7cad0f0-671a-11d8-bdeb-000a95bc6fae)

FreeBSD : databases/postgresql\*-client -- multiple vulnerabilities (174b8864-6237-11e1-be18-14dae938ec40)

FreeBSD : databases/postgresql\*-server -- crypt vulnerabilities (a8864f8f-aa9e-11e1-a284-0023ae8e59f0)

FreeBSD : databases/postgresql\*-server -- multiple vulnerabilities (07234e78-e899-11e1-b38d-0023ae8e59f0)

FreeBSD : davmail -- fix potential CVE-2014-3566 vulnerability (POODLE) (384fc0b2-0144-11e5-8fda-002590263bf5) (POODLE)

FreeBSD : dbmail (1583)

FreeBSD : dbus -- incomplete fix for CVE-2014-3636 part A (c1930f45-6982-11e4-80e1-bcaec565249c)

FreeBSD : dbus -- local dos (4e9e410b-d462-11e2-8d57-080027019be0)

FreeBSD : dbus -- local DoS (52bbc7e8-f13c-11e3-bc09-bcaec565249c)

FreeBSD : dbus -- match\_rule\_equal() Weakness (5b47b70d-8ba9-11db-81d5-00123ffe8333)

FreeBSD : dbus -- multiple vulnerabilities (38242d51-3e58-11e4-ac2f-bcaec565249c)

FreeBSD : dbus -- multiple vulnerabilities (e6a7636a-02d0-11e4-88b6-080027671656)

FreeBSD : dbus-glib -- privledge escalation (77bb0541-c1aa-11e3-a5ac-001b21614864)

FreeBSD : dcraw -- integer overflow condition (57325ecf-facc-11e4-968f-b888e347c638)

FreeBSD : devel/ipython -- CSRF possible remote execution vulnerability (81326883-2905-11e5-a4a5-002590263bf5)

FreeBSD : devel/ipython -- multiple vulnerabilities (290351c9-6f5c-11e5-a2a1-002590263bf5)

FreeBSD : devel/ipython -- remote execution (a4460ac7-192c-11e5-9c01-bcaec55be5e5)

FreeBSD : devel/subversion -- contrib hook-scripts can allow arbitrary code execution (6d0bf320-ca39-11e2-9673-001e8c75030d)

FreeBSD : devel/subversion -- fsfs repositories can be corrupted by newline characters in filenames (787d21b9-ca38-11e2-9673-001e8c75030d)

FreeBSD : devel/subversion -- svnserve remotely triggerable DoS (ce502902-ca39-11e2-9673-001e8c75030d)

FreeBSD : dhcpcd -- multiple vulnerabilities (df587aa2-b5a5-11e5-9728-002590263bf5)

FreeBSD : dhcpcd -- remote code execution/denial of service (092156c9-04d7-11e6-b1ce-002590263bf5)

FreeBSD : dhcpcd -- remote code execution/denial of service (6ec9f210-0404-11e6-9aee-bc5ff4fb5ea1)

FreeBSD : dia -- remote command execution vulnerability (25eb365c-fd11-11dd-8424-c213de35965d)

FreeBSD : dia -- XFig Import Plugin Buffer Overflow (b5fc63ad-c4c3-11da-9699-00123ffe8333)

FreeBSD : diffoscope -- arbitrary file write (077bbadf-f2f4-11e6-92a7-902b34361349)

FreeBSD : dillo -- format string vulnerability (28ab7ddf-61ab-11d9-a9e7-0001020eed82)

FreeBSD : dircproxy -- remote denial of service (a1ef3fc0-8ad0-11dc-9490-0016179b2dd5)

FreeBSD : distcc -- incorrect parsing of IP access control rules (e8d4800f-1547-11d9-90a3-00010327614a)

FreeBSD : Django -- AdminURLFieldWidget XSS (ffc73e87-87f0-11e9-ad56-fcaa147e860e)

FreeBSD : Django -- Content spoofing possibility in the default 404 page (3e41c1a6-10bc-11e9-bd85-fcaa147e860e)

FreeBSD : django -- CSRF protection bypass on a site with Google Analytics (bb022643-84fb-11e6-a4a1-60a44ce6887b)

FreeBSD : django -- denial-of-service attack (87917d6f-ba76-11de-bac2-001a4d563a0f)

FreeBSD : django -- denial-of-service via large passwords (05dc6efa-2370-11e3-95b7-00e0814cab4e)

FreeBSD : django -- Fixed session flushing in the cached\_db backend (48504af7-07ad-11e5-879c-00e0814cab4e)

FreeBSD : Django -- Incorrect HTTP detection with reverse-proxy connecting via HTTPS (b805d7b4-9c0c-11e9-97f0-000c29e96db4)

FreeBSD : django -- information leak vulnerability (11c52bc6-97aa-11e5-b8df-14dae9d210b8)

FreeBSD : Django -- information leakage (d696473f-9f32-42c5-a106-bf4536fb1f74)

FreeBSD : django -- multiple vulnerabilities (14a37474-1383-11e0-8a58-00215c6a37bb)

FreeBSD : django -- multiple vulnerabilities (1b769b72-582b-11e2-b66b-00e0814cab4e)

FreeBSD : django -- multiple vulnerabilities (21c59f5e-7cc5-11e2-9c11-080027a5ec9a)

FreeBSD : django -- multiple vulnerabilities (37ed8e9c-2651-11e5-86ff-14dae9d210b8)

FreeBSD : django -- multiple vulnerabilities (3c5579f7-294a-11e4-99f6-00e0814cab4e)

FreeBSD : Django -- multiple vulnerabilities (4e3fa78b-1577-11ea-b66e-080027bdabe8)

FreeBSD : django -- multiple vulnerabilities (59e72db2-cae6-11e3-8420-00e0814cab4e)

FreeBSD : django -- multiple vulnerabilities (5f326d75-1db9-11e2-bc8f-d0df9acfd7e5)

FreeBSD : django -- multiple vulnerabilities (62287f51-d43d-11e4-879c-00e0814cab4e)

FreeBSD : Django -- multiple vulnerabilities (6e65dfea-b614-11e9-a3a2-1506e15611cc)

FreeBSD : django -- multiple vulnerabilities (9c7b6c20-a324-11e4-879c-00e0814cab4e)

FreeBSD : django -- multiple vulnerabilities (a851b305-1bc3-11e3-95b7-00e0814cab4e)

FreeBSD : django -- multiple vulnerabilities (b0e54dc1-45d2-11e5-adde-14dae9d210b8)

FreeBSD : django -- multiple vulnerabilities (bd760627-3493-11e0-8103-00215c6a37bb)

FreeBSD : django -- multiple vulnerabilities (cb116651-79db-4c09-93a2-c38f9df46724)

FreeBSD : django -- multiple vulnerabilities (d01d10c7-de2d-11e0-b215-00215c6a37bb)

FreeBSD : django -- multiple vulnerabilities (dc880d6c-195d-11e7-8c63-0800277dcc69)

FreeBSD : django -- multiple vulnerabilities (f01292a0-db3c-11e1-a84b-00e0814cab4e)

FreeBSD : django -- multiple vulnerabilities (f9e6c0d1-e4cc-11e5-b2bd-002590263bf5)

FreeBSD : Django -- password hash disclosure (004d8c23-c710-11e8-98c7-000c29434208)

FreeBSD : Django -- possible XSS in traceback section of technical 500 debug page (aaab03be-932d-11e7-92d8-4b26fc968492)

FreeBSD : Django -- potential SQL injection vulnerability (1685144e-63ff-11ea-a93a-080027846a02)

FreeBSD : Django -- potential SQL injection vulnerability (5a45649a-4777-11ea-bdec-08002728f74c)

FreeBSD : django -- regression in permissions model (6b1d8a39-ddb3-11e5-8fa8-14dae9d210b8)

FreeBSD : django -- XSS vulnerability (3ff95dd3-c291-11df-b0dc-00215c6a37bb)

FreeBSD : django -- XSS vulnerability (f49ba347-2190-11dd-907c-001c2514716c)

FreeBSD : django-cms -- XSS Vulnerability (3886cafe-668c-11e2-94b8-1c4bd681f0cf)

FreeBSD : dnrd -- remote buffer and stack overflow vulnerabilities (e72fd82b-fa01-11d9-bc08-0001020eed82)

FreeBSD : dns/bind9\* -- A recursive resolver can be crashed by a query for a malformed zone (72f35727-ce83-11e2-be04-005056a37f68)

FreeBSD : dns/bind9\* -- crash on deliberately constructed combination of records (57a700f9-12c0-11e2-9f86-001d923933b6)

FreeBSD : dns/bind9\* -- Heavy DNSSEC Validation Load Can Cause a 'Bad Cache' Assertion Failure (0bc67930-d5c3-11e1-bef6-0024e81297ae)

FreeBSD : dns/bind9\* -- Malicious Regex Can Cause Memory Exhaustion (7a282e49-95b6-11e2-8433-0800273fe665)

FreeBSD : dns/bind9\* -- servers using DNS64 can be crashed by a crafted query (2892a8e2-3d68-11e2-8e01-0800273fe665)

FreeBSD : dns/bind9\* -- Several vulnerabilities (53a0ddef-0208-11e2-8afa-0024e830109b)

FreeBSD : dns/bind9\* -- zero-length RDATA can cause named to terminate, reveal memory (1ecc0d3f-ae8e-11e1-965b-0024e88a8c98)

FreeBSD : dns/nsd -- DoS vulnerability from non-standard DNS packet (ce82bfeb-d276-11e1-92c6-14dae938ec40)

FreeBSD : dnscrypt-proxy -- code execution (515b4327-cf8a-11e5-96d6-14dae9d210b8)

FreeBSD : dnsdist -- multiple vulnerabilities (198d82f3-8777-11e7-950a-e8e0b747a45a)

FreeBSD : dnsmasq -- data exposure and denial of service (37569eb7-0125-11e5-9d98-080027ef73ec)

FreeBSD : dnsmasq -- denial of service (875e4cf8-3f0e-11e6-b3c8-14dae9d210b8)

FreeBSD : dnsmasq -- multiple vulnerabilities (b77b5646-a778-11e7-ac58-b499baebfeaf)

FreeBSD : dnsmasq -- remotely exploitable buffer overflow in release candidate (7927165a-0126-11e5-9d98-080027ef73ec)

FreeBSD : dnsmasq -- TFTP server remote code injection vulnerability (80aa98e0-97b4-11de-b946-0030843d3802)

FreeBSD : doas -- Prevent passing of environment variables (7f7d6412-bae5-11e9-be92-3085a9a95629)

FreeBSD : dojo -- XSS and other vulnerabilities (805603a1-3e7a-11df-a5a1-0050568452ac)

FreeBSD : dokuwiki -- Local File Inclusion with register\_globals on (4f838b74-50a1-11de-b01f-001c2514716c)

FreeBSD : dokuwiki -- multiple privilege escalation vulnerabilities (7580f00e-280c-11e0-b7c8-00215c6a37bb)

FreeBSD : dokuwiki -- multiple vulnerabilities (23573650-f99a-11da-994e-00142a5f241c)

FreeBSD : dokuwiki -- multiple vulnerabilities (450b76ee-5068-11db-a5ae-00508d6a62df)

FreeBSD : dokuwiki -- multiple vulnerabilities (848539dc-0458-11df-8dd7-002170daae37)

FreeBSD : dokuwiki -- multiple vulnerabilities (fcba5764-506a-11db-a5ae-00508d6a62df)

FreeBSD : dokuwiki -- spellchecker remote PHP code execution (af8dba15-f4cc-11da-87a1-000c6ec775d9)

FreeBSD : Dokuwiki -- XSS vulnerability (0b535cd0-9b90-11e0-800a-00215c6a37bb)

FreeBSD : Dokuwiki -- XSS vulnerability (2fe4b57f-d110-11e1-ac76-10bf48230856)

FreeBSD : Dokuwiki -- XSS vulnerability (a04247f1-8d9c-11e1-93c7-00215c6a37bb)

FreeBSD : dokuwiki -- XSS vulnerability in spellchecker backend (cddde37a-39b5-11dc-b3da-001921ab2fa4)

FreeBSD : DomainKeys Identified Mail (DKIM) Verifiers may inappropriately convey message trust (a537b449-2b19-11e2-b339-90e6ba652cce)

FreeBSD : dovecot -- abort of SASL authentication results in a memory leak (92b8b284-a3a2-41b1-956c-f9cf8b74f500)

FreeBSD : dovecot -- ACL plugin bypass vulnerabilities (75c24c1d-b688-11dd-88fd-001c2514716c)

FreeBSD : dovecot -- Buffer overflow reading extension header (7862213c-5152-11e9-8b26-a4badb296695)

FreeBSD : dovecot -- denial of service vulnerability (0b53f5f7-ca8a-11e0-aea3-00215c6a37bb)

FreeBSD : dovecot -- Dovecot DoS when passdb dict was used for authentication (a8c8001b-216c-11e7-80aa-005056925db4)

FreeBSD : Dovecot -- improper input validation (abaaecda-ea16-43e2-bad0-d34a9ac576b1)

FreeBSD : dovecot -- Insecure directory permissions (30211c45-e52a-11de-b5cd-00e0815b8da8)

FreeBSD : dovecot -- json encoder crash (a64aa22f-61ec-11e9-85b9-a4badb296695)

FreeBSD : Dovecot -- Multiple vulnerabilities (3f98ccb3-6b8a-11e9-9b5c-a4badb296695)

FreeBSD : dovecot -- multiple vulnerabilities (74db0d02-b140-4c32-aac6-1f1e81e1ad30)

FreeBSD : dovecot -- NULL pointer deref in notify with empty headers (b7dc4dde-2e48-43f9-967a-c68461537cf2)

FreeBSD : dovecot -- security hole in blocking passdbs (b39bdc06-ee42-11dc-8678-00a0cce0781e)

FreeBSD : dovecot -- Specific LDAP + auth cache configuration may mix up user logins (cf484358-b5d6-11dc-8de0-001c2514716c)

FreeBSD : dovecot-managesieve -- Script Name Directory Traversal Vulnerability (3efc106e-c451-11dd-a721-0030843d3802)

FreeBSD : dpkg -- stack-based buffer overflow (876768aa-ab1e-11e5-8a30-5453ed2e2b49)

FreeBSD : drm graphics drivers -- Local privilege escalation and denial of service (ecb7fdec-0b82-11ea-874d-0c9d925bbbc0)

FreeBSD : drm graphics drivers -- potential information disclusure via local access (d2c2c815-3793-11ea-8be3-54e1ad3d6335)

FreeBSD : dropbear (1291)

FreeBSD : dropbear -- arbitrary code execution (eba70db4-6640-11e1-98af-00262d8b701d)

FreeBSD : dropbear -- authorized\_keys command= bypass (8eb78cdc-e9ec-11e5-85be-14dae9d210b8)

FreeBSD : dropbear -- exposure of sensitive information, DoS (8c9b48d1-3715-11e3-a624-00262d8b701d)

FreeBSD : dropbear -- multiple vulnerabilities (bc19dcca-7b13-11e6-b99e-589cfc0654e1)

FreeBSD : Dropbear -- two vulnerabilities (60931f98-55a7-11e7-8514-589cfc0654e1)

FreeBSD : drupal -- cross site request forgeries (937d5911-5f16-11db-ae08-0008743bf21a)

FreeBSD : drupal -- Cross site request forgeries (98dd7788-3d13-11dc-b3d3-0016179b2dd5)

FreeBSD : drupal -- cross site request forgery (4451a4c9-c05e-11dc-982e-001372fd0af2)

FreeBSD : drupal -- Drupal core - Access bypass (19d648e0-ab69-11e9-bfef-000ffec0b3e1)

FreeBSD : drupal -- Drupal core - Arbitrary PHP code execution (e00ed3d9-1c27-11e9-a257-000ffec0b3e1)

FreeBSD : drupal -- Drupal core - Highly critical - Remote Code Execution (002b4b05-35dd-11e9-94a8-000ffec0b3e1)

FreeBSD : drupal -- Drupal core - Moderately critical (2bad8b5d-66fb-11e9-9815-78acc0a3b880)

FreeBSD : drupal -- Drupal core - Moderately critical (33174280-43fa-11e8-aad5-6cf0497db129)

FreeBSD : drupal -- Drupal core - Moderately critical (9b8a52fc-89c1-11e9-9ba0-4c72b94353b5)

FreeBSD : drupal -- Drupal core - Moderately critical - XSS (94d63fd7-508b-11e9-9ba0-4c72b94353b5)

FreeBSD : drupal -- Drupal Core - Multiple Vulnerabilities (140a14b5-d615-11e8-b3cb-00e04c1ea73d)

FreeBSD : drupal -- Drupal Core - Multiple Vulnerabilities (3da0352f-2397-11ea-966e-000ffec0b3e1)

FreeBSD : drupal -- Drupal Core - Multiple Vulnerabilities (473b6a9e-8493-11e7-b24b-6cf0497db129)

FreeBSD : drupal -- Drupal Core - Multiple Vulnerabilities (4fc2df49-6279-11e7-be0f-6cf0497db129)

FreeBSD : drupal -- Drupal Core - Multiple Vulnerabilities (57580fcc-1a61-11e8-97e0-00e04c1ea73d)

FreeBSD : drupal -- Drupal Core - Multiple Vulnerabilities (89ca6f7d-4f00-11e8-9b1d-00e04c1ea73d)

FreeBSD : drupal -- Drupal Core - Multiple Vulnerabilities (a9e466e8-4144-11e8-a292-00e04c1ea73d) (Drupalgeddon 2)

FreeBSD : drupal -- HTML attribute injection (19207592-5f17-11db-ae08-0008743bf21a)

FreeBSD : drupal -- multiple vulnerabilities (070b5b22-6d74-11dd-aa18-0030843d3802)

FreeBSD : drupal -- multiple vulnerabilities (10720fe8-51e0-11e1-91c1-00215c6a37bb)

FreeBSD : drupal -- multiple vulnerabilities (12efc567-9879-11dd-a5e7-0030843d3802)

FreeBSD : drupal -- multiple vulnerabilities (1827f213-633e-11e2-8d93-c8600054b392)

FreeBSD : drupal -- multiple vulnerabilities (3d8d3548-9d02-11db-a541-000ae42e9b93)

FreeBSD : drupal -- multiple vulnerabilities (40a0185f-ec32-11da-be02-000c6ec775d9)

FreeBSD : drupal -- multiple vulnerabilities (59a0af97-dbd4-11e5-8fa8-14dae9d210b8)

FreeBSD : drupal -- multiple vulnerabilities (609c790e-ce0a-11dd-a721-0030843d3802)

FreeBSD : drupal -- multiple vulnerabilities (6779e82f-b60b-11da-913d-000ae42e9b93)

FreeBSD : drupal -- multiple vulnerabilities (6d85dc62-f2bd-11dd-9f55-0030843d3802)

FreeBSD : drupal -- multiple vulnerabilities (6da7344b-128a-11db-b25f-00e00c69a70d)

FreeBSD : drupal -- multiple vulnerabilities (706c9eef-a077-11dd-b413-001372fd0af2)

FreeBSD : drupal -- multiple vulnerabilities (7932548e-3427-11e6-8e82-002590263bf5)

FreeBSD : drupal -- multiple vulnerabilities (9393213d-489b-11e5-b8c7-d050996490d0)

FreeBSD : drupal -- multiple vulnerabilities (b3531fe1-2b03-11df-b6db-00248c9b4be7)

FreeBSD : drupal -- multiple vulnerabilities (bad1b090-a7ca-11de-873f-0030843d3802)

FreeBSD : drupal -- multiple vulnerabilities (be927298-6f97-11de-b444-001372fd0af2)

FreeBSD : drupal -- multiple vulnerabilities (d605edb1-1616-11e5-a000-d050996490d0)

FreeBSD : drupal -- multiple vulnerabilities (d9649816-5e0d-11e3-8d23-3c970e169bc2)

FreeBSD : drupal -- multiple vulnerabilities (ecedde1c-5128-11dd-a4e1-0030843d3802)

FreeBSD : drupal -- multiple vulnerabilities (faca0843-6281-11da-8630-00123ffe8333)

FreeBSD : drupal -- multiple XSS (751823d4-f189-11de-9344-00248c9b4be7)

FreeBSD : drupal -- Multiple XSS vulnerabilities (1f5b711b-3d0e-11dc-b3d3-0016179b2dd5)

FreeBSD : drupal -- multiple XSS vulnerabilities (b2383758-5f15-11db-ae08-0008743bf21a)

FreeBSD : drupal -- open redirect vulnerability (75f39413-7a00-11e5-a2a1-002590263bf5)

FreeBSD : drupal -- PHP code execution vulnerabilities (f241641e-f5ea-11d9-a6db-000d608ed240)

FreeBSD : drupal -- SQL injection vulnerability (fa708908-a8c7-11dc-b41d-000fb5066b20)

FreeBSD : drupal -- XSS (7a1ab8d4-35c1-11de-9672-0030843d3802)

FreeBSD : drupal -- XSS (a6605f4b-4067-11de-b444-001372fd0af2)

FreeBSD : drupal -- XSS (register\_globals) (f0fa19dd-c060-11dc-982e-001372fd0af2)

FreeBSD : drupal -- XSS (utf8) (6f736456-c060-11dc-982e-001372fd0af2)

FreeBSD : drupal -- XSS vulnerability (c905298c-2274-11db-896e-000ae42e9b93)

FreeBSD : drupal --- multiple vulnerabilities (9c00d446-8208-11dc-9283-0016179b2dd5)

FreeBSD : Drupal Code -- Multiple Vulnerabilities (8db24888-b2f5-11e6-8153-00248c0c745d)

FreeBSD : Drupal Views plugin -- XSS (ff8b419a-0ffa-11e0-becc-0022156e8794)

FreeBSD : drupal-pubcookie -- authentication may be bypassed (c0fd7890-4346-11db-89cc-000ae42e9b93)

FreeBSD : drupal6 -- multiple vulnerabilities (1acf9ec5-877d-11e0-b937-001372fd0af2)

FreeBSD : drupal6-cck -- XSS (03d22656-2690-11de-8226-0030843d3802)

FreeBSD : drupal7 -- Denial of service (a4d71e4c-7bf4-11e2-84cd-d43d7e0c7c02)

FreeBSD : drupal7 -- multiple vulnerabilities (2adc3e78-22d1-11e2-b9f0-d0df9acfd7e5)

FreeBSD : drupal7 -- SQL injection (6f825fa4-5560-11e4-a4c3-00a0986f28c4)

FreeBSD : drupal8 -- Drupal Core - Critical - Access Bypass (1455c86c-26c2-11e7-9daa-6cf0497db129)

FreeBSD : drupal8 -- multiple vulnerabilities (2730c668-0b1c-11e7-8d52-6cf0497db129)

FreeBSD : dtc -- multiple vulnerabilities (879b0242-c5b6-11e0-abd1-0017f22d6707)

FreeBSD : Dulwich -- Remote code execution (e426eda9-dae1-11e4-8107-94de806b0af9)

FreeBSD : duo -- Two-factor authentication bypass (738e8ae1-46dd-11e7-a539-0050569f7e80)

FreeBSD : e107 -- code execution and XSS vulnerabilities (a4746a86-4c89-11df-83fb-0015587e2cc1)

FreeBSD : e2fsprogs -- buffer overflow if s\_first\_meta\_bg too big (0f488b7b-bbb9-11e4-903c-080027ef73ec)

FreeBSD : e2fsprogs -- heap buffer overflow (299e3f81-aee7-11dc-b781-0016179b2dd5)

FreeBSD : e2fsprogs -- maliciously corrupted file systems can trigger buffer overruns in the quota code used by e2fsck (ad3451b9-23e0-11ea-8b36-f1925a339a82)

FreeBSD : e2fsprogs -- potential buffer overflow in closefs() (2a4bcd7d-bbb8-11e4-903c-080027ef73ec)

FreeBSD : e2fsprogs -- potential buffer overrun bugs in the blkid library and in the fsck program (2aa9967c-27e0-11e8-9ae1-080027ac955c)

FreeBSD : e2fsprogs -- rehash.c/pass 3a mutate\_name() code execution vulnerability (8b61308b-322a-11ea-b34b-1de6fb24355d)

FreeBSD : ecartis -- unauthorised access to admin interface (be543d74-539a-11d9-a9e7-0001020eed82)

FreeBSD : ecartis buffer overflows and input validation bugs (3e9be8c4-8192-11d8-9645-0020ed76ef5a)

FreeBSD : eggdrop -- denial of service vulnerability (399f4cd7-4d59-11de-8811-0030843d3802)

FreeBSD : egroupware -- arbitrary file download in JiNN (39953788-6bbb-11d9-8bc9-000a95bc6fae)

FreeBSD : egroupware -- multiple XSS (XSS) and SQL injection vulnerabilities (b4892b5b-fb1c-11d9-96ba-00909925db3e)

FreeBSD : egroupware -- two vulnerabilities (e39caf05-2d6f-11df-aec2-000c29ba66d2)

FreeBSD : ejabberd -- queue overload denial of service vulnerability (a04a3c13-4932-11df-83fb-0015587e2cc1)

FreeBSD : ejabberd -- remote denial of service vulnerability (01d3ab7d-9c43-11e0-bc0f-0014a5e3cda6)

FreeBSD : ejabberd -- XSS vulnerability (cf91c1e4-2b6d-11de-931b-00e0815b8da8)

FreeBSD : ekg -- insecure temporary file creation (9a035a56-eff0-11d9-8310-0001020eed82)

FreeBSD : elasticsearch -- directory traversal attack via snapshot API (ae8c09cb-32da-11e5-a4a5-002590263bf5)

FreeBSD : elasticsearch -- directory traversal attack with site plugins (a71e7440-1ba3-11e5-b43d-002590263bf5)

FreeBSD : elasticsearch -- remote code execution via transport protocol (fb3668df-32d7-11e5-a4a5-002590263bf5)

FreeBSD : elasticsearch -- remote OS command execution via Groovy scripting engine (026759e0-1ba3-11e5-b43d-002590263bf5)

FreeBSD : elasticsearch -- security fix for shared file-system repositories (23232028-1ba4-11e5-b43d-002590263bf5)

FreeBSD : elasticsearch -- XSS vulnerability in the CORS functionality (5951fb49-1ba2-11e5-b43d-002590263bf5)

FreeBSD : elasticsearch and logstash -- remote OS command execution via dynamic scripting (43ac9d42-1b9a-11e5-b43d-002590263bf5)

FreeBSD : electrum -- JSONRPC vulnerability (aa743ee4-0f16-11e8-8fd2-10bf48e1088e)

FreeBSD : ElGamal sign+encrypt keys created by GnuPG can be compromised (81313647-2d03-11d8-9355-0020ed76ef5a)

FreeBSD : elinks -- buffer overflow vulnerability (2544f543-c178-11de-b175-001cc0377035)

FreeBSD : elm -- remote buffer overflow in Expires header (f66e011d-13ff-11da-af41-0004614cc33d)

FreeBSD : emacs -- enriched text remote code execution vulnerability (47e2e52c-975c-11e7-942d-5404a68a61a2)

FreeBSD : emacs -- movemail format string vulnerability (3e3c860d-7dae-11d9-a9e7-0001020eed82)

FreeBSD : emacs -- remote code execution vulnerability (c1e5f35e-f93d-11e1-b07f-00235a5f2c9a)

FreeBSD : emacs -- run-python vulnerability (66657bd5-ac92-11dd-b541-001f3b19d541)

FreeBSD : End of Life Ports (7fe7df75-6568-11e6-a590-14dae9d210b8)

FreeBSD : Enhanced cTorrent -- stack-based overflow (83d7d149-b965-11de-a515-0022156e8794)

FreeBSD : enscript -- arbitrary code execution vulnerability (a1126054-b57c-11dd-8892-0017319806e7)

FreeBSD : enscript -- multiple vulnerabilities (72da8af6-7c75-11d9-8cc5-000854d03344)

FreeBSD : eog -- out-of-bounds write (f5035ead-688b-11e6-8b1d-c86000169601)

FreeBSD : eperl -- Remote code execution (73efb1b7-07ec-11e2-a391-000c29033c32)

FreeBSD : epiphany -- untrusted search path vulnerability (e848a92f-0e7d-11de-92de-000bcdc1757a)

FreeBSD : Erlang -- ssh library uses a weak random number generator (e4833927-86e5-11e0-a6b4-000a5e1e33c6)

FreeBSD : ethereal -- Multiple Protocol Dissector Vulnerabilities (21c223f2-d596-11da-8098-00123ffe8333)

FreeBSD : ethereal -- multiple protocol dissectors vulnerabilities (5d51d245-00ca-11da-bc08-0001020eed82)

FreeBSD : ethereal -- multiple protocol dissectors vulnerabilities (76adaab0-e4e3-11d9-b875-0001020eed82)

FreeBSD : ethereal -- multiple protocol dissectors vulnerabilities (831a6a66-79fa-11d9-a9e7-0001020eed82)

FreeBSD : ethereal -- multiple protocol dissectors vulnerabilities (cb470368-94d2-11d9-a9e0-0001020eed82)

FreeBSD : ethereal -- multiple vulnerabilities (efa1344b-5477-11d9-a9e7-0001020eed82)

FreeBSD : ettercap -- buffer overflow in target list parsing (1b9b199f-5efd-11e2-a1ee-c48508086173)

FreeBSD : ettercap -- out-of-bound read vulnerability (b79ec16b-9da7-11e9-a0ea-a92fe7db4867)

FreeBSD : evince -- Buffer Overflow Vulnerability (779a2d55-8ba8-11db-81d5-00123ffe8333)

FreeBSD : evince and atril -- command injection vulnerability in CBT handler (01a197ca-67f1-11e7-a266-28924a333806)

FreeBSD : evolution -- arbitrary code execution vulnerability (b8943e61-6e68-11d9-a9e7-0001020eed82)

FreeBSD : evolution -- remote format string vulnerabilities (e5afdf63-1746-11da-978e-0001020eed82)

FreeBSD : evolution-data-server -- remote execution of arbitrary code vulnerability (b1b5c125-2308-11dc-b91a-001921ab2fa4)

FreeBSD : exim -- a buffer overflow vulnerability, remote code execution (316b3c3e-0e98-11e8-8d41-97657151f8c2)

FreeBSD : exim -- DKIM private key leak (e7002b26-caaa-11e6-a76a-9f7324e5534e)

FreeBSD : Exim -- heap-based buffer overflow in string\_vformat leading to RCE (e917caba-e291-11e9-89f1-152fed202bb7)

FreeBSD : exim -- local privilege escalation (44ccfab0-3564-11e0-8e81-0022190034c0)

FreeBSD : exim -- local privilege escalation (e4fcf020-0447-11e0-becc-0022156e8794)

FreeBSD : exim -- local privillege escalation (7d09b9ee-e0ba-11e5-abc4-6fb07af136d2)

FreeBSD : exim -- Privilege escalation via multiple memory leaks (8c1a271d-56cf-11e7-b9fe-c13eb7bcbf4f) (Stack Clash)

FreeBSD : Exim -- RCE in ${sort} expansion (3e0da406-aece-11e9-8d41-97657151f8c2)

FreeBSD : Exim -- RCE in deliver\_message() function (45bea6b5-8855-11e9-8d41-97657151f8c2)

FreeBSD : Exim -- RCE with root privileges in TLS SNI handler (61db9b88-d091-11e9-8d41-97657151f8c2)

FreeBSD : Exim -- remote code execution (b0f3ab1f-1f3b-11e2-8fe9-0022156e8794)

FreeBSD : Exim -- remote code execution and information disclosure (36594c54-7be7-11e0-9838-0022156e8794)

FreeBSD : exim -- remote code execution, deny of service in BDAT (68b29058-d348-11e7-b9fe-c13eb7bcbf4f)

FreeBSD : exim -- remote DoS attack in BDAT processing (75dd622c-d5fd-11e7-b9fe-c13eb7bcbf4f)

FreeBSD : exim -- two buffer overflow vulnerabilities (ca9ce879-5ebb-11d9-a01c-0050569f0001)

FreeBSD : exim buffer overflow when verify = header\_syntax is used (5f29c2e4-9f6a-11d8-abbc-00e08110b673)

FreeBSD : expat -- denial of service vulnerability on malformed input (57b3aba7-1e25-11e6-8dd3-002590263bf5)

FreeBSD : expat -- multiple vulnerabilities (c9c252f5-2def-11e6-ae88-002590263bf5)

FreeBSD : expat -- multiple vulnerabilities (e375ff3f-7fec-11e8-8088-28d244aee256)

FreeBSD : expat2 -- buffer over-read and crash (e9fca207-e399-11de-881e-001aa0166822)

FreeBSD : expat2 -- denial of service (ff76f0e0-3f11-11e6-b3c8-14dae9d210b8)

FreeBSD : expat2 -- Fix extraction of namespace prefixes from XML names (6856d798-d950-11e9-aae4-f079596b62f9)

FreeBSD : expat2 -- Fix extraction of namespace prefixes from XML names (c5bd8a25-99a6-11e9-a598-f079596b62f9)

FreeBSD : expat2 -- Parser crash with specially formatted UTF-8 sequences (5f030587-e39a-11de-881e-001aa0166822)

FreeBSD : extman -- password bypass vulnerability (44c8694a-12f9-11dd-9b26-001c2514716c)

FreeBSD : eyeOS -- multiple XSS security bugs (d3527663-4ccb-11db-b48d-00508d6a62df)

FreeBSD : ez-ipupdate -- format string vulnerability (e69ba632-326f-11d9-b5b7-000854d03344)

FreeBSD : ezbounce remote format string vulnerability (c480eb5e-7f00-11d8-868e-000347dd607f)

FreeBSD : f2c -- insecure temporary files (43cb40b3-c8c2-11da-a672-000e0c2e438a)

FreeBSD : faad2 -- heap overflow vulnerability (445ed958-b0d9-11dd-a55e-00163e000016)

FreeBSD : fcron -- multiple vulnerabilities (e480ccb2-6bc8-11d9-8dbe-000a95bc6fae)

FreeBSD : fd\_set -- bitmap index overflow in multiple applications (4c005a5e-2541-4d95-80a0-00c76919aa66)

FreeBSD : fetchmail -- address parsing vulnerability (af0296be-2455-11d8-82e5-0020ed76ef5a)

FreeBSD : fetchmail -- chosen plaintext attack against SSL CBC initialization vectors (18ce9a90-f269-11e1-be53-080027ef73ec) (BEAST)

FreeBSD : fetchmail -- crash when bouncing a message (f11d3b22-88c6-11da-a7b2-0060084a00e5)

FreeBSD : fetchmail -- crashes when refusing a message bound for an MDA (37e30313-9d8c-11db-858b-0060084a00e5)

FreeBSD : fetchmail -- denial of service on reject of local warning message (45500f74-5947-11dc-87c1-000e2e5785ad)

FreeBSD : fetchmail -- denial of service vulnerability (09910d76-4c82-11df-83fb-0015587e2cc1)

FreeBSD : fetchmail -- denial of service/crash from malicious POP3 server (3f4ac724-fa8b-11d9-afcf-0060084a00e5)

FreeBSD : fetchmail -- denial-of-service vulnerability (ac4b9d18-67a9-11d8-80e3-0020ed76ef5a)

FreeBSD : fetchmail -- fetchmailconf local password exposure (baf74e0b-497a-11da-a4f4-0060084a00e5)

FreeBSD : fetchmail -- heap overflow on verbose X.509 display (2a6a966f-1774-11df-b5c1-0026189baca3)

FreeBSD : fetchmail -- improper SSL certificate subject verification (5179d85c-8683-11de-91b9-0022157515b2)

FreeBSD : fetchmail -- insecure APOP authentication (f1c4d133-e6d3-11db-99ea-0060084a00e5)

FreeBSD : fetchmail -- NULL pointer dereference in multidrop mode with headerless email (f7eb0b23-7099-11da-a15c-0060084a00e5)

FreeBSD : fetchmail -- potential crash in -v -v verbose mode (168190df-3e9a-11dd-87bc-000ea69a5213)

FreeBSD : fetchmail -- potential crash in -v -v verbose mode (revised patch) (1e8e63c0-478a-11dd-a88d-000ea69a5213)

FreeBSD : fetchmail -- remote root/code injection from malicious POP3 server (3497d7be-2fef-45f4-8162-9063751b573a)

FreeBSD : fetchmail -- STARTTLS denial of service (f7d838f2-9039-11e0-a051-080027ef73ec)

FreeBSD : fetchmail -- TLS enforcement problem/MITM attack/password exposure (5238ac45-9d8c-11db-858b-0060084a00e5)

FreeBSD : fetchmail -- two vulnerabilities in NTLM authentication (83f9e943-e664-11e1-a66d-080027ef73ec)

FreeBSD : ffmpeg -- 4xm processing memory corruption vulnerability (6733e1bf-125f-11de-a964-0030843d3802)

FreeBSD : ffmpeg -- heap overflow in lavf/mov.c (7f9b696f-f11b-11e6-b50e-5404a68ad561)

FreeBSD : ffmpeg -- libavcodec buffer overflow vulnerability (964161cd-6715-11da-99f6-00123ffe8333)

FreeBSD : ffmpeg -- multiple vulnerabilities (3d950687-b4c9-4a86-8478-c56743547af8)

FreeBSD : ffmpeg -- multiple vulnerabilities (4bae544d-06a3-4352-938c-b3bcbca89298)

FreeBSD : ffmpeg -- multiple vulnerabilities (5ccbb2f8-c798-11e7-a633-009c02a2ab30)

FreeBSD : ffmpeg -- multiple vulnerabilities (65b14d39-d01f-419c-b0b8-5df60b929973)

FreeBSD : ffmpeg -- multiple vulnerabilities (b0da85af-21a3-4c15-a137-fe9e4bc86002)

FreeBSD : ffmpeg -- multiple vulnerabilities (ea2ddc49-3e8e-11e1-8095-5404a67eef98)

FreeBSD : FFmpeg -- multiple vulnerabilities (ed73829d-af6d-11e7-a633-009c02a2ab30)

FreeBSD : ffmpeg -- out-of-bounds array access (80c66af0-d1c5-449e-bd31-63b12525ff88)

FreeBSD : ffmpeg -- remote attacker can access local files (046fedd1-bd01-11e5-bbf4-5404a68ad561)

FreeBSD : ffmpeg -- remote denial of service in JPEG2000 decoder (6ac79ed8-ccc2-11e5-932b-5404a68ad561)

FreeBSD : ffmpeg -- use-after-free (da434a78-e342-4d9a-87e2-7497e5f117ba)

FreeBSD : fidogate -- write files as `news' user (3243e839-f489-11d8-9837-000c41e2cdad)

FreeBSD : file -- buffer overruns and missing buffer size tests (84203724-296b-11e4-bebd-000c2980a9f3)

FreeBSD : file -- denial of service (815dbcf9-a2d6-11e3-8088-002590860428)

FreeBSD : file -- Heap buffer overflow possible (381deebb-f5c9-11e9-9c4f-74d435e60b7c)

FreeBSD : file -- multiple vulnerabilities (9575259a-92d5-11e4-bce6-d050992ecde8)

FreeBSD : file -- out-of-bounds access in search rules with offsets from input file (7e61a839-b714-11e3-8195-001966155bea)

FreeBSD : file disclosure in phpMyAdmin (cc0fb686-6550-11d8-80e3-0020ed76ef5a)

FreeBSD : file-roller -- path traversal vulnerability (ad479f89-9020-11e6-a590-14dae9d210b8)

FreeBSD : findutils -- GNU locate heap buffer overrun (7ca2a709-103b-11dc-8e82-00001cd613f9)

FreeBSD : firebird -- multiple remote buffer overflow vulnerabilities (91ed69f9-72c7-11dc-981a-001921ab2fa4)

FreeBSD : firebird -- Remote Stack Buffer Overflow (6adca5e9-95d2-11e2-8549-68b599b52a02)

FreeBSD : firefox & mozilla -- buffer overflow vulnerability (8665ebb9-2237-11da-978e-0001020eed82)

FreeBSD : firefox & mozilla -- command line URL shell command injection (2e28cefb-2aee-11da-a263-0001020eed82)

FreeBSD : firefox & mozilla -- multiple vulnerabilities (5d72701a-f601-11d9-bcd1-02061b08fc24)

FreeBSD : firefox & mozilla -- multiple vulnerabilities (8f5dd74b-2c61-11da-a263-0001020eed82)

FreeBSD : firefox -- arbitrary code execution from sidebar panel (741f8841-9c6b-11d9-9dbe-000a95bc6fae)

FreeBSD : firefox -- arbitrary code execution in sidebar panel (1f2fdcff-ae60-11d9-a788-0001020eed82)

FreeBSD : firefox -- Arbitrary code execution through unsanitized browser UI (103bf96a-6211-45ab-b567-1555ebb3a86a)

FreeBSD : firefox -- Crash in TransportSecurityInfo due to cached data (3284d948-140c-4a3e-aa76-3b440e2006a8)

FreeBSD : firefox -- Cross-origin restriction bypass using Fetch (79c68ef7-c8ae-4ade-91b4-4b8221b7c72a)

FreeBSD : firefox -- Dangling pointer crash regression from plugin parameter array fix (c2eac2b5-9a7d-11df-8e32-000f20797ede)

FreeBSD : firefox -- denial of service vulnerability (e2476979-da74-11da-a67b-0013d4a4a40e)

FreeBSD : firefox -- Heap buffer overflow rasterizing paths in SVG with Skia (e3e68fe8-d9cb-4ba8-b09c-9e3a28588eb7)

FreeBSD : firefox -- integer overflow in createImageBitmap() (5f453b69-abab-4e76-b6e5-2ed0bafcaee3)

FreeBSD : firefox -- javascript garbage collector vulnerability (67bd39ba-12b5-11dd-bab7-0016179b2dd5)

FreeBSD : firefox -- multiple remote unspecified memory corruption vulnerabilities (f1f6f6da-9d2f-11dc-9114-001c2514716c)

FreeBSD : firefox -- multiple vulnerabilities (8b491182-f842-11dd-94d9-0030843d3802)

FreeBSD : firefox -- OnUnload Javascript browser entrapment vulnerability (e24797af-803d-11dc-b787-003048705d5a)

FreeBSD : firefox -- PLUGINSPAGE privileged javascript execution (ce6ac624-aec8-11d9-a788-0001020eed82)

FreeBSD : firefox -- Re-use of freed object due to scope confusion (ec8f449f-40ed-11df-9edc-000f20797ede)

FreeBSD : firefox -- Same-origin-policy violation using Service Workers with plugins (172b22cb-d3f6-11e5-ac9e-485d605f4717)

FreeBSD : firefox -- WOFF heap corruption due to integer overflow (5d5ed535-3653-11df-9edc-000f20797ede)

FreeBSD : fish -- local privilege escalation and remote code execution (6c083cf8-4830-11e4-ae2c-c80aa9043978)

FreeBSD : Fix a buffer overflow in the tiff reader (38fec4bd-90f7-11e8-aafb-1c39475b9f84)

FreeBSD : flac -- media file processing integer overflow vulnerabilities (ff65eecb-91e4-11dc-bd6c-0016179b2dd5)

FreeBSD : flac -- Multiple vulnerabilities (a33addf6-74e6-11e4-a615-f8b156b6dcc8)

FreeBSD : flac123 -- stack overflow in comment parsing (32d38cbb-2632-11dc-94da-0016179b2dd5)

FreeBSD : flash -- multiple vulnerabilities (07888b49-35c4-11e6-8e82-002590263bf5)

FreeBSD : flash -- multiple vulnerabilities (0c6b008d-35c4-11e6-8e82-002590263bf5)

FreeBSD : flash -- multiple vulnerabilities (0e3dfdde-35c4-11e6-8e82-002590263bf5)

FreeBSD : flash -- multiple vulnerabilities (2482c798-93c6-11e6-846f-bc5ff4fb5ea1)

FreeBSD : flash -- multiple vulnerabilities (2a7bdc56-d7a3-11e6-ae1b-002590263bf5)

FreeBSD : flash -- multiple vulnerabilities (4e3e8a50-65c1-11e5-948e-bcaec565249c)

FreeBSD : flash -- multiple vulnerabilities (547fbd98-8b1f-11e5-b48b-bcaec565249c)

FreeBSD : flash -- multiple vulnerabilities (5d8e56c3-9e67-4d5b-81c9-3a409dfd705f)

FreeBSD : flash -- multiple vulnerabilities (84c7ea88-bf04-4bdc-973b-36744bf540ab)

FreeBSD : flash -- multiple vulnerabilities (96f6bf10-a731-11e6-95ca-0011d823eebd)

FreeBSD : flash -- multiple vulnerabilities (a522d6ac-4aed-11e6-97ea-002590263bf5)

FreeBSD : flash -- multiple vulnerabilities (a63f2c06-726b-11e5-a12b-bcaec565249c)

FreeBSD : flash -- multiple vulnerabilities (c8842a84-9ddd-11e5-8c2f-c485083ca99c)

FreeBSD : flash -- multiple vulnerabilities (f7b3d1eb-f738-11e5-a710-0011d823eebd)

FreeBSD : flash -- remote code execution (84147b46-e876-486d-b746-339ee45a8bb9)

FreeBSD : flash -- remote code execution (de6d01d5-9c44-11e6-ba67-0011d823eebd)

FreeBSD : Flash Player -- arbitrary code execution (8f128c72-ecf9-11e8-aa00-6451062f0f7a)

FreeBSD : Flash Player -- arbitrary code execution (9558d49c-534c-11e8-8177-d43d7ef03aa6)

FreeBSD : Flash Player -- arbitrary code execution (a99923a9-768c-11e9-885a-6451062f0f7a)

FreeBSD : Flash Player -- arbitrary code execution (ab099d2c-8c8c-11e9-8ba7-6451062f0f7a)

FreeBSD : Flash Player -- arbitrary code execution (d460b640-4cdf-11ea-a59e-6451062f0f7a)

FreeBSD : Flash Player -- information disclosure (9c016563-f582-11e7-b33c-6451062f0f7a)

FreeBSD : Flash Player -- information disclosure (b69292e8-e798-11e8-ae07-6451062f0f7a)

FreeBSD : Flash Player -- information disclosure (de11a8fb-2eda-11e9-8fb5-6451062f0f7a)

FreeBSD : Flash Player -- information disclosure (f9d73a20-b5f0-11e8-b1da-6451062f0f7a)

FreeBSD : Flash player -- Multiple security vulnerabilities in www/linux-\*-flashplugin11 (ca44b64c-4453-11e4-9ea1-c485083ca99c)

FreeBSD : Flash Player -- multiple vulnerabilities (2dde5a56-6ab1-11e8-b639-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (313078e3-26e2-11e8-9920-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (45d89773-5b64-11e9-80ed-d43d7ef03aa6)

FreeBSD : Flash Player -- multiple vulnerabilities (49cbe200-f92a-11e8-a89d-d43d7ef03aa6)

FreeBSD : Flash Player -- multiple vulnerabilities (4ffb633c-0a3b-11e7-a9f2-0011d823eebd)

FreeBSD : Flash Player -- multiple vulnerabilities (52f10525-caff-11e7-b590-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (531aae08-97f0-11e7-aadd-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (5c6f7482-3ced-11e8-b157-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (756a8631-0b84-11e8-a986-6451062f0f7a) (Underminer)

FreeBSD : Flash Player -- multiple vulnerabilities (7e3d3e9a-7d8f-11e7-a02b-d43d7ef03aa6)

FreeBSD : Flash Player -- multiple vulnerabilities (98b603c8-9ff3-11e8-ad63-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (a03e043a-67f1-11e7-beff-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (c6f19fe6-d42a-11e9-b4f9-6451062f0f7a)

FreeBSD : Flash Player -- multiple vulnerabilities (cd944b3f-51f6-11e7-b7b2-001c25e46b1d)

FreeBSD : Flash Player -- multiple vulnerabilities (e78732b2-8528-11e8-9c42-6451062f0f7a)

FreeBSD : Flash Player -- Remote code execution (a73518da-b2fa-11e7-98ef-d43d7ef03aa6)

FreeBSD : flyspray -- authentication bypass (209f0d75-4b5c-11dc-a6cd-000fb5066b20)

FreeBSD : flyspray -- multiple vulnerabilities (9d3020e4-a2c4-11dd-a9f9-0030843d3802)

FreeBSD : flyspray -- XSS vulnerabilities (f4b95430-51d8-11da-8e93-0010dc4afb40)

FreeBSD : fontconfig -- insufficiently cache file validation (44989c29-67d1-11e6-8b1d-c86000169601)

FreeBSD : foreman-proxy SSL verification issue (c30c3a2e-4fb1-11e4-b275-14dae9d210b8)

FreeBSD : Format string vulnerability in SSLtelnet (4aec9d58-ce7b-11d8-858d-000d610a3b12)

FreeBSD : foswiki -- Script Insertion Vulnerability via unchecked user registration fields (495b46fd-a30f-11e1-82c9-d0df9acfd7e5)

FreeBSD : FreeBSD (1414)

FreeBSD : FreeBSD -- bhyve - privilege escalation vulnerability (a479a725-9adb-11e6-a298-14dae9d210b8)

FreeBSD : FreeBSD -- Bhyve out-of-bounds read in XHCI device (edf064fb-b30b-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- bhyve(8) virtual machine escape (e722e3c6-bbee-11e6-b1cf-14dae9d210b8)

FreeBSD : FreeBSD -- BIND named(8) cache poisoning with DNSSEC validation (e500b9bf-ca3e-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- BIND remote denial of service (13031d98-9bd1-11e2-a7be-8c705af55518)

FreeBSD : FreeBSD -- BIND remote DoS with deliberately crafted DNS64 query (4671cdc9-7c6d-11e2-809b-6c626d99876c)

FreeBSD : FreeBSD -- bootpd buffer overflow (fa6a4a69-03d1-11e9-be12-a4badb2f4699)

FreeBSD : FreeBSD -- bsnmpd remote denial of service vulnerability (4c96ecf2-5fd9-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Buffer overflow in handling of UNIX socket addresses (f56390a4-4638-11e1-9f47-00e0815b8da8)

FreeBSD : FreeBSD -- Buffer overflow in keyboard driver (7bbc0e8c-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Buffer overflow in stdio (74ded00e-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Buffer overflow in tcpdump(1) (2dc764fa-40c0-11dc-aeac-02e0185f8d72)

FreeBSD : FreeBSD -- Cross-mount links between nullfs(5) mounts (b72bad1c-20ed-11e3-be06-000c29ee3065)

FreeBSD : FreeBSD -- Deadlock in the NFS server (6a384960-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Denial of service attack against sshd(8) (73e9a137-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Denial of Service in TCP packet processing (729c4a9f-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Denial of Service with IPv6 Router Advertisements (0bb55a18-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- devfs rules not applied by default for jails (6b6ca5b6-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- EAP-pwd message reassembly issue with unexpected fragment (a207bbd8-6572-11e9-8e67-206a8a720317)

FreeBSD : FreeBSD -- EAP-pwd missing commit validation (2da3cb25-6571-11e9-8e67-206a8a720317)

FreeBSD : FreeBSD -- EAP-pwd side-channel attack (60129efe-656d-11e9-8e67-206a8a720317)

FreeBSD : FreeBSD -- errors handling corrupt compress file in compress(1) and gzip(1) (fee94342-4638-11e1-9f47-00e0815b8da8)

FreeBSD : FreeBSD -- File description reference count leak (0d3f99f7-b30c-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- File description reference count leak (86c89abf-2d91-11e9-bf3e-a4badb2f4699)

FreeBSD : FreeBSD -- glob(3) related resource exhaustion (3c90e093-7c6e-11e2-809b-6c626d99876c)

FreeBSD : FreeBSD -- heap overflow in file(1) (8e01ab5b-0949-11dc-8163-000e0c2e438a)

FreeBSD : FreeBSD -- Heap overflow vulnerability in bspatch (ce808022-8ee6-11e6-a590-14dae9d210b8)

FreeBSD : FreeBSD -- Heap vulnerability in bspatch (7d4f4955-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- heimdal KDC-REP service name validation vulnerability (420243e9-a840-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- ICMP/ICMP6 packet filter bypass in pf (59c5f255-b309-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- ICMPv6 / MLDv2 out-of-bounds memory access (41d2f3e6-f680-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- iconv buffer overflow (f62bba56-b309-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- iconv(3) NULL pointer dereference and out-of-bounds array access (6f91a709-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Improper ELF header parsing (a67c122a-b693-11e8-ac58-a4badb2f4699)

FreeBSD : FreeBSD -- Improper environment sanitization in rtld(1) (ad08d14b-ca3d-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- Inappropriate directory permissions in freebsd-update(8) (6e87b696-ca3e-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- Incorrect argument handling in sendmsg(2) (7c0bac69-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Incorrect argument validation in sysarch(2) (7b6a11b5-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Incorrect crypt() hashing (185ff22e-c066-11e1-b5e0-000c299b62e1)

FreeBSD : FreeBSD -- Incorrect error handling in PAM policy parser (6e8f9003-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Incorrect handling of zero-length RDATA fields in named(8) (fc5231b6-c066-11e1-b5e0-000c299b62e1)

FreeBSD : FreeBSD -- Incorrect privilege validation in the NFS server (e5d2442d-5e76-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Incorrect user-controlled pointer use in epair (0cc7e547-6a0a-11ea-92ab-00163e433440)

FreeBSD : FreeBSD -- Information leak in kldstat(2) (759059ac-dab3-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- Insecure default GELI keyfile permissions (0b65f297-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Insecure default snmpd.config permissions (7a31dfba-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Insufficient bounds checking in bhyve(8) device model (32498c8f-fc84-11e8-be12-a4badb2f4699)

FreeBSD : FreeBSD -- Insufficient credential checks in network ioctl(2) (4d87d357-202c-11e3-be06-000c29ee3065)

FreeBSD : FreeBSD -- Insufficient environment sanitization in jail(8) (f6eb2279-ca3f-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- Insufficient ixl(4) ioctl(2) privilege checking (b2b83761-6a09-11ea-92ab-00163e433440)

FreeBSD : FreeBSD -- Insufficient message length validation for EAP-TLS messages (f115f693-36b2-11e2-a633-902b343deec9)

FreeBSD : FreeBSD -- Insufficient message length validation in bsnmp library (45a95fdd-f680-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Insufficient oce(4) ioctl(2) privilege checking (3c10ccdf-6a09-11ea-92ab-00163e433440)

FreeBSD : FreeBSD -- Insufficient validation of guest-supplied data (e1000 device) (499b22a3-f680-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Integer overflow in bzip2 decompression (18dc48fe-ca42-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- Integer overflow in IGMP protocol (0afe8b29-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- integer overflow in IP\_MSFILTER (0844632f-5e78-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Intel CPU Microcode Update (fbe10a8a-05a1-11ea-9dfa-f8b156ac3ff9) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (Spectre)

FreeBSD : FreeBSD -- ipfilter(4) fragment handling panic (51d1282d-420e-11e7-82c5-14dae9d210b8)

FreeBSD : FreeBSD -- ipsec crash or denial of service (c0c5afef-38db-11e8-8b7f-a4badb2f469b)

FreeBSD : FreeBSD -- ipsec validation and use-after-free (dca7ced0-2796-11e8-95ec-a4badb2f4699)

FreeBSD : FreeBSD -- IPv6 fragment reassembly panic in pf(4) (3d02520d-b309-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- IPv6 remote Denial-of-Service (4d3d4f64-f680-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Kernel data leak via ptrace(PT\_LWPINFO) (34a3f9b5-dab3-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- kernel memory disclosure from /dev/midistat (5027b62e-f680-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Kernel memory disclosure in control messages and SCTP (7240de58-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Kernel memory disclosure in freebsd32\_ioctl (6b856e00-b30a-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Kernel memory disclosure in sctp(4) (dd48d9b9-5e7e-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Kernel memory disclosure with nested jails (6b90acba-6a0a-11ea-92ab-00163e433440)

FreeBSD : FreeBSD -- kernel stack data disclosure (6025d173-4279-11ea-b184-f8b156ac3ff9)

FreeBSD : FreeBSD -- Kernel stack disclosure in 4.3BSD compatibility layer (7cad4795-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Kernel stack disclosure in Linux compatibility layer (7c5d64dd-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Kernel stack disclosure in setlogin(2) / getlogin(2) (74389f22-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Kernel stack disclosure in UFS/FFS (ff82610f-b309-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- ktrace kernel memory disclosure (6e04048b-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- L1 Terminal Fault (L1TF) Kernel Information Disclosure (2310b814-a652-11e8-805b-a4badb2f4699) (Foreshadow)

FreeBSD : FreeBSD -- Lazy FPU State Restore Information Disclosure (4e07d94f-75a5-11e8-85d1-a4badb2f4699)

FreeBSD : FreeBSD -- libfetch buffer overflow (22b41bc5-4279-11ea-b184-f8b156ac3ff9)

FreeBSD : FreeBSD -- link\_ntoa(3) buffer overflow (0282269d-bbee-11e6-b1cf-14dae9d210b8)

FreeBSD : FreeBSD -- Linux compatibility layer incorrect futex handling (793fb19c-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Linux compatibility layer input validation error (5536c8e4-36b3-11e2-a633-902b343deec9)

FreeBSD : FreeBSD -- Linux compatibility layer issetugid(2) system call (7ac28df1-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Linux compatibility layer setgroups(2) system call (798f63e0-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Local privilege escalation in IRET handler (0dfa5dde-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Lost mbuf flag resulting in data corruption (7a09a8df-ca41-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- Machine Check Exception on Page Size Change (edc0bf7e-05a1-11ea-9dfa-f8b156ac3ff9)

FreeBSD : FreeBSD -- memory leak in sandboxed namei lookup (73964eac-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Microarchitectural Data Sampling (MDS) (a633651b-b309-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Mishandling of x86 debug exceptions (521ce804-52fd-11e8-9123-a4badb2f4699)

FreeBSD : FreeBSD -- Missing IPsec anti-replay window check (5797c807-4279-11ea-b184-f8b156ac3ff9)

FreeBSD : FreeBSD -- Multiple Denial of Service vulnerabilities with named(8) (4b79538b-a450-11e2-9898-001060e06fd4)

FreeBSD : FreeBSD -- Multiple integer overflows in expat (libbsdxml) XML parser (0da8a68e-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Multiple libarchive vulnerabilities (1a71a972-8ee7-11e6-a590-14dae9d210b8)

FreeBSD : FreeBSD -- Multiple ntp vulnerabilities (7cfcea05-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Multiple OpenSSL vulnerabilities (7b1a4a27-600a-11e6-a6c3-14dae9d210b8) (DROWN)

FreeBSD : FreeBSD -- Multiple portsnap vulnerabilities (e7dcd69d-8ee6-11e6-a590-14dae9d210b8)

FreeBSD : FreeBSD -- Multiple vulnerabilities in bzip2 (3c7edc7a-f680-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Multiple vulnerabilities in file(1) and libmagic(3) (70140f20-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Multiple vulnerabilities in NFS server code (268a4289-fc84-11e8-be12-a4badb2f4699)

FreeBSD : FreeBSD -- Multiple vulnerabilities of ntp (3c0237f5-420e-11e7-82c5-14dae9d210b8)

FreeBSD : FreeBSD -- Multiple vulnerabilities of ntp (fcedcdbb-c86e-11e6-b1cf-14dae9d210b8)

FreeBSD : FreeBSD -- named(8) DNSSEC validation Denial of Service (0f020b7b-e033-11e1-90a2-000c299b62e1)

FreeBSD : FreeBSD -- Network ACL mishandling in mountd(8) (87261557-a450-11e2-9898-001060e06fd4)

FreeBSD : FreeBSD -- NFS remote denial of service (e66a6e2f-b0d5-11e2-9164-0016e6dcb562)

FreeBSD : FreeBSD -- ntpd mode 7 denial of service (48103b0a-ca3f-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- OpenSSH Denial of Service vulnerability (6ed5c5e3-a840-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- OpenSSH multiple vulnerabilities (2c948527-d823-11e6-9171-14dae9d210b8)

FreeBSD : FreeBSD -- OpenSSH Remote Denial of Service vulnerability (6a2cfcdc-9dea-11e6-a298-14dae9d210b8)

FreeBSD : FreeBSD -- OpenSSL multiple vulnerabilities (2ae114de-c064-11e1-b5e0-000c299b62e1)

FreeBSD : FreeBSD -- OpenSSL multiple vulnerabilities (69bfc852-9bd0-11e2-a7be-8c705af55518)

FreeBSD : FreeBSD -- OpenSSL multiple vulnerabilities (9442a811-dab3-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- OpenSSL multiple vulnerabilities (9f7a0f39-ddc0-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- OpenSSL Remote DoS vulnerability (0fcd3af0-a0fe-11e6-b1cf-14dae9d210b8)

FreeBSD : FreeBSD -- OPIE off-by-one stack overflow (768cfe70-ca40-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- pam\_ssh improperly grants access when user account has unencrypted SSH private keys (eda151d8-4638-11e1-9f47-00e0815b8da8)

FreeBSD : FreeBSD -- pam\_ssh() does not validate service names (e51d5b1a-4638-11e1-9f47-00e0815b8da8)

FreeBSD : FreeBSD -- POSIX shm allows jails to access global namespace (5b1463dd-dab3-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- Possible login(1) argument injection in telnetd(8) (e00304d2-bbed-11e6-b1cf-14dae9d210b8)

FreeBSD : FreeBSD -- Predictable query ids in named(8) (3de342fb-40be-11dc-aeac-02e0185f8d72)

FreeBSD : FreeBSD -- Privilege escalation in cd(4) driver (14a3b376-b30a-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Privilege escalation via mmap (abef280d-d829-11e2-b71c-8c705af55518)

FreeBSD : FreeBSD -- Privilege escalation when returning from kernel (aed44c4e-c067-11e1-b5e0-000c299b62e1)

FreeBSD : FreeBSD -- pts(4) write-after-free (5721ae65-b30a-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Reference count overflow in mqueue filesystem (deb6e164-b30b-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Reference count overflow in mqueue filesystem 32-bit compat (53b3474c-f680-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Remote command execution in ftp(1) (7488378d-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- remotely exploitable crash in OpenSSL (2539)

FreeBSD : FreeBSD -- Resource exhaustion due to sessions stuck in LAST\_ACK state (0c064c43-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Resource exhaustion in IP fragment reassembly (359e1548-a652-11e8-805b-a4badb2f4699)

FreeBSD : FreeBSD -- Resource exhaustion in non-default RACK TCP stack (c294c2e6-b309-11e9-a87f-a4badb2f4699) (ERC)

FreeBSD : FreeBSD -- Resource exhaustion in TCP reassembly (0cb9d5bb-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Resource exhaustion in TCP reassembly (3c2eea8c-99bf-11e8-8bee-a4badb2f4699)

FreeBSD : FreeBSD -- routed(8) remote denial of service vulnerability (0d584493-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- routed(8) remote denial of service vulnerability (734233f4-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- rpcbind(8) remote denial of service [REVISED] (0e5d6969-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- rtsold(8) remote buffer overflow vulnerability (72ee7111-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- SAE confirm missing state validation (98b71436-656d-11e9-8e67-206a8a720317)

FreeBSD : FreeBSD -- SAE side-channel attacks (7e53f9cc-656d-11e9-8e67-206a8a720317)

FreeBSD : FreeBSD -- SCTP ICMPv6 error message vulnerability (78f06a6c-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- SCTP SCTP\_SS\_VALUE kernel memory corruption and disclosure (0a5cf6d8-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- SCTP stream reset vulnerability (0aad3ce5-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- sendmail improper close-on-exec flag handling (6d9eadaf-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- shell injection vulnerability in patch(1) (0c6759dd-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- shell injection vulnerability in patch(1) (0d090952-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- Speculative Execution Vulnerabilities (74daa370-2797-11e8-95ec-a4badb2f4699) (Meltdown) (Spectre)

FreeBSD : FreeBSD -- SSL protocol flaw (406779fd-ca3b-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- System call kernel data register leak (683c714d-2d91-11e9-bf3e-a4badb2f4699)

FreeBSD : FreeBSD -- TCP IPv6 SYN cache kernel information disclosure (0e06013e-6a06-11ea-92ab-00163e433440)

FreeBSD : FreeBSD -- TCP MD5 signature denial of service (79dfc135-600a-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- TCP reassembly vulnerability (6d472244-6007-11e6-a6c3-14dae9d210b8)

FreeBSD : FreeBSD -- telnet(1) client multiple vulnerabilities (39f6cbff-b30a-11e9-a87f-a4badb2f4699)

FreeBSD : FreeBSD -- Unauthenticated EAPOL-Key Decryption Vulnerability (45671c0e-a652-11e8-805b-a4badb2f4699)

FreeBSD : FreeBSD -- Unvalidated input in nfsclient (0dc91089-ca41-11df-aade-0050568f000c)

FreeBSD : FreeBSD -- vt console memory disclosure (a5cf3ecd-38db-11e8-8b7f-a4badb2f469b)

FreeBSD : FreeBSD -- WPA2 protocol vulnerability (1f8de723-dab3-11e7-b5af-a4badb2f4699)

FreeBSD : FreeBSD -- ZFS ZIL playback with insecure permissions (97f09f2f-ca3f-11df-aade-0050568f000c)

FreeBSD : freeciv -- Denial of Service Vulnerabilities (2d9ad236-4d26-11db-b48d-00508d6a62df)

FreeBSD : freeciv -- Packet Parsing Denial of Service Vulnerability (339fbbc1-4d23-11db-b48d-00508d6a62df)

FreeBSD : freeimage -- code execution vulnerability (5b1631dc-eafd-11e6-9ac1-a4badb2f4699)

FreeBSD : freeimage -- multiple integer overflows (33459061-a1d6-11e5-8794-bcaec565249c)

FreeBSD : freeradius -- arbitrary code execution for TLS-based authentication (3bbbe3aa-fbeb-11e1-8bd8-0022156e8794)

FreeBSD : freeradius -- authentication bypass vulnerability (1a216dfd-f710-11da-9156-000e0c2e438a)

FreeBSD : freeradius -- denial-of-service vulnerability (20dfd134-1d39-11d9-9be9-000c6e8f12ef)

FreeBSD : freeradius -- EAP-MSCHAPv2 Authentication Bypass (37a5c10f-bf56-11da-b0e9-00123ffe8333)

FreeBSD : freeradius -- EAP-TTLS Tunnel Memory Leak Remote DOS Vulnerability (c110eda2-e995-11db-a944-0012f06707f0)

FreeBSD : freeradius -- insufficient CRL application vulnerability (379788f3-2900-11e5-a4a5-002590263bf5)

FreeBSD : FreeRadius -- Multiple vulnerabilities (79bbec7e-8141-11e7-b5af-a4badb2f4699)

FreeBSD : freeradius -- multiple vulnerabilities (ec2f2ff5-f710-11da-9156-000e0c2e438a)

FreeBSD : freeradius -- remote packet of death vulnerability (1b3f854b-e4bd-11de-b276-000d8787e1be)

FreeBSD : freeradius -- sql injection and denial of service vulnerability (2fbe16c2-cab6-11d9-9aed-000e0c2e438a)

FreeBSD : FreeRADIUS -- TLS resumption authentication bypass (673dce46-46d0-11e7-a539-0050569f7e80)

FreeBSD : freeradius3 -- insufficient validation on packets (0c2c4d84-42a2-11e5-9daa-14dae9d210b8)

FreeBSD : freetype -- LWFN Files Buffer Overflow Vulnerability (b975763f-5210-11db-8f1a-000a48049292)

FreeBSD : freetype -- Multiple vulnerabilities (1ae613c3-5728-11e2-9483-14dae938ec40)

FreeBSD : freetype -- multiple vulnerabilities (462e2d6c-8017-11e1-a571-bcaec565249c)

FreeBSD : freetype -- Out of bounds stack-based read/write (567beb1e-7e0a-11e4-b9cc-bcaec565249c)

FreeBSD : freetype -- Some type 1 fonts handling vulnerabilities (54075e39-04ac-11e1-a94e-bcaec565249c)

FreeBSD : FreeType 2 -- Heap overflow vulnerability (de2fab2d-0a37-11dc-aae2-00304881ac9a)

FreeBSD : FreeType 2 -- Multiple Vulnerabilities (4fb43b2f-46a9-11dd-9d38-00163e000016)

FreeBSD : freetype2 -- buffer overflows (4a088d67-3af2-11e7-9d75-c86000169601)

FreeBSD : freetype2 -- execute arbitrary code or cause denial of service (5d374b01-c3ee-11e0-8aa5-485d60cb5385)

FreeBSD : freetype2 -- multiple vulnerabilities (20b4f284-2bfc-11de-bdeb-0030843d3802)

FreeBSD : freetype2 -- Out of bounds read/write (1a0de610-a761-11e3-95fe-bcaec565249c)

FreeBSD : freexl -- integer overflow (a59e263a-45cd-11e5-adde-14dae9d210b8)

FreeBSD : freexl -- multiple vulnerabilities (ac98d090-45cc-11e5-adde-14dae9d210b8)

FreeBSD : frontpage -- XSS vulnerability (c0171f59-ea8a-11da-be02-000c6ec775d9)

FreeBSD : froxlor -- database password information leak (9ee72858-4159-11e5-93ad-002590263bf5)

FreeBSD : frr -- BGP Mishandled attribute length on Error (bf266183-cec7-11e7-af2d-2047478f2f70)

FreeBSD : fsp buffer overflow and directory traversal vulnerabilities (20be2982-4aae-11d8-96f2-0020ed76ef5a)

FreeBSD : fsplib -- multiple vulnerabilities (4a338d17-412d-11dc-bdb0-0016179b2dd5)

FreeBSD : fswiki -- command injection vulnerability (6e27f3b6-189b-11da-b6be-0090274e8dbb)

FreeBSD : fswiki -- XSS problem in file upload form (84479a62-ca5f-11d9-b772-000c29b00e99)

FreeBSD : fswiki -- XSS vulnerability (a86f30e7-dce7-11da-bf3f-02e081235dab)

FreeBSD : fuser -- missing user's privileges check (4d6076fe-ee7a-11de-9cd0-001a926c7637)

FreeBSD : fwbuilder -- security issue in temporary file handling (113cd7e9-a4e2-11de-84af-001195e39404)

FreeBSD : gaim (1980)

FreeBSD : gaim -- AIM/ICQ away message buffer overflow (6d1761d2-0b23-11da-bc08-0001020eed82)

FreeBSD : gaim -- AIM/ICQ non-UTF-8 filename crash (09db2844-0b21-11da-bc08-0001020eed82)

FreeBSD : gaim -- AIM/ICQ remote denial of service vulnerability (8b0e94cc-b5cd-11d9-a788-0001020eed82)

FreeBSD : gaim -- buffer overflow in MSN protocol support (1e6c4008-245f-11d9-b584-0050fc56d258)

FreeBSD : gaim -- Content-Length header denial-of-service vulnerability (ad61657d-26b9-11d9-9289-000c41e2cdad)

FreeBSD : gaim -- heap overflow exploitable by malicious GroupWise server (e16293f0-26b7-11d9-9289-000c41e2cdad)

FreeBSD : gaim -- jabber remote crash (ecf68408-a9f5-11d9-a788-0001020eed82)

FreeBSD : gaim -- malicious smiley themes (635bf5f4-26b7-11d9-9289-000c41e2cdad)

FreeBSD : gaim -- MSN denial-of-service vulnerabilities (f2d6a5e1-26b9-11d9-9289-000c41e2cdad)

FreeBSD : gaim -- MSN remote DoS vulnerability (ad5e70bb-c429-11d9-ac59-02061b08fc24)

FreeBSD : gaim -- MSN Remote DoS vulnerability (b6612eee-df5f-11d9-b875-0001020eed82)

FreeBSD : gaim -- multiple buffer overflows (4260eacb-26b8-11d9-9289-000c41e2cdad)

FreeBSD : gaim -- remote crash on some protocols (889061af-c427-11d9-ac59-02061b08fc24)

FreeBSD : gaim -- remote DoS on receiving certain messages over IRC (ec09baa3-a9f5-11d9-a788-0001020eed82)

FreeBSD : gaim -- remote DoS on receiving malformed HTML (142353df-b5cc-11d9-a788-0001020eed82)

FreeBSD : gaim -- remote DoS on receiving malformed HTML (3fa2b372-a9f5-11d9-a788-0001020eed82)

FreeBSD : gaim -- Yahoo! remote crash vulnerability (2701611f-df5c-11d9-b875-0001020eed82)

FreeBSD : gaim remotely exploitable vulnerabilities in MSN component (5b8f9a02-ec93-11d8-b913-000c41e2cdad)

FreeBSD : gallery (1290)

FreeBSD : gallery -- multiple vulnerabilities (9b037a0d-ef2c-11e2-b4a0-8c705af55518)

FreeBSD : gallery -- multiple vulnerabilities (fc9e73b2-8685-11dd-bb64-0030843d3802)

FreeBSD : gallery -- remote code injection via HTTP\_POST\_VARS (12b1a62d-6056-4d90-9e21-45fcde6abae4)

FreeBSD : gallery -- XSS (5752a0df-60c5-4876-a872-f12f9a02fa05)

FreeBSD : Gallery 1.4.3 and ealier user authentication bypass (253ea131-bd12-11d8-b071-00e08110b673)

FreeBSD : gallery2 -- file disclosure vulnerability (47bdabcf-3cf9-11da-baa2-0004614cc33d)

FreeBSD : gallery2 -- multiple vulnerabilities (4aab7bcd-b294-11dc-a6f0-00a0cce0781e)

FreeBSD : gallery2 -- multiple vulnerabilities (9b718b82-8ef5-11dc-8e42-001c2514716c)

FreeBSD : ganglia -- buffer overflow vulnerability (b9077cc4-6d04-4bcb-a37a-9ceaebfdcc9e)

FreeBSD : ganglia-webfrontend -- auth bypass (d68df01b-564e-11e5-9ad8-14dae9d210b8)

FreeBSD : ganglia-webfrontend -- XSS vulnerabilities (fee7e059-acec-11dc-807f-001b246e4fdf)

FreeBSD : gcab -- stack overflow (2cceb80e-c482-4cfd-81b3-2088d2c0ad53)

FreeBSD : gd -- '\_gdGetColors' remote buffer overflow vulnerability (4e8344a3-ca52-11de-8ee8-00215c6a37bb)

FreeBSD : gd -- integer overflow (62239968-2f2a-11d9-a9e7-0001020eed82)

FreeBSD : gd -- multiple vulnerabilities (556d2286-5a51-11e6-a6c3-14dae9d210b8)

FreeBSD : gd -- multiple vulnerabilities (6e099997-25d8-11dc-878b-000c29c5647f)

FreeBSD : gdcm -- multiple vulnerabilities (e00d8b94-c88a-11e5-b5fe-002590263bf5)

FreeBSD : gdk-pixbuf -- image decoding vulnerabilities (3d1e9267-073f-11d9-b45d-000c41e2cdad)

FreeBSD : gdk-pixbuf -- multiple vulnerabilities (5a1f1a86-8f4c-11e7-b5af-a4badb2f4699)

FreeBSD : gdk-pixbuf2 -- head overflow and DoS (9272a5b0-6b40-11e5-bd7f-bcaec565249c)

FreeBSD : gdk-pixbuf2 -- heap overflow and DoS (f5b8b670-465c-11e5-a49d-bcaec565249c)

FreeBSD : gdk-pixbuf2 -- heap overflow and DoS affecting Firefox and other programs (95eee71d-3068-11e5-a9b5-bcaec565249c)

FreeBSD : gdk-pixbuf2 -- integer overflows (ed0ecad5-531d-11e5-9850-bcaec565249c)

FreeBSD : gdm -- lock screen bypass when holding escape key (68847b20-8ddc-11e5-b69c-c86000169601)

FreeBSD : gdm -- privilege escalation vulnerability (c6fbd447-59ed-11e0-8d04-0015f2db7bde)

FreeBSD : gedit -- format string vulnerability (e319da0b-a228-11da-b410-000e0c2e438a)

FreeBSD : geeklog xss vulnerability (60e1792b-c380-11dc-821a-000bcdc1757a)

FreeBSD : getmail -- symlink vulnerability during maildir delivery (8c33b299-163b-11d9-ac1b-000d614f7fad)

FreeBSD : gforge -- directory traversal vulnerability (fe903533-ff96-4c7a-bd3e-4d40efa71897)

FreeBSD : gforge -- XSS and email flood vulnerabilities (d7cd5015-08c9-11da-bc08-0001020eed82)

FreeBSD : gftp -- directory traversal vulnerability (2d8cf857-81ea-11d9-a9e7-0001020eed82)

FreeBSD : gftp -- multiple vulnerabilities (f8b0f83c-8bb3-11dc-bffa-0016179b2dd5)

FreeBSD : Ghostscript -- arbitrary code execution (30c0f878-b03e-11e8-be8a-0011d823eebd)

FreeBSD : ghostscript -- buffer overflow vulnerability (f0f97b94-3f95-11de-a3fd-0030843d3802)

FreeBSD : ghostscript -- denial of service (crash) via crafted Postscript files (fc1f6658-4f53-11e5-934b-002590263bf5)

FreeBSD : ghostscript -- insecure temporary file creation vulnerability (27a70a01-5f6c-11da-8d54-000cf18bbe54)

FreeBSD : Ghostscript -- Security bypass vulnerabilities (22ae307a-1ac4-11ea-b267-001cc0382b2f)

FreeBSD : Ghostscript -- Security bypass vulnerability (5ed7102e-6454-11e9-9a3a-001cc0382b2f)

FreeBSD : ghostscript -- zseticcspace() function buffer overflow vulnerability (ca8e56d5-e856-11dc-b5af-0017319806e7)

FreeBSD : giflib -- heap overflow (90c8385a-dc9f-11e5-8fa8-14dae9d210b8)

FreeBSD : GIMP - Heap Buffer Overflow Vulnerability (bfda2d80-0858-11e8-ad5c-0021ccb9e74d)

FreeBSD : git -- Arbitrary command execution on case-insensitive filesystems (1d567278-87a5-11e4-879c-000c292ee6b8)

FreeBSD : git -- buffer overflow vulnerability (827bc2b7-95ed-11df-9160-00e0815b8da8)

FreeBSD : git -- denial of service vulnerability (d9b01c08-59b3-11de-828e-00e0815b8da8)

FreeBSD : Git -- Execute arbitrary code (7f645ee5-7681-11e5-8519-005056ac623e)

FreeBSD : Git -- Fix memory out-of-bounds and remote code execution vulnerabilities (CVE-2018-11233 and CVE-2018-11235) (c7a135f4-66a4-11e8-9e63-3085a9a47796)

FreeBSD : git -- gitweb privilege escalation (ecad44b9-e663-11dd-afcd-00e0815b8da8)

FreeBSD : git -- integer overflow (d2a84feb-ebe0-11e5-92ce-002590263bf5)

FreeBSD : git -- potential code execution (93ee802e-ebde-11e5-92ce-002590263bf5)

FreeBSD : gitea -- information disclosure (fd10aa77-fb5e-11e9-af7b-0800274e5f20)

FreeBSD : gitea -- insufficient privilege check (63e36475-119f-11e9-aba7-080027fee39c)

FreeBSD : gitea -- multiple vulnerabilities (3b2ee737-c12d-11e9-aabc-0800274e5f20)

FreeBSD : gitea -- multiple vulnerabilities (41c1cd6f-2645-11e9-b5f1-080027fee39c)

FreeBSD : gitea -- multiple vulnerabilities (7f6146aa-2157-11e9-9ba0-4c72b94353b5)

FreeBSD : gitea -- multiple vulnerabilities (a1de4ae9-6fda-11e9-9ba0-4c72b94353b5)

FreeBSD : gitea -- multiple vulnerabilities (a512a412-3a33-11ea-af63-0800274e5f20)

FreeBSD : gitea -- multiple vulnerabilities (b12a341a-0932-11ea-bf09-080027e0baa0)

FreeBSD : gitea -- multiple vulnerabilities (be088777-6085-11ea-8609-08002731610e)

FreeBSD : gitea -- multiple vulnerabilities (cb539d4e-cd68-11e8-8819-00e04c1ea73d)

FreeBSD : gitea -- multiple vulnerabilities (e7392840-c520-11e9-a4ef-0800274e5f20)

FreeBSD : gitea -- multiple vulnerabilities (e7b69694-b3b5-11e9-9bb6-0800274e5f20)

FreeBSD : gitea -- privilege escalation, XSS (29d34524-0542-11e9-a444-080027fee39c)

FreeBSD : gitea -- remote code execution (b747783f-5fb6-11e9-b2ac-08002705f877)

FreeBSD : gitea -- remote code exeution (deb4f633-de1d-11e8-a9fb-080027f43a02)

FreeBSD : gitea -- TOTP passcode reuse (bcf56a42-9df8-11e8-afb0-589cfc0f81b0)

FreeBSD : gitea -- XSS vulnerability (a8ba7358-4b02-11e9-9ba0-4c72b94353b5)

FreeBSD : Gitlab -- Arbitrary File read in Gitlab project import (70b774a8-05bc-11e9-87ad-001b217b3468)

FreeBSD : Gitlab -- Arbitrary File read in GitLab project import with Git LFS (757e6ee8-ff91-11e8-a148-001b217b3468)

FreeBSD : Gitlab -- Arbitrary repo read in Gitlab project import (ff50192c-19eb-11e9-8573-001b217b3468)

FreeBSD : gitlab -- Directory traversal via 'import/export' feature (10968dfd-a687-11e6-b2d3-60a44ce6887b)

FreeBSD : Gitlab -- Disclosure Vulnerabilities (0762fa72-e530-11e9-86e9-001b217b3468)

FreeBSD : Gitlab -- Disclosure Vulnerabilities (6eddfa51-fb44-11e9-86e9-001b217b3468)

FreeBSD : Gitlab -- Group Runner Registration Token Exposure (a0602fa0-5c1c-11e9-abd6-001b217b3468)

FreeBSD : Gitlab -- Information Disclosure (4faac805-6be0-11e9-a685-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (01bde18a-2e09-11ea-a935-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (065b3b72-c5ab-11e8-9ae2-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (085a087b-3897-11e8-ac53-d8cb8abf62dd)

FreeBSD : Gitlab -- Multiple Vulnerabilities (08fba28b-6f9f-11ea-bd0b-001b217b3468)

FreeBSD : Gitlab -- Multiple vulnerabilities (11292460-3f2f-11e9-adcb-001b217b3468)

FreeBSD : Gitlab -- Multiple vulnerabilities (1138b39e-6abb-11e9-a685-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (1aa7a094-1147-11ea-b537-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (1cd89254-b2db-11e9-8001-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (21944144-1b90-11ea-a2d4-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (23413442-c8ea-11e8-b35c-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (2da838f9-9168-11e8-8c75-d8cb8abf62dd)

FreeBSD : Gitlab -- Multiple Vulnerabilities (4091069e-860b-11e9-a05f-001b217b3468)

FreeBSD : GitLab -- multiple vulnerabilities (418c172b-b96f-11e7-b627-d43d7e971a1b)

FreeBSD : Gitlab -- Multiple vulnerabilities (43ee6c1d-29ee-11e9-82a1-001b217b3468)

FreeBSD : Gitlab -- Multiple vulnerabilities (467b7cbe-257d-11e9-8573-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (4ce7c28a-11ac-11ea-b537-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (4ea507d1-9da8-11e9-a759-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (570706ff-7ee0-11ea-bd0b-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (62f2182c-5f7a-11ea-abb7-001b217b3468)

FreeBSD : GitLab -- multiple vulnerabilities (6a177c87-9933-11e7-93f7-d43d7e971a1b)

FreeBSD : GitLab -- multiple vulnerabilities (86291013-16e6-11e8-ae9f-d43d7e971a1b)

FreeBSD : Gitlab -- Multiple vulnerabilities (8a4aba2d-f33e-11e8-9416-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (9557dc72-64da-11e8-bc32-d8cb8abf62dd)

FreeBSD : Gitlab -- Multiple vulnerabilities (9d3428d4-f98c-11e8-a148-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (9dfe61c8-4d15-11e8-8f2f-d8cb8abf62dd)

FreeBSD : Gitlab -- Multiple Vulnerabilities (b17c86b9-e52e-11e9-86e9-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (b2789b2d-d521-11e9-86e9-001b217b3468)

FreeBSD : Gitlab -- Multiple vulnerabilities (b2f4ab91-0e6b-11e9-8700-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (b68cc195-cae7-11e9-86e9-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (b950a83b-789e-11e8-8545-d8cb8abf62dd)

FreeBSD : Gitlab -- multiple vulnerabilities (b9591212-dba7-11e8-9416-001b217b3468)

FreeBSD : Gitlab -- Multiple Vulnerabilities (c5bd9068-440f-11ea-9cdb-001b217b3468)

FreeBSD : Gitlab -- Multiple vulnerabilities (d889d32c-ecd9-11e8-9416-001b217b3468)

FreeBSD : Gitlab -- Multiple vulnerabilities (da459dbc-5586-11e9-abd6-001b217b3468)

FreeBSD : Gitlab -- multiple vulnerabilities (dc0c201c-31da-11e8-ac53-d8cb8abf62dd)

FreeBSD : Gitlab -- Multiple Vulnerabilities (ddd48087-bd86-11e9-b13f-001b217b3468)

FreeBSD : GitLab -- multiple vulnerabilities (e72a8864-e0bc-11e7-b627-d43d7e971a1b)

FreeBSD : Gitlab -- multiple vulnerabilities (ffeb25d0-ac94-11e8-ab15-d8cb8abf62dd)

FreeBSD : Gitlab -- Private objects exposed through project import (f929b172-369e-11ea-9cdb-001b217b3468)

FreeBSD : gitlab -- privilege escalation via 'impersonate' feature (be72e773-1131-11e6-94fa-002590263bf5)

FreeBSD : gitlab -- Remote code execution on project import (65fab89f-2231-46db-8541-978f4e87f32a)

FreeBSD : Gitlab -- Remote Code Execution Vulnerability in GitLab Projects Import (8fc615cc-8a66-11e8-8c75-d8cb8abf62dd)

FreeBSD : Gitlab -- SSRF in Kubernetes integration (b51d9e83-de08-11e8-9416-001b217b3468)

FreeBSD : GitLab -- two vulnerabilities (abcc5ad3-7e6a-11e7-93f7-d43d7e971a1b)

FreeBSD : gitlab -- Various security issues (5d62950f-3bb5-11e7-93f7-d43d7e971a1b)

FreeBSD : GitLab -- Various security issues (85ebfa0c-5d8d-11e7-93f7-d43d7e971a1b)

FreeBSD : GitLab -- Various security issues (92f4191a-6d25-11e7-93f7-d43d7e971a1b)

FreeBSD : gitlab -- Various security issues (9704930c-3bb7-11e7-93f7-d43d7e971a1b)

FreeBSD : Gitlab -- Vulnerability (1ece5591-4ea9-11ea-86f0-001b217b3468)

FreeBSD : Gitlab -- Vulnerability (7ba5a3d0-4b18-11e9-adcb-001b217b3468)

FreeBSD : Gitlab -- Vulnerability (9a09eaa2-6448-11ea-abb7-001b217b3468)

FreeBSD : Gitlab -- Vulnerability (e0382fde-4bb0-11e9-adcb-001b217b3468)

FreeBSD : gitolite -- path traversal vulnerability (f94befcd-1289-11e2-a25e-525400272390)

FreeBSD : gld -- format string and buffer overflow vulnerabilities (6c2d4f29-af3e-11d9-837d-000e0c2e438a)

FreeBSD : glibc -- getaddrinfo stack-based buffer overflow (2dd7e97e-d5e8-11e5-bcbd-bc5ff45d0f28)

FreeBSD : glibc -- gethostbyname buffer overflow (0765de84-a6c1-11e4-a0c1-c485083ca99c) (GHOST)

FreeBSD : global -- gozilla vulnerability (48cca164-e269-11e7-be51-6599c735afc8)

FreeBSD : globus -- Multiple tmpfile races (5039ae61-2c9f-11db-8401-000ae42e9b93)

FreeBSD : glpi -- remote attack via crafted POST request (7c769c89-53c2-11e1-8e52-00163e22ef61)

FreeBSD : glpi -- SQL Injection (2ffb1b0d-ecf5-11dd-abae-00219b0fc4d8)

FreeBSD : gnats -- format string vulnerability (fc99c736-3499-11d9-98a7-0090962cff2a)

FreeBSD : GNATS local privilege elevation (4d837296-cc28-11d8-a54c-02e0185c0b53)

FreeBSD : gnome-screensaver -- Multiple monitor hotplug issues (0a82ac0c-1886-11df-b0d1-0015f2db7bde)

FreeBSD : gnomevfs -- unsafe URI handling (7884d56f-f7a1-11d8-9837-000c41e2cdad)

FreeBSD : GNU Anubis buffer overflows and format string vulnerabilities (8471bb85-6fb0-11d8-873f-0020ed76ef5a)

FreeBSD : GNU binutils -- multiple vulnerabilities (f6a014cd-d268-11e4-8339-001e679db764)

FreeBSD : GNU cpio -- multiple vulnerabilities (f59af308-07f3-11ea-8c56-f8b156b6dcc8)

FreeBSD : GNU finger vulnerability (610bc692-a2ad-11dc-900c-000bcdc1757a)

FreeBSD : GNU gatekeeper -- denial of service (342176a8-f464-11e1-8bd8-0022156e8794)

FreeBSD : GNU libtool insecure temporary file handling (cacaffbc-5e64-11d8-80e3-0020ed76ef5a)

FreeBSD : gnu-radius -- SNMP-related denial-of-service (e6f0edd8-0b40-11d9-8a8a-000c41e2cdad)

FreeBSD : gnupg -- 2 more possible memory allocation attacks (ed529baa-21c6-11db-b625-02e081235dab)

FreeBSD : gnupg -- attacker who obtains 4640 bits from the RNG can trivially predict the next 160 bits of output (e1c71d8d-64d9-11e6-b38a-25a46b33f2ed)

FreeBSD : gnupg -- buffer overflow (34c93ae8-7e6f-11db-bf00-02e081235dab)

FreeBSD : GnuPG -- denial of service (23f65f58-a261-11e9-b444-002590acae31)

FreeBSD : gnupg -- false positive signature verification (63fe4189-9f97-11da-ac32-0001020eed82)

FreeBSD : gnupg -- memory corruption vulnerability (30394651-13e1-11dd-bab7-0016179b2dd5)

FreeBSD : gnupg -- OpenPGP symmetric encryption vulnerability (8375a73f-01bf-11da-bc08-0001020eed82)

FreeBSD : gnupg -- possible DoS using garbled compressed data packets (1c840eb9-fb32-11e3-866e-b499baab0cbe)

FreeBSD : gnupg -- possible infinite recursion in the compressed packet parser (749b5587-2da1-11e3-b1a9-b499baab0cbe)

FreeBSD : gnupg -- remotely controllable function pointer (4db1669c-8589-11db-ac4f-02e081235dab)

FreeBSD : gnupg -- RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis attack (2e5715f8-67f7-11e3-9811-b499baab0cbe)

FreeBSD : gnupg -- side channel attack on RSA secret keys (80771b89-f57b-11e2-bf21-b499baab0cbe)

FreeBSD : gnupg -- unsanitized output (CVE-2018-12020) (7da0417f-6b24-11e8-84cc-002590acae31)

FreeBSD : gnupg -- user id integer overflow vulnerability (f900bda8-0472-11db-bbf7-000c6ec775d9)

FreeBSD : GnuPG and Libgcrypt -- side-channel attack vulnerability (689c2bf7-0701-11e3-9a25-002590860428)

FreeBSD : GnuPG does not detect injection of unsigned data (948921ad-afbc-11da-bad9-02e081235dab)

FreeBSD : gnutls -- 'gnutls\_handshake()' Denial of Service (d864a0a7-6f27-11dd-acfe-00104b9e1a4a)

FreeBSD : gnutls -- certificate chain verification DoS (84ab58cf-e4ac-11d8-9b0a-000347a4fa7d)

FreeBSD : gnutls -- client session resumption vulnerability (bdec8dc2-0b3b-11e1-b722-001cc0476564)

FreeBSD : gnutls -- client-side memory corruption (027af74d-eb56-11e3-9032-000c2980a9f3)

FreeBSD : gnutls -- client-side memory corruption (9733c480-ebff-11e3-970b-206a8a720317)

FreeBSD : gnutls -- denial of service (9065b930-3d8b-11e3-bd1a-e840f2096bd0)

FreeBSD : GnuTLS -- Denial of service vulnerability (b33fb1e0-4c37-11e7-afeb-0011d823eebd)

FreeBSD : gnutls -- double free in certificate DN decoding (ec6a2a1e-429d-11e5-9daa-14dae9d210b8)

FreeBSD : GnuTLS -- double free, invalid pointer access (fb30db8f-62af-11e9-b0de-001cc0382b2f)

FreeBSD : gnutls -- file overwrite by setuid programs (9c196cfd-2ccc-11e6-94b0-0011d823eebd)

FreeBSD : GnuTLS -- flaw in DTLS protocol implementation (d887b3d9-7366-11ea-b81a-001cc0382b2f)

FreeBSD : GnuTLS -- improper SSL certificate verification (856a6f84-8b30-11de-8062-00e0815b8da8)

FreeBSD : gnutls -- MD5 downgrade in TLS signatures (3de36a19-429d-11e5-9daa-14dae9d210b8)

FreeBSD : GnuTLS -- Memory corruption vulnerabilities (0c5369fc-d671-11e6-a9a5-b499baebfeaf)

FreeBSD : gnutls -- multiple certificate verification issues (f645aa90-a3e8-11e3-a422-3c970e169bc2)

FreeBSD : GnuTLS -- multiple vulnerabilities (b31a1088-460f-11de-a11a-0022156e8794)

FreeBSD : gnutls -- OCSP validation issue (a0128291-7690-11e6-95a8-0011d823eebd)

FreeBSD : gnutls -- possible overflow/Denial of service vulnerabilities (aecee357-739e-11e1-a883-001cc0a36e12)

FreeBSD : gnutls -- RSA Signature Forgery Vulnerability (64bf6234-520d-11db-8f1a-000a48049292)

FreeBSD : gnutls -- X.509 certificate chain validation vulnerability (45298931-b3bf-11dd-80f8-001cc0377035)

FreeBSD : go -- information disclosure vulnerability (6809c6db-bdeb-11e5-b5fe-002590263bf5)

FreeBSD : go -- invalid headers are normalized, allowing request smuggling (a92dcc5c-e05c-11e9-b589-10c37b4ac2ea)

FreeBSD : go -- multiple vulnerabilities (4464212e-4acd-11e5-934b-002590263bf5)

FreeBSD : go -- remote denial of service (f2217cdf-01e4-11e6-b1ce-002590263bf5)

FreeBSD : gogs -- open redirect vulnerability (e53a908d-a645-11e8-8acd-10c37b4ac2ea)

FreeBSD : golddig -- local buffer overflow vulnerabilities (949c470e-528f-11d9-ac20-00065be4b5b6)

FreeBSD : google-earth -- heap overflow in the KML engine (5c9a2769-5ade-11db-a5ae-00508d6a62df)

FreeBSD : gpgme -- heap-based buffer overflow in gpgsm status handler (90ca3ba5-19e6-11e4-8616-001b3856973b)

FreeBSD : grafana -- LDAP and OAuth login vulnerability (1f8d5806-ac51-11e8-9cb6-10c37b4ac2ea)

FreeBSD : GraphicsMagick -- multiple vulnerabilities (25f73c47-68a8-4a30-9cbc-1ca5eea4d6ba)

FreeBSD : GraphicsMagick -- multiple vulnerabilities (82c07dfa-9016-11e9-af2f-712c38aa3e4c)

FreeBSD : GraphicsMagick -- SVG/Rendering vulnerability (e714b7d2-39f6-4992-9f48-e6b2f5f949df)

FreeBSD : graphite2 -- code execution vulnerability (8f10fa04-cf6a-11e5-96d6-14dae9d210b8)

FreeBSD : graphite2 -- multiple vulnerabilities (adffe823-e692-4921-ae9c-0b825c218372)

FreeBSD : graphite2 -- out-of-bounds write with malicious font (cf133acc-82e7-4755-a66a-5ddf90dacbe6)

FreeBSD : graphviz -- format string vulnerability (5300711b-4e61-11e5-9ad8-14dae9d210b8)

FreeBSD : greed -- insecure GRX file processing (bd579366-5290-11d9-ac20-00065be4b5b6)

FreeBSD : grip -- CDDB response multiple matches buffer overflow vulnerability (bcf27002-94c3-11d9-a9e0-0001020eed82)

FreeBSD : groff -- groffer uses temporary files unsafely (169f422f-bd88-11d9-a281-02e018374e71)

FreeBSD : groff -- pic2graph and eqn2graph are vulnerable to symlink attack through temporary files (01bb84e2-bd88-11d9-a281-02e018374e71)

FreeBSD : groovy -- remote execution of untrusted code (67b3fef2-2bea-11e5-86ff-14dae9d210b8)

FreeBSD : groovy -- remote execution of untrusted code/DoS vulnerability (4af92a40-db33-11e6-ae1b-002590263bf5)

FreeBSD : grub2-bhyve -- multiple privilege escalations (9d6a48a7-4dad-11ea-8a1d-7085c25400ea)

FreeBSD : gsoap -- remote code execution via via overflow (8745c67e-7dd1-4165-96e2-fcf9da2dc5b5) (Devil's Ivy)

FreeBSD : gstreamer-ffmpeg -- Multiple vulnerabilities in bundled libav (4d087b35-0990-11e3-a9f4-bcaec565249c)

FreeBSD : gstreamer-plugins-good -- multiple memory overflows (37a365ed-1269-11de-a964-0030843d3802)

FreeBSD : gtar -- buffer overflow in rmt client (c175d72f-3773-11df-8bb8-0211d880e350)

FreeBSD : gtar -- Directory traversal vulnerability (d944719e-42f4-4864-89ed-f045b541919f)

FreeBSD : gtar -- GNU TAR safer\_name\_suffix Remote Denial of Service Vulnerability (0809ce7d-f672-4924-9b3b-7c74bc279b83)

FreeBSD : gtar -- GNUTYPE\_NAMES directory traversal vulnerability (3dd7eb58-80ae-11db-b4ec-000854d03344)

FreeBSD : gtar -- invalid headers buffer overflow (6107efb9-aae3-11da-aea1-000854d03344)

FreeBSD : gtetrinet -- remote code execution (0b79743b-3ab7-11db-81e1-000e0c2e438a)

FreeBSD : gtk-vnc -- bounds checking vulnerabilities (79bbb8f8-f049-11e6-8a6a-bcaec565249c)

FreeBSD : guile2 -- multiple vulnerabilities (b4ecf774-eb01-11e6-9ac1-a4badb2f4699)

FreeBSD : gzip -- directory traversal and permission race vulnerabilities (63bd4bad-dffe-11d9-b875-0001020eed82)

FreeBSD : gzip -- multiple vulnerabilities (11a84092-8f9f-11db-ab33-000e0c2e438a)

FreeBSD : h2o -- directory traversal vulnerability (31ea7f73-5c55-11e5-8607-74d02b9a84d5)

FreeBSD : h2o -- directory traversal vulnerability (6c808811-bb9a-11e5-a65c-485d605f4717)

FreeBSD : h2o -- DoS in workers (10c0fabc-b5da-11e7-816e-00bd5d1fff09)

FreeBSD : h2o -- fix DoS attack vector (08664d42-7989-11e6-b7a8-74d02b9a84d5)

FreeBSD : h2o -- heap buffer overflow during logging (ce39379f-7eb7-11e8-ab03-00bd7f19ff09)

FreeBSD : h2o -- multiple HTTP/2 vulnerabilities (72a5579e-c765-11e9-8052-0028f8d09152) (Ping Flood) (Reset Flood) (Settings Flood)

FreeBSD : h2o -- multiple HTTP/2 vulnerabilities (73b1e734-c74e-11e9-8052-0028f8d09152) (Ping Flood) (Reset Flood) (Settings Flood)

FreeBSD : h2o -- use after free on premature connection close (65bb1858-27de-11e6-b714-74d02b9a84d5)

FreeBSD : h2o -- Use-after-free vulnerability (d0b12952-cb86-11e6-906f-0cc47a065786)

FreeBSD : habari -- XSS Vulnerability (578f6322-c450-11dd-a721-0030843d3802)

FreeBSD : hadoop2 -- unauthorized disclosure of data vulnerability (5dd39f26-ed68-11e5-92ce-002590263bf5)

FreeBSD : hafiye -- lack of terminal escape sequence filtering (027380b7-3404-11d9-ac1b-000d614f7fad)

FreeBSD : haproxy -- buffer overflow (617959ce-a5f6-11e1-a284-0023ae8e59f0)

FreeBSD : haproxy -- denial of service (f1c219ba-3f14-11e6-b3c8-14dae9d210b8)

FreeBSD : haproxy -- information leak vulnerability (cbfa8bd7-24b6-11e5-86ff-14dae9d210b8)

FreeBSD : HAproxy -- serious vulnerability affecting the HPACK decoder used for HTTP/2 (7f829d44-7509-11ea-b47c-589cfc0f81b0)

FreeBSD : hashcash -- format string vulnerability (5ebfe901-a3cb-11d9-b248-000854d03344)

FreeBSD : hashcash -- heap overflow vulnerability (2be7c122-0614-11db-9156-000e0c2e438a)

FreeBSD : hdf5 -- multiple vulnerabilities (91e039ed-d689-11e6-9171-14dae9d210b8)

FreeBSD : heartbeat -- insecure temporary file creation vulnerability (f6447303-9ec9-11da-b410-000e0c2e438a)

FreeBSD : heimdal -- bypass of capath policy (40a8d798-4615-11e7-8080-a4badb2f4699)

FreeBSD : heimdal -- Multiple vulnerabilities (b62c80c2-b81a-11da-bec5-00123ffe8333)

FreeBSD : heimdal kadmind remote heap buffer overflow (446dbecb-9edc-11d8-9366-0020ed76ef5a)

FreeBSD : Helm -- client unpacking chart that contains malicious content (2a8b79c3-1b6e-11e9-8cf4-1c39475b9f84)

FreeBSD : helvis -- arbitrary file deletion problem (0cf3480d-5fdf-11d9-b721-00065be4b5b6)

FreeBSD : helvis -- information leak vulnerabilities (bb99f803-5fde-11d9-b721-00065be4b5b6)

FreeBSD : hiawatha -- integer overflow in Content-Length header parsing (b13414c9-50ba-11e0-975a-000c29cc39d3)

FreeBSD : hiawatha -- memory leak in PreventSQLi routine (eef56761-11eb-11e1-bb94-001c140104d4)

FreeBSD : hive -- authorization logic vulnerability (a5c204b5-4153-11e6-8dfe-002590263bf5)

FreeBSD : hlstats -- multiple XSS vulnerabilities (09639ccc-3abb-11db-81e1-000e0c2e438a)

FreeBSD : horde -- 'url' disclosure of sensitive information vulnerability (c7c09579-b466-11da-82d0-0050bf27ba24)

FreeBSD : horde -- Horde Page Title XSS Vulnerability (396ee517-a607-11d9-ac72-000bdb1444a4)

FreeBSD : horde -- multiple parameter XSS vulnerabilities (09429f7c-fd6e-11da-b1cd-0050bf27ba24)

FreeBSD : horde -- multiple vulnerabilities (7d239578-7ff2-11dd-8de5-0030843d3802)

FreeBSD : horde -- Phishing and XSS Vulnerabilities (e2e8d374-2e40-11db-b683-0008743bf21a)

FreeBSD : horde -- remote code execution vulnerability in the help viewer (2db97aa6-be81-11da-9b82-0050bf27ba24)

FreeBSD : horde -- various problems in dereferrer (e94cb43d-0c4a-11db-9016-0050bf27ba24)

FreeBSD : horde -- XSS vulnerabilities (338d1723-5f03-11d9-92a7-000bdb1444a4)

FreeBSD : horde -- XSS vulnerabilities (3aa8b781-d2c4-11e5-b2bd-002590263bf5)

FreeBSD : horde -- XSS vulnerabilities in MIME viewers (873a6542-5b8d-11da-b96e-000fb586ba73)

FreeBSD : horde -- XSS vulnerabilities in several of Horde's templates (01356ccc-6a87-11da-b96e-000fb586ba73)

FreeBSD : horde -- XSS vulnerability in help window (ed1d404d-2784-11d9-b954-000bdb1444a4)

FreeBSD : horde-base -- multiple vulnerabilities (ee23aa09-a175-11de-96c0-0011098ad87f)

FreeBSD : horde-base -- XSS and CSRF vulnerabilities (8fc55043-cb1e-11df-9c1b-0011098ad87f)

FreeBSD : horde-base -- XSS: VCARD attachments vulnerability (a3314314-f731-11df-a757-0011098ad87f)

FreeBSD : horde-gollem -- XSS vulnerability (e08c596e-cb28-11df-9c1b-0011098ad87f)

FreeBSD : horde-imp -- XSS vulnerability (6c4db192-cb23-11df-9c1b-0011098ad87f)

FreeBSD : hostapd -- multiple vulnerabilities (04bc4e23-9a70-42cb-9fec-3613632d34bc)

FreeBSD : hostapd and wpa\_supplicant -- multiple vulnerabilities (976567f6-05c5-11e6-94fa-002590263bf5)

FreeBSD : hostapd and wpa\_supplicant -- multiple vulnerabilities (bbc0db92-084c-11e5-bb90-002590263bf5)

FreeBSD : hostapd and wpa\_supplicant -- psk configuration parameter update allowing arbitrary data to be written (967b852b-1e28-11e6-8dd3-002590263bf5)

FreeBSD : hplip -- hpssd Denial of Service (37940643-be1b-11dd-a578-0030843d3802)

FreeBSD : hsftp format string vulnerabilities (316e1c9b-671c-11d8-9aad-000a95bc6fae)

FreeBSD : htdig -- XSS vulnerability (673aec6f-1cae-11da-bc01-000e0c2e438a)

FreeBSD : HTMLDOC -- buffer overflow issues when reading AFM files and parsing page sizes (6d08fa63-83bf-11e3-bdba-080027ef73ec)

FreeBSD : hylafax -- unauthorized login vulnerability (8eabaad9-641f-11d9-92a7-000a95bc6fae)

FreeBSD : i2p -- Multiple Vulnerabilities (13419364-1685-11e4-bf04-60a44c524f57)

FreeBSD : icecast -- HTTP header overflow (741c3957-1d69-11d9-a804-0050fc56d258)

FreeBSD : icecast -- XSS Vulnerability (b2cfb400-1df0-11d9-a859-0050fc56d258)

FreeBSD : icecast 1.x multiple vulnerabilities (5e92e8a2-5d7b-11d8-80e3-0020ed76ef5a)

FreeBSD : icecast2 (1996)

FreeBSD : Icinga -- buffer overflow in classic web interface (4e95eb4e-b737-11e3-87cd-f0def10dca57)

FreeBSD : icingaweb2 -- remote code execution (ad9b77f6-4163-11e6-b05b-14dae9d210b8)

FreeBSD : icoutils -- check\_offset overflow on 64-bit systems (57facd35-ddf6-11e6-915d-001b3856973b)

FreeBSD : icu -- multiple vulnerabilities (607f8b57-7454-42c6-a88a-8706f327076d)

FreeBSD : id Tech 3 -- remote code execution vulnerability (e48355d7-1548-11e7-8611-0090f5f2f347)

FreeBSD : id3lib -- insecure temporary file creation (15ec9123-7061-11dc-b372-001921ab2fa4)

FreeBSD : ident2 double byte buffer overflow (99230277-8fb4-11d8-8b29-0020ed76ef5a)

FreeBSD : ifmail -- unsafe set-user-ID application (746ca1ac-21ec-11d9-9289-000c41e2cdad)

FreeBSD : ikiwiki -- authentication bypass vulnerability (7b35a77a-0151-11e7-ae1b-002590263bf5)

FreeBSD : ikiwiki -- cleartext passwords (90db9983-2f53-11dd-a0d8-0016d325a0ed)

FreeBSD : ikiwiki -- cross site request forging (8d2c0ce1-08b6-11dd-94b4-0016d325a0ed)

FreeBSD : ikiwiki -- empty password security hole (09066828-2ef1-11dd-a0d8-0016d325a0ed)

FreeBSD : ikiwiki -- improper symlink verification vulnerability (31d9fbb4-9d09-11dc-a29d-0016d325a0ed)

FreeBSD : ikiwiki -- insufficient blacklisting in teximg plugin (6e8f54af-a07d-11de-a649-000c2955660f)

FreeBSD : ikiwiki -- javascript insertion via uris (739329c8-d8f0-11dc-ac2f-0016d325a0ed)

FreeBSD : ikiwiki -- multiple vulnerabilities (5ed094a0-0150-11e7-ae1b-002590263bf5)

FreeBSD : ikiwiki -- tty hijacking via ikiwiki-mass-rebuild (3145faf1-974c-11e0-869e-000c29249b2e)

FreeBSD : ikiwiki -- XSS vulnerability (0297b260-2b3b-11e6-ae88-002590263bf5)

FreeBSD : ImageMagick -- BMP decoder buffer overflow (b6cad7f3-fb59-11d8-9837-000c41e2cdad)

FreeBSD : imagemagick -- buffer overflow (82b702e0-1907-11e6-857b-00221503d280)

FreeBSD : ImageMagick -- denial of service via a crafted font file (16fb4f83-a2ab-11e7-9c14-009c02a2ab30)

FreeBSD : ImageMagick -- EXIF parser buffer overflow (eeb1c128-33e7-11d9-a9e7-0001020eed82)

FreeBSD : ImageMagick -- format string vulnerability (713c3913-8c2b-11d9-b58c-0001020eed82)

FreeBSD : ImageMagick -- heap overflow vulnerability (19d35b0f-ba73-11e6-b1cf-14dae9d210b8)

FreeBSD : ImageMagick -- multiple vulnerabilities (0d724b05-687f-4527-9c03-af34d3b094ec) (ImageTragick)

FreeBSD : ImageMagick -- multiple vulnerabilities (10f7f782-901c-11e6-a590-14dae9d210b8)

FreeBSD : ImageMagick -- multiple vulnerabilities (183d700e-ec70-487e-a9c4-632324afa934)

FreeBSD : ImageMagick -- multiple vulnerabilities (50776801-4183-11e7-b291-b499baebfeaf)

FreeBSD : ImageMagick -- multiple vulnerabilities (5140dc69-b65e-11e1-9425-001b21614864)

FreeBSD : ImageMagick -- multiple vulnerabilities (f5b29ec0-71f9-11dc-8c6a-00304881ac9a)

FreeBSD : ImageMagick -- PSD handler heap overflow vulnerability (597e2bee-68ea-11d9-a9e7-0001020eed82)

FreeBSD : ImageMagick -- ReadPNMImage() heap overflow vulnerability (cd286cc5-b762-11d9-bfb7-000c6ec775d9)

FreeBSD : ImageMagick -- SGI Image File heap overflow vulnerability (18e3a5be-81f9-11db-95a2-0012f06707f0)

FreeBSD : ImageMagick and GraphicsMagick -- DoS via specially crafted PNG file (98690c45-0361-11e2-a391-000c29033c32)

FreeBSD : ImageMagick png vulnerability fix (a713c0f9-ec54-11d8-9440-000347a4fa7d)

FreeBSD : ImageMagick7 -- multiple vulnerabilities (e1f67063-aab4-11e6-b2d3-60a44ce6887b)

FreeBSD : imap-uw -- authentication bypass when CRAM-MD5 is enabled (d1bbc235-c0c9-45cd-8d2d-c1b8fd22e616)

FreeBSD : imap-uw -- imap c-client buffer overflow (69a20ce4-dfee-11dd-a765-0030843d3802)

FreeBSD : imap-uw -- local buffer overflow vulnerabilities (a6713190-dfea-11dd-a765-0030843d3802)

FreeBSD : imap-uw -- mailbox name handling remote buffer vulnerability (1f6e2ade-35c2-11da-811d-0050bf27ba24)

FreeBSD : imap-uw -- University of Washington IMAP c-client Remote Format String Vulnerability (5ed2f96b-33b7-4863-8c6b-540d22344424)

FreeBSD : imlib -- BMP decoder heap buffer overflow (00644f03-fb58-11d8-9837-000c41e2cdad)

FreeBSD : imlib -- xpm heap buffer overflows and integer overflows (2001103a-6bbd-11d9-851d-000a95bc6fae)

FreeBSD : imlib2 -- BMP decoder buffer overflow (ba005226-fb5b-11d8-9837-000c41e2cdad)

FreeBSD : imlib2 -- denial of service vulnerabilities (99d3a8a5-c13c-11e5-96d6-14dae9d210b8)

FreeBSD : Imlib2 -- multiple image file processing vulnerabilities (92442c4b-6f4a-11db-bd28-0012f06707f0)

FreeBSD : imlib2 -- XPM processing buffer overflow vulnerability (910486d5-ba4d-11dd-8f23-0019666436c2)

FreeBSD : imp (1649)

FreeBSD : imp (2010)

FreeBSD : imp3 -- XSS hole in the HTML viewer (efc4819b-0b2d-11d9-bfe1-000bdb1444a4)

FreeBSD : imwheel -- insecure handling of PID file (e31d44a2-21e3-11d9-9289-000c41e2cdad)

FreeBSD : Incorrect cross-realm trust handling in Heimdal (bfb36941-84fa-11d8-a41f-0020ed76ef5a)

FreeBSD : Information disclosure - Gitea leaks email addresses (7c750960-b129-11e8-9fcd-080027f43a02)

FreeBSD : ingo -- local arbitrary shell command execution (18a14baa-5ee5-11db-ae08-0008743bf21a)

FreeBSD : inn -- plaintext command injection into encrypted channel (a7975581-ee26-11e1-8bd8-0022156e8794)

FreeBSD : insecure temporary file creation in xine-check, xine-bugreport (fde53204-7ea6-11d8-9645-0020ed76ef5a)

FreeBSD : inspircd -- authentication bypass vulnerability (70c85c93-743c-11e6-a590-14dae9d210b8)

FreeBSD : inspircd -- buffer overflow (f5f00804-a03b-11e1-a284-0023ae8e59f0)

FreeBSD : inspircd -- DoS (b808c3a8-ae30-11e5-b864-14dae9d210b8)

FreeBSD : Intel(R) NVMUpdate -- Intel(R) Ethernet Controller X710/XL710 NVM Security Vulnerability (a4b7def1-e165-11e6-9d84-90e2ba9881c8)

FreeBSD : iodined -- authentication bypass (0981958a-f733-11e3-8276-071f1604ef8a)

FreeBSD : iperf3 -- buffer overflow (d6bbf2d8-2cfc-11e6-800b-080027468580)

FreeBSD : ipsec-tools -- Memory leak leading to denial of service (35431f79-fe3e-11e4-ba63-000c292ee6b8)

FreeBSD : ipsec-tools -- remotely exploitable computational-complexity attack (974a6d32-3fda-11e8-aea4-001b216d295b)

FreeBSD : ipset-tools -- Denial of Service Vulnerabilities (abcacb5a-e7f1-11dd-afcd-00e0815b8da8)

FreeBSD : IRC Services-- Denial of Service Vulnerability (e5a9de5f-c6bc-11dc-b9f1-00a0cce0781e)

FreeBSD : irc-ratbox -- multiple vulnerabilities (192609c8-0c51-11df-82a0-00248c9b4be7)

FreeBSD : irc/bitchx -- multiple vulnerabilities (0a799a8e-c9d4-11e2-a424-14dae938ec40)

FreeBSD : ircd-hybrid-ru (1456)

FreeBSD : ircd-ratbox and charybdis -- remote DoS vulnerability (4108cc57-54d7-11e2-9483-14dae938ec40)

FreeBSD : irssi -- heap corruption and missing boundary checks (e78261e4-803d-11e6-a590-14dae9d210b8)

FreeBSD : irssi -- multiple vulnerabilities (31001c6b-63e7-11e7-85aa-a4badb2f4699)

FreeBSD : irssi -- multiple vulnerabilities (3b7967f1-49e8-11df-83fb-0015587e2cc1)

FreeBSD : Irssi -- multiple vulnerabilities (3d6be69b-d365-11e6-a071-001e67f15f5a)

FreeBSD : irssi -- multiple vulnerabilities (7afc5e56-156d-11e8-95f2-005056925db4)

FreeBSD : irssi -- multiple vulnerabilities (85e2c7eb-b74b-11e7-8546-5cf3fcfdd1f1)

FreeBSD : irssi -- multiple vulnerabilities (a3764767-f31e-11e7-95f2-005056925db4)

FreeBSD : irssi -- remote DoS (165e8951-4be0-11e7-a539-0050569f7e80)

FreeBSD : irssi -- Use after free (d38bbb79-14f3-11e9-9ce2-28d244aee256)

FreeBSD : irssi -- Use after free when sending SASL login to the server (475f952c-9b29-11e9-a8a5-6805ca0b38e8)

FreeBSD : irssi -- use-after-free potential code execution (06f931c0-0be0-11e7-b4bf-5404a68ad561)

FreeBSD : isakmpd (2056)

FreeBSD : isakmpd payload handling denial-of-service vulnerabilities (b7cb488c-8349-11d8-a41f-0020ed76ef5a)

FreeBSD : ISC KEA -- Multiple vulnerabilities (20b92374-d62a-11e9-af73-001b217e4ee5)

FreeBSD : isc-dhcp -- Multiple vulnerabilities (2040c7f5-1e3a-11e8-8ae9-0050569f0b83)

FreeBSD : isc-dhcp -- multiple vulnerabilities (c7fa3618-d5ff-11e1-90a2-000c299b62e1)

FreeBSD : isc-dhcp-client -- dhclient does not strip or escape shell meta-characters (7e69f00d-632a-11e0-9f3a-001d092480a4)

FreeBSD : isc-dhcp-client -- Stack overflow vulnerability (c444c8b7-7169-11de-9ab7-000c29a67389)

FreeBSD : isc-dhcp-server -- DHCPv6 crash (dc9f8335-2b3b-11e0-a91b-00e0815b8da8)

FreeBSD : isc-dhcp-server -- DoS in DHCPv6 (1800886c-3dde-11e1-89b4-001ec9578670)

FreeBSD : isc-dhcp-server -- Empty link-address denial of service (f154a3c7-f7f4-11df-b617-00e0815b8da8)

FreeBSD : isc-dhcp-server -- Remote DoS (93be487e-211f-11e1-89b4-001ec9578670)

FreeBSD : isc-dhcp-server -- server halt upon processing certain packets (510b630e-c43b-11e0-916c-00e0815b8da8)

FreeBSD : isc-dhcp3 (1286)

FreeBSD : isc-dhcp3 (2477)

FreeBSD : isc-dhcp3-server buffer overflow in logging mechanism (7a9d5dfe-c507-11d8-8898-000d6111a684)

FreeBSD : isc-dhcpd -- Denial of Service (05eeb7e9-b987-11e5-83ef-14dae9d210b8)

FreeBSD : isc-dhcpd -- format string vulnerabilities (ccd325d2-fa08-11d9-bc08-0001020eed82)

FreeBSD : isolate -- local root exploit (b74a8076-9b1f-11df-9f58-021e8c343e76)

FreeBSD : Istio -- Security vulnerabilities (484d3f5e-653a-11e9-b0e3-1c39475b9f84)

FreeBSD : ja-squirrelmail (1976)

FreeBSD : jabberd -- 3 buffer overflows (55041d37-ff62-11d9-a9a5-000ae4641456)

FreeBSD : jabberd -- authentication bypass vulnerability (76d80b33-7211-11e7-998a-08606e47f965)

FreeBSD : jabberd -- denial-of-service vulnerability (2e25d38b-54d1-11d9-b612-000c6e8f12ef)

FreeBSD : jabberd -- domain spoofing in server dialback protocol (4d1d2f6d-ec94-11e1-8bd8-0022156e8794)

FreeBSD : jabberd -- remote buffer overflow vulnerability (553224e7-4325-11d9-a3d5-000c6e8f12ef)

FreeBSD : jabberd -- SASL Negotiation Denial of Service Vulnerability (f4af098d-d921-11da-ad4a-00123ffe8333)

FreeBSD : james -- multiple vulnerabilities (be3069c9-67e7-11e5-9909-002590263bf5)

FreeBSD : jansson -- local denial of service vulnerabilities (a6cd01fa-11bd-11e6-bb3c-9cb654ea3e1c)

FreeBSD : jasper -- buffer overflow (8ff84335-a7da-11e2-b3f5-003067c2616f)

FreeBSD : jasper -- multiple vulnerabilities (006e3b7c-d7d7-11e5-b85f-0018fe623f2b)

FreeBSD : jasper -- multiple vulnerabilities (f1692469-45ce-11e5-adde-14dae9d210b8)

FreeBSD : java -- multiple vulnerabilities (a5934ba8-a376-11e5-85e9-14dae9d210b8)

FreeBSD : Java 1.7 -- security manager bypass (16846d1e-f1de-11e1-8bd8-0022156e8794)

FreeBSD : java 7.x -- security manager bypass (d5e0317e-5e45-11e2-a113-c48508086173)

FreeBSD : jdk -- jar directory traversal vulnerability (18e5428f-ae7c-11d9-837d-000e0c2e438a)

FreeBSD : jdk/jre -- Applet Caching May Allow Network Access Restrictions to be Circumvented (c93e4d41-75c5-11dc-b903-0016179b2dd5)

FreeBSD : jdk/jre -- Security Vulnerability With Java Plugin (ac619d06-3ef8-11d9-8741-c942c075aa41)

FreeBSD : jenkins -- HTTP access to the server to retrieve the master cryptographic key (3a65d33b-5950-11e2-b66b-00e0814cab4e)

FreeBSD : jenkins -- multiple issues (1c2a9d76-9d98-43c3-8f5d-8c059b104d99)

FreeBSD : jenkins -- multiple issues (6dc3c61c-e866-4c27-93f7-ae50908594fd)

FreeBSD : jenkins -- multiple vulnerabilities (06ab7724-0fd7-427e-a5ce-fe436302b10c)

FreeBSD : jenkins -- multiple vulnerabilities (20a1881e-8a9e-11e8-bddf-d017c2ca229d)

FreeBSD : jenkins -- multiple vulnerabilities (22dc4a22-d1e5-11e4-879c-00e0814cab4e)

FreeBSD : jenkins -- multiple vulnerabilities (23af0425-9eac-11e5-b937-00e0814cab4e)

FreeBSD : jenkins -- multiple vulnerabilities (3350275d-cd5a-11e8-a7be-3497f683cb16)

FreeBSD : jenkins -- multiple vulnerabilities (3aa27226-f86f-11e8-a085-3497f683cb16)

FreeBSD : jenkins -- multiple vulnerabilities (3e0507c6-9614-11e3-b3a5-00e0814cab4e)

FreeBSD : jenkins -- multiple vulnerabilities (5bf6ed6d-9002-4f43-ad63-458f59e45384)

FreeBSD : jenkins -- multiple vulnerabilities (5cfa9d0c-73d7-4642-af4f-28fbed9e9404)

FreeBSD : jenkins -- multiple vulnerabilities (622e14b1-b40c-11e2-8441-00e0814cab4e)

FreeBSD : jenkins -- multiple vulnerabilities (631c4710-9be5-4a80-9310-eb2847fe24dd)

FreeBSD : jenkins -- multiple vulnerabilities (6905f05f-a0c9-11e8-8335-8c164535ad80)

FreeBSD : jenkins -- multiple vulnerabilities (7480b6ac-adf1-443e-a33c-3a3c0becba1e)

FreeBSD : jenkins -- multiple vulnerabilities (7a7891fc-6318-447a-ba45-31d525ec11a0)

FreeBSD : jenkins -- multiple vulnerabilities (7e01df39-db7e-11e5-b937-00e0814cab4e)

FreeBSD : jenkins -- multiple vulnerabilities (7fe5b84a-78eb-11e2-8441-00e0814cab4e)

FreeBSD : jenkins -- multiple vulnerabilities (8e9c3f5a-715b-4336-8d05-19babef55e9e)

FreeBSD : jenkins -- multiple vulnerabilities (9720bb39-f82a-402f-9fe4-e2c875bdda83)

FreeBSD : jenkins -- multiple vulnerabilities (a250539d-d1d4-4591-afd3-c8bdfac335d8)

FreeBSD : jenkins -- multiple vulnerabilities (aaba17aa-782e-4843-8a79-7756cfa2bf89)

FreeBSD : jenkins -- multiple vulnerabilities (d846af5b-00f4-11e2-b6d0-00e0814cab4e)

FreeBSD : jenkins -- multiple vulnerabilities (debf6353-5753-4e9a-b710-a83ecdd743de)

FreeBSD : jenkins -- multiple vulnerabilities (df3db21d-1a4d-4c78-acf7-4639e5a795e0)

FreeBSD : jenkins -- multiple vulnerabilities (e387834a-17ef-11e6-9947-7054d2909b71)

FreeBSD : jenkins -- Path traversal vulnerability allows access to files outside plugin resources (5d374fbb-bae3-45db-afc0-795684ac7353)

FreeBSD : jenkins -- remote code execution via unsafe deserialization (b665668a-91db-4f13-8113-9e4b5b0e47f7)

FreeBSD : jenkins -- Remote code execution vulnerability in remoting module (27eee66d-9474-44a5-b830-21ec12a1c307)

FreeBSD : jenkins -- remote execution, privilege escalation, XSS, password exposure, ACL hole, DoS (549a2771-49cc-11e4-ae2c-c80aa9043978)

FreeBSD : jenkins -- slave-originated arbitrary code execution on master servers (0dad9114-60cc-11e4-9e84-0022156e8794)

FreeBSD : jenkins -- Two startup race conditions (7136e6b7-e1b3-11e7-a4d3-000c292ee6b8)

FreeBSD : jenkins -- XSS vulnerability (9448a82f-6878-11e1-865f-00e0814cab4e)

FreeBSD : jetty -- multiple vulnerabilities (6ae7cef2-a6ae-11dc-95e6-000c29c5647f)

FreeBSD : jetty -- multiple vulnerability (0832ee18-cf77-11dc-8c6a-00304881ac9a)

FreeBSD : joomla -- flaw in the reset token validation (8514b6e7-6f0f-11dd-b3db-001c2514716c)

FreeBSD : joomla -- multiple remote vulnerabilities (7bb127c1-a5aa-11db-9ddc-0011098b2f36)

FreeBSD : joomla -- multiple vulnerabilities (0ab423e7-3822-11db-81e1-000e0c2e438a)

FreeBSD : Joomla -- multiple vulnerabilities (1f935f61-075d-11db-822b-728b50d539a3)

FreeBSD : joomla -- multiple vulnerabilities (4872d9a7-4128-11dc-bdb0-0016179b2dd5)

FreeBSD : joomla -- multiple vulnerabilities (8d10038e-515c-11df-83fb-0015587e2cc1)

FreeBSD : joomla -- multiple vulnerabilities (a9f60ce8-a4e0-11e5-b864-14dae9d210b8)

FreeBSD : joomla -- multiple vulnerabilities (bdccd14b-5aac-11de-a438-003048590f9e)

FreeBSD : joomla -- Privilege Escalation (f46c4c6a-ba25-11e1-806a-001143cd36d8)

FreeBSD : Joomla! -- Core - ACL Violation vulnerabilities (03e54e42-7ac6-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core - CSRF Protection vulnerabilities (ec2d1cfd-7ac5-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core - Multiple Vulnerabilities (9fa1a0ac-b2e0-11e3-bb07-6cf0490a8c18)

FreeBSD : Joomla! -- Core - Open Redirect vulnerability (deaba148-7ac5-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core - Remote File Execution/Denial of Service vulnerabilities (cec4d01a-7ac5-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core - SQL Injection/ACL Violation vulnerabilities (0ebc6e78-7ac6-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core - Unauthorized Login vulnerability (beb3d5fc-7ac5-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core - XSS Vulnerability (adbb32d9-7ac5-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core - XSS Vulnerability (f8c37915-7ac5-11e5-b35a-002590263bf5)

FreeBSD : Joomla! -- Core XSS Vulnerabilities (4158c57e-5d39-11e3-bc1e-6cf0490a8c18)

FreeBSD : Joomla! -- multiple vulnerabilities (624b45c0-c7f3-11e6-ae1b-002590263bf5)

FreeBSD : Joomla! -- multiple vulnerabilities (a27d234a-c7f2-11e6-ae1b-002590263bf5)

FreeBSD : Joomla! -- multiple vulnerabilities (c0ef061a-c7f0-11e6-ae1b-002590263bf5)

FreeBSD : Joomla! -- multiple vulnerabilities (f0806cad-c7f1-11e6-ae1b-002590263bf5)

FreeBSD : Joomla! -- XXS and DDoS vulnerabilities (57df803e-af34-11e2-8d62-6cf0490a8c18)

FreeBSD : joomla15 -- com\_mailto Timeout Issue (739b94a4-838b-11de-938e-003048590f9e)

FreeBSD : Joomla3 -- SQL Injection (3c2549b3-3bed-11e7-a9f0-a4badb296695)

FreeBSD : joomla3 -- vulnerabilitiesw (6aa398d0-1c4d-11e9-96dd-a4badb296695)

FreeBSD : joomla3 -- vulnerabilitiesw (bf2b9c56-b93e-11e8-b2a8-a4badb296695)

FreeBSD : jpgraph2 -- XSS vulnerability (77b7ffb7-e937-11e5-8bed-5404a68ad561)

FreeBSD : junkbuster -- heap corruption vulnerability and configuration modification vulnerability (97edf5ab-b319-11d9-837d-000e0c2e438a)

FreeBSD : Jupyter notebook -- cross-site inclusion (XSSI) vulnerability (72a6e3be-483a-11e9-92d7-f1590402501e)

FreeBSD : Jupyter notebook -- open redirect vulnerability (fe7e322f-522d-11e9-98b5-216e512dad89)

FreeBSD : Jupyter Notebook -- vulnerability (b3edc7d9-9af5-4daf-88f1-61f68f4308c2)

FreeBSD : kaffeine -- buffer overflow vulnerability (4bfcd857-c628-11da-b2fb-000e0c2e438a)

FreeBSD : kamailio - buffer overflow (5af6378b-bd88-4997-bccc-b9ba2daecdd2)

FreeBSD : kamailio -- SEAS Module Heap overflow (c428de09-ed69-11e5-92ce-002590263bf5)

FreeBSD : kanboard -- multiple privilege escalation vulnerabilities (7d7e05fb-64da-435a-84fb-4061493b89b9)

FreeBSD : kauth: Local privilege escalation (0baee383-356c-11e7-b9a9-50e549ebab6c)

FreeBSD : KDE -- multiple vulnerabilities (6f358f5a-c7ea-11de-a9f3-0030843d3802)

FreeBSD : KDE Frameworks -- malicious .desktop files execute code (f5f0a640-bae8-11e9-bb3a-001e2a3f778d)

FreeBSD : kde-runtime -- incorrect CBC encryption handling (7a8a74d1-9c34-11e4-a40b-5453ed2e2b49)

FreeBSD : kde-runtime -- kdesu: displayed command truncated by unicode string terminator (41fe4724-06a2-11e7-8e3e-5453ed2e2b49)

FreeBSD : kde-workspace -- privilege escalation (dafa13a8-6e9b-11e4-8ef7-5453ed2e2b49)

FreeBSD : kdebase (1516)

FreeBSD : kdebase -- Kate backup file permission leak (2e116ba5-f7c3-11d9-928e-000b5d7e6dd5)

FreeBSD : kdegraphics (1796)

FreeBSD : kdelibs (1739)

FreeBSD : kdelibs (2097)

FreeBSD : kdelibs -- directory traversal vulnerability (4472ab39-6c66-11e6-9ca5-50e549ebab6c)

FreeBSD : kdelibs -- insecure temporary file creation (29dd0065-81fa-11d9-a9e7-0001020eed82)

FreeBSD : kdelibs -- integer overflow in khtml (d8fbf13a-6215-11db-a59e-0211d85f11fb)

FreeBSD : kdelibs -- KAuth PID Reuse Flaw (2f90556f-18c6-11e4-9cc4-5453ed2e2b49)

FreeBSD : kdelibs -- kimgio input validation errors (06404241-b306-11d9-a788-0001020eed82)

FreeBSD : kdelibs -- konqueror cross-domain cookie injection (2797b27a-f55b-11d8-81b0-000347a4fa7d)

FreeBSD : kdelibs -- local DCOP denial of service vulnerability (972697a7-9a42-11d9-a256-0001020eed82)

FreeBSD : kdelibs insecure temporary file handling (603fe36d-ec9d-11d8-b913-000c41e2cdad)

FreeBSD : kdelibs3 -- konqueror FTP command injection vulnerability (832e9d75-5bfc-11d9-a9e7-0001020eed82)

FreeBSD : kdelibs4 -- KMail/KIO POP3 SSL Man-in-the-middle Flaw (4a114331-0d24-11e4-8dd2-5453ed2e2b49)

FreeBSD : kdelibs4, rekonq -- input validation failure (6d21a287-fce0-11e0-a828-00235a5f2c9a)

FreeBSD : kdepim exploitable buffer overflow in VCF reader (da6f265b-8f3d-11d8-8b29-0020ed76ef5a)

FreeBSD : kdepimlibs -- directory traversal on KTNEF (e550fc62-069a-11e7-8e3e-5453ed2e2b49)

FreeBSD : kdeutils4 -- Directory traversal vulnerability (7fb9e739-0e6d-11e1-87cd-00235a5f2c9a)

FreeBSD : kdewebdev -- kommander untrusted code execution vulnerability (91f1adc7-b3e9-11d9-a788-0001020eed82)

FreeBSD : KDM -- local privilege escalation vulnerability (3987c5d1-47a9-11df-a0d5-0016d32f24fb)

FreeBSD : kdm -- passwordless login vulnerability (79b616d0-66d1-11dc-b25f-02e0185f8d72)

FreeBSD : kea -- unexpected termination while handling a malformed packet (59e7eb28-b309-11e5-af83-80ee73b5dcf5)

FreeBSD : KeePassX -- information disclosure (918a5d1f-9d40-11e5-8f5c-002590263bf5)

FreeBSD : kf5-kauth -- Insecure handling of arguments in helpers (e8bcac84-2d5c-11e9-9a74-e0d55e2a8bf9)

FreeBSD : kibana4 -- CSRF vulnerability (fb2475c2-9125-11e5-bd18-002590263bf5)

FreeBSD : kibana4 -- XSS vulnerability (a7a4e96c-ba50-11e5-9728-002590263bf5)

FreeBSD : kio-extras -- HTML Thumbnailer automatic remote file access (1460aa25-e6ab-11e8-a733-e0d55e2a8bf9)

FreeBSD : kio: Information Leak when accessing https when using a malicious PAC file (f714d8ab-028e-11e7-8042-50e549ebab6c)

FreeBSD : koffice (2414)

FreeBSD : konquerer -- address bar spoofing (14ad2a28-66d2-11dc-b25f-02e0185f8d72)

FreeBSD : konqueror -- Password Disclosure for SMB Shares (4593cb09-4c81-11d9-983e-000c6e8f12ef)

FreeBSD : konversation -- crash in IRC message parsing (795ccee1-c7ed-11e7-ad7d-001e2a3f778d)

FreeBSD : Konversation -- out-of-bounds read on a heap-allocated array (0167f5ad-64ea-11e4-98c1-00269ee29e57)

FreeBSD : konversation -- shell script command injection (5c7bb4dd-6a56-11d9-97ec-000c6e8f12ef)

FreeBSD : kpdf -- heap based buffer overflow (432bf98d-9e25-11da-b410-000e0c2e438a)

FreeBSD : kpopup -- local root exploit and local denial of service (1613db79-8e52-11da-8426-000fea0a9611)

FreeBSD : krb5 (1676)

FreeBSD : krb5 -- ASN.1 decoder denial-of-service vulnerability (bd60922b-fb8d-11d8-a13e-000a95bc6fae)

FreeBSD : krb5 -- client impersonation vulnerability (4ccbd40d-03f7-11e0-bf50-001a926c7637)

FreeBSD : krb5 -- double-free vulnerabilities (86a98b57-fb8e-11d8-9343-000a95bc6fae)

FreeBSD : krb5 -- heap buffer overflow vulnerability in libkadm5srv (0bb7677d-52f3-11d9-a9e7-0001020eed82)

FreeBSD : krb5 -- KDC denial of service vulnerability (62d45229-4fa0-11e6-9d13-206a8a720317)

FreeBSD : krb5 -- KDC double free vulnerability (86b8b655-4d1a-11df-83fb-0015587e2cc1)

FreeBSD : krb5 -- KDC NULL pointer dereference in TGS handling (6c7d9a35-2608-11e1-89b4-001ec9578670)

FreeBSD : krb5 -- MITKRB5-SA-2011-001, kpropd denial of service (64f24a1e-66cf-11e0-9deb-f345f3aa24f0)

FreeBSD : krb5 -- MITKRB5-SA-2011-002, KDC vulnerable to hang when using LDAP back end (4ab413ea-66ce-11e0-bf05-d445f3aa24f0)

FreeBSD : krb5 -- MITKRB5-SA-2011-003, KDC vulnerable to double-free when PKINIT enabled (7edac52a-66cd-11e0-9398-5d45f3aa24f0)

FreeBSD : krb5 -- MITKRB5-SA-2011-004, kadmind invalid pointer free() [CVE-2011-0285] (6a3c3e5c-66cb-11e0-a116-c535f3aa24f0)

FreeBSD : krb5 -- multiple checksum handling vulnerabilities (0d57c1d9-03f4-11e0-bf50-001a926c7637)

FreeBSD : krb5 -- multiple checksum handling vulnerabilities (11bbccbc-03ee-11e0-bcdb-001fc61c2a55)

FreeBSD : krb5 -- multiple denial of service vulnerabilities (9ac0f9c4-492b-11df-83fb-0015587e2cc1)

FreeBSD : krb5 -- Multiple vulnerabilities (3f3837cc-48fb-4414-aa46-5b1c23c9feae)

FreeBSD : krb5 -- NULL pointer dereference in the KDC PKINIT code [CVE-2013-1415] (f54584bc-7d2b-11e2-9bd1-206a8a720317)

FreeBSD : krb5 -- remote denial of service vulnerability (a30573dc-4893-11df-a5f9-001641aeabdf)

FreeBSD : krb5 -- requires\_preauth bypass in PKINIT-enabled KDC (406636fe-055d-11e5-aab1-d050996490d0)

FreeBSD : krb5 -- RFC 3961 key-derivation checksum handling vulnerability (1d193bba-03f6-11e0-bf50-001a926c7637)

FreeBSD : krb5 -- UDP ping-pong vulnerability in the kpasswd (password changing) service. [CVE-2002-2443] (e3f64457-cccd-11e2-af76-206a8a720317)

FreeBSD : krb5 -- unkeyed PAC checksum handling vulnerability (9f971cea-03f5-11e0-bf50-001a926c7637)

FreeBSD : krb5 -- Vulnerabilities in kadmind, libgssrpc, gss\_process\_context\_token VU#540092 (24ce5597-acab-11e4-a847-206a8a720317)

FreeBSD : krb5 -- Vulnerabilities in kadmind, libgssrpc, gss\_process\_context\_token VU#540092 (3a888a1e-b321-11e4-83b2-206a8a720317)

FreeBSD : krb5 1.11 -- New release/fix multiple vulnerabilities (dbf9e66c-bd50-11e4-a7ba-206a8a720317)

FreeBSD : krb5 1.12 -- New release/fix multiple vulnerabilities (63527d0d-b9de-11e4-8a48-206a8a720317)

FreeBSD : krb5-appl -- telnetd code execution vulnerability (4ddc78dc-300a-11e1-a2aa-0016ce01e285)

FreeBSD : krfb -- Multiple security issues in bundled libvncserver (fb25333d-442f-11e4-98f3-5453ed2e2b49)

FreeBSD : krfb -- Possible Denial of Service or code execution via integer overflow (be5421ab-1b56-11e4-a767-5453ed2e2b49)

FreeBSD : kronolith -- arbitrary local file inclusion vulnerability (a8af7d70-8007-11db-b280-0008743bf21a)

FreeBSD : kronolith -- XSS vulnerabilities in several of the calendar name and event data fields (36494478-6a88-11da-b96e-000fb586ba73)

FreeBSD : ksh93 -- certain environment variables interpreted as arithmetic expressions on startup, leading to code injection (8b20d716-49df-11ea-9f7b-206a8a720317)

FreeBSD : kstars -- exploitable set-user-ID application fliccd (0512b761-70fb-40d3-9954-aa4565528fa8)

FreeBSD : ktorrent -- multiple vulnerabilities (73f53712-d028-11db-8c07-0211d85f11fb)

FreeBSD : Kubectl -- Potential directory traversal (6a0129bf-54ad-11e9-987c-1c39475b9f84)

FreeBSD : kvirc -- multiple vulnerabilities (8685d412-8468-11df-8d45-001d7d9eb79a)

FreeBSD : KWallet-PAM -- Access to privileged files (83a548b5-4fa5-11e8-9a8e-001e2a3f778d)

FreeBSD : kwebkitpart, kde-runtime -- insufficient input validation (890b6b22-70fa-11e4-91ae-5453ed2e2b49)

FreeBSD : L2TP, ISAKMP, and RADIUS parsing vulnerabilities in tcpdump (96ba2dae-4ab0-11d8-96f2-0020ed76ef5a)

FreeBSD : l2tpd (1919)

FreeBSD : lbreakout2 vulnerability in environment variable handling (ad4f6ca4-6720-11d8-9fb5-000a95bc6fae)

FreeBSD : lcdproc (1760)

FreeBSD : lcms2 -- NULL pointer Dereference Denial of Service Vulnerability (9a0a892e-05d8-11e3-ba09-000c29784fd1)

FreeBSD : ldapscripts -- Command Line User Credentials Disclosure (3a81017a-8154-11dc-9283-0016179b2dd5)

FreeBSD : leafnode -- denial of service vulnerability (b5ffaa2a-ee50-4498-af99-61bc1b163c00)

FreeBSD : leafnode -- fetchnews denial-of-service triggered by transmission abort/timeout (66dbb2ee-99b8-45b2-bb3e-640caea67a60)

FreeBSD : leafnode denial-of-service triggered by article request (f7a3b18c-624c-4703-9756-b6b27429e5b0)

FreeBSD : leafnode fetchnews denial-of-service triggered by missing header (7b0208ff-3f65-4e16-8d4d-48fd9851f085)

FreeBSD : leafnode fetchnews denial-of-service triggered by truncated transmission (a051a4ec-3aa1-4dd1-9bdc-a61eb5700153)

FreeBSD : ledger -- multiple vulnerabilities (d843a984-7f22-484f-ba81-483ddbe30dc3)

FreeBSD : lftp -- multiple HTTP client download filename vulnerability (29b7e3f4-b6a9-11df-ae63-f255a795cb21)

FreeBSD : lftp HTML parsing vulnerability (d7af61c8-2cc0-11d8-9355-0020ed76ef5a)

FreeBSD : lha (1709)

FreeBSD : lha -- numerous vulnerabilities when extracting archives (273cc1a3-0d6b-11d9-8a8a-000c41e2cdad)

FreeBSD : lha buffer overflows and path traversal issues (a2ffb627-9c53-11d8-9366-0020ed76ef5a)

FreeBSD : libarchive -- Infinite loop in corrupt archives handling in libarchive (792bc222-c5d7-11db-9f82-000e0c2e438a)

FreeBSD : libarchive -- multiple vulnerabilities (4a0d9b53-395d-11e6-b3c8-14dae9d210b8)

FreeBSD : libarchive -- multiple vulnerabilities (7c63775e-be31-11e5-b5fe-002590263bf5)

FreeBSD : libarchive -- RCE vulnerability (2b4c8e1f-1609-11e6-b55e-b499baebfeaf)

FreeBSD : libaudiofile -- heap-based overflow in Microsoft ADPCM compression module (09f47c51-c1a6-11e3-a5ac-001b21614864)

FreeBSD : libav -- divide by zero (a928960a-2bdc-11e5-86ff-14dae9d210b8)

FreeBSD : libbson -- Denial of Service (10214bda-0902-4e3b-a2f9-9a68ef206a73)

FreeBSD : libcdaudio -- remote buffer overflow and code execution (bd730827-dfe0-11dd-a765-0030843d3802)

FreeBSD : libcloud -- possible SSL MITM due to invalid regexp used to validate target server hostname (a14dee30-e3d7-11e1-a084-50e5492bd3dc)

FreeBSD : libdwarf -- multiple vulnerabilities (83041ca7-d690-11e6-9171-14dae9d210b8)

FreeBSD : libebml -- multiple vulnerabilities (a130bd8c-eafe-11e6-9ac1-a4badb2f4699)

FreeBSD : libetpan -- null dereference vulnerability in MIME parsing component (57600032-34fe-11e7-8965-bcaec524bf84)

FreeBSD : libevent -- integer overflow in evbuffers (daa8a49b-99b9-11e4-8f66-3085a9a4510d)

FreeBSD : libevent -- multiple vulnerabilities (b8ee7a81-a879-4358-9b30-7dd1bd4c14b1)

FreeBSD : libexif -- buffer overflow vulnerability (624fe633-9006-11d9-a22c-0001020eed82)

FreeBSD : libexif -- multiple remote vulnerabilities (d881d254-70c6-11e2-862d-080027a5ec9a)

FreeBSD : libexif -- privilege escalation (00f30cba-4d23-11ea-86ba-641c67a117d8)

FreeBSD : libgadu -- multiple vulnerabilities (3b4a6982-0b24-11da-bc08-0001020eed82)

FreeBSD : libgcrypt -- ECDSA timing attack (c9c6c2f8-cd54-11e9-af89-080027ef1a23)

FreeBSD : libgcrypt -- side-channel attack on ECDH (95b92e3b-d451-11e5-9794-e8e0b747a45a)

FreeBSD : libgcrypt -- side-channel attack on RSA secret keys (ed3bf433-5d92-11e7-aa14-e8e0b747a45a)

FreeBSD : libgcrypt -- side-channel attack vulnerability (22f28bb3-8d98-11e7-8c37-e8e0b747a45a)

FreeBSD : libgcrypt -- side-channel attack vulnerability (9b5162de-6f39-11e8-818e-e8e0b747a45a)

FreeBSD : libgd -- Denial of servica via double free (a60a2e95-acba-4b11-bc32-ffb47364e07d)

FreeBSD : libgd -- integer overflow which could lead to heap buffer overflow (2a526c78-84ab-11e6-a4a1-60a44ce6887b)

FreeBSD : Libgit2 -- Fixing insufficient validation of submodule names (5a1589ad-68f9-11e8-83f5-d8cb8abf62dd)

FreeBSD : Libgit2 -- multiple vulnerabilities (3c9b7698-84da-11e8-8c75-d8cb8abf62dd)

FreeBSD : Libgit2 -- multiple vulnerabilities (8c08ab4c-d06c-11e8-b35c-001b217b3468)

FreeBSD : Libgit2 -- multiple vulnerabilities (d51b52cf-c199-11e9-b13f-001b217b3468)

FreeBSD : libidn -- multiple vulnerabilities (cb5189eb-572f-11e6-b334-002590263bf5)

FreeBSD : libidn -- out-of-bounds read issue with invalid UTF-8 input (4caf01e2-30e6-11e5-a4a5-002590263bf5)

FreeBSD : libidn2 -- roundtrip check vulnerability (f04f840d-0840-11ea-8d66-75d3253ef913)

FreeBSD : libjpeg-turbo -- heap-based buffer overflow (a460035e-d111-11e1-aff7-001fd056c417)

FreeBSD : libksba -- local denial of service vulnerabilities (a1134048-10c6-11e6-94fa-002590263bf5)

FreeBSD : libmad -- multiple vulnerabilities (b48e7b14-052a-11ea-a1de-53b029d2b061)

FreeBSD : libmms -- stack-based buffer overflow (f6bff909-4a26-11db-a4cc-000a48049292)

FreeBSD : libmspack -- frame\_end overflow which could cause infinite loop (cc7548ef-06e1-11e5-8fda-002590263bf5)

FreeBSD : libmspack -- infinite loop denial of service (43024078-9b63-11df-8983-001d60d86f38)

FreeBSD : libmusicbrainz -- multiple buffer overflow vulnerabilities (ed124f8c-82a2-11db-b46b-0012f06707f0)

FreeBSD : libofx -- exploitable buffer overflow (58fafead-cd13-472f-a9bd-d0173ba1b04c)

FreeBSD : libotr -- buffer overflows (c651c898-e90d-11e1-b230-0024e830109b)

FreeBSD : libotr -- integer overflow (c2b1652c-e647-11e5-85be-14dae9d210b8)

FreeBSD : libpgf -- use-after-free (9a71953a-474a-11e5-adde-14dae9d210b8)

FreeBSD : libpng buffer overflow in png\_set\_PLTE (1886e195-8b87-11e5-90e7-b499baebfeaf)

FreeBSD : libpng denial-of-service (3a408f6f-9c52-11d8-9366-0020ed76ef5a)

FreeBSD : libpng stack-based buffer overflow and other code concerns (f9e3e60b-e650-11d8-9b0a-000347a4fa7d)

FreeBSD : libproxy -- stack-based buffer overflow (3b5c2362-bd07-11e5-b7ef-5453ed2e2b49)

FreeBSD : libpurple -- Invalid memory dereference in the XMPP protocol plug-in by processing a series of specially crafted file transfer requests (64f8b72d-9c4e-11e1-9c94-000bcdf0a03b)

FreeBSD : libpurple -- multiple vulnerabilities (549787c1-8916-11e2-8549-68b599b52a02)

FreeBSD : libpurple -- Remote DoS via an MSN OIM message that lacks UTF-8 encoding (7289214f-7c55-11e1-ab3b-000bcdf0a03b)

FreeBSD : libpurple/pidgin -- multiple vulnerabilities (d057c5e6-5b20-11e4-bebd-000c2980a9f3)

FreeBSD : libraw -- buffer overflow (d9f96741-47bd-4426-9aba-8736c0971b24)

FreeBSD : libraw -- denial of service and remote code execution (4cd857d9-26d2-4417-b765-69701938f9e0)

FreeBSD : libraw -- index overflow in smal\_decode\_segment (db04bf07-9cc8-11e5-8c2b-c335fa8985d7)

FreeBSD : libraw -- memory objects not properly initialized (6bc6eed2-9cca-11e5-8c2b-c335fa8985d7)

FreeBSD : libraw -- multiple DoS vulnerabilities (6f0b0cbf-1274-11e8-8b5b-4ccc6adda413)

FreeBSD : libraw -- multiple DoS vulnerabilities (c60804f1-126f-11e8-8b5b-4ccc6adda413)

FreeBSD : libraw -- Out-of-bounds Read (02bee9ae-c5d1-409b-8a79-983a88861509)

FreeBSD : LibreOffice -- Remote arbitrary file disclosure vulnerability via WEBSERVICE formula (289269f1-0def-11e8-99b0-d017c2987f9a)

FreeBSD : libreoffice -- use-after-free vulnerability (3159cd70-4aaa-11e6-a7bd-14dae9d210b8)

FreeBSD : LibreSSL -- DTLS vulnerability (f9c388c5-a256-11e4-992a-7b2a515a1247)

FreeBSD : LibreSSL -- Memory leak and buffer overflow (e75a96df-73ca-11e5-9b45-b499baebfeaf)

FreeBSD : libressl -- NULL pointer dereference (215e740e-9c56-11e5-90e7-b499baebfeaf)

FreeBSD : LibreSSL -- TLS verification vulnerability (24673ed7-2bf3-11e7-b291-b499baebfeaf)

FreeBSD : librsvg2 -- denial of service vulnerability (d6c51737-a84b-11e5-8f5c-002590263bf5)

FreeBSD : librsvg2 -- denial of service vulnerability (da634091-a84a-11e5-8f5c-002590263bf5)

FreeBSD : librsvg2 -- multiple vulnabilities (b66583ae-5aee-4cd5-bb31-b2d397f8b6b3)

FreeBSD : librsync -- collision vulnerability (b22b016b-b633-11e5-83ef-14dae9d210b8)

FreeBSD : libsamplerate -- multiple vulnerabilities (d44129d6-b22e-4e9c-b200-6a46e8bd3e60)

FreeBSD : libsndfile -- CAF processing integer overflow vulnerability (c5af0747-1262-11de-a964-0030843d3802)

FreeBSD : libsndfile -- multiple vulnerabilities (2b386075-1d9c-11e8-b6aa-4ccc6adda413)

FreeBSD : libsndfile -- multiple vulnerabilities (5a97805e-93ef-4dcb-8d5e-dbcac263bfc2)

FreeBSD : libsndfile -- multiple vulnerabilities (6355efdb-4d4d-11de-8811-0030843d3802)

FreeBSD : libsndfile -- out-of-bounds read memory access (004debf9-1d16-11e8-b6aa-4ccc6adda413)

FreeBSD : libsndfile -- out-of-bounds reads (30704aba-1da4-11e8-b6aa-4ccc6adda413)

FreeBSD : libsndfile -- PAF file processing integer overflow (b9f3ffa3-dd6c-11e0-b7fc-000a5e1e33c6)

FreeBSD : libsoup -- stack based buffer overflow (8e7bbddd-8338-11e7-867f-b499baebfeaf)

FreeBSD : libsoup -- unintentionally allow access to entire local filesystem (30cb4522-b94d-11e0-8182-485d60cb5385)

FreeBSD : libspf2 -- Buffer overflow (2ddbfd29-a455-11dd-a55e-00163e000016)

FreeBSD : libsrtp -- DoS via crafted RTP header vulnerability (6171eb07-d8a9-11e5-b2bd-002590263bf5)

FreeBSD : libssh -- authentication bypass vulnerability (2383767c-d224-11e8-9623-a4badb2f4699)

FreeBSD : libssh -- NULL pointer dereference (0b040e24-f751-11e4-b24d-5453ed2e2b49)

FreeBSD : libssh -- PRNG state reuse on forking servers (f8c88d50-5fb3-11e4-81bd-5453ed2e2b49)

FreeBSD : libssh -- Unsanitized location in scp could lead to unwanted command execution (1e7fa41b-f6ca-4fe8-bd46-0e176b42b14f)

FreeBSD : libssh -- weak Diffie-Hellman secret generation (6b3591ea-e2d2-11e5-a6be-5453ed2e2b49)

FreeBSD : libssh2 -- denial of service vulnerability (9770d6ac-614d-11e5-b379-14dae9d210b8)

FreeBSD : libssh2 -- multiple issues (6e58e1e9-2636-413e-9f84-4c0e21143628)

FreeBSD : libtasn1 -- ASN.1 length decoding vulnerability (2e7e9072-73a0-11e1-a883-001cc0a36e12)

FreeBSD : libtasn1 -- denial of service parsing malicious DER certificates (1b0d2938-0766-11e6-94fa-002590263bf5)

FreeBSD : libtasn1 -- stack-based buffer overflow in asn1\_der\_decoding (82595123-e8b8-11e4-a008-047d7b492d07)

FreeBSD : libtiff -- Improper Input Validation (9b5a905f-e556-452f-a00c-8f070a086181)

FreeBSD : libtomcrypt -- weak signature scheme with ECC keys (a78299e7-9ef3-11da-b410-000e0c2e438a)

FreeBSD : libtool -- Library Search Path Privilege Escalation Issue (77c14729-dc5e-11de-92ae-02e0184b8d35)

FreeBSD : libtorrent -- remote DoS (e4dd787e-0ea9-11e8-95f2-005056925db4)

FreeBSD : libtorrent-rasterbar -- denial of service (093584f2-3f14-11e6-b3c8-14dae9d210b8)

FreeBSD : libtremor -- memory corruption (40497e81-fee3-4e54-9d5f-175a5c633b73)

FreeBSD : libtremor -- multiple vulnerabilities (3dac84c9-bce1-4199-9784-d68af1eb7b2e)

FreeBSD : libutp -- remote denial of service or arbitrary code execution (0523fb7e-8444-4e86-812d-8de05f6f0dce)

FreeBSD : libuv -- incorrect revocation order while relinquishing privileges (996bce94-d23d-11e4-9463-9cb654ea3e1c)

FreeBSD : libvirt -- ACL bypass using ../ to access beyond storage pool (f714b4c9-a6c1-11e5-88d7-047d7b492d07)

FreeBSD : libvncserver -- memory corruption (b5e654c3-5644-11e5-9ad8-14dae9d210b8)

FreeBSD : libvncserver -- multiple buffer overflows (64be967a-d379-11e6-a071-001e67f15f5a)

FreeBSD : libvncserver -- multiple security vulnerabilities (cb3f036d-8c7f-11e6-924a-60a44ce6887b)

FreeBSD : libvorbis -- Multiple memory corruption flaws (b73335a5-3bbe-11dc-8e83-0016179b2dd5)

FreeBSD : libvorbis -- multiple vulnerabilities (64ee858e-e035-4bb4-9c77-2468963dddb8)

FreeBSD : libvorbis -- multiple vulnerabilities (94edff42-d93d-11de-a434-0211d880e350)

FreeBSD : libvorbis -- various security issues (f5a76faf-244c-11dd-b143-0211d880e350)

FreeBSD : libvpx -- buffer overflow in vp9\_init\_context\_buffers (6ca7eddd-d436-486a-b169-b948436bcf14)

FreeBSD : libvpx -- multiple buffer overflows (34e60332-2448-4ed6-93f0-12713749f250)

FreeBSD : libvpx -- out-of-bounds write (42c98cef-62b1-4b8b-9065-f4621e08d526)

FreeBSD : libwmf -- embedded GD library Use-After-Free vulnerability (6a245f31-4254-11de-b67a-0030843d3802)

FreeBSD : libwmf -- integer overflow vulnerability (48aab1d0-4252-11de-b67a-0030843d3802)

FreeBSD : libwmf -- multiple vulnerabilities (ca139c7f-2a8c-11e5-a4a5-002590263bf5)

FreeBSD : libwww -- multiple vulnerabilities (18449f92-ab39-11e6-8011-005056925db4)

FreeBSD : libX11 -- Multiple vulnerabilities (fe99d3ca-a63a-11e8-a7c6-54e1ad3d6335)

FreeBSD : libXcursor -- integer overflow that can lead to heap buffer overflow (ddecde18-e33b-11e7-a293-54e1ad3d6335)

FreeBSD : libXdmcp -- insufficient entropy generating session keys (1b6a10e9-4b7b-11e9-9e89-54e1ad3d6335)

FreeBSD : libXfont -- BDF parsing issues (f7d79fac-cd49-11e4-898f-bcaec565249c)

FreeBSD : libXfont -- multiple memory leaks (3b9590a1-e358-11e7-a293-54e1ad3d6335)

FreeBSD : libXfont -- permission bypass when opening files through symlinks (08a125f3-e35a-11e7-a293-54e1ad3d6335)

FreeBSD : libXfont -- possible local privilege escalation (304409c3-c3ef-11e0-8aa5-485d60cb5385)

FreeBSD : libXfont -- Stack buffer overflow in parsing of BDF font files in libXfont (28c575fa-784e-11e3-8249-001cc0380077)

FreeBSD : libXfont -- X Font Service Protocol and Font metadata file handling issues (b060ee50-daba-11e3-99f2-bcaec565249c)

FreeBSD : libxine (1939)

FreeBSD : libxine -- array index vulnerability (7a7c5853-10a3-11dd-8eb8-00163e000016)

FreeBSD : libxine -- buffer overflow vulnerability (02eedd3c-c6b5-11dc-93b6-000e35248ad7)

FreeBSD : libxine -- buffer overflow vulnerability (107e2ee5-f941-11da-b1fa-020039488e34)

FreeBSD : libxine -- buffer overflow vulnerability (6ecd0b42-ce77-11dc-89b1-000e35248ad7)

FreeBSD : libxine -- buffer overflow vulnerability (e8a6a16d-e498-11dc-bb89-000bcdc1757a)

FreeBSD : libxine -- buffer-overflow vulnerability in aiff support (64c8cc2a-59b1-11d9-8a99-000c6e8f12ef)

FreeBSD : libxine -- denial of service vulnerability (06eac338-9ddf-11dd-813f-000e35248ad7)

FreeBSD : libxine -- DVD subpicture decoder heap overflow (131bd7c4-64a3-11d9-829a-000a95bc6fae)

FreeBSD : libxine -- format string vulnerability (3bc5691e-38dd-11da-92f5-020039488e34)

FreeBSD : libxine -- multiple buffer overflow vulnerabilities (1b043693-8617-11db-93b2-000e35248ad7)

FreeBSD : libxine -- multiple buffer overflows in RTSP (1b70bef4-649f-11d9-a30e-000a95bc6fae)

FreeBSD : libxine -- multiple vulnerabilities (48e14d86-42f1-11de-ad22-000e35248ad7)

FreeBSD : libxine -- multiple vulnerabilities (51d1d428-42f0-11de-ad22-000e35248ad7)

FreeBSD : libxine -- multiple vulnerabilities in VideoCD handling (b6939d5b-64a1-11d9-9106-000a95bc6fae)

FreeBSD : libxml -- Integer overflow (7be92050-a450-11e2-9898-001060e06fd4)

FreeBSD : libxml -- Multiple use-after-free vulnerabilities (ce4b3af8-0b7c-11e1-846b-00235409fd3e)

FreeBSD : libxml -- remote buffer overflows (9ff4c91e-328c-11d9-a9e7-0001020eed82)

FreeBSD : libxml -- Stack consumption vulnerability (5a7d4110-0b7a-11e1-846b-00235409fd3e)

FreeBSD : libxml2 -- An off-by-one out-of-bounds write by XPointer (b8ae4659-a0da-11e1-a294-bcaec565249c)

FreeBSD : libxml2 -- cpu consumption Dos (843a4641-9816-11e2-9c51-080027019be0)

FreeBSD : libxml2 -- Denial of service (0642b064-56c4-11e4-8b87-bcaec565249c)

FreeBSD : libxml2 -- Enforce the reader to run in constant memory (9c7177ff-1fe1-11e5-9a01-bcaec565249c)

FreeBSD : libxml2 -- entity substitution DoS (efdd0edc-da3d-11e3-9ecb-2c4138874f7d)

FreeBSD : libxml2 -- heap buffer overflow (57f1a624-6197-11e1-b98c-bcaec565249c)

FreeBSD : libxml2 -- lack of end-of-document check DoS (e7bb3885-da40-11e3-9ecb-2c4138874f7d)

FreeBSD : libxml2 -- Multiple Issues (76e59f55-4f7a-4887-bcb0-11604004163a)

FreeBSD : libxml2 -- multiple vulnerabilities (e195679d-045b-4953-bb33-be0073ba2ac6)

FreeBSD : libxml2 -- multiple vulnerabilities (e5423caf-8fb8-11e5-918c-bcaec565249c)

FreeBSD : libxml2 -- multiple vulnerabilities (f1e0164e-b67b-11dd-a55e-00163e000016)

FreeBSD : libxml2 -- two vulnerabilities (d71da236-9a94-11dd-8f42-001c2514716c)

FreeBSD : libxml2 stack buffer overflow in URI parsing (847ade05-6717-11d8-b321-000a95bc6fae)

FreeBSD : libxslt -- Denial of Service (1a2aa04f-3718-11e6-b3c8-14dae9d210b8)

FreeBSD : libxslt -- DoS vulnerability due to type confusing error (ecc268f2-8fc2-11e5-918c-bcaec565249c)

FreeBSD : libxslt -- security framework bypass (93167bef-9752-11e9-b61c-b885849ded8e)

FreeBSD : libyaml heap overflow resulting in possible code execution (111f1f84-1d14-4ff2-a9ea-cf07119c0d3b)

FreeBSD : LibYAML input sanitization errors (580cc46b-bb1e-11e3-b144-2c4138874f7d)

FreeBSD : libzip -- denial of service (b2952517-07e5-4d19-8850-21c5b7e0623f)

FreeBSD : libzip -- integer overflow (264749ae-d565-11e4-b545-00269ee29e57)

FreeBSD : libzmq4 -- Remote Code Execution Vulnerability (8e48365a-214d-11e9-9f8a-0050562a4d7b)

FreeBSD : libzmq4 -- V3 protocol handler vulnerable to downgrade attacks (10a6d0aa-0b1c-11e5-bb90-002590263bf5)

FreeBSD : libzrtpcpp -- multiple security vulnerabilities (04320e7d-ea66-11e2-a96e-60a44c524f57)

FreeBSD : lifetype -- ADOdb 'server.php' Insecure Test Script Security Issue (116b0820-d59c-11da-8098-00123ffe8333)

FreeBSD : lighttpd - multiple vulnerabilities (ef0033ad-5823-11e6-80cc-001517f335e2)

FreeBSD : lighttpd - use-after-free vulnerabilities (92a6efd0-e40d-11e8-ada4-408d5cf35399)

FreeBSD : lighttpd -- denial of service vulnerability (1a3bd81f-1b25-11df-bd1a-002170daae37)

FreeBSD : lighttpd -- DOS when access files with mtime 0 (5678da43-ea99-11db-a802-000fea2763ce)

FreeBSD : lighttpd -- FastCGI header overrun in mod\_fastcgi (4b673ae7-5f9a-11dc-84dd-000102cc8983)

FreeBSD : lighttpd -- Log injection vulnerability in mod\_auth (dd7f29cc-3ee9-11e5-93ad-002590263bf5)

FreeBSD : lighttpd -- multiple vulnerabilities (90b27045-9530-11e3-9d09-000c2980a9f3)

FreeBSD : lighttpd -- multiple vulnerabilities (fb911e31-8ceb-11dd-bb29-000c6e274733)

FreeBSD : lighttpd -- multiple vulnerabilities (fc9c217e-3791-11dc-bb1a-000fea449b8a)

FreeBSD : lighttpd -- OpenSSL Error Queue Denial of Service Vulnerability (1ac77649-0908-11dd-974d-000fea2763ce)

FreeBSD : lighttpd -- Remote DOS in CRLF parsing (d2b48d30-ea97-11db-a802-000fea2763ce)

FreeBSD : lighttpd -- remote DoS in header parsing (1cd3ca42-33e6-11e2-a255-5404a67eef98)

FreeBSD : lighttpd -- remote DoS in HTTP authentication (c6521b04-314b-11e1-9cf4-5404a67eef98)

FreeBSD : lighttpd -- script source disclosure vulnerability (bdad9ada-8a52-11d9-9e53-000a95bc6fae)

FreeBSD : links -- denial of service (2a92555f-a6f8-11e8-8acd-10c37b4ac2ea)

FreeBSD : linux-aspell (2197)

FreeBSD : linux-flashplugin -- arbitrary code execution vulnerability (83421018-b3ef-11da-a32d-000c6ec775d9)

FreeBSD : linux-flashplugin -- critical vulnerabilities (b42e8c32-34f6-11dc-9bc9-001921ab2fa4)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (0e8e1212-0ce5-11e1-849b-003067b2972c)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (144e524a-77eb-11df-ae06-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (15236023-a21b-11e2-a460-208984377b34)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (1657a3e6-4585-11e2-a396-10bf48230856)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (20923a0d-82ba-11e1-8d7b-003067b2972c)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (2c12ae0c-c38d-11e0-8eb7-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (36533a59-2770-11e2-bb44-003067b2972c)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (38195f00-b215-11e1-8132-003067b2972c)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (3c1a672e-e508-11de-9f4a-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (414e6a41-7204-11e2-8599-001060e06fd4)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (4a3482da-3624-11e0-b995-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (4b8b748e-2a24-11e2-bb44-003067b2972c)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (53e531a7-e559-11e0-b481-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (562cf6c4-b9f1-11dc-a302-000102cc8983)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (5bd6811f-1c75-11e3-ba72-98fc11cdc4f5)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (5ff40cb4-8b92-11e2-bdb6-001060e06fd4)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (688e73a2-e514-11e3-a52a-98fc11cdc4f5)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (76b597e4-e9c6-11df-9e10-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (78f456fd-9c87-11dd-a55e-00163e000016)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (9da3834b-6a50-11e1-91af-003067b2972c)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (a0c65049-bddd-11e2-a0f6-001060e06fd4)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (adcbdba2-4c27-11e3-9848-98fc11cdc4f5)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (b7a7576d-8e0a-11e3-9976-9c4e36909cc0)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (c0ef849e-84ac-11e3-bec4-9c4e36909cc0)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (d226626c-857f-11e0-95cc-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (dbdac023-80e1-11e2-9a29-001060e06fd4)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (df428c01-ed91-11e2-9466-98fc11cdc4f5)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (e19e74a4-a712-11df-b234-001b2134ef46)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (f63bf080-619d-11e1-91af-003067b2972c)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (fce67546-d2e7-11e2-a9bf-98fc11cdc4f5)

FreeBSD : linux-flashplugin -- multiple vulnerabilities (ff6519ad-18e5-11df-9bdd-001b2134ef46)

FreeBSD : linux-flashplugin -- remote code execution (8a34d9e6-c662-11df-b2e1-001b2134ef46)

FreeBSD : linux-flashplugin -- remote code execution vulnerability (32b05547-6913-11e0-bdc4-001b2134ef46)

FreeBSD : linux-flashplugin -- remote code execution vulnerability (501ee07a-5640-11e0-985a-001b2134ef46)

FreeBSD : linux-flashplugin -- remote code execution vulnerability (55a528e8-9787-11e0-b24a-001b2134ef46)

FreeBSD : linux-flashplugin -- unspecified remote code execution vulnerability (04c6187d-2d8f-11dd-98c9-00163e000016)

FreeBSD : linux-flashplugin -- XSS vulnerability (57573136-920e-11e0-bdc9-001b2134ef46)

FreeBSD : linux-flashplugin7 -- arbitrary code execution vulnerabilities (7c75d48c-429b-11db-afae-000c6ec775d9)

FreeBSD : linux-png (1413)

FreeBSD : linux-realplayer -- buffer overrun (25858c37-bdab-11da-b7d4-00123ffe8333)

FreeBSD : linux-realplayer -- heap overflow (fe4c84fc-bdb5-11da-b7d4-00123ffe8333)

FreeBSD : linux-realplayer -- multiple vulnerabilities (f762ccbb-baed-11dc-a302-000102cc8983)

FreeBSD : linux-realplayer -- RealText parsing heap overflow (95ee96f2-e488-11d9-bf22-080020c11455)

FreeBSD : linux\_base -- vulnerabilities in Red Hat 7.1 libraries (bf2e7483-d3fa-440d-8c6e-8f1f2f018818)

FreeBSD : liveMedia -- DoS vulnerability (821afaa2-9e9a-11dc-a7e3-0016360406fa)

FreeBSD : liveMedia -- potential remote code execution (fa194483-dabd-11e8-bf39-5404a68ad561)

FreeBSD : lives -- insecure files permissions (a8e9d834-a916-11e6-b9b4-bcaec524bf84)

FreeBSD : lldpd -- Buffer overflow/Denial of service (2a4a112a-7c1b-11e5-bd77-0800275369e2)

FreeBSD : logstash -- Directory traversal vulnerability in the file output plugin (24bde04f-1a10-11e5-b43d-002590263bf5)

FreeBSD : logstash -- password disclosure vulnerability (f2d4f879-0d7c-11e6-925f-6805ca0b3d42)

FreeBSD : logstash -- Remote command execution in Logstash zabbix and nagios\_nsca outputs (2184ccad-1a10-11e5-b43d-002590263bf5)

FreeBSD : logstash -- SSL/TLS vulnerability with Lumberjack input (c470bcc7-33fe-11e5-a4a5-002590263bf5)

FreeBSD : logstash-forwarder and logstash -- susceptibility to POODLE vulnerability (ad4d3871-1a0d-11e5-b43d-002590263bf5)

FreeBSD : Loofah -- XSS vulnerability (36a2a89e-7ee1-4ea4-ae22-7ca38019c8d0)

FreeBSD : Loofah -- XSS vulnerability (a90d040e-f5b0-11e9-acc4-4576b265fda6)

FreeBSD : Loofah -- XSS vulnerability (ba6d0c9b-f5f6-4b9b-a6de-3cce93c83220)

FreeBSD : lsh -- multiple vulnerabilities (72cdf2ab-5b87-11dc-812d-0011098b2f36)

FreeBSD : lshell -- Multiple security issues (f353525a-d8b8-11e6-a071-001e67f15f5a)

FreeBSD : lshell -- Shell autocomplete reveals forbidden directories (07d04eef-d8e2-11e6-a071-001e67f15f5a)

FreeBSD : lxr -- multiple XSS vulnerabilities (0491d15a-5875-11df-8d80-0015587e2cc1)

FreeBSD : lynx -- multiple vulnerabilities (03532a19-d68e-11e6-9171-14dae9d210b8) (POODLE)

FreeBSD : lynx -- remote buffer overflow (c01170bf-4990-11da-a1b8-000854d03344)

FreeBSD : LZO -- potential buffer overrun when processing malicious input data (d1f5e12a-fd5a-11e3-a108-080027ef73ec)

FreeBSD : Macromedia flash player -- swf file handling arbitrary code (aed343b4-5480-11da-b579-001125afbed7)

FreeBSD : magento -- multiple vulnerabilities (ea1d2530-72ce-11e5-a2a1-002590263bf5)

FreeBSD : mahara -- sql injection vulnerability (5053420c-4935-11df-83fb-0015587e2cc1)

FreeBSD : mail-notification -- denial-of-service vulnerability (3030ae22-1c7f-11d9-81a4-0050fc56d258)

FreeBSD : mail/dovecot -- Suitable client certificate can be used to login as other user (1340fcc1-2953-11e9-bc44-a4badb296695)

FreeBSD : mail/sympa\* -- Multiple vulnerabilities in Sympa archive management (de6d8290-aef7-11e1-898f-14dae938ec40)

FreeBSD : mail/trojita -- may leak mail contents (not user credentials) over unencrypted connection (36f9ac43-b2ac-11e3-8752-080027ef73ec)

FreeBSD : mailman (1493)

FreeBSD : mailman -- content spoofing with invalid list names in web UI (b4f0ad36-94a5-11e8-9007-080027ac955c)

FreeBSD : mailman -- CSRF hardening in parts of the web interface (9e50dcc3-740b-11e6-94a2-080027ef73ec)

FreeBSD : mailman -- CSRF protection enhancements (b11ab01b-6e19-11e6-ab24-080027ef73ec)

FreeBSD : mailman -- directory traversal vulnerability (c7ccc33f-7d31-11d9-a9e7-0001020eed82)

FreeBSD : mailman -- generated passwords are poor quality (b3cd00f7-c0c5-452d-87bc-086c5635333e)

FreeBSD : mailman -- hardening against malicious listowners injecting evil HTML scripts (739948e3-78bf-11e8-b23c-080027ac955c)

FreeBSD : mailman -- Multiple Vulnerabilities (fffa9257-3c17-11db-86ab-00123ffe8333)

FreeBSD : mailman -- password disclosure (ad9d2518-3471-4737-b60b-9a1f51023b28)

FreeBSD : mailman -- path traversal vulnerability (a5f160fa-deee-11e4-99f8-080027ef73ec)

FreeBSD : mailman -- Private Archive Script XSS (8be2e304-cce6-11da-a3b1-00123ffe8333)

FreeBSD : mailman -- script insertion vulnerability (f47f2746-12c5-11dd-bab7-0016179b2dd5)

FreeBSD : Mailman -- XSS (XSS) vulnerability in the web UI (3d0eeef8-0cf9-11e8-99b0-d017c2987f9a)

FreeBSD : Mailman -- XSS in web interface (4ab29e12-e787-11df-adfa-00e0815b8da8)

FreeBSD : mailman -- XSS vulnerability (64691c49-4b22-11e0-a226-00e0815b8da8)

FreeBSD : mailman denial-of-service vulnerability in MailCommandHandler (b0e76877-67a8-11d8-80e3-0020ed76ef5a)

FreeBSD : mailman XSS in admin script (3cb88bb2-67a6-11d8-80e3-0020ed76ef5a)

FreeBSD : mailman XSS in create script (429249d2-67a7-11d8-80e3-0020ed76ef5a)

FreeBSD : mailman XSS in user options page (00263aa3-67a8-11d8-80e3-0020ed76ef5a)

FreeBSD : mambo -- 'register\_globals' emulation layer overwrite vulnerability (ffb82d3a-610f-11da-8823-00123ffe8333)

FreeBSD : mambo -- multiple SQL injection vulnerabilities (8a5770b4-54b5-11db-a5ae-00508d6a62df)

FreeBSD : mambo -- multiple vulnerabilities (0bf9d7fb-05b3-11da-bc08-0001020eed82)

FreeBSD : mambo -- SQL injection vulnerabilities (f70d09cb-0c46-11db-aac7-000c6ec775d9)

FreeBSD : mantis -- 't\_core\_path' file inclusion vulnerability (82a41084-6ce7-11da-b90c-000e0c2e438a)

FreeBSD : mantis -- 'view\_filters\_page.php' XSS vulnerability (592815da-9eed-11da-b410-000e0c2e438a)

FreeBSD : mantis -- 'view\_filters\_page.php' XSS vulnerability (6e3b12e2-6ce3-11da-b90c-000e0c2e438a)

FreeBSD : mantis -- information disclosure vulnerability (e1b5318c-aa4d-11e5-8f5c-002590263bf5)

FreeBSD : mantis -- multiple vulnerabilities (0822a4cf-9318-11e8-8d88-00e04c1ea73d)

FreeBSD : mantis -- multiple vulnerabilities (29255141-c3df-11dd-a721-0030843d3802)

FreeBSD : mantis -- multiple vulnerabilities (55587adb-b49d-11e1-8df1-0004aca374af)

FreeBSD : mantis -- multiple vulnerabilities (81fcc2f9-e15a-11e9-abbf-800dd28b22bd)

FreeBSD : mantis -- php code execution vulnerability (af2745c0-c3e0-11dd-a721-0030843d3802)

FreeBSD : mantis -- session hijacking vulnerability (00d6040a-b8e0-11dd-a578-0030843d3802)

FreeBSD : mantis -- XSS vulnerability (2b63e964-eb04-11e6-9ac1-a4badb2f4699)

FreeBSD : mantis -- XSS vulnerability (6bf71117-c0c9-11e8-b760-6023b685b1ee)

FreeBSD : maradns -- CNAME record resource rotation denial of service (f358de71-bf64-11dc-928b-0016179b2dd5)

FreeBSD : maradns -- denial of service when resolving a long DNS hostname (8015600f-2c80-11e0-9cc1-00163e5bf4f9)

FreeBSD : MariaDB -- unspecified vulnerability (b7d89082-e7c0-11e7-ac58-b499baebfeaf)

FreeBSD : MariaDB -- Vulnerability in C API (cb0183bb-45f6-11ea-a1c7-b499baebfeaf)

FreeBSD : mathopd -- directory traversal vulnerability (6e7ad1d7-4e27-11e1-8e12-90e6ba8a36a2)

FreeBSD : Mathopd buffer overflow (96fdbf5b-2cfd-11d8-9355-0020ed76ef5a)

FreeBSD : matomo -- XSS vulnerability (44864c84-d3b8-11e8-b3cb-00e04c1ea73d)

FreeBSD : mbed TLS (PolarSSL) -- multiple vulnerabilities (d8382a69-4728-11e8-ba83-0011d823eebd)

FreeBSD : mbed TLS (PolarSSL) -- multiple vulnerabilities (f41e3e54-076b-11e7-a9f2-0011d823eebd)

FreeBSD : mbed TLS (PolarSSL) -- remote code execution (c2f107e1-2493-11e8-b3e8-001cc0382b2f)

FreeBSD : Mbed TLS -- Cache attack against RSA key import in SGX (056ea107-5729-11ea-a2f3-001cc0382b2f)

FreeBSD : Mbed TLS -- Local timing attack on RSA decryption (293f40a0-ffa1-11e8-b258-0011d823eebd)

FreeBSD : mbed TLS -- plaintext recovery vulnerabilities (f4876dd4-9ca8-11e8-aa17-0011d823eebd)

FreeBSD : Mbed TLS -- Side channel attack on deterministic ECDSA (1c948fd3-dac0-11e9-81b2-0011d823eebd)

FreeBSD : Mbed TLS -- Side channel attack on ECDSA (b70b880f-5727-11ea-a2f3-001cc0382b2f)

FreeBSD : Mbed TLS -- Side channel attack on ECDSA (bf1f47c4-7f1b-11ea-bf94-001cc0382b2f)

FreeBSD : mbedTLS/PolarSSL -- DoS and possible remote code execution (07a1a76c-734b-11e5-ae81-14dae9d210b8)

FreeBSD : mbedTLS/PolarSSL -- multiple vulnerabilities (5d280761-6bcf-11e5-9909-002590263bf5)

FreeBSD : mbedTLS/PolarSSL -- multiple vulnerabilities (953aaa57-6bce-11e5-9909-002590263bf5)

FreeBSD : mbedTLS/PolarSSL -- SLOTH attack on TLS 1.2 server authentication (4084168e-b531-11e5-a98c-0011d823eebd)

FreeBSD : mc -- multiple vulnerabilities (2b2b333b-6bd3-11d9-95f8-000a95bc6fae)

FreeBSD : mcollective -- cert valication issue (ecea9e92-0be5-4931-88da-8772d044972a)

FreeBSD : mcweject -- exploitable buffer overflow (84d3fbb2-e607-11db-8a32-000c76189c4c)

FreeBSD : mDNSResponder -- corrupted stack crash when parsing bad resolv.conf (1cd87e2a-81e3-11df-81d8-00262d5ed8ee)

FreeBSD : mediawiki -- authenticated CSRF vulnerability (694da5b4-5877-11df-8d80-0015587e2cc1)

FreeBSD : mediawiki -- Clickjacking vulnerabilities (e177c410-1943-11e0-9d1c-000c29ba66d2)

FreeBSD : mediawiki -- hardcoded placeholder string security bypass vulnerability (99015cf5-c4dd-11da-b2fb-000e0c2e438a)

FreeBSD : mediawiki -- multiple vulnerabilities (090763f6-7030-11ea-93dd-080027846a02)

FreeBSD : mediawiki -- multiple vulnerabilities (298829e2-ccce-11e7-92e4-000c29649f92)

FreeBSD : mediawiki -- multiple vulnerabilities (3c5a4fe0-9ebb-11e9-9169-fcaa147e860e)

FreeBSD : mediawiki -- multiple vulnerabilities (3fadb7c6-7b0a-11e0-89b4-001ec9578670)

FreeBSD : mediawiki -- multiple vulnerabilities (61b07d71-ce0e-11dd-a721-0030843d3802)

FreeBSD : mediawiki -- multiple vulnerabilities (6241b5df-42a1-11e5-93ad-002590263bf5)

FreeBSD : mediawiki -- multiple vulnerabilities (7c0fecd6-f42f-11e1-b17b-000c2977ec30)

FreeBSD : mediawiki -- multiple vulnerabilities (8d04cfbd-344d-11e0-8669-0025222482c5)

FreeBSD : mediawiki -- multiple vulnerabilities (b50f53ce-2151-11e6-8dd3-002590263bf5)

FreeBSD : mediawiki -- multiple vulnerabilities (b973a763-7936-11e5-a2a1-002590263bf5)

FreeBSD : mediawiki -- multiple vulnerabilities (be1aada2-be6c-11e8-8fc6-000c29434208)

FreeBSD : mediawiki -- multiple vulnerabilities (c32285fe-fde4-11e9-9525-000c29c4dc65)

FreeBSD : mediawiki -- multiple vulnerabilities (f36bbd66-aa44-11e5-8f5c-002590263bf5)

FreeBSD : mediawiki -- two security vulnerabilities (fc55e396-6deb-11df-8b8e-000c29ba66d2)

FreeBSD : mediawiki -- XSS vulnerability (74b7403c-c4d5-11da-b2fb-000e0c2e438a)

FreeBSD : mediawiki -- XSS vulnerability (c9c14242-6843-11dc-82b6-02e0185f8d72)

FreeBSD : memcached -- memcached stats maps Information Disclosure Weakness (86ada694-8b30-11de-b9d0-000c6e274733)

FreeBSD : memcached -- multiple vulnerabilities (f4bf713f-6ac7-4b76-8980-47bf90c5419f)

FreeBSD : Memory leak bug in Toxcore (4c11b51e-cd8d-11e8-b0cb-a0f3c100ae18)

FreeBSD : Memory leak in different components (efe43d2b-8f35-11e8-b9e8-dcfe074bd614)

FreeBSD : mencoder -- potential buffer overrun when processing malicious lzo compressed input (17dfd984-feba-11e3-b938-5404a68ad561)

FreeBSD : mercurial -- arbitrary code execution vulnerability (78abc022-0fee-11e6-9a1c-0014a5a57822)

FreeBSD : mercurial -- multiple issues (b0628e53-092a-4037-938b-29805a7cd31b)

FreeBSD : Mercurial -- multiple vulnerabilities (1d33cdee-7f6b-11e7-a9b5-3debb10a6871)

FreeBSD : mercurial -- multiple vulnerabilities (e1085b15-f609-11e5-a230-0014a5a57822)

FreeBSD : messagelib -- HTML email can open browser window automatically (c7b1af20-f34f-11e8-9cde-e0d55e2a8bf9)

FreeBSD : metamail format string bugs and buffer overflows (a20082c3-6255-11d8-80e3-0020ed76ef5a)

FreeBSD : mgetty+sendfax -- symlink attack via insecure temporary files (44ee8160-c453-11dd-a721-0030843d3802)

FreeBSD : Midnight Commander buffer overflow during symlink resolution (322d4ff6-85c3-11d8-a41f-0020ed76ef5a)

FreeBSD : Midnight Commander buffer overflows, format string bugs, and insecure temporary file handling (0c6f3fde-9c51-11d8-9366-0020ed76ef5a)

FreeBSD : milter-bogom -- headerless message crash (6d9a28f8-8152-11da-817c-0001020eed82)

FreeBSD : mini\_httpd -- buffer overflow via snprintf (84dc49b0-b267-11e5-8a5b-00262d5ed8ee)

FreeBSD : mini\_httpd -- disclose arbitrary files is some circumstances (33c384f3-5af6-4662-9741-0acb21c7e499)

FreeBSD : mini\_httpd,thttpd -- Buffer overflow in htpasswd (f5524753-67b1-4c88-8114-29c2d258b383)

FreeBSD : miniupnpc -- buffer overflow (06fefd2f-728f-11e5-a371-14dae9d210b8)

FreeBSD : miniupnpc -- integer signedness error (da1d5d2e-3eca-11e7-8861-0018fe623f2b)

FreeBSD : mkbold-mkitalic -- format string vulnerability (32d4f0f1-85c3-11d9-b6dc-0007e900f747)

FreeBSD : mksh -- TTY attachment privilege escalation (86c05550-12c1-11dd-bab7-0016179b2dd5)

FreeBSD : mkvtoolnix -- code execution via specially crafted files (aeb7874e-8df1-11e6-a082-5404a68ad561)

FreeBSD : mnemo -- XSS vulnerabilities in several of the notepad name and note data fields (2506f558-6a8a-11da-b96e-000fb586ba73)

FreeBSD : mnGoSearch buffer overflow in UdmDocToTextBuf() (87cc48fd-5fdd-11d8-80e3-0020ed76ef5a)

FreeBSD : mod\_access\_referer -- NULL pointer dereference vulnerability (af747389-42ba-11d9-bd37-00065be4b5b6)

FreeBSD : mod\_dav -- lock related denial-of-service (013fa252-0724-11d9-b45d-000c41e2cdad)

FreeBSD : mod\_dosevasive -- insecure temporary file creation (88ff90f2-6e43-11d9-8c87-000a95bc6fae)

FreeBSD : mod\_fcgid -- possible heap buffer overwrite (9003b500-31e3-11e3-b0d0-20cf30e32f6d)

FreeBSD : mod\_jk -- information disclosure (47aa4343-44fa-11e5-9daa-14dae9d210b8)

FreeBSD : mod\_jk -- information disclosure (d9405748-1342-11dc-a35c-001485ab073e)

FreeBSD : mod\_jk -- long URL stack overflow vulnerability (cf86c644-cb6c-11db-8e9d-000c6ec775d9)

FreeBSD : mod\_pagespeed -- critical XSS (XSS) vulnerability (4e23644c-cb93-4f83-9e20-5bc07ad9b39f)

FreeBSD : mod\_pagespeed -- multiple vulnerabilities (178ba4ea-fd40-11e1-b2ae-001fd0af1a4c)

FreeBSD : mod\_perl -- remote DoS in PATH\_INFO parsing (ef2ffb03-f2b0-11db-ad25-0010b5a0a860)

FreeBSD : mod\_perl -- XSS (4a638895-41b7-11de-b1cc-00219b0fc4d8)

FreeBSD : mod\_perl2 -- execute arbitrary Perl code (c360d057-ea8b-11e9-859b-b885849ded8e)

FreeBSD : mod\_pubcookie -- Empty Authentication Security Advisory (1ca8228f-858d-11e0-a76c-000743057ca2)

FreeBSD : mod\_pubcookie -- XSS vulnerability (91afa94c-c452-11da-8bff-000ae42e9b93)

FreeBSD : mod\_python -- information leakage vulnerability (5192e7ca-7d4f-11d9-a9e7-0001020eed82)

FreeBSD : mod\_python denial-of-service vulnerability in parse\_qs (1a448eb7-6988-11d8-873f-0020ed76ef5a)

FreeBSD : mod\_ssl -- SSLCipherSuite bypass (4238151d-207a-11d9-bfe2-0090962cff2a)

FreeBSD : ModSecurity -- XML External Entity Processing Vulnerability (2070c79a-8e1e-11e2-b34d-000c2957946c)

FreeBSD : ModSecurity for Apache 2.x remote off-by-one overflow (c2e10368-77ab-11d8-b9e8-00e04ccb0a62)

FreeBSD : mohawk -- multiple vulnerabilities (670d732a-cdd4-11e3-aac2-0022fb6fcf92)

FreeBSD : moinmoin -- ACL group bypass (1ecf4ca1-f7ad-11d8-96c9-00061bc2ad93)

FreeBSD : moinmoin -- Multiple vulnerabilities (a264b1b0-5726-11e2-9483-14dae938ec40)

FreeBSD : moinmoin -- multiple vulnerabilities (f113bbeb-e3ac-11dc-bb89-000bcdc1757a)

FreeBSD : moinmoin -- multiple XSS vulnerabilities (6a523dba-eeab-11dd-ab4f-0030843d3802)

FreeBSD : moinmoin -- multiple XSS vulnerabilities (fc4d0ae8-3fa3-11de-a3fd-0030843d3802)

FreeBSD : moinmoin -- superuser privilege escalation (c4ba95b2-39ce-11dd-98c9-00163e000016)

FreeBSD : moinmoin -- wrong processing of group membership (4f99e2ef-f725-11e1-8bd8-0022156e8794)

FreeBSD : moinmoin -- XSS via RST parser (4a8a98ab-f745-11e1-8bd8-0022156e8794)

FreeBSD : MoinMoin -- XSS vulnerabilities (4c017345-1d89-11e0-bbee-0014a5e3cda6)

FreeBSD : moinmoin -- XSS vulnerabilities (ab804e60-d693-11e6-9171-14dae9d210b8)

FreeBSD : moinmoin -- XSS vulnerabilities (bfe218a5-4218-11de-b67a-0030843d3802)

FreeBSD : MoinMoin administrative group name privilege escalation vulnerability (da9e6438-bfc0-11d8-b00e-000347a4fa7d)

FreeBSD : mongodb -- Attach IDs to users (880bca8f-e201-11e9-8af7-08002720423d)

FreeBSD : mongodb -- Bump Windows package dependencies (fd2e0ca8-e3ae-11e9-8af7-08002720423d)

FreeBSD : mongodb -- Our init scripts check /proc/[pid]/stat should validate that `(${procname})` is the process' command name. (273c6c43-e3ad-11e9-8af7-08002720423d)

FreeBSD : monitorix -- serious bug in the built-in HTTP server (620cf713-5a99-11e3-878d-20cf30e32f6d)

FreeBSD : monkey -- improper input validation vulnerability (4465c897-ee5c-11de-b6ef-00215c6a37bb)

FreeBSD : mono -- 'System.CodeDom.Compiler' Insecure Temporary Creation (5a39a22e-5478-11db-8f1a-000a48049292)

FreeBSD : mono -- DoS and code execution (4b3a7e70-afce-11e5-b864-14dae9d210b8)

FreeBSD : mono -- TLS bugs (c0cae920-c4e9-11e4-898e-90e6ba741e35)

FreeBSD : mono -- XML signature HMAC truncation spoofing (708c65a5-7c58-11de-a994-0030843d3802)

FreeBSD : monotone -- remote denial of service in default setup (c9a6ae4a-df8b-11df-9573-00262d5ed8ee)

FreeBSD : moodle -- Login CSRF vulnerability (889e35f4-f6a0-11e8-82dc-fcaa147e860e)

FreeBSD : moodle -- multiple vulnerabilities (074cb225-bb2d-11e8-90e1-fcaa147e860e)

FreeBSD : moodle -- multiple vulnerabilities (2d299950-ddb0-11e5-8fa8-14dae9d210b8)

FreeBSD : moodle -- multiple vulnerabilities (3ddcb42b-5b78-11e6-b334-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (43891162-2d5e-11e5-a4a5-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (66759ce6-7530-11df-9c33-000c29ba66d2)

FreeBSD : moodle -- multiple vulnerabilities (82b3ca2a-8c07-11e5-bd18-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (8656cf5f-4170-11e6-8dfe-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (a430e15d-f93f-11e5-92ce-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (ab02f981-ab9e-11e6-ae1b-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (c2fcbec2-5daa-11e5-9909-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (cdb4d962-34f9-11e8-92db-080027907385)

FreeBSD : moodle -- multiple vulnerabilities (df45b4bd-0b7f-11e7-970f-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (f6429c24-4fc9-11df-83fb-0015587e2cc1)

FreeBSD : moodle -- multiple vulnerabilities (f6565fbf-ab9e-11e6-ae1b-002590263bf5)

FreeBSD : moodle -- multiple vulnerabilities (f72d98d1-0b7e-11e7-970f-002590263bf5)

FreeBSD : mozilla -- 'Wrapped' javascript: urls bypass security checks (a81746a1-c2c7-11d9-89f7-02061b08fc24)

FreeBSD : mozilla -- arbitrary code execution vulnerability (cbfde1cd-87eb-11d9-aa18-0001020eed82)

FreeBSD : mozilla -- automated file upload (6e740881-0cae-11d9-8a8a-000c41e2cdad)

FreeBSD : mozilla -- BMP decoder vulnerabilities (ab9c559e-115a-11d9-bc4a-000c41e2cdad)

FreeBSD : mozilla -- built-in CA certificates may be overridden (8d823883-0ca9-11d9-8a8a-000c41e2cdad)

FreeBSD : mozilla -- code execution through javascript: favicons (1989b511-ae62-11d9-a788-0001020eed82)

FreeBSD : mozilla -- code execution via javascript: IconURL vulnerability (eca6195a-c233-11d9-804c-02061b08fc24)

FreeBSD : mozilla -- code execution via Quicktime media-link files (3ce8c7e2-66cf-11dc-b25f-02e0185f8d72)

FreeBSD : mozilla -- corrupt JIT state after deep return from native function (c1ef9b33-72a6-11de-82ea-0030843d3802)

FreeBSD : mozilla -- data: URL can inherit wrong origin after an HTTP redirect (f90fce70-ecfa-4f4d-9ee8-c476dbf4bf0e)

FreeBSD : mozilla -- heap buffer overflow in GIF image processing (7d2aac52-9c6b-11d9-99a7-000a95bc6fae)

FreeBSD : mozilla -- Heap buffer overflow mixing document.write and DOM insertion (c223b00d-e272-11df-8e32-000f20797ede)

FreeBSD : mozilla -- heap overflow in NNTP handler (3fbf9db2-658b-11d9-abad-000a95bc6fae)

FreeBSD : mozilla -- heap-buffer overflow (d7dbd2db-599c-11e1-a2fb-14dae9ebcf89)

FreeBSD : mozilla -- hostname spoofing bug (5360a659-131c-11d9-bc4a-000c41e2cdad)

FreeBSD : mozilla -- insecure permissions for some downloaded files (a77849a5-696f-11d9-ae49-000c41e2cdad)

FreeBSD : mozilla -- insecure temporary directory vulnerability (d022754d-8839-11d9-aa18-0001020eed82)

FreeBSD : mozilla -- javascript 'lambda' replace exposes memory contents (45b75152-ae5f-11d9-a788-0001020eed82)

FreeBSD : mozilla -- multiple heap buffer overflows (93d6162f-1153-11d9-bc4a-000c41e2cdad)

FreeBSD : mozilla -- multiple vulnerabilities (01c57d20-ea26-11de-bd39-00248c9b4be7)

FreeBSD : Mozilla -- multiple vulnerabilities (04b7d46c-7226-11e0-813a-6c626dd55a41)

FreeBSD : mozilla -- multiple vulnerabilities (05463e0a-abd3-4fa4-bd5f-cd5ed132d4c6)

FreeBSD : mozilla -- multiple vulnerabilities (0592f49f-b3b8-4260-b648-d1718762656c)

FreeBSD : mozilla -- multiple vulnerabilities (05da6b56-3e66-4306-9ea3-89fafe939726)

FreeBSD : mozilla -- multiple vulnerabilities (0998e79d-0055-11e3-905b-0025905a4771)

FreeBSD : mozilla -- multiple vulnerabilities (0a9e2b72-4cb7-11e1-9146-14dae9ebcf89)

FreeBSD : mozilla -- multiple vulnerabilities (0cea6e0a-7a39-4dac-b3ec-dbc13d404f76)

FreeBSD : mozilla -- multiple vulnerabilities (1098a15b-b0f6-42b7-b5c7-8a8646e8be07)

FreeBSD : mozilla -- multiple vulnerabilities (12b336c6-fe36-11dc-b09c-001c2514716c)

FreeBSD : mozilla -- multiple vulnerabilities (12bd6ecf-c430-11db-95c5-000c6ec775d9)

FreeBSD : mozilla -- multiple vulnerabilities (1753f0ff-8dd5-11e3-9b45-b4b52fce4ce8)

FreeBSD : mozilla -- multiple vulnerabilities (18211552-f650-4d86-ba4f-e6d5cbfcdbeb)

FreeBSD : mozilla -- multiple vulnerabilities (1d8ff4a2-0445-11e0-8e32-000f20797ede)

FreeBSD : Mozilla -- multiple vulnerabilities (1fade8a3-e9e8-11e0-9580-4061862b8c22)

FreeBSD : mozilla -- multiple vulnerabilities (2225c5b4-1e5a-44fc-9920-b3201c384a15)

FreeBSD : mozilla -- multiple vulnerabilities (2273879e-8a2f-11dd-a6fe-0030843d3802)

FreeBSD : mozilla -- multiple vulnerabilities (237a201c-888b-487f-84d3-7d92266381d6)

FreeBSD : mozilla -- multiple vulnerabilities (29f5bfc5-ce04-11dd-a721-0030843d3802)

FreeBSD : mozilla -- multiple vulnerabilities (2b8cad90-f289-11e1-a215-14dae9ebcf89)

FreeBSD : mozilla -- multiple vulnerabilities (2c2d1c39-1396-459a-91f5-ca03ee7c64c6)

FreeBSD : mozilla -- multiple vulnerabilities (2c57c47e-8bb3-4694-83c8-9fc3abad3964)

FreeBSD : mozilla -- multiple vulnerabilities (2d56c7f4-b354-428f-8f48-38150c607a05)

FreeBSD : mozilla -- multiple vulnerabilities (380e8c56-8e32-11e1-9580-4061862b8c22)

FreeBSD : Mozilla -- multiple vulnerabilities (39bc2294-ff32-4972-9ecb-b9f40b4ccb74)

FreeBSD : mozilla -- multiple vulnerabilities (3b18e237-2f15-11de-9672-0030843d3802)

FreeBSD : mozilla -- multiple vulnerabilities (44b6dfbf-4ef7-4d52-ad52-2b1b05d81272)

FreeBSD : mozilla -- multiple vulnerabilities (44d9daee-940c-4179-86bb-6e3ffd617869) (Logjam)

FreeBSD : mozilla -- multiple vulnerabilities (45f102cd-4456-11e0-9580-4061862b8c22)

FreeBSD : Mozilla -- multiple vulnerabilities (49beb00f-a6e1-4a42-93df-9cb14b4c2bee)

FreeBSD : mozilla -- multiple vulnerabilities (49e8f2ee-8147-11de-a994-0030843d3802)

FreeBSD : mozilla -- multiple vulnerabilities (4a1ca8a4-bd82-11e2-b7a0-d43d7e0c7c02)

FreeBSD : mozilla -- multiple vulnerabilities (4a21ce2c-bb13-11df-8e32-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (4f00dac0-1e18-4481-95af-7aaad63fd303)

FreeBSD : mozilla -- multiple vulnerabilities (512c0ffd-cd39-4da4-b2dc-81ff4ba8e238)

FreeBSD : mozilla -- multiple vulnerabilities (555b244e-6b20-4546-851f-d8eb7d6c1ffa)

FreeBSD : mozilla -- multiple vulnerabilities (56cfe192-329f-11df-abb2-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (5aefc41e-d304-4ec8-8c82-824f84f08244)

FreeBSD : mozilla -- multiple vulnerabilities (5e0a038a-ca30-416d-a2f5-38cbf5e7df33)

FreeBSD : mozilla -- multiple vulnerabilities (610de647-af8d-11e3-a25b-b4b52fce4ce8)

FreeBSD : mozilla -- multiple vulnerabilities (6a09c80e-6ec7-442a-bc65-d72ce69fd887)

FreeBSD : mozilla -- multiple vulnerabilities (6b3b1b97-207c-11e2-a03f-c8600054b392)

FreeBSD : mozilla -- multiple vulnerabilities (6c8ad3e8-0a30-11e1-9580-4061862b8c22)

FreeBSD : mozilla -- multiple vulnerabilities (6cec1b0a-da15-467d-8691-1dea392d4c8d)

FreeBSD : mozilla -- multiple vulnerabilities (6e5a9afd-12d3-11e2-b47d-c8600054b392)

FreeBSD : mozilla -- multiple vulnerabilities (76ff65f4-17ca-4d3f-864a-a3d6026194fb)

FreeBSD : mozilla -- multiple vulnerabilities (7943794f-707f-4e31-9fea-3bbf1ddcedc1)

FreeBSD : mozilla -- multiple vulnerabilities (7ae61870-9dd2-4884-a2f2-f19bb5784d09)

FreeBSD : mozilla -- multiple vulnerabilities (7c3a02b9-3273-4426-a0ba-f90fad2ff72e)

FreeBSD : mozilla -- multiple vulnerabilities (7dfed67b-20aa-11e3-b8d8-0025905a4771)

FreeBSD : mozilla -- multiple vulnerabilities (8065d37b-8e7c-4707-a608-1b0a2b8509c3)

FreeBSD : mozilla -- multiple vulnerabilities (810a5197-e0d9-11dc-891a-02061b08fc24)

FreeBSD : mozilla -- multiple vulnerabilities (81f866ad-41a4-11e3-a4af-0025905a4771)

FreeBSD : mozilla -- multiple vulnerabilities (834591a9-c82f-11e0-897d-6c626dd55a41)

FreeBSD : mozilla -- multiple vulnerabilities (84630f4a-cd8c-11da-b7b9-000c6ec775d9)

FreeBSD : mozilla -- multiple vulnerabilities (888a0262-f0d9-11e3-ba0c-b4b52fce4ce8)

FreeBSD : mozilla -- multiple vulnerabilities (8c2ea875-9499-11df-8e32-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (8eee06d4-c21d-4f07-a669-455151ff426f)

FreeBSD : mozilla -- multiple vulnerabilities (92d44f83-a7bf-41cf-91ee-3d1b8ecf579f)

FreeBSD : mozilla -- multiple vulnerabilities (94976433-9c74-11e2-a9fc-d43d7e0c7c02)

FreeBSD : mozilla -- multiple vulnerabilities (96eca031-1313-4daf-9be2-9d6e1c4f1eb5)

FreeBSD : mozilla -- multiple vulnerabilities (978b0f76-122d-11e4-afe3-bc5ff4fb5e7b)

FreeBSD : mozilla -- multiple vulnerabilities (985d4d6c-cfbd-11e3-a003-b4b52fce4ce8)

FreeBSD : Mozilla -- multiple vulnerabilities (98f1241f-8c09-4237-ad0d-67fb4158ea7a)

FreeBSD : mozilla -- multiple vulnerabilities (99029172-8253-407d-9d8b-2cfeab9abf81)

FreeBSD : mozilla -- multiple vulnerabilities (99858b7c-7ece-11df-a007-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (9c1495ac-8d8c-4789-a0f3-8ca6b476619c)

FreeBSD : mozilla -- multiple vulnerabilities (9ccfee39-3c3b-11df-9edc-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (9d04936c-75f1-4a2c-9ade-4c1708be5df9)

FreeBSD : mozilla -- multiple vulnerabilities (a1050b8b-6db3-11e1-8b37-0011856a6e37)

FreeBSD : mozilla -- multiple vulnerabilities (a4ed6632-5aa9-11e2-8fcb-c8600054b392)

FreeBSD : mozilla -- multiple vulnerabilities (a891c5b4-3d7a-4de9-9c71-eef3fd698c77)

FreeBSD : Mozilla -- multiple vulnerabilities (aa1aefe3-6e37-47db-bfda-343ef4acb1b5)

FreeBSD : mozilla -- multiple vulnerabilities (aaa9f3db-13b5-4a0e-9ed7-e5ab287098fa)

FreeBSD : mozilla -- multiple vulnerabilities (b1f7d52f-fc42-48e8-8403-87d4c9d26229)

FreeBSD : mozilla -- multiple vulnerabilities (b3fcb387-de4b-11e2-b1c6-0025905a4771)

FreeBSD : mozilla -- multiple vulnerabilities (b7e23050-2d5d-4e61-9b48-62e89db222ca)

FreeBSD : mozilla -- multiple vulnerabilities (b8321d76-24e7-4b72-a01d-d12c4445d826)

FreeBSD : mozilla -- multiple vulnerabilities (bd62c640-9bb9-11e4-a5ad-000c297fb80f)

FreeBSD : mozilla -- multiple vulnerabilities (bfecf7c1-af47-11e1-9580-4061862b8c22)

FreeBSD : mozilla -- multiple vulnerabilities (c4f067b9-dc4a-11df-8e32-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (c4f39920-781f-4aeb-b6af-17ed566c4272)

FreeBSD : mozilla -- multiple vulnerabilities (c66a5632-708a-4727-8236-d65b2d5b2739)

FreeBSD : mozilla -- multiple vulnerabilities (c71cdc95-3c18-45b7-866a-af28b59aabb5)

FreeBSD : mozilla -- multiple vulnerabilities (c87aa2d2-c3c4-11de-ab08-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (c96d416a-eae7-4d5d-bc84-40deca9329fb)

FreeBSD : mozilla -- multiple vulnerabilities (cd81806c-26e7-4d4a-8425-02724a2f48af)

FreeBSD : mozilla -- multiple vulnerabilities (d0c97697-df2c-4b8b-bff2-cec24dc35af8)

FreeBSD : mozilla -- multiple vulnerabilities (d10b49b2-8d02-49e8-afde-0844626317af)

FreeBSD : mozilla -- multiple vulnerabilities (d1853110-07f4-4645-895b-6fd462ad0589)

FreeBSD : mozilla -- multiple vulnerabilities (d23119df-335d-11e2-b64c-c8600054b392)

FreeBSD : mozilla -- multiple vulnerabilities (d9b43004-f5fd-4807-b1d7-dbf66455b244)

FreeBSD : mozilla -- multiple vulnerabilities (da185955-5738-11de-b857-000f20797ede)

FreeBSD : mozilla -- multiple vulnerabilities (dbf338d0-dce5-11e1-b655-14dae9ebcf89)

FreeBSD : mozilla -- multiple vulnerabilities (dd116b19-64b3-11e3-868f-0025905a4771)

FreeBSD : mozilla -- multiple vulnerabilities (dfe40cff-9c3f-11e0-9bec-6c626dd55a41)

FreeBSD : mozilla -- multiple vulnerabilities (e190ca65-3636-11dc-a697-000c6ec775d9)

FreeBSD : mozilla -- multiple vulnerabilities (e2a92664-1d60-11db-88cf-000c6ec775d9)

FreeBSD : mozilla -- multiple vulnerabilities (e3f0374a-7ad6-11e2-84cd-d43d7e0c7c02)

FreeBSD : mozilla -- multiple vulnerabilities (e3ff776b-2ba6-11e1-93c6-0011856a6e37)

FreeBSD : mozilla -- multiple vulnerabilities (e60169c4-aa86-46b0-8ae2-0d81f683df09)

FreeBSD : mozilla -- multiple vulnerabilities (e6296105-449b-11db-ba89-000c6ec775d9)

FreeBSD : mozilla -- multiple vulnerabilities (f29fea8f-b19f-11dd-a55e-00163e000016)

FreeBSD : mozilla -- multiple vulnerabilities (f78eac48-c3d1-4666-8de5-63ceea25a578)

FreeBSD : mozilla -- multiple vulnerabilities (f82c85d8-1c6e-11df-abb2-000f20797ede)

FreeBSD : mozilla -- NULL bytes in FTP URLs (7c188c55-0cb0-11d9-8a8a-000c41e2cdad)

FreeBSD : mozilla -- POP client heap overflow (c1d97a8b-05ed-11d9-b45d-000c41e2cdad)

FreeBSD : mozilla -- privilege escalation via DOM property overrides (f650d5b8-ae62-11d9-a788-0001020eed82)

FreeBSD : mozilla -- privilege escalation via non-DOM property overrides (a6427195-c2c7-11d9-89f7-02061b08fc24)

FreeBSD : mozilla -- scripting vulnerabilities (b2e6d1d6-1339-11d9-bc4a-000c41e2cdad)

FreeBSD : mozilla -- security icon spoofing (e9f9d232-0cb2-11d9-8a8a-000c41e2cdad)

FreeBSD : mozilla -- SOAPParameter integer overflow (a4fd8f53-05eb-11d9-b45d-000c41e2cdad)

FreeBSD : mozilla -- Speculative execution side-channel attack (8429711b-76ca-474e-94a0-6b980f1e2d47)

FreeBSD : Mozilla -- Stored passwords in 'Saved Logins' can be copied without master password entry (0f31b4e9-c827-11e9-9626-589cfc01894a)

FreeBSD : Mozilla -- SVG Animation Remote Code Execution (18f39fb6-7400-4063-acaf-0806e92c094f)

FreeBSD : mozilla -- update to HTTPS certificate blacklist (b2f09169-55af-11e0-9d6f-000f20797ede)

FreeBSD : mozilla -- use-after-free (738fc80d-5f13-4ccb-aa9a-7965699e5a10)

FreeBSD : mozilla -- use-after-free in compositor (23f59689-0152-42d3-9ade-1658d6380567)

FreeBSD : mozilla -- use-after-free in HTML Editor (630c8c08-880f-11e2-807f-d43d7e0c7c02)

FreeBSD : mozilla -- use-after-free in nsXBLDocumentInfo::ReadPrototypeBindings (eba9aa94-549c-11e1-b6b7-0011856a6e37)

FreeBSD : mozilla -- users may be lured into bypassing security dialogs (a7e0d783-131b-11d9-bc4a-000c41e2cdad)

FreeBSD : mozilla -- vCard stack buffer overflow (da690355-1159-11d9-bc4a-000c41e2cdad)

FreeBSD : Mozilla / Firefox user interface spoofing vulnerability (730db824-e216-11d8-9b0a-000347a4fa7d)

FreeBSD : Mozilla certificate spoofing (abe47a5a-e23c-11d8-9b0a-000347a4fa7d)

FreeBSD : mozilla firefox -- multiple vulnerabilities (922d2398-9e2d-11de-a998-0030843d3802)

FreeBSD : mpack -- Information disclosure (e465159c-4817-11e1-89b4-001ec9578670)

FreeBSD : MPD -- buffer overflows in http output (765d165b-fbfe-11e6-aae7-5404a68ad561)

FreeBSD : mpg123 (1881)

FreeBSD : mpg123 -- buffer overflow in URL handling (20d16518-2477-11d9-814e-0001020eed82)

FreeBSD : mpg123 -- buffer overflow vulnerability (3cc84400-6576-11d9-a9e7-0001020eed82)

FreeBSD : mpg123 -- playlist processing buffer overflow vulnerability (877e918e-5362-11d9-96d4-00065be4b5b6)

FreeBSD : mpg123 buffer overflow (15e0e963-02ed-11d9-a209-00061bc2ad93)

FreeBSD : mpg123 vulnerabilities (9fccad5a-7096-11d8-873f-0020ed76ef5a)

FreeBSD : mplayer & libxine -- MMS and Real RTSP buffer overflow vulnerabilities (91c606fc-b5d0-11d9-a788-0001020eed82)

FreeBSD : mplayer (1618)

FreeBSD : mplayer (2335)

FreeBSD : mplayer -- buffer overflow in the code for RealMedia RTSP streams. (b2ff68b2-9f29-11db-a4e4-0211d87675b7)

FreeBSD : mplayer -- cddb stack overflow (3ac80dd2-14df-11dc-bcfc-0016179b2dd5)

FreeBSD : mplayer -- DMO File Parsing Buffer Overflow Vulnerability (abeb9b64-ce50-11db-bc24-0016179b2dd5)

FreeBSD : mplayer -- heap overflow in the ASF demuxer (104beb63-af4d-11da-8414-0013d4a4a40e)

FreeBSD : mplayer -- multiple integer overflows (724e6f93-8f2a-11dd-821f-001cc0377035)

FreeBSD : mplayer -- Multiple integer overflows (c7526a14-c4dc-11da-9699-00123ffe8333)

FreeBSD : mplayer -- multiple vulnerabilities (85d76f02-5380-11d9-a9e7-0001020eed82)

FreeBSD : mplayer -- multiple vulnerabilities (de4d4110-ebce-11dc-ae14-0016179b2dd5)

FreeBSD : mplayer -- potential buffer overrun when processing malicious lzo compressed input (9ab3a22c-feb8-11e3-b938-5404a68ad561)

FreeBSD : mplayer -- twinvq processing buffer overflow vulnerability (7c5bd5b8-d652-11dd-a765-0030843d3802)

FreeBSD : mplayer -- vulnerability in STR files processor (5ccb1c14-e357-11dd-a765-0030843d3802)

FreeBSD : mplayer heap overflow in http requests (5e7f58c3-b3f8-4258-aeb8-795e5e940ff8)

FreeBSD : mpv -- arbitrary code execution via crafted website (3ee6e521-0d32-11e8-99b0-d017c2987f9a)

FreeBSD : msmtp -- certificate-verification issue (f0416fb5-3130-11e9-a5ba-e0d55e883e26)

FreeBSD : MT -- Search Unspecified XSS (350a5bd9-520b-11db-8f1a-000a48049292)

FreeBSD : mt-daapd -- denial of service vulnerability (a7080c30-91a2-11dc-b2eb-00b0d07e6c7e)

FreeBSD : mt-daapd -- integer overflow (86a4d810-1884-11dd-a914-0016179b2dd5)

FreeBSD : multi-gnome-terminal (2282)

FreeBSD : multiple buffer overflows in xboing (e25566d5-6d3f-11d8-83a4-000a95bc6fae)

FreeBSD : Multiple exploitable heap-based buffer overflow vulnerabilities exists in FreeXL 1.0.3 (555cd806-b031-11e7-a369-14dae9d59f67)

FreeBSD : Multiple implementations -- DoS via hash algorithm collision (91be81e7-3fea-11e1-afc7-2c4138874f7d)

FreeBSD : Multiple ports -- Proxy HTTP header vulnerability (httpoxy) (cf0b5668-4d1b-11e6-b2ec-b499baebfeaf)

FreeBSD : Multiple Potential Buffer Overruns in Samba (2de14f7a-dad9-11d8-b59a-00061bc2ad93)

FreeBSD : Multiple vulnerabilities in Botan (4cd9b19f-f66d-11e5-b94c-001999f8d30b)

FreeBSD : multiple vulnerabilities in ethereal (265c8b00-d2d0-11d8-b479-02e0185c0b53)

FreeBSD : multiple vulnerabilities in ethereal (74d06b67-d2cf-11d8-b479-02e0185c0b53)

FreeBSD : multiple vulnerabilities in ethereal (cdf18ed9-7f4a-11d8-9645-0020ed76ef5a)

FreeBSD : multiple vulnerabilities in phpBB (c551ae17-7f00-11d8-868e-000347dd607f)

FreeBSD : mumble -- multiple vulnerabilities (77e2e631-e742-11e3-9a25-5404a6a6412c)

FreeBSD : mumble -- NULL pointer dereference and heap-based buffer overflow (c2c8c84b-e734-11e3-9a25-5404a6a6412c)

FreeBSD : mupdf -- multiple vulnerabilities (47157c14-9013-11e6-a590-14dae9d210b8)

FreeBSD : mupdf -- Remote System Access (53bde960-356b-11e0-8e81-0022190034c0)

FreeBSD : Mutiple browser frame injection vulnerability (641859e8-eca1-11d8-b913-000c41e2cdad)

FreeBSD : mutt -- buffer overflow vulnerability (863f95d3-3df1-11dc-b3d3-0016179b2dd5)

FreeBSD : mutt -- denial of service via crafted mail message (c3d43001-8064-11e4-801f-0022156e8794)

FreeBSD : mutt -- denial of service, potential remote code execution (eb426e82-ab68-11e3-9d09-000c2980a9f3)

FreeBSD : mutt -- Remote Buffer Overflow Vulnerability (d2a43243-087b-11db-bc36-0008743bf21a)

FreeBSD : mutt -- remote code injection and path traversal vulnerability (a2f35081-8a02-11e8-8fa5-4437e6ad11c4)

FreeBSD : mutt-devel -- failure to check SMTP TLS server certificate (49314321-7fd4-11e1-9582-001b2134ef46)

FreeBSD : mutt/neomutt -- multiple vulnerabilities (fe12ef83-8b47-11e8-96cc-001a4a7ec6be)

FreeBSD : mybb -- multiple vulnerabilities (7761288c-d148-11e7-87e5-00e04c1ea73d)

FreeBSD : mybb -- multiple vulnerabilities (addad6de-d752-11e7-99bf-00e04c1ea73d)

FreeBSD : mybb -- multiple vulnerabilities (beb6f4a8-add5-11de-8b55-0030843d3802)

FreeBSD : mybb -- multiple vulnerabilities (d50a50a2-2f3e-11e8-86f8-00e04c1ea73d)

FreeBSD : mybb -- vulnerabilities (13960f55-8d35-11e9-9ba0-4c72b94353b5)

FreeBSD : mybb -- vulnerabilities (395ed9d5-3cca-11e9-9ba0-4c72b94353b5)

FreeBSD : mybb -- vulnerabilities (ab38d9f8-b787-11e8-8e7a-00e04c1ea73d)

FreeBSD : mybb -- vulnerabilities (bfd5d004-81d4-11e8-a29a-00e04c1ea73d)

FreeBSD : mybb -- vulnerabilities (db2acdac-b5a7-11e8-8f6f-00e04c1ea73d)

FreeBSD : MySQL - Multiple vulnerabilities (851a0eea-88aa-11e5-90e7-b499baebfeaf)

FreeBSD : mysql -- ALTER MERGE denial of service vulnerability (06a6b2cf-484b-11d9-813c-00065be4b5b6)

FreeBSD : mysql -- command line client input validation vulnerability (4775c807-8f30-11dd-821f-001cc0377035)

FreeBSD : mysql -- database 'case-sensitive' privilege escalation (a0e92718-6603-11db-ab90-000e35fd8194)

FreeBSD : mysql -- database suid privilege escalation (a9c51caf-6603-11db-ab90-000e35fd8194)

FreeBSD : mysql -- denial of service vulnerability (7c27192f-0bc3-11e7-9940-b499baebfeaf)

FreeBSD : mysql -- empty bit-string literal denial of service (66a770b4-e008-11dd-a765-0030843d3802)

FreeBSD : mysql -- erroneous access restrictions applied to table renames (035d17b2-484a-11d9-813c-00065be4b5b6)

FreeBSD : mysql -- format string vulnerability (fcb90eb0-2ace-11db-a6e2-000e0c2e438a)

FreeBSD : mysql -- FTS request denial of service vulnerability (29edd807-438d-11d9-8bb9-00065be4b5b6)

FreeBSD : mysql -- GRANT access restriction problem (01c231cd-4393-11d9-8bb9-00065be4b5b6)

FreeBSD : mysql -- heap buffer overflow with prepared statements (77420ebb-0cf4-11d9-8a8a-000c41e2cdad)

FreeBSD : MySQL -- Information Disclosure and Buffer Overflow Vulnerabilities (4913886c-e875-11da-b9f4-00123ffe8333)

FreeBSD : MySQL -- Multiple vulerabilities (198e6220-ac8b-11e9-a1c7-b499baebfeaf)

FreeBSD : MySQL -- Multiple vulerabilities (a6cf65ad-37d2-11ea-a1c7-b499baebfeaf)

FreeBSD : MySQL -- Multiple vulerabilities (fc91f2ef-fd7b-11e9-a1c7-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (22373c43-d728-11e6-a9a5-b499baebfeaf)

FreeBSD : mysql -- multiple vulnerabilities (4d2f9d09-ddb7-11e6-a9a5-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (4e1997e8-5de0-11e9-b95c-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (57aec168-453e-11e8-8777-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (8c2b2f11-0ebe-11e6-b55e-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (909be51b-9b3b-11e8-add2-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (9bc14850-a070-11e6-a881-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (c41bedfd-b3f9-11e7-ac58-b499baebfeaf)

FreeBSD : MySQL -- Multiple vulnerabilities (ca5cb202-4f51-11e6-b2ec-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (cda2f3c2-6c8b-11e7-867f-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (d3d02d3a-2242-11e9-b95c-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (d9e01c35-2531-11e7-b291-b499baebfeaf) (Riddle)

FreeBSD : MySQL -- multiple vulnerabilities (e3445736-fd01-11e7-ac58-b499baebfeaf)

FreeBSD : mysql -- multiple vulnerabilities (e5186c65-d729-11e6-a9a5-b499baebfeaf)

FreeBSD : MySQL -- multiple vulnerabilities (ec5072b0-d43a-11e8-a6d2-b499baebfeaf)

FreeBSD : mysql -- MyISAM table privileges security bypass vulnerability (388d9ee4-7f22-11dd-a66a-0019666436c2)

FreeBSD : mysql -- MyISAM table privileges security bypass vulnerability for symlinked paths (738f8f9e-d661-11dd-a765-0030843d3802)

FreeBSD : mysql -- mysql\_real\_connect buffer overflow vulnerability (835256b8-46ed-11d9-8ce0-00065be4b5b6)

FreeBSD : mysql -- mysqlhotcopy insecure temporary file creation (0c4d5973-f2ab-11d8-9837-000c41e2cdad)

FreeBSD : mysql -- privilege escalation and overwrite of the system table information (8c451386-dff3-11dd-a765-0030843d3802)

FreeBSD : mysql -- remote dos via malformed password packet (240ac24c-dff3-11dd-a765-0030843d3802)

FreeBSD : mysql -- Remote Root Code Execution (856b88bf-7984-11e6-81e7-d050996490d0)

FreeBSD : mysql -- renaming of arbitrary tables by authenticated users (bb4e9a44-dff2-11dd-a765-0030843d3802)

FreeBSD : MySQL -- SQL-injection security vulnerability (7f8cecea-f199-11da-8422-00123ffe8333)

FreeBSD : mysql -- SSL Downgrade (36bd352d-299b-11e5-86ff-14dae9d210b8) (BACKRONYM)

FreeBSD : MySQL authentication bypass / buffer overflow (e5e2883d-ceb9-11d8-8898-000d6111a684)

FreeBSD : MySQL insecure temporary file creation (mysqlbug) (2e129846-8fbb-11d8-8b29-0020ed76ef5a)

FreeBSD : mysql-scripts -- mysqlaccess insecure temporary file creation (ce109fd4-67f3-11d9-a9e7-0001020eed82)

FreeBSD : mysql-server -- insecure temporary file creation (eeae6cce-d05c-11d9-9aed-000e0c2e438a)

FreeBSD : mysql-server -- multiple remote vulnerabilities (619ef337-949a-11d9-b813-00d05964249f)

FreeBSD : mysql/mariadb/percona server -- multiple vulnerabilities (8c773d7f-6cbb-11e2-b242-c8600054b392)

FreeBSD : mysql50-server -- COM\_TABLE\_DUMP arbitrary code execution (a8d8713e-dc83-11da-a22b-000c6ec775d9)

FreeBSD : nag -- XSS vulnerabilities in several of the tasklist name and task data fields (ee6b5956-6a89-11da-b96e-000fb586ba73)

FreeBSD : nagios -- buffer overflow in history.cgi (97c22a94-5b8b-11e2-b131-000c299b62e1)

FreeBSD : nagios -- Command Injection Vulnerability (3ebd4cb5-657f-11de-883a-00e0815b8da8)

FreeBSD : nagios -- denial of service vulnerability (ba04a373-7d20-11e3-8992-00132034b086)

FreeBSD : nagios -- web interface privilege escalation vulnerability (d4a358d3-e09a-11dd-a765-0030843d3802)

FreeBSD : Nagios -- XSS Vulnerability (fbd7aa81-2cc1-11dd-8cfb-00e0815b8da8)

FreeBSD : nagios-plugins -- Long Location Header Buffer Overflow Vulnerability (7453c85d-7830-11dc-b4c8-0016179b2dd5)

FreeBSD : nap allows arbitrary file access (83119e27-5d7c-11d8-80e3-0020ed76ef5a)

FreeBSD : nas -- multiple vulnerabilities (bf7912f5-c1a8-11e3-a5ac-001b21614864)

FreeBSD : nbd-server -- buffer overflow vulnerability (43770b1c-72f6-11da-8c1d-000e0c2e438a)

FreeBSD : nbsmtp -- format string vulnerability (debbb39c-fdb3-11d9-a30d-00b0d09acbfc)

FreeBSD : ncurses -- multiple issues (b84dbd94-e894-4c91-b8cd-d328537b1b2b)

FreeBSD : neon -- NULL pointer dereference in Digest domain support (755fa519-80a9-11dd-8de5-0030843d3802)

FreeBSD : neon date parsing vulnerability (8d075001-a9ce-11d8-9c6d-0020ed76ef5a)

FreeBSD : neon format string vulnerabilities (84237895-8f39-11d8-8b29-0020ed76ef5a)

FreeBSD : nessus-devel (1298)

FreeBSD : net-snmp -- denial of service via GETBULK request (92f86b93-923f-11dc-a2bf-02e081235dab)

FreeBSD : net-snmp -- DoS for SNMP agent via crafted GETBULK request (daf045d7-b211-11dd-a987-000c29ca8953)

FreeBSD : net-snmp -- fixproc insecure temporary file creation (3e0072d4-d05b-11d9-9aed-000e0c2e438a)

FreeBSD : net-snmp -- Remote DoS (5d85976a-9011-11e1-b5e0-000c299b62e1)

FreeBSD : net-snmp -- remote DoS vulnerability (b2a1a3b5-ed95-11d9-8310-0001020eed82)

FreeBSD : net-snmp -- snmp\_pdu\_parse() function incomplete initialization (381183e8-3798-11e5-9970-14dae9d210b8)

FreeBSD : net-snmp -- snmptrapd crash (4622635f-37a1-11e5-9970-14dae9d210b8)

FreeBSD : net/openafs -- buffer overflow (0bf376b7-cc6b-11e2-a424-14dae938ec40)

FreeBSD : netatalk -- arbitrary command execution in papd daemon (72cba7b0-13cd-11de-a964-0030843d3802)

FreeBSD : netatalk3 -- remote code execution vulnerability (9c9023ff-9057-11e9-b764-00505632d232)

FreeBSD : netpbm -- buffer overflow in pnmtopng (ae9fb0d7-c4dc-11da-b2fb-000e0c2e438a)

FreeBSD : newsfetch -- server response buffer overflow vulnerability (76e0b133-6bfd-11d9-a5df-00065be4b5b6)

FreeBSD : newsgrab -- directory traversal vulnerability (35f6093c-73c3-11d9-8a93-00065be4b5b6)

FreeBSD : newsgrab -- insecure file and directory creation (cd7e260a-6bff-11d9-a5df-00065be4b5b6)

FreeBSD : newspost -- server response buffer overflow vulnerability (7f13607b-6948-11d9-8937-00065be4b5b6)

FreeBSD : nexus2-oss -- Multiple vulerabilities (b2f9573a-008c-11ea-9801-10c37b4ac2ea)

FreeBSD : nfsen -- remote command execution (6e83b2f3-e4e3-11e6-9ac1-a4badb2f4699)

FreeBSD : nfsen -- remote command execution (70372cda-6771-11de-883a-00e0815b8da8)

FreeBSD : nghttp2 -- Denial of service due to NULL pointer dereference (1fccb25e-8451-438c-a2b9-6a021e4d7a31)

FreeBSD : nghttp2 -- multiple vulnerabilities (121fec01-c042-11e9-a73f-b36f5969f162) (Data Dribble) (Resource Loop)

FreeBSD : nghttp2 -- Out of memory in nghttpd, nghttp, and libnghttp2\_asio (07718e2b-d29d-11e5-a95f-b499baebfeaf)

FreeBSD : nghttp2 -- use after free (93eadedb-c6a6-11e5-96d6-14dae9d210b8)

FreeBSD : nginx -- a specially crafted request might result in an integer overflow (b28adc5b-6693-11e7-ad43-f0def16c5c1b)

FreeBSD : nginx -- a specially crafted request might result in worker process crash (36cf7670-2774-11e6-af29-f0def16c5c1b)

FreeBSD : nginx -- Buffer overflow in the ngx\_http\_mp4\_module (0c14dfa7-879e-11e1-a2a0-00500802d8f7)

FreeBSD : NGINX -- HTTP request smuggling (c1202de8-4b29-11ea-9673-4c72b94353b5)

FreeBSD : nginx -- inject commands into SSL session vulnerability (77b784bb-3dc6-11e4-b191-f0def16c5c1b)

FreeBSD : nginx -- inject commands into SSL session vulnerability (ad747a01-1fee-11e4-8ff1-f0def16c5c1b)

FreeBSD : NGINX -- Multiple vulnerabilities (84ca56be-e1de-11e8-bcfd-00e04c1ea73d)

FreeBSD : NGINX -- Multiple vulnerabilities (87679fcb-be60-11e9-9051-4c72b94353b5) (0-Length Headers Leak) (Data Dribble) (Resource Loop)

FreeBSD : nginx -- multiple vulnerabilities (c1c18ee1-c711-11e5-96d6-14dae9d210b8)

FreeBSD : nginx -- multiple vulnerabilities (efaa4071-b700-11e2-b1b9-f0def16c5c1b)

FreeBSD : nginx -- potential information leak (29194cb8-6e9f-11e1-8376-f0def16c5c1b)

FreeBSD : nginx -- remote denial of service vulnerability (152b27f0-a158-11de-990c-e5b1d4c882e0)

FreeBSD : nginx -- Request line parsing vulnerability (94b6264a-5140-11e3-8b22-f0def16c5c1b)

FreeBSD : nginx -- SPDY heap buffer overflow (fc28df92-b233-11e3-99ca-f0def16c5c1b)

FreeBSD : nginx -- SPDY memory corruption (89db3b31-a4c3-11e3-978f-f0def16c5c1b)

FreeBSD : nginx-devel -- SPDY heap buffer overflow (da4b89ad-b28f-11e3-99ca-f0def16c5c1b)

FreeBSD : ngircd -- buffer overflow vulnerability (7f6dd1bd-7d99-11d9-a9e7-0001020eed82)

FreeBSD : ngircd -- format string vulnerability (bc4a7efa-7d9a-11d9-a9e7-0001020eed82)

FreeBSD : node -- access to unintended files (1257718e-be97-458a-9744-d938b592db42)

FreeBSD : node -- multiple vulnerabilities (6d33b3e5-ea03-11e5-85be-14dae9d210b8)

FreeBSD : node -- private information disclosure (a1d0911f-987a-11e1-a2ef-001fd0af1a4c)

FreeBSD : node, iojs, and v8 -- denial of service (864e6f75-2372-11e5-86ff-14dae9d210b8)

FreeBSD : node.js -- ares\_create\_query single byte out of buffer write (28bb6ee5-9b5c-11e6-b799-19bef72f4b7c)

FreeBSD : node.js -- Data Confidentiality/Integrity Vulnerability, December 2017 (bea84a7a-e0c9-11e7-b4f3-11baa0c2df21)

FreeBSD : node.js -- DoS Vulnerability (206f9826-a06d-4927-9a85-771c37010b32)

FreeBSD : Node.js -- multiple vulnerabilities (0032400f-624f-11ea-b495-000d3ab229d6)

FreeBSD : node.js -- multiple vulnerabilities (0904e81f-a89d-11e8-afbb-bc5ff4f77b71)

FreeBSD : node.js -- multiple vulnerabilities (27180c99-9b5c-11e6-b799-19bef72f4b7c)

FreeBSD : node.js -- multiple vulnerabilities (2a86f45a-fc3c-11e8-a414-00155d006b02)

FreeBSD : node.js -- multiple vulnerabilities (3eff66c5-66c9-11e7-aa1d-3d2e663cef42)

FreeBSD : node.js -- multiple vulnerabilities (45b8e2eb-7056-11e8-8fab-63ca6e0e13a2)

FreeBSD : node.js -- multiple vulnerabilities (5a9bbb6e-32d3-11e8-a769-6daaba161086)

FreeBSD : Node.js -- multiple vulnerabilities (b71d7193-3c54-11e9-a3f9-00155d006b02)

FreeBSD : Node.js -- multiple vulnerabilities (c97a940b-c392-11e9-bb38-000d3ab229d6) (0-Length Headers Leak) (Data Dribble) (Empty Frames Flood) (Internal Data Buffering) (Ping Flood) (Reset Flood) (Resource Loop) (Settings Flood)

FreeBSD : Node.js -- remote DOS security vulnerability (d7d1cc94-b971-11e7-af3a-f1035dd0da62)

FreeBSD : Nokogiri -- injection vulnerability (0569146e-bdef-11e9-bd31-8de4a4470bbb)

FreeBSD : nsd -- buffer overflow vulnerability (37a8603d-4494-11de-bea7-000c29a67389)

FreeBSD : nsd -- Denial of Service (17f369dc-d7e7-11e1-90a2-000c299b62e1)

FreeBSD : nsd -- Stack-based Buffer Overflow (56778a31-c2a1-11e9-9051-4c72b94353b5)

FreeBSD : nss (1772)

FreeBSD : nss -- exploitable buffer overflow in SSLv2 protocol handler (129)

FreeBSD : nss -- exploitable buffer overflow in SSLv2 protocol handler (207f8ff3-f697-11d8-81b0-000347a4fa7d)

FreeBSD : NSS -- MD5 downgrade in TLS 1.2 signatures (10f7bc76-0335-4a88-b391-0b05b3a8ce1c) (SLOTH)

FreeBSD : NSS -- multiple vulnerabilities (32166082-53fa-41fa-b081-207e7a989a0a)

FreeBSD : NSS -- multiple vulnerabilities (4cb165f0-6e48-423e-8147-92255d35c0f7)

FreeBSD : NSS -- multiple vulnerabilities (75091516-6f4b-4059-9884-6727023dc366)

FreeBSD : NSS -- multiple vulnerabilities (c4292768-5273-4f17-a267-c5fe35125ce4)

FreeBSD : NSS -- RSA Signature Forgery (48108fb0-751c-4cbb-8f33-09239ead4b55)

FreeBSD : nss -- Use-after-free in TLS 1.2 generating handshake hashes (e71fd9d3-af47-11e7-a633-009c02a2ab30)

FreeBSD : nss-pam-ldapd -- file descriptor buffer overflow (58c15292-7b61-11e2-95da-001e8c1a8a0e)

FreeBSD : nss/ca\_root\_nss -- fraudulent certificates issued by DigiNotar.nl (aa5bc971-d635-11e0-b3cf-080027ef73ec)

FreeBSD : ntp -- 13 low- and medium-severity vulnerabilities (c4a18a12-77fc-11e5-a687-206a8a720317)

FreeBSD : ntp -- control message remote Denial of Service vulnerability (0d0f3050-1f69-11e5-9ba9-d050996490d0)

FreeBSD : ntp -- Crafted null dereference attack from a trusted source with an authenticated mode 6 packet (c2576e14-36e2-11e9-9eda-206a8a720317)

FreeBSD : ntp -- denial of service vulnerability (4eae4f46-b5ce-11e5-8a2b-d050996490d0)

FreeBSD : ntp -- multiple vulnerabilities (4033d826-87dd-11e4-9079-3c970e169bc2)

FreeBSD : ntp -- multiple vulnerabilities (5237f5d7-c020-11e5-b397-d050996490d0)

FreeBSD : ntp -- Multiple vulnerabilities (591a706b-5cdc-11ea-9a0a-206a8a720317)

FreeBSD : ntp -- multiple vulnerabilities (8db8d62a-b08b-11e6-8eba-d050996490d0)

FreeBSD : ntp -- multiple vulnerabilities (af485ef4-1c58-11e8-8477-d05099c0ae8c)

FreeBSD : ntp -- multiple vulnerabilities (b2487d9a-0c30-11e6-acd0-d050996490d0)

FreeBSD : ntp -- multiple vulnerabilities (ebd84c96-dd7e-11e4-854e-3c970e169bc2)

FreeBSD : ntp -- stack-based buffer overflow (4175c811-f690-4898-87c5-755b3cf1bac6)

FreeBSD : ntpd DRDoS / Amplification Attack using ntpdc monlist command (3d95c9a7-7d5c-11e3-a8c1-206a8a720317)

FreeBSD : nut -- upsd can be remotely crashed (47f13540-c4cb-4971-8dc6-28d0dabfd9cd)

FreeBSD : NVIDIA UNIX driver -- access to arbitrary system memory (b91234e7-9a8b-11e1-b666-001636d274f3)

FreeBSD : NVIDIA UNIX driver -- arbitrary root code execution vulnerability (a6d9da4a-5d5e-11db-8faf-000c6ec775d9)

FreeBSD : NVIDIA UNIX driver -- ARGB cursor buffer overflow in 'NoScanout' mode (1431f2d6-a06e-11e2-b9e0-001636d274f3)

FreeBSD : NVIDIA UNIX driver -- multiple vulnerabilities in the kernel mode layer handler (057e6616-1885-11e7-bb4d-a0d3c19bfa21)

FreeBSD : NVIDIA UNIX driver -- multiple vulnerabilities in the kernel mode layer handler (f52e3a8d-3f7e-11e7-97a9-a0d3c19bfa21)

FreeBSD : NVIDIA UNIX driver -- remote denial of service or arbitrary code execution (fdf72a0e-8371-11e4-bc20-001636d274f3)

FreeBSD : nwclient -- multiple vulnerabilities (d177d9f9-e317-11d9-8088-00123f0f7307)

FreeBSD : OCaml -- Multiple Security Vulnerabilities (8d2af843-7d8e-11e9-8464-c85b76ce9b5a)

FreeBSD : oftpd denial-of-service vulnerability (PORT command) (290d81b9-80f1-11d8-9645-0020ed76ef5a)

FreeBSD : Okular -- Local binary execution via action links (c3600a64-64ea-11ea-bdff-e0d55e2a8bf9)

FreeBSD : oniguruma -- multiple vulnerabilities (a8d87c7a-d1b1-11e9-a616-0992a4564e7c)

FreeBSD : oniguruma -- multiple vulnerabilities (b396cf6c-62e6-11e7-9def-b499baebfeaf)

FreeBSD : oops -- format string vulnerability (1033750f-cab4-11d9-9aed-000e0c2e438a)

FreeBSD : Open DC Hub -- remote buffer overflow vulnerability (cdf14b68-3ff9-11d9-8405-00065be4b5b6)

FreeBSD : openafs -- Denial of Service (c0c31b27-bff3-11e3-9d09-000c2980a9f3)

FreeBSD : openafs -- information disclosure (017a493f-7db6-11e5-a762-14dae9d210b8)

FreeBSD : openafs -- local DoS vulnerability (2e8fe57e-2b46-11e6-ae88-002590263bf5)

FreeBSD : openafs -- multiple vulnerabilities (bcbd3fe0-2b46-11e6-ae88-002590263bf5)

FreeBSD : openafs -- single-DES cell-wide key brute-force vulnerability (c4d412c8-f4d1-11e2-b86c-000c295229d5)

FreeBSD : OpenEXR -- heap buffer overflow, and out-of-memory bugs (e4d9dffb-2a32-11ea-9693-e1b3f6feec79)

FreeBSD : OpenEXR -- multiple remote code execution and denial of service vulnerabilities (803879e9-4195-11e7-9b08-080027ef73ec)

FreeBSD : openfire -- multiple vulnerabilities (937adf01-b64a-11dd-a55e-00163e000016)

FreeBSD : openfire -- multiple vulnerabilities (c3aba586-ea77-11dd-9d1e-000bcdc1757a)

FreeBSD : openfire -- Openfire No Password Changes Security Bypass (e3e30d99-58a8-4a3f-8059-a8b7cd59b881)

FreeBSD : openfire -- unspecified denial of service (b84a992a-12ab-11dd-bab7-0016179b2dd5)

FreeBSD : OpenJPEG -- integer overflow (5efd7a93-2dfb-11e9-9549-e980e869c2e9)

FreeBSD : openjpeg -- Multiple vulnerabilities (02db20d7-e34a-11e3-bd92-bcaec565249c)

FreeBSD : OpenJPEG -- multiple vulnerabilities (11dc3890-0e64-11e8-99b0-d017c2987f9a)

FreeBSD : openjpeg -- multiple vulnerabilities (b7d56d0b-7a11-11e6-af78-589cfc0654e1)

FreeBSD : openjpeg -- use-after-free vulnerability (a233d51f-5d4c-11e5-9ad8-14dae9d210b8)

FreeBSD : openldap -- denial of service vulnerability (4910d161-58a4-11e5-9ad8-14dae9d210b8)

FreeBSD : OpenLDAP -- incorrect handling of NULL in certificate Common Name (abad20bf-c1b4-11e3-a5ac-001b21614864)

FreeBSD : openldap -- modrdn Denial of Service vulnerability (e5d29309-e0db-11dc-97b2-001c2514716c)

FreeBSD : openldap -- multiple remote denial of service vulnerabilities (db449245-870d-11dc-a3ec-001921ab2fa4)

FreeBSD : openldap -- slapd acl selfwrite Security Issue (ae7124ff-547c-11db-8f1a-000a48049292)

FreeBSD : openldap -- two remote denial of service vulnerabilities (a0c45e53-ae51-11e4-8ac7-d050992ecde8)

FreeBSD : openldap -- two security bypass vulnerabilities (be3dfe33-410b-11e0-9e02-00215c6a37bb)

FreeBSD : openoffice -- arbitrary code execution vulnerabilities (842bafdd-be2f-11dd-a578-0030843d3802)

FreeBSD : openoffice -- arbitrary command execution vulnerability (e595e170-6771-11dc-8be8-02e0185f8d72)

FreeBSD : openoffice -- DOC document heap overflow vulnerability (b206dd82-ac67-11d9-a788-0001020eed82)

FreeBSD : openoffice -- document disclosure (c62dc69f-05c8-11d9-b45d-000c41e2cdad)

FreeBSD : openoffice -- information disclosure vulnerability (ab947396-9018-11e6-a590-14dae9d210b8)

FreeBSD : OpenOffice 4.1.1 -- multiple vulnerabilities (18b3c61b-83de-11e5-905b-ac9e174be3af)

FreeBSD : openoffice.org -- multiple vulnerabilities (c97d7a37-2233-11df-96dd-001b2134ef46)

FreeBSD : openoffice.org -- Multiple vulnerabilities (f2b43905-3545-11e0-8e81-0022190034c0)

FreeBSD : opensaml2 -- unauthenticated login (9f14cb36-b6fc-11e0-a044-445c73746d79)

FreeBSD : openslp -- denial of service vulnerability (3c259621-5d4a-11e5-9ad8-14dae9d210b8)

FreeBSD : OpenSMTPd -- critical LPE / RCE vulnerability (08f5c27d-4326-11ea-af8b-00155d0a0200)

FreeBSD : OpenSMTPd -- Local information disclosure (76f1ce19-5749-11ea-bff8-c85b76ce9b5a)

FreeBSD : OpenSMTPd -- LPE and RCE in OpenSMTPD's default install (40c75597-574a-11ea-bff8-c85b76ce9b5a)

FreeBSD : OpenSMTPd -- LPE and RCE in OpenSMTPD's default install (f0683976-5779-11ea-8a77-1c872ccb1e42)

FreeBSD : OpenSMTPD -- multiple vulnerabilities (42852f72-6bd3-11e5-9909-002590263bf5)

FreeBSD : OpenSMTPD -- multiple vulnerabilities (ee7bdf7f-11bb-4eea-b054-c692ab848c20)

FreeBSD : openssh -- command injection when X11Forwarding is enabled (e4644df8-e7da-11e5-829d-c80aa9043978)

FreeBSD : openssh -- information disclosure (dfe0cdc1-baf2-11e5-863a-b499baebfeaf)

FreeBSD : OpenSSH -- MaxAuthTries limit bypass via duplicates in KbdInteractiveDevices (5b74a5bc-348f-11e5-ba05-c80aa9043978)

FreeBSD : OpenSSH -- Memory corruption in sshd (5709d244-4873-11e3-8a46-000d601460a4)

FreeBSD : openssh -- multiple vulnerabilities (2aedd15f-ca8b-11e6-a9a5-b499baebfeaf)

FreeBSD : openssh -- multiple vulnerabilities (32db37a5-50c3-11db-acf3-000c6ec775d9)

FreeBSD : OpenSSH -- PAM vulnerabilities (2920c449-4850-11e5-825f-c80aa9043978)

FreeBSD : OpenSSH -- PermitRootLogin may allow password connections with 'without-password' (27fed73e-484f-11e5-825f-c80aa9043978)

FreeBSD : openssh -- sshd -- remote valid user discovery and PAM /bin/login attack (adccefd1-7080-11e6-a2cb-c80aa9043978)

FreeBSD : openssl -- alternate chains certificate forgery vulnerability (075952fe-267e-11e5-9d03-3c970e169bc2)

FreeBSD : OpenSSL -- Cache timing vulnerability (8f353420-4197-11e8-8777-b499baebfeaf)

FreeBSD : OpenSSL -- ChaCha20-Poly1305 nonce vulnerability (e56f2f7c-410e-11e9-b95c-b499baebfeaf)

FreeBSD : OpenSSL -- Client DoS due to large DH parameter (c82ecac5-6e3f-11e8-8777-b499baebfeaf)

FreeBSD : OpenSSL -- CMS and S/MIME Bleichenbacher attack (60eb344e-6eb1-11e1-8ad7-00e0815b8da8)

FreeBSD : openssl -- crash on handshake (1a802ba9-f444-11e6-9940-b499baebfeaf)

FreeBSD : openssl -- denial of service (0ca24682-3f03-11e6-b3c8-14dae9d210b8)

FreeBSD : openssl -- denial of service in DTLS implementation (82b55df8-4d5a-11de-8811-0030843d3802)

FreeBSD : OpenSSL -- DTLS and TLS 1.1, 1.2 denial of service (dba5d1c9-9f29-11e1-b511-003067c2616f)

FreeBSD : OpenSSL -- DTLS Denial of Service (5c5f19ce-43af-11e1-89b4-001ec9578670)

FreeBSD : openssl -- Incorrect PKCS#1 v1.5 padding validation in crypto(3) (077c2dca-8f9a-11db-ab33-000e0c2e438a)

FreeBSD : OpenSSL -- integer conversions result in memory corruption (7184f92e-8bb8-11e1-8d7b-003067b2972c)

FreeBSD : OpenSSL -- Local Information Disclosure (7ccd4def-c1be-11e3-9d09-000c2980a9f3)

FreeBSD : OpenSSL -- Multiple problems in crypto(3) (0f37d765-c5d4-11db-9f82-000e0c2e438a)

FreeBSD : OpenSSL -- multiple vulnerabilities (01d729ca-1143-11e6-b55e-b499baebfeaf)

FreeBSD : OpenSSL -- multiple vulnerabilities (03175e62-5494-11e4-9cc1-bc5ff4fb5e7b) (POODLE)

FreeBSD : OpenSSL -- multiple vulnerabilities (2ecb7b20-d97e-11e0-b2e2-00215c6a37bb)

FreeBSD : openssl -- multiple vulnerabilities (3679fd10-c5d1-11e5-b85f-0018fe623f2b)

FreeBSD : OpenSSL -- multiple vulnerabilities (3bb451fc-db64-11e7-ac58-b499baebfeaf)

FreeBSD : OpenSSL -- multiple vulnerabilities (43eaa656-80bc-11e6-bf52-b499baebfeaf)

FreeBSD : openssl -- multiple vulnerabilities (4c8d1d72-9b38-11e5-aece-d050996490d0)

FreeBSD : OpenSSL -- multiple vulnerabilities (4e536c14-9791-11e4-977d-d050992ecde8) (FREAK)

FreeBSD : openssl -- multiple vulnerabilities (50751310-a763-11e6-a881-b499baebfeaf)

FreeBSD : openssl -- multiple vulnerabilities (5aaa257e-772d-11e3-a65a-3c970e169bc2)

FreeBSD : OpenSSL -- multiple vulnerabilities (5ac53801-ec2e-11e3-9cf3-3c970e169bc2)

FreeBSD : OpenSSL -- multiple vulnerabilities (78cc8a46-3e56-11e1-89b4-001ec9578670)

FreeBSD : openssl -- multiple vulnerabilities (8305e215-1080-11e5-8ba2-000c2980a9f3) (Logjam)

FreeBSD : OpenSSL -- multiple vulnerabilities (8aff07eb-1dbd-11e4-b6ba-3c970e169bc2)

FreeBSD : OpenSSL -- multiple vulnerabilities (91a337d8-83ed-11e6-bf52-b499baebfeaf)

FreeBSD : OpenSSL -- multiple vulnerabilities (9d15355b-ce7c-11e4-9db0-d050992ecde8) (FREAK)

FreeBSD : OpenSSL -- Multiple vulnerabilities (9e0c6f7a-d46d-11e9-a1c7-b499baebfeaf)

FreeBSD : OpenSSL -- multiple vulnerabilities (b7cff5a9-31cc-11e8-8f07-b499baebfeaf)

FreeBSD : OpenSSL -- multiple vulnerabilities (d455708a-e3d3-11e6-9940-b499baebfeaf)

FreeBSD : OpenSSL -- Multiple vulnerabilities (f40f07aa-c00f-11e7-ac58-b499baebfeaf)

FreeBSD : OpenSSL -- Multiple vulnerabilities in 1.1 branch (238ae7de-dba2-11e8-b713-b499baebfeaf)

FreeBSD : OpenSSL -- NULL pointer dereference / DoS (1959e847-d4f0-11e3-84b0-0018fe623f2b)

FreeBSD : OpenSSL -- Overflow vulnerability (d778ddb0-2338-11ea-a1c7-b499baebfeaf)

FreeBSD : OpenSSL -- Padding oracle vulnerability (7700061f-34f7-11e9-b95c-b499baebfeaf)

FreeBSD : openssl -- potential SSL 2.0 rollback (60e26a40-3b25-11da-9484-00123ffe8333)

FreeBSD : OpenSSL -- Remote Data Injection / DoS (0b8d7194-ca88-11e3-9d8d-c80aa9043978)

FreeBSD : OpenSSL -- Remote Information Disclosure (5631ae98-be9e-11e3-b5e3-c80aa9043978)

FreeBSD : openssl -- timing attack vulnerability (7caebe30-d7f1-11e6-a9a5-b499baebfeaf)

FreeBSD : OpenSSL -- timing vulnerability (6f170cf2-e6b7-11e8-a9a8-b499baebfeaf)

FreeBSD : OpenSSL -- TLS 1.1, 1.2 denial of service (00b0d8cd-7097-11e2-98d9-003067c2616f)

FreeBSD : openssl -- TLS extension parsing race condition (3042c33a-f237-11df-9d02-0018fe623f2b)

FreeBSD : OpenSSL -- vulnerability in DSA signing (6f0529e2-2e82-11e6-b2ec-b499baebfeaf)

FreeBSD : OpenSSL ChangeCipherSpec denial-of-service vulnerability (68233cba-7774-11d8-89ed-0020ed76ef5a)

FreeBSD : OpenTTD -- Buffer overflows in savegame loading (78c25ed7-f3f9-11e0-8b5c-b482fe3f522d)

FreeBSD : OpenTTD -- Denial of Service (0f62be39-e8e0-11e1-bea0-002354ed89bc)

FreeBSD : OpenTTD -- Denial of service (server) via infinite loop (b6069837-aadc-11df-82df-0015f2db7bde)

FreeBSD : OpenTTD -- Denial of service (server) via slow read attack (1ac858b0-3fae-11e1-a127-0013d3ccd9df)

FreeBSD : OpenTTD -- Denial of service (server/client) via invalid read (373e412e-f748-11df-96cd-0015f2db7bde)

FreeBSD : OpenTTD -- Denial of service using forcefully crashed aircrafts (d2073237-5b52-11e3-80f7-c86000cbc6ec)

FreeBSD : OpenTTD -- Denial of service via improperly validated commands (e77befb5-f3f9-11e0-8b5c-b482fe3f522d)

FreeBSD : OpenTTD -- Multiple buffer overflows in validation of external data (9bad5ab1-f3f6-11e0-8b5c-b482fe3f522d)

FreeBSD : openvpn -- arbitrary code execution on client through malicious or compromised server (6129fdc7-6462-456d-a3ef-8fc3fbf44d16)

FreeBSD : OpenVPN -- Buffer overflow in PAM authentication and DoS through port sharing (0dc8be9e-19af-11e6-8de0-080027ef73ec)

FreeBSD : OpenVPN -- denial of service security vulnerability (23ab5c3e-79c3-11e4-8b1e-d050992ecde8)

FreeBSD : openvpn -- denial of service: client certificate validation can disconnect unrelated clients (a51ad838-2077-48b2-a136-e888a7db5f8d)

FreeBSD : openvpn -- denial of service: malicious authenticated 'tap' client can deplete server virtual memory (1986449a-8b74-40fa-b7cc-0d8def8aad65)

FreeBSD : openvpn -- denial of service: undecryptable packet from authorized client can disconnect unrelated clients (d1c39c8e-05ab-4739-870f-765490fa2052)

FreeBSD : openvpn -- illegal client float can break VPN session for other users (8604121c-7fc2-11ea-bcac-7781e90b0c8f)

FreeBSD : openvpn -- LD\_PRELOAD code execution on client through malicious or compromised server (be4ccb7b-c48b-11da-ae12-0002b3b60e4c)

FreeBSD : openvpn -- multiple TCP clients connecting with the same certificate at the same time can crash the server (5ad3e437-e527-4514-b9ed-280b2ca1a8c9)

FreeBSD : OpenVPN -- out-of-bounds write in legacy key-method 1 (3dd6ccf4-a3c6-11e7-a52e-0800279f2ff8)

FreeBSD : openvpn -- potential denial-of-service on servers in TCP mode (3de49331-0dec-422c-93e5-e4719e9869c5)

FreeBSD : OpenVPN -- potential side-channel/timing attack when comparing HMACs (92f30415-9935-11e2-ad4c-080027ef73ec)

FreeBSD : OpenVPN -- several vulnerabilities (9f65d382-56a4-11e7-83e3-080027ef73ec)

FreeBSD : OpenVPN -- two remote denial-of-service vulnerabilities (04cc7bd2-3686-11e7-aa64-080027ef73ec)

FreeBSD : openvpn-devel -- arbitrary code execution (c61ca9cb-64c3-11dd-954d-006097bcc5f4)

FreeBSD : openvswitch -- MPLS buffer overflow (b53bbf58-257f-11e6-9f4d-20cf30e32f6d)

FreeBSD : openx -- remote code execution vulnerability (80b6d6cc-c970-11df-bb18-0015587e2cc1)

FreeBSD : OpenX -- SQL injection vulnerability (3e33a0bb-6b2f-11e3-b042-20cf30e32f6d)

FreeBSD : openx -- sql injection vulnerability (55616fda-a2d0-11dd-a9f9-0030843d3802)

FreeBSD : OpenX -- SQL injection vulnerability (dee44ba9-08ab-11e2-a044-d0df9acfd7e5)

FreeBSD : openx -- undisclosed security issue (46aeba13-64a1-11e1-bc16-0023ae8e59f0)

FreeBSD : opera (1341)

FreeBSD : opera -- 'data:' URI handler spoofing vulnerability (20c9bb14-81e6-11d9-a9e7-0001020eed82)

FreeBSD : opera -- 'javascript:' URL XSS vulnerability (40856a51-e1d9-11d9-b875-0001020eed82)

FreeBSD : Opera -- code injection vulnerability through broken frameset handling (e666498a-852a-11e0-8f78-080027ef73ec)

FreeBSD : opera -- command line URL shell command injection (dfc1daa8-61de-11da-b64c-0001020eed82)

FreeBSD : opera -- Data URIs can be used to allow XSS (77b9f9bc-7fdf-11df-8a8d-0008743bf21a)

FreeBSD : opera -- download dialog spoofing vulnerability (a2aa24fd-00d4-11da-bc08-0001020eed82)

FreeBSD : opera -- execution of arbitrary code (0925716f-34e2-11e2-aa75-003067c2616f)

FreeBSD : opera -- execution of arbitrary code (85f33a8d-492f-11e2-aa75-003067c2616f)

FreeBSD : opera -- execution of arbitrary code (ea0f45e2-6c4b-11e2-98d9-003067c2616f)

FreeBSD : opera -- image dragging vulnerability (934b1de4-00d7-11da-bc08-0001020eed82)

FreeBSD : opera -- kfmclient exec command execution vulnerability (d8e55d65-81d6-11d9-a9e7-0001020eed82)

FreeBSD : opera -- moderately severe issue (cebed39d-9e6f-11e2-b3f5-003067c2616f)

FreeBSD : opera -- multiple vulnerabilities (0e30e802-a9db-11dd-93a2-000bcdf0a03b)

FreeBSD : opera -- multiple vulnerabilities (12d266b6-363f-11dc-b6c9-000c6ec775d9)

FreeBSD : opera -- multiple vulnerabilities (225bc349-ce10-11dd-a721-0030843d3802)

FreeBSD : opera -- multiple vulnerabilities (2eda0c54-34ab-11e0-8103-00215c6a37bb)

FreeBSD : opera -- multiple vulnerabilities (2fda6bd2-c53c-11de-b157-001999392805)

FreeBSD : opera -- multiple vulnerabilities (30c560ff-e0df-11dc-891a-02061b08fc24)

FreeBSD : opera -- multiple vulnerabilities (31b045e7-ae75-11dc-a5f9-001a4d49522b)

FreeBSD : opera -- multiple vulnerabilities (38daea4f-2851-11e2-9483-14dae938ec40)

FreeBSD : opera -- multiple vulnerabilities (44224e08-8306-11dc-9283-0016179b2dd5)

FreeBSD : opera -- multiple vulnerabilities (4582948a-9716-11de-83a5-001999392805)

FreeBSD : opera -- multiple vulnerabilities (6431c4db-deb4-11de-9078-0030843d3802)

FreeBSD : opera -- multiple vulnerabilities (71273c4d-a6ec-11df-8a8d-0008743bf21a)

FreeBSD : opera -- multiple vulnerabilities (73ec1008-72f0-11dd-874b-0030843d3802)

FreeBSD : opera -- multiple vulnerabilities (78ad2525-9d0c-11db-a5f6-000c6ec775d9)

FreeBSD : opera -- multiple vulnerabilities (8c5205b4-11a0-11de-a964-0030843d3802)

FreeBSD : opera -- multiple vulnerabilities (a4a809d8-25c8-11e1-b531-00215c6a37bb) (BEAST)

FreeBSD : opera -- multiple vulnerabilities (aab187d4-e0f3-11df-b1ea-001999392805)

FreeBSD : opera -- multiple vulnerabilities (ad4a00fa-0157-11dd-8bd3-001372ae3ab9)

FreeBSD : opera -- multiple vulnerabilities (d6b092bd-61e1-11da-b64c-0001020eed82)

FreeBSD : opera -- multiple vulnerabilities (f5c4d7f7-9f4b-11dd-bab1-001999392805)

FreeBSD : opera -- multiple vulnerabilities (fb84d5dd-9528-11dd-9a00-001999392805)

FreeBSD : opera -- multiple vulnerabilities in Java implementation (1489df94-6bcb-11d9-a21e-000a95bc6fae)

FreeBSD : opera -- redirection XSS vulnerability (985bfcf0-e1d7-11d9-b875-0001020eed82)

FreeBSD : opera -- RSA Signature Forgery (1fe734bf-4a06-11db-b48d-00508d6a62df)

FreeBSD : opera -- URL parsing heap overflow vulnerability (4867ae85-608d-11db-8faf-000c6ec775d9)

FreeBSD : opera -- Vulnerability in javascript handling (df4a7d21-4b17-11dc-9fc2-001372ae3ab9)

FreeBSD : opera -- XMLHttpRequest security bypass (79217c9b-e1d9-11d9-b875-0001020eed82)

FreeBSD : optipng -- arbitrary code execution via crafted BMP image (2bc960c4-e665-11dd-afcd-00e0815b8da8)

FreeBSD : optipng -- multiple vulnerabilities (8fedf75c-ef2f-11e6-900e-003048f78448)

FreeBSD : optipng -- use-after-free vulnerability (a8818f7f-9182-11e2-9bdf-d48564727302)

FreeBSD : optipng -- use-after-free vulnerability (bab05188-5d4b-11e5-9ad8-14dae9d210b8)

FreeBSD : osc -- shell command injection via crafted \_service files (f450587b-d7bd-11e4-b5a4-14dae9d5a9d2)

FreeBSD : osip -- Improper Restriction of Operations within the Bounds of a Memory Buffer (15a62f22-098a-443b-94e2-2d26c375b993)

FreeBSD : otrs -- Clickjacking issue (ffa7c6e4-bb29-11e3-8136-60a44c524f57)

FreeBSD : otrs -- Incomplete Access Control (0c5cf7c4-856e-11e4-a089-60a44c524f57)

FreeBSD : otrs -- information disclosure (8b97d289-d8cf-11e2-a1f5-60a44c524f57)

FreeBSD : otrs -- information disclosure (a5b24a6b-c37c-11e2-addb-60a44c524f57)

FreeBSD : otrs -- Information disclosure and Data manipulation (eae8e3cf-9dfe-11e2-ac7f-001fd056c417)

FreeBSD : otrs -- multiple vulnerabilities (c7b5d72b-886a-11e3-9533-60a44c524f57)

FreeBSD : OTRS -- Multiple vulnerabilities (cebd05d6-ed7b-11e7-95f2-005056925db4)

FreeBSD : OTRS -- Multiple XSS and denial of service vulnerabilities (96e776c7-e75c-11df-8f26-00151735203a)

FreeBSD : otrs -- Scheduler Process ID File Access (1e7f0c11-673a-11e5-98c8-60a44c524f57)

FreeBSD : OTRS -- Several XSS attacks possible (a4372a68-652c-11e0-a25a-00151735203a)

FreeBSD : otrs -- SQL injection (6b575419-14cf-11df-a628-001517351c22)

FreeBSD : otrs -- Sql Injection + Xss Issue (e3e788aa-e9fd-11e2-a96e-60a44c524f57)

FreeBSD : OTRS -- Vulnerabilities in OTRS-Core allows read access to any file on local file system (86baa0d4-c997-11e0-8a8e-00151735203a)

FreeBSD : otrs -- XSS Issue (70b72a52-9e54-11e3-babe-60a44c524f57)

FreeBSD : otrs -- XSS vulnerability (13320091-52a6-11e2-a289-1c4bd681f0cf)

FreeBSD : otrs -- XSS vulnerability (661bd031-c37d-11e2-addb-60a44c524f57)

FreeBSD : otrs -- XSS vulnerability could lead to remote code execution (84065569-7fb4-11e2-9c5a-000d601460a4)

FreeBSD : otrs -- XSS vulnerability in Firefox and Opera (95a69d1a-52a5-11e2-a289-1c4bd681f0cf)

FreeBSD : otrs -- XSS vulnerability in Firefox and Opera could lead to remote code execution (d60199df-7fb3-11e2-9c5a-000d601460a4)

FreeBSD : otrs -- XSS vulnerability in Internet Explorer (49a6026a-52a3-11e2-a289-1c4bd681f0cf)

FreeBSD : otrs -- XSS vulnerability in Internet Explorer could lead to remote code execution (b50cbbc0-7fb2-11e2-9c5a-000d601460a4)

FreeBSD : owncloud -- Multiple security vulnerabilities (d7a43ee6-d2d5-11e2-9894-002590082ac6)

FreeBSD : owncloud -- multiple vulnerabilities (3166222b-c6a4-11e5-96d6-14dae9d210b8)

FreeBSD : owncloudclient -- Improper validation of certificates when using self-signed certificates (71af4ded-8864-11e5-af1b-001999f8d30b)

FreeBSD : p5-Archive-Zip -- virus detection evasion (a5742055-300a-11d9-a9e7-0001020eed82)

FreeBSD : p5-Config-IniFiles -- unsafe temporary file creation (725ab25a-987b-11e1-a2ef-001fd0af1a4c)

FreeBSD : p5-Dancer -- possible to abuse session cookie values (968d1e74-1740-11e5-a643-40a8f0757fb4)

FreeBSD : p5-DBI -- insecure temporary file creation vulnerability (8cfb6f42-d2b0-11da-a672-000e0c2e438a)

FreeBSD : p5-Email-Address-List -- DDoS related vulnerability (22b90fe6-258e-11e9-9c8d-6805ca0b3d42)

FreeBSD : p5-File-Path -- rmtree allows creation of setuid files (13b0c8c8-bee0-11dd-a708-001fc66e7203)

FreeBSD : p5-HTML-Parser -- denial of service (68bda678-caab-11de-a97e-be89dfd1042e)

FreeBSD : p5-HTML-Scrubber -- XSS vulnerability (2f7f4db2-8819-11e5-ab94-002590263bf5)

FreeBSD : p5-Imager -- possibly exploitable buffer overflow (632c98be-aad2-4af2-849f-41a6862afd6a)

FreeBSD : p5-libwww -- possibility to remote servers to create file with a .(dot) character (3a7c5fc4-b50c-11df-977b-ecc31dd8ad06)

FreeBSD : p5-Mail-SpamAssassin (2208)

FreeBSD : p5-Mail-SpamAssassin -- denial of service vulnerability (cc4ce06b-e01c-11d9-a8bd-000cf18bbe54)

FreeBSD : p5-Mail-SpamAssassin -- local user symlink-attack DoS vulnerability (8092b820-1d6f-11dc-a0b2-001921ab2fa4)

FreeBSD : p5-Mail-SpamAssassin -- long message header denial of service (7f3fdef7-51d2-11da-8e93-0010dc4afb40)

FreeBSD : p5-Mojolicious -- cookie-handling vulnerability (a183acb5-1414-11e8-9542-002590acae31)

FreeBSD : p5-Net-DNS -- multiple Vulnerabilities (d2b8a963-3d59-11dc-b3d3-0016179b2dd5)

FreeBSD : p5-PathTools -- File::Spec::canonpath loses taint (333f655a-b93a-11e5-9efa-5453ed2e2b49)

FreeBSD : p5-RT-Authen-ExternalAuth -- privilege escalation (cdc4ff0e-d736-11e1-8221-e0cb4e266481)

FreeBSD : p5-UI-Dialog -- shell command execution vulnerability (00dadbf0-6f61-11e5-a2a1-002590263bf5)

FreeBSD : p5-XSLoader -- local arbitrary code execution (3e08047f-5a6c-11e6-a6c3-14dae9d210b8)

FreeBSD : p7zip -- directory traversal vulnerability (8f5c9dd6-5cac-11e5-9ad8-14dae9d210b8)

FreeBSD : p7zip -- heap overflow vulnerability (a9bcaf57-4a7b-11e6-97f7-5453ed2e2b49)

FreeBSD : p7zip -- heap-based buffer overflow (6d337396-0e4a-11e8-94c0-5453ed2e2b49)

FreeBSD : p7zip -- NULL pointer dereference (48e83187-b6e9-11e6-b6cf-5453ed2e2b49)

FreeBSD : p7zip -- out-of-bounds read vulnerability (d706a3a3-4a7c-11e6-97f7-5453ed2e2b49)

FreeBSD : p7zip-codec-rar -- insufficient error handling (7a2e0063-0e4e-11e8-94c0-5453ed2e2b49)

FreeBSD : palemoon -- multiple vulnerabilities (5044bd23-08cb-11e8-b08f-00012e582166)

FreeBSD : palemoon -- multiple vulnerabilities (6056bf68-f570-4e70-b740-b9f606971283)

FreeBSD : pam\_ldap -- authentication bypass vulnerability (38c76fcf-1744-11da-978e-0001020eed82)

FreeBSD : pango -- integer overflow (4b172278-3f46-11de-becb-001cc0377035)

FreeBSD : pango -- remote DoS vulnerability (5a757a31-f98e-4bd4-8a85-f1c0f3409769)

FreeBSD : passenger -- client controlled header overwriting (84fdd1bb-9d37-11e5-8f5c-002590263bf5)

FreeBSD : passenger -- security vulnerability (1225549f-ca91-11e2-b3b8-f0def16c5c1b)

FreeBSD : password-store -- GPG parsing vulnerabilities (53eb9e1e-7014-11e8-8b1f-3065ec8fd3ec)

FreeBSD : patch -- multiple vulnerabilities (791841a3-d484-4878-8909-92ef9ce424f4)

FreeBSD : pavuk (2472)

FreeBSD : Pavuk HTTP Location header overflow (76904dce-ccf3-11d8-babb-000854d03344)

FreeBSD : payara -- Code execution via crafted PUT requests to JSPs (22bc5327-f33f-11e8-be46-0019dbb15b3f)

FreeBSD : payara -- Default typing issue in Jackson Databind (93f8e0ff-f33d-11e8-be46-0019dbb15b3f)

FreeBSD : payara -- Multiple vulnerabilities (d70c9e18-f340-11e8-be46-0019dbb15b3f)

FreeBSD : pcal -- buffer overflow vulnerabilities (58fc2752-5f74-11d9-a9e7-0001020eed82)

FreeBSD : pcre -- arbitrary code execution (bfd6eef4-8c94-11dc-8c55-001c2514716c)

FreeBSD : pcre -- buffer overflow vulnerability (f9e96930-e6df-11dc-8c6a-00304881ac9a)

FreeBSD : pcre -- heap overflow vulnerability (497b82e0-f9a0-11e5-92ce-002590263bf5)

FreeBSD : pcre -- heap overflow vulnerability (6900e6f1-4a79-11e5-9ad8-14dae9d210b8)

FreeBSD : pcre -- heap overflow vulnerability in '(?|' situations (ff0acfb4-3efa-11e5-93ad-002590263bf5)

FreeBSD : pcre -- Heap Overflow Vulnerability in find\_fixedlength() (8a1d0e63-1e07-11e5-b43d-002590263bf5)

FreeBSD : pcre -- multiple vulnerabilities (4a88e3ed-00d3-11e5-a072-d050996490d0)

FreeBSD : pcre -- multiple vulnerabilities (e69af246-0ae2-11e5-90e4-d050996490d0)

FreeBSD : pcre -- regular expression buffer overflow (b971d2a6-1670-11da-978e-0001020eed82)

FreeBSD : pcre -- stack buffer overflow (7033b42d-ef09-11e5-b766-14dae9d210b8)

FreeBSD : pdfjam -- insecure temporary files (a02c9595-e018-11dd-a765-0030843d3802)

FreeBSD : PEAR -- Net\_Ping and Net\_Traceroute remote arbitrary command injection (56ba8728-f987-11de-b28d-00215c6a37bb)

FreeBSD : pear-Horde\_Image -- DoS vulnerability (00e4050b-56c1-11e7-8e66-08606e46faad)

FreeBSD : pear-Horde\_Image -- remote code execution vulnerability (a7003121-56bf-11e7-8e66-08606e46faad)

FreeBSD : pear-PEAR -- PEAR installer arbitrary code execution vulnerability (44e5f5bd-4d76-11da-bf37-000fb586ba73)

FreeBSD : pear-twig -- remote code execution (705b759c-7293-11e5-a371-14dae9d210b8)

FreeBSD : pear-XML\_RPC -- arbitrary remote code execution (523fad14-eb9d-11d9-a8bd-000cf18bbe54)

FreeBSD : pear-XML\_RPC -- information disclosure vulnerabilities (b64481d9-eff4-11d9-8310-0001020eed82)

FreeBSD : pear-XML\_RPC -- remote PHP code injection vulnerability (e65ad1bf-0d8b-11da-90d0-00304823c0d3)

FreeBSD : pecl-phar -- format string vulnerability (da3d381b-0ee6-11e0-becc-0022156e8794)

FreeBSD : peercast -- arbitrary code execution (402ae710-26a2-11dd-ae05-825f4c35000a)

FreeBSD : peercast -- buffer overflow vulnerability (31435fbc-ae73-11dc-a5f9-001a4d49522b)

FreeBSD : perdition -- str\_vwrite format string vulnerability (617a4021-8bf0-11dc-bffa-0016179b2dd5)

FreeBSD : perl -- denial of service via algorithmic complexity attack on hashing routines (68c1f75b-8824-11e2-9996-c48508086173)

FreeBSD : perl -- Directory Permissions Race Condition (4a99d61c-f23a-11dd-9f55-0030843d3802)

FreeBSD : perl -- File::Path insecure file/directory permissions (c418d472-6bd1-11d9-93ca-000a95bc6fae)

FreeBSD : perl -- local arbitrary code execution (72bfbb09-5a6a-11e6-a6c3-14dae9d210b8)

FreeBSD : perl -- multiple vulnerabilities (41c96ffd-29a6-4dcc-9a88-65f5038fa6eb)

FreeBSD : perl -- multiple vulnerabilities (d9e82328-a129-11e7-987e-4f174049b30a)

FreeBSD : perl -- regular expressions unicode data buffer overflow (5b47c279-8cb5-11dc-8878-0016179b2dd5)

FreeBSD : perl -- vulnerabilities in PERLIO\_DEBUG handling (a5eb760a-753c-11d9-a36f-000a95bc6fae)

FreeBSD : perl, webmin, usermin -- perl format string integer wrap vulnerability (bb33981a-7ac6-11da-bf72-00123f589060)

FreeBSD : perl5 -- taint mechanism bypass vulnerability (d9f99491-1656-11e6-94fa-002590263bf5)

FreeBSD : pgbouncer -- failed auth\_query lookup leads to connection as auth\_user (d76961da-56f6-11e5-934b-002590263bf5)

FreeBSD : pgbouncer -- remote denial of service (8fbd4187-0f18-11e5-b6a8-002590263bf5)

FreeBSD : php -- \_ecalloc Integer Overflow Vulnerability (e329550b-54f7-11db-a5ae-00508d6a62df)

FreeBSD : php -- arbitrary code execution (5a1d5d74-29a0-11e5-86ff-14dae9d210b8)

FreeBSD : php -- arbitrary remote code execution vulnerability (3fd040be-4f0b-11e1-9e32-0025900931f8)

FreeBSD : php -- corruption of $GLOBALS and $this variables via extract() method (f3148a05-0fa7-11e0-becc-0022156e8794)

FreeBSD : php -- crash on crafted tag in exif (cc3bfec6-56cd-11e0-9668-001fd0d616cf)

FreeBSD : PHP -- crypt() returns only the salt for MD5 (3f1df2f9-cd22-11e0-9bb2-00215c6a37bb)

FreeBSD : PHP -- denial of service attack (de7a2b32-bd7d-11e7-b627-d43d7e971a1b)

FreeBSD : php -- env\_path\_info underflow in fpm\_main.c can lead to RCE (6a7c2ab0-00dd-11ea-83ce-705a0f828759)

FreeBSD : php -- ini database truncation inside dba\_replace() function (1e8031be-4258-11de-b67a-0030843d3802)

FreeBSD : php -- input validation error in safe\_mode (ee6fa2bd-406a-11dd-936a-0015af872849)

FreeBSD : php -- integer overflow vulnerability (f6377f08-12a7-11dd-bab7-0016179b2dd5)

FreeBSD : php -- memory\_limit related vulnerability (dd7aa4f1-102f-11d9-8a8a-000c41e2cdad)

FreeBSD : php -- multiple security vulnerabilities (392b5b1d-9471-11dc-9db7-001c2514716c)

FreeBSD : php -- multiple vulnerabilities (057bf770-cac4-11e0-aea3-00215c6a37bb)

FreeBSD : PHP -- multiple vulnerabilities (1b61ecef-cdb9-11e6-a9a5-b499baebfeaf)

FreeBSD : php -- multiple vulnerabilities (27d01223-c457-11dd-a721-0030843d3802)

FreeBSD : php -- multiple vulnerabilities (2b6ed5c7-1a7f-11e0-b61d-000c29d1636d)

FreeBSD : php -- multiple vulnerabilities (2cde1892-913e-11e1-b44c-001fd0af1a4c)

FreeBSD : PHP -- Multiple vulnerabilities (2d56308b-c0a8-11e6-a9a5-b499baebfeaf)

FreeBSD : php -- multiple vulnerabilities (31de2e13-00d2-11e5-a072-d050996490d0)

FreeBSD : php -- multiple vulnerabilities (39a25a63-eb5c-11de-b650-00215c6a37bb)

FreeBSD : php -- multiple vulnerabilities (3d675519-5654-11e5-9ad8-14dae9d210b8)

FreeBSD : php -- multiple vulnerabilities (482d40cb-f9a3-11e5-92ce-002590263bf5)

FreeBSD : php -- multiple vulnerabilities (5764c634-10d2-11e6-94fa-002590263bf5)

FreeBSD : php -- multiple vulnerabilities (59b68b1e-9c78-11e1-b5e0-000c299b62e1)

FreeBSD : php -- multiple vulnerabilities (66d77c58-3b1d-11e6-8e82-002590263bf5)

FreeBSD : PHP -- multiple vulnerabilities (6821a2db-4ab7-11da-932d-00055d790c25)

FreeBSD : PHP -- multiple vulnerabilities (6972668d-cdb7-11e6-a9a5-b499baebfeaf)

FreeBSD : php -- multiple vulnerabilities (6b110175-246d-11e6-8dd3-002590263bf5)

FreeBSD : php -- multiple vulnerabilities (6b771fe2-b84e-11e5-92f9-485d605f4717)

FreeBSD : php -- multiple vulnerabilities (71d903fc-602d-11dc-898c-001921ab2fa4)

FreeBSD : php -- multiple vulnerabilities (7fcf1727-be71-11db-b2ec-000c6ec775d9)

FreeBSD : php -- multiple vulnerabilities (85eb4e46-cf16-11e5-840f-485d605f4717)

FreeBSD : PHP -- multiple vulnerabilities (8d5180a6-86fe-11e6-8d93-00248c0c745d)

FreeBSD : php -- multiple vulnerabilities (b6402385-533b-11e6-a7bd-14dae9d210b8) (httpoxy)

FreeBSD : php -- multiple vulnerabilities (c1da8b75-6aef-11e5-9909-002590263bf5)

FreeBSD : php -- multiple vulnerabilities (d3921810-3c80-11e1-97e8-00215c6a37bb)

FreeBSD : php -- multiple vulnerabilities (d47e9d19-5016-11d9-9b5f-0050569f0001)

FreeBSD : php -- multiple vulnerabilities (ea09c5df-4362-11db-81e1-000e0c2e438a)

FreeBSD : PHP -- multiple vulnerabilities (f471032a-8700-11e6-8d93-00248c0c745d)

FreeBSD : php -- multiple vulnerabilities (f5e52bf5-fc77-11db-8163-000e0c2e438a)

FreeBSD : PHP -- Multiple vulnerabilities in EXIF module (c2d1693b-73cb-11e9-a1c7-b499baebfeaf)

FreeBSD : php -- NULL byte poisoning (3761df02-0f9c-11e0-becc-0022156e8794)

FreeBSD : php -- open\_basedir bypass (73634294-0fa7-11e0-becc-0022156e8794)

FreeBSD : php -- open\_basedir Race Condition Vulnerability (edabe438-542f-11db-a5ae-00508d6a62df)

FreeBSD : php -- php\_variables memory disclosure (ad74a1bd-16d2-11d9-bc4a-000c41e2cdad)

FreeBSD : php -- potential overflow in \_php\_stream\_scandir (bdab0acd-d4cd-11e1-8a1c-14dae9ebcf89)

FreeBSD : php -- readfile() DoS vulnerability (07f3fe15-a9de-11d9-a788-0001020eed82)

FreeBSD : php -- strip\_tags XSS vulnerability (edf61c61-0f07-11d9-8393-000103ccf9d6)

FreeBSD : PHP -- undisclosed vulnerabilities (709e025a-de8b-11e6-a9a5-b499baebfeaf)

FreeBSD : php -- use-after-free vulnerability (3d39e927-29a2-11e5-86ff-14dae9d210b8)

FreeBSD : php -- use-after-free vulnerability (af7fbd91-29a1-11e5-86ff-14dae9d210b8)

FreeBSD : php -- vulnerability in certain CGI-based setups (60de13d5-95f0-11e1-806a-001143cd36d8)

FreeBSD : php -- vulnerability in RFC 1867 file upload processing (562a3fdf-16d6-11d9-bc4a-000c41e2cdad)

FreeBSD : php -- ZipArchive segfault with FL\_UNCHANGED on empty archive (fe853666-56ce-11e0-9668-001fd0d616cf)

FreeBSD : PHP multiple vulnerabilities (d2a892b9-2605-11e4-9da0-00a0986f28c4)

FreeBSD : php-filter -- Denial of Service (c623f058-10e7-11e0-becc-0022156e8794)

FreeBSD : php-gd and gd -- Buffer over-read into uninitialized memory (5033e2fc-98ec-4ef5-8e0b-87cfbbc73081)

FreeBSD : php-imap -- Denial of Service (1a0704e7-0edf-11e0-becc-0022156e8794)

FreeBSD : php-imap -- imap\_open allows to run arbitrary shell commands via mailbox parameter (ec49f6b5-ee39-11e8-b2f4-74d435b63d51)

FreeBSD : php-mbstring -- php mbstring buffer overflow vulnerability (a2074ac6-124c-11de-a964-0030843d3802)

FreeBSD : php-phar -- multiple vulnerabilities (8b1f53f3-2da5-11e5-86ff-14dae9d210b8)

FreeBSD : php-zip -- multiple Denial of Service vulnerabilities (2a41233d-10e7-11e0-becc-0022156e8794)

FreeBSD : php5 -- Denial of Service in php\_date\_parse\_tzfile() (9b2a5e88-02b8-11e2-92d1-000d601460a4)

FreeBSD : php5 -- header splitting attack via carriage-return character (918f38cd-f71e-11e1-8bd8-0022156e8794)

FreeBSD : php5 -- Heap based buffer overflow in quoted\_printable\_encode (59e7163c-cf84-11e2-907b-0025905a4770)

FreeBSD : PHP5 -- Heap corruption in XML parser (31b145f2-d9d3-49a9-8023-11cf742205dc)

FreeBSD : PHP5 -- Integer overflow in Calendar module (5def3175-f3f9-4476-ba40-b46627cc638c)

FreeBSD : PHP5 -- memory corruption in openssl\_x509\_parse() (47b4e713-6513-11e3-868f-0025905a4771)

FreeBSD : php5 -- Multiple security issues (437a68cf-b752-11de-b6eb-00e0815b8da8)

FreeBSD : php5 -- Multiple vulnerabilities (1d23109a-9005-11e2-9602-d43d7e0c7c02)

FreeBSD : php5 -- multiple vulnerabilities (787ef75e-44da-11e5-93ad-002590263bf5)

FreeBSD : php5 -- multiple vulnerabilities (cdff0af2-1492-11e5-a1cf-002590263bf5)

FreeBSD : php5 -- multiple vulnerabilities (e991ef79-e920-11e5-92ce-002590263bf5)

FreeBSD : php5 -- multiple vulnerabilities (f7a9e415-bdca-11e4-970c-000c292ee6b8) (GHOST)

FreeBSD : php5 -- potential magic\_quotes\_gpc vulnerability (1f9e2376-c52f-11dd-8cbc-00163e000016)

FreeBSD : php5-gd -- uninitialized memory information disclosure vulnerability (58a3c266-db01-11dd-ae30-001cc0377035)

FreeBSD : php5-sqlite -- open\_basedir bypass (ec255bd8-02c6-11e2-92d1-000d601460a4)

FreeBSD : php7 -- multiple vulnerabilities (5af511e5-e928-11e5-92ce-002590263bf5)

FreeBSD : phpbb (2258)

FreeBSD : phpbb -- arbitrary command execution and other vulnerabilities (e3cf89f0-53da-11d9-92b7-ceadd4ac2edd)

FreeBSD : phpbb -- Insuffient check against HTML code in usercp\_register.php (4a0b334d-8d8d-11d9-afa0-003048705d5a)

FreeBSD : phpbb -- multiple information disclosure vulnerabilities (03653079-8594-11d9-afa0-003048705d5a)

FreeBSD : phpbb -- multiple vulnerabilities (28c9243a-72ed-11da-8c1d-000e0c2e438a)

FreeBSD : phpbb -- multiple vulnerabilities (326c517a-d029-11d9-9aed-000e0c2e438a)

FreeBSD : phpbb -- NULL byte injection vulnerability (86526ba4-53c8-11db-8f1a-000a48049292)

FreeBSD : phpbb -- privilege elevation and path disclosure (53e711ed-8972-11d9-9ff8-00306e01dda2)

FreeBSD : phpbb -- remote PHP code execution vulnerability (4afacca1-eb9d-11d9-a8bd-000cf18bbe54)

FreeBSD : phpBB IP address spoofing (cfe17ca6-6858-4805-ba1d-a60a61ec9b4d)

FreeBSD : phpBB session table exhaustion (a56a72bb-9f72-11d8-9585-0020ed76ef5a)

FreeBSD : phpbb3 -- multiple issues (8e89a89a-fd15-11e7-bdf6-00e04c1ea73d)

FreeBSD : phpgedview (2245)

FreeBSD : phpgroupware (1767)

FreeBSD : phpgroupware (1929)

FreeBSD : phpgroupware (2041)

FreeBSD : phpicalendar -- file disclosure vulnerability (f1f163ce-9e09-11da-b410-000e0c2e438a)

FreeBSD : phpicalendar -- XSS vulnerability (12f9d9e9-9e1e-11da-b410-000e0c2e438a)

FreeBSD : phpLDAPadmin -- Remote PHP code injection vulnerability (edf47177-fe3f-11e0-a207-0014a5e3cda6)

FreeBSD : phpldapadmin -- XSS and Script Insertion vulnerabilities (6d78202e-e2f9-11da-8674-00123ffe8333)

FreeBSD : phplist -- local file inclusion vulnerability (40774927-f6b4-11dd-94d9-0030843d3802)

FreeBSD : phpList -- SQL injection and XSS vulnerability (fd8bac56-c444-11e1-864b-001cc0877741)

FreeBSD : phpmailer -- Multiple vulnerability (b036faba-edd8-11e8-b3b7-00e04c1ea73d)

FreeBSD : phpmailer -- Remote Code Execution (3c4693de-ccf7-11e6-a9a5-b499baebfeaf)

FreeBSD : phpmailer -- Remote Code Execution (7ae0be99-d8bb-11e6-9b7f-d43d7e971a1b)

FreeBSD : phpmailer -- Remote Code Execution (c7656d4c-cb60-11e6-a9a5-b499baebfeaf)

FreeBSD : PHPmailer -- SMTP injection vulnerability (8a90dc87-89f9-11e5-a408-00248c0c745d)

FreeBSD : phpmailer -- XSS in code example and default exeception handler (c5d79773-8801-11e7-93f7-d43d7e971a1b)

FreeBSD : phpMyAdmin (1691)

FreeBSD : phpmyadmin -- 'set\_theme' XSS (7b55f5c2-c58b-11da-9110-00123ffe8333)

FreeBSD : phpmyadmin -- arbitrary file include and XSS vulnerabilities (882ef43b-901f-11d9-a22c-0001020eed82)

FreeBSD : phpMyAdmin -- bypass 'no password' restriction (68611303-149e-11e7-b9bb-6805ca0b3d42)

FreeBSD : phpMyAdmin -- clickJacking protection can be bypassed (17326fd5-fcfb-11e2-9bb9-6805ca0b3d42)

FreeBSD : phpmyadmin -- Code execution vulnerability (74bf1594-8493-11dd-bb64-0030843d3802)

FreeBSD : phpmyadmin -- command execution vulnerability (0ff0e9a6-4ee0-11d9-a9e7-0001020eed82)

FreeBSD : phpMyAdmin -- Content spoofing vulnerability (08d11134-79c5-11e5-8987-6805ca0b3d42)

FreeBSD : phpmyadmin -- cross site request forgery vulnerabilities (35e54755-54e4-11dd-ad8b-0030843d3802)

FreeBSD : phpmyadmin -- cross-site request forgery vulnerability (54f72962-c7ba-11dd-a721-0030843d3802)

FreeBSD : phpmyadmin -- CSRF vulnerabilities (19b17ab4-51e0-11db-a5ae-00508d6a62df)

FreeBSD : phpmyadmin -- CSRF vulnerabilities (2ecd02e2-e864-11da-b9f4-00123ffe8333)

FreeBSD : phpmyadmin -- CSRF vulnerability allowing arbitrary SQL execution (ac7da39b-4405-11e8-afbe-6805ca0b3d42)

FreeBSD : phpMyAdmin -- CSRF vulnerability in login form (a5681027-8e03-11e9-85f4-6805ca0b3d42)

FreeBSD : phpMyAdmin -- File disclosure and SQL injection (111aefca-2213-11e9-9c8d-6805ca0b3d42)

FreeBSD : phpmyadmin -- file disclosure vulnerability (9f0a405e-4edd-11d9-a9e7-0001020eed82)

FreeBSD : phpmyadmin -- Full path disclosure vulnerability in SQL parser (78b4ebfb-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpMyAdmin -- Global variable scope injection (1b93f6fe-e1c1-11e2-948d-6805ca0b3d42)

FreeBSD : phpmyadmin -- HTTP Response Splitting vulnerability (c55f9ed0-56a7-11da-a3f0-00123ffe8333)

FreeBSD : phpmyadmin -- increased privilege vulnerability (6192ae3d-9595-11d9-a9e0-0001020eed82)

FreeBSD : phpmyadmin -- information disclosure vulnerability (a7062952-9023-11d9-a22c-0001020eed82)

FreeBSD : phpmyadmin -- Insecure password generation in JavaScript (6f0c2d1b-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpmyadmin -- insufficient output sanitizing when generating configuration file (06f9174f-190f-11de-b2f0-001c2514716c)

FreeBSD : phpmyadmin -- insufficient output sanitizing when generating configuration file (1a0e4cc6-29bf-11de-bdeb-0030843d3802)

FreeBSD : phpmyadmin -- Local file inclusion (1f6ee708-0d22-11e1-b5bd-14dae938ec40)

FreeBSD : phpmyadmin -- local file inclusion vulnerability (9b7053fd-3ab5-11da-9484-00123ffe8333)

FreeBSD : phpmyadmin -- Multiple full path disclosure vulnerabilities (5d6a204f-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpmyadmin -- Multiple full path disclosure vulnerabilities (740badcb-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpMyAdmin -- Multiple security vulnerabilities (8c8fa44d-ad15-11e2-8cea-6805ca0b3d42)

FreeBSD : phpMyAdmin -- multiple vulnerabilities (6fe72178-b2e3-11e6-8b2a-6805ca0b3d42)

FreeBSD : phpMyAdmin -- Multiple vulnerabilities (7721562b-e20a-11e6-b2e2-6805ca0b3d42)

FreeBSD : phpmyadmin -- multiple vulnerabilities (7e4e5c53-a56c-11e0-b180-00216aa06fc2)

FreeBSD : phpmyadmin -- multiple vulnerabilities (ca3fe5b3-185e-11ea-9673-4c72b94353b5)

FreeBSD : phpMyAdmin -- multiple vulnerabilities (cd68ff50-362b-11e0-ad36-00215c6a37bb)

FreeBSD : phpmyadmin -- multiple vulnerabilities (d79fc873-b5f9-11e0-89b4-001ec9578670)

FreeBSD : phpMyAdmin -- multiple vulnerabilities (e7028e1d-3f9b-11e6-81f9-6805ca0b3d42)

FreeBSD : phpMyAdmin -- multiple vulnerabilities (ed10ed3f-fddc-11e8-94cf-6805ca0b3d42)

FreeBSD : phpmyadmin -- multiple vulnerabilities (ef70b201-645d-11e6-9cdc-6805ca0b3d42)

FreeBSD : phpMyAdmin -- multiple vulnerabilities (f4a0212f-f797-11e2-9bb9-6805ca0b3d42)

FreeBSD : phpMyAdmin -- Multiple XSS (8c83145d-2c95-11e1-89b4-001ec9578670)

FreeBSD : phpMyAdmin -- Multiple XSS (ed536336-1c57-11e1-86f4-e0cb4e266481)

FreeBSD : phpmyadmin -- multiple XSS and a man-in-the-middle vulnerability (f682a506-df7c-11e5-81e4-6805ca0b3d42)

FreeBSD : phpMyAdmin -- Multiple XSS due to unescaped HTML output in Trigger, Procedure and Event pages and Fetching the version information from a non-SSL site is vulnerable to a MITM attack (ef417da3-1640-11e2-999b-e0cb4e266481)

FreeBSD : phpMyAdmin -- Multiple XSS in Table operations, Database structure, Trigger and Visualize GIS data pages (db1d3340-e83b-11e1-999b-e0cb4e266481)

FreeBSD : phpmyadmin -- Multiple XSS vulnerabilities (6cc06eec-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpMyAdmin -- multiple XSS vulnerabilities (75e26236-ce9e-11e0-b26a-00215c6a37bb)

FreeBSD : phpMyAdmin -- multiple XSS vulnerabilities (e44fe906-df27-11e0-a333-001cc0a36e12)

FreeBSD : phpMyAdmin -- multiple XSS vulnerabilities, missing validation (3f09ca29-0e48-11e4-b17a-6805ca0b3d42)

FreeBSD : phpMyAdmin -- Path disclosure due to missing library (aca0d7e0-e38a-11e1-999b-e0cb4e266481)

FreeBSD : phpMyAdmin -- Path disclosure due to missing verification of file presence (a81161d2-790f-11e1-ac16-e0cb4e266481)

FreeBSD : phpMyAdmin -- path disclosure vulnerability (88f75070-abcf-11e5-83d3-6805ca0b3d42)

FreeBSD : phpMyAdmin -- reCaptcha bypass (3904f759-5659-11e5-a207-6805ca0b3d42)

FreeBSD : phpmyadmin -- register\_globals emulation 'import\_blacklist' manipulation (23afd91f-676b-11da-99f6-00123ffe8333)

FreeBSD : phpmyadmin -- remote code inclusion and XSS scripting (17cb6ff3-7670-11e8-8854-6805ca0b3d42)

FreeBSD : phpmyadmin -- remote command execution vulnerability (fc07c9ca-22ce-11d9-814e-0001020eed82)

FreeBSD : phpMyAdmin -- Risk of BREACH attack due to reflected parameter (81b4c118-c586-11e4-8495-6805ca0b3d42)

FreeBSD : phpMyAdmin -- self XSS in central columns feature (261ca31c-179f-11e8-b8b9-6805ca0b3d42)

FreeBSD : phpMyAdmin -- Self-XSS due to unescaped HTML output in import. (0871d18b-9638-11e3-a371-6805ca0b3d42)

FreeBSD : phpmyadmin -- Several XSS vulnerabilities (274922b8-ad20-11df-af1f-00e0814cab4e)

FreeBSD : phpmyadmin -- Shared Host Information Disclosure (fe971a0f-1246-11dd-bab7-0016179b2dd5)

FreeBSD : phpMyAdmin -- SQL injection (16aed7b7-344a-11ea-9cdb-001b217b3468)

FreeBSD : phpMyAdmin -- SQL injection (97fcc60a-6ec0-11ea-a84a-4c72b94353b5)

FreeBSD : phpmyadmin -- SQL injection vulnerability (ce2f2ade-e7df-11dc-a701-000bcdc1757a)

FreeBSD : phpMyAdmin -- two XSS vulnerabilities due to unescaped db/table names (c4892644-f8c6-11e3-9f45-6805ca0b3d42)

FreeBSD : phpmyadmin -- Unsafe comparison of XSRF/CSRF token (71b24d99-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpmyadmin -- Unsafe generation of XSRF/CSRF token (60ab0e93-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpmyadmin -- Username/Password Session File Information Disclosure (6eb1dc51-1244-11dd-bab7-0016179b2dd5)

FreeBSD : phpMyAdmin -- XSRF and man-in-the-middle vulnerabilities (c6e31869-f99f-11e4-9f91-6805ca0b3d42)

FreeBSD : phpMyAdmin -- XSRF/CSRF due to DOM based XSS in the micro history feature (cc627e6c-3b89-11e4-b629-6805ca0b3d42)

FreeBSD : phpMyAdmin -- XSRF/CSRF vulnerability (63eb2b11-e802-11e7-a58c-6805ca0b3d42)

FreeBSD : phpmyadmin -- XSS (15485ae8-9848-11dc-9e48-0016179b2dd5)

FreeBSD : phpMyAdmin -- XSS and DoS vulnerabilities (c9c46fbf-7b83-11e4-a96e-6805ca0b3d42)

FreeBSD : phpMyAdmin -- XSS and information disclosure vulnerabilities (a5d4a82a-7153-11e4-88c7-6805ca0b3d42)

FreeBSD : phpmyadmin -- XSS and sensitive data leakage (00ec1be1-22bb-11e6-9ead-6805ca0b3d42)

FreeBSD : phpmyadmin -- XSS and SQL injection vulnerabilities (4769914e-b844-11de-b159-0030843d3802)

FreeBSD : phpMyAdmin -- XSS attack in database search (753f8185-5ba9-42a4-be02-3f55ee580093)

FreeBSD : phpMyAdmin -- XSS due to unescaped HTML output in Create View page (6b97436c-ce1e-11e2-9cb2-6805ca0b3d42)

FreeBSD : phpMyAdmin -- XSS due to unescaped HTML output in GIS visualisation page (7280c3f6-a99a-11e2-8cef-6805ca0b3d42)

FreeBSD : phpMyAdmin -- XSS in replication setup (fdd1c316-5a3d-11e1-8d3e-e0cb4e266481)

FreeBSD : phpmyadmin -- XSS in the import dialog (9e205ef5-a649-11e8-b1f6-6805ca0b3d42)

FreeBSD : phpMyAdmin -- XSS vulnerabilities (3e8b7f8a-49b0-11e4-b711-6805ca0b3d42)

FreeBSD : phpmyadmin -- XSS vulnerabilities (59ada6e5-676a-11da-99f6-00123ffe8333)

FreeBSD : phpMyAdmin -- XSS vulnerabilities (6a33477e-3a9c-11d9-84ad-000c6e8f12ef)

FreeBSD : phpmyadmin -- XSS Vulnerabilities (e285a1f4-4568-11dd-ae96-0030843d3802)

FreeBSD : phpmyadmin -- XSS vulnerabilities (fba75b43-c588-11da-9110-00123ffe8333)

FreeBSD : phpMyAdmin -- XSS vulnerabilities (fbb01289-2645-11e4-bc44-6805ca0b3d42)

FreeBSD : phpMyAdmin -- XSS vulnerabilities in SQL debug output and server monitor page. (25b78f04-59c8-11e4-b711-6805ca0b3d42)

FreeBSD : phpmyadmin -- XSS Vulnerability (150e4548-8950-11dd-a6fe-0030843d3802)

FreeBSD : phpmyadmin -- XSS vulnerability (229577a8-0936-11db-bf72-00046151137e)

FreeBSD : phpmyadmin -- XSS vulnerability (2d2dcbb4-906c-11dc-a951-0016179b2dd5)

FreeBSD : phpmyadmin -- XSS vulnerability (498a8731-7cfc-11dc-96e6-0012f06707f0)

FreeBSD : phpmyadmin -- XSS vulnerability (51b51d4a-7c0f-11dc-9e47-0011d861d5e2)

FreeBSD : phpmyadmin -- XSS vulnerability (58247a96-01c8-11da-bc08-0001020eed82)

FreeBSD : phpmyadmin -- XSS Vulnerability (85b0bbc8-a7a5-11dd-8283-001c2514716c)

FreeBSD : phpmyadmin -- XSS vulnerability (ba73f494-65a8-11de-aef5-001c2514716c)

FreeBSD : phpmyadmin -- XSS vulnerability in normalization page (7694927f-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpmyadmin -- XSS vulnerability in SQL editor (7a59e283-c60b-11e5-bf36-6805ca0b3d42)

FreeBSD : phpmyfaq -- arbitrary PHP code execution vulnerability (3b86583a-66a7-11e3-868f-0025905a4771)

FreeBSD : phpmyfaq -- cross-site request forgery vulnerability (f87a9376-0943-11e6-8fc4-00a0986f28c4)

FreeBSD : phpmyfaq -- multiple issues (33888815-631e-4bba-b776-a9b46fe177b5)

FreeBSD : phpmyfaq -- multiple vulnerabilities (4dd575b8-8f82-11e3-bb11-0025905a4771)

FreeBSD : phpmyfaq -- Remote PHP Code Execution Vulnerability (c80a3d93-8632-11e1-a374-14dae9ebcf89)

FreeBSD : phpmyfaq -- Remote PHP Code Injection Vulnerability (395e0faa-ffa7-11e0-8ac4-6c626dd55a41)

FreeBSD : phpmyfaq -- SQL injection, takeover, path disclosure, remote code execution (c6b9aee8-3071-11da-af18-000ae4641456)

FreeBSD : phpmyfaq -- XSS vulnerabilities (99021f88-ca3c-11df-be21-00e018aa7788)

FreeBSD : phppgadmin -- 'formLanguage' local file inclusion vulnerability (88188a8c-eff6-11d9-8310-0001020eed82)

FreeBSD : phppgadmin -- directory traversal with register\_globals enabled (4ce3c20b-124b-11de-a964-0030843d3802)

FreeBSD : phppgadmin -- XSS vulnerability (3d0e724e-129b-11dc-9f79-0016179b2dd5)

FreeBSD : phpSysInfo -- 'register\_globals' emulation layer overwrite vulnerability (9c1cea79-548a-11da-b53f-0004614cc33d)

FreeBSD : phpsysinfo -- url XSS (88260dfe-3d21-11dc-b3d3-0016179b2dd5)

FreeBSD : phpSysInfo -- XSS vulnerability (50457509-d05e-11d9-9aed-000e0c2e438a)

FreeBSD : phpwebftp -- 'language' Local File Inclusion (d9dc2697-dadf-11da-912f-00123ffe8333)

FreeBSD : picasm -- buffer overflow vulnerability (8a3ece40-3315-11da-a263-0001020eed82)

FreeBSD : pidgin -- MSN overflow parsing SLP messages (59e7af2d-8db7-11de-883b-001e3300a30d)

FreeBSD : pidgin -- multiple remote denial of service vulnerabilities (a2c4d3d5-4c7b-11df-83fb-0015587e2cc1)

FreeBSD : pidgin -- multiple vulnerabilities (b1ca65e6-5aaf-11de-bc9b-0030843d3802)

FreeBSD : pidgin-otr -- format string vulnerability (aa71daaa-9f8c-11e1-bd0a-0082a0c18826)

FreeBSD : pidgin-otr -- use after free (77e0b631-e6cf-11e5-85be-14dae9d210b8)

FreeBSD : Pillow -- Allocation of resources without limits or throttling (998ca824-ef55-11e9-b81f-3085a9a95629)

FreeBSD : Pillow -- Multiple vulnerabilities (0700e76c-3eb0-11ea-8478-3085a9a95629)

FreeBSD : Pillow -- multiple vulnerabilities (bc4898d5-a794-11e6-b2d3-60a44ce6887b)

FreeBSD : pine insecure URL handling (34134fd4-5d81-11d8-80e3-0020ed76ef5a)

FreeBSD : pine remote denial-of-service attack (5abfee2d-5d82-11d8-80e3-0020ed76ef5a)

FreeBSD : pine remotely exploitable buffer overflow in newmail.c (5789a92e-5d7f-11d8-80e3-0020ed76ef5a)

FreeBSD : pine remotely exploitable vulnerabilities (39bd57e6-5d83-11d8-80e3-0020ed76ef5a)

FreeBSD : pitivi -- code execution (6540c8f0-dca3-11e5-8fa8-14dae9d210b8)

FreeBSD : pivot-weblog -- file deletion vulnerability (0fe73a4a-1b18-11de-8226-0030843d3802)

FreeBSD : PivotX -- 'ajaxhelper.php' XSS Vulnerability (0d3547ab-9b69-11e1-bdb1-525401003090)

FreeBSD : PivotX -- administrator password reset vulnerability (ae0e5835-3cad-11e0-b654-00215c6a37bb)

FreeBSD : pivotx -- Multiple unrestricted file upload vulnerabilities (7313b0e3-27b4-11e5-a15a-50af736ef1c0)

FreeBSD : PivotX -- Remote File Inclusion Vulnerability of TimThumb (e454ca2f-f88d-11e0-b566-00163e01a509)

FreeBSD : pivotx -- XSS (XSS) vulnerability (14d846d6-27b3-11e5-a15a-50af736ef1c0)

FreeBSD : piwigo -- CSRF/Path Traversal (edd201a5-8fc3-11e2-b131-000c299b62e1)

FreeBSD : Piwik -- Local File Inclusion Vulnerability (26e1c48a-9fa7-11df-81b5-00e0814cab4e)

FreeBSD : piwik -- multiple vulnerabilities (11351c82-9909-11e5-a9c8-14dae9d5a9d2)

FreeBSD : piwik -- php code execution (fcbf56dd-e667-11de-920a-00248c9b4be7)

FreeBSD : Piwik -- remote command execution vulnerability (23c8423e-9bff-11e0-8ea2-0019d18c446a)

FreeBSD : piwik -- unknown critical vulnerabilities (411ecb79-f9bc-11e0-a7e6-6c626dd55a41)

FreeBSD : piwik -- xss and click-jacking issues (da317bc9-59a6-11e1-bc16-0023ae8e59f0)

FreeBSD : piwik -- XSS vulnerability (22775cdd-395a-11e6-b3c8-14dae9d210b8)

FreeBSD : piwik -- XSS vulnerability (28bf62ef-5e2c-11e6-a15f-00248c0c745d)

FreeBSD : piwik -- XSS vulnerability (c0869649-5a0c-11df-942d-0015587e2cc1)

FreeBSD : PJSIP -- TCP denial of service in PJProject (e21474c6-031a-11e6-aa86-001999f8d30b)

FreeBSD : pkg -- vulnerability in libfetch (2af10639-4299-11ea-aab1-98fa9bfec35a)

FreeBSD : plans -- multiple vulnerabilities (1709084d-4d21-11db-b48d-00508d6a62df)

FreeBSD : Plex Media Server -- Information Disclosure Vulnerability (337960ec-b5dc-11e8-ac58-a4badb2f4699)

FreeBSD : plib -- buffer overflow (13bf0602-c08a-11e2-bb21-083e8ed0f47b)

FreeBSD : plib -- remote code execution via buffer overflow (ba51c2f7-5b43-11e1-8288-00262d5ed8ee)

FreeBSD : plib -- stack-based buffer overflow (c72a2494-c08b-11e2-bb21-083e8ed0f47b)

FreeBSD : pligg -- XSS and Cross-Site Request Forgery (bec38383-e6cb-11de-bdd4-000c2930e89b)

FreeBSD : Pligg CMS -- XSS Vulnerability (c290f093-c89e-11e6-821e-68f7288bdf41)

FreeBSD : plone -- 'member\_id' Parameter Portrait Manipulation Vulnerability (22c6b826-cee0-11da-8578-00123ffe8333)

FreeBSD : plone -- multiple vulnerabilities (6b3374d4-6b0b-11e5-9909-002590263bf5)

FreeBSD : plone -- Remote Security Bypass (7c492ea2-3566-11e0-8e81-0022190034c0)

FreeBSD : plone -- unprotected MembershipTool methods (b6c18956-5fa3-11db-ad2d-0016179b2dd5)

FreeBSD : plone -- unsafe data interpreted as pickles (ffba6ab0-90b5-11dc-9835-003048705d5a)

FreeBSD : plone -- user can masquerade as a group (f4ff7434-9505-11db-9ddc-0011098b2f36)

FreeBSD : png -- DoS crash vulnerability (4cb9c513-03ef-11dc-a51d-0019b95d4f14)

FreeBSD : png -- heap overflow for 32-bit builds (c564f9bd-8ba7-11e4-801f-0022156e8794)

FreeBSD : png -- libpng decompression buffer overflow (edef3f2f-82cf-11df-bcce-0018f3e2eb82)

FreeBSD : png -- libpng decompression denial of service (4fb5d2cd-4c77-11df-83fb-0015587e2cc1)

FreeBSD : png -- memory corruption/possible remote code execution (262b92fe-81c8-11e1-8899-001ec9578670)

FreeBSD : png -- multiple vulnerabilities (172acf78-780c-11dc-b3f4-0016179b2dd5)

FreeBSD : png -- unknown chunk processing uninitialized memory access (57c705d6-12ae-11dd-bab7-0016179b2dd5)

FreeBSD : pngcrush -- libpng Uninitialised Pointer Arrays Vulnerability (ea2411a4-08e8-11de-b88a-0022157515b2)

FreeBSD : polarssl -- denial of service vulnerability (72bf9e21-03df-11e3-bd8d-080027ef73ec)

FreeBSD : polarssl -- Remote attack using crafted certificates (a5856eba-a015-11e4-a680-1c6f65c3c4ff)

FreeBSD : PolarSSL -- Security Fix Backports (d3216606-2b47-11e5-a668-080027ef73ec)

FreeBSD : polarssl -- Timing attack against protected RSA-CRT implementation (ccefac3e-2aed-11e3-af10-000c29789cb5)

FreeBSD : polkit -- multiple vulnerabilities (631fc042-b636-11e5-83ef-14dae9d210b8)

FreeBSD : popfile file disclosure (12c7b7ae-ec90-11d8-b913-000c41e2cdad)

FreeBSD : poppler -- multiple denial of service issues (eca2d861-76f4-42ed-89d2-23a2cb396c87)

FreeBSD : poppler -- Poppler Multiple Vulnerabilities (50d233d9-374b-46ce-922d-4e6b3f777bef)

FreeBSD : poppler -- uninitialized pointer (bc20510f-4dd4-11dd-93e7-0211d880e350)

FreeBSD : portaudit -- auditfile remote code execution (6d329b64-6bbb-11e1-9166-001e4f0fb9b1)

FreeBSD : portupgrade -- insecure temporary file handling vulnerability (22f00553-a09d-11d9-a788-0001020eed82)

FreeBSD : portupgrade-devel -- lack of distfile checksums (b428e6b3-926c-11e1-8d7b-003067b2972c)

FreeBSD : Postfix -- memory corruption vulnerability (3eb2c100-738b-11e0-89f4-001e90d46635)

FreeBSD : postfix -- plaintext command injection with SMTP over TLS (14a6f516-502f-11e0-b448-bbfa2731f9c7)

FreeBSD : postfix-policyd-weight -- working directory symlink vulnerability (072a53e0-0397-11dd-bd06-0017319806e7)

FreeBSD : postfixadmin -- Multiple Vulnerabilities (93688f8f-4935-11e1-89b4-001ec9578670)

FreeBSD : postfixadmin -- SQL injection vulnerability (ff98087f-0a8f-11e4-b00b-5453ed2e2b49)

FreeBSD : PostgreSQL -- anonymous remote access data corruption vulnerability (3f332f16-9b6b-11e2-8fe9-08002798f6ff)

FreeBSD : postgresql -- bitsubstr overflow (e050119b-3856-11df-b2b2-002170daae37)

FreeBSD : postgresql -- character conversion and tsearch2 vulnerabilities (486aff57-9ecd-11da-b410-000e0c2e438a)

FreeBSD : PostgreSQL -- Denial-of-Service and Code Injection Vulnerabilities (ca16fd0b-5fd1-11e6-a6f2-6cc21735f730)

FreeBSD : postgresql -- encoding based SQL injection (17f53c1d-2ae9-11db-a6e2-000e0c2e438a)

FreeBSD : PostgreSQL -- Memory disclosure in partition routing (e66a5440-7258-11e9-b0e1-6cc21735f730)

FreeBSD : PostgreSQL -- minor security problems. (97a24d2e-f74c-11e5-8458-6cc21735f730)

FreeBSD : PostgreSQL -- minor security problems. (a0182578-6e00-11e5-a90c-0026551a22dc)

FreeBSD : PostgreSQL -- minor security problems. (fc38cd83-00b3-11e5-8ebd-0026551a22dc)

FreeBSD : PostgreSQL -- multiple buffer overflows and memory issues (3b40bf2c-ad83-11e4-a2b2-0026551a22dc)

FreeBSD : postgresql -- multiple buffer overflows in PL/PgSQL parser (6b4b0b3f-8127-11d9-a9e7-0001020eed82)

FreeBSD : PostgreSQL -- multiple privilege issues (42d42090-9a4d-11e3-b029-08002798f6ff)

FreeBSD : postgresql -- multiple vulnerabilities (51436b4c-1250-11dd-bab7-0016179b2dd5)

FreeBSD : postgresql -- multiple vulnerabilities (65c8ecf9-2adb-11db-a6e2-000e0c2e438a)

FreeBSD : postgresql -- multiple vulnerabilities (e7bc5600-eaa0-11de-bd9c-00215c6a37bb)

FreeBSD : postgresql -- privilege escalation vulnerability (5d425189-7a03-11d9-a9e7-0001020eed82)

FreeBSD : PostgreSQL -- Security Fixes for Regular Expressions, PL/Java. (e8b6605b-d29f-11e5-8458-6cc21735f730)

FreeBSD : PostgreSQL -- Selectivity estimators bypass row security policies (065890c3-725e-11e9-b0e1-6cc21735f730)

FreeBSD : PostgreSQL -- SQL injection in pg\_upgrade and pg\_dump (1c27a706-e3aa-11e8-b77a-6cc21735f730)

FreeBSD : PostgreSQL -- Stack-based buffer overflow via setting a password (245629d4-991e-11e9-82aa-6cc21735f730)

FreeBSD : PostgreSQL -- two vulnerabilities (96eab874-9c79-11e8-b34b-6cc21735f730)

FreeBSD : PostgreSQL vulnerabilities (1f02af5d-c566-11e7-a12d-6cc21735f730)

FreeBSD : PostgreSQL vulnerabilities (414c18bf-3653-11e7-9550-6cc21735f730)

FreeBSD : PostgreSQL vulnerabilities (982872f1-7dd3-11e7-9736-6cc21735f730)

FreeBSD : PostgreSQL vulnerabilities (c602c791-0cf4-11e8-a2ec-6cc21735f730)

FreeBSD : PostgreSQL vulnerabilities (e3eeda2e-1d67-11e8-a2ec-6cc21735f730)

FreeBSD : postgresql-contrib -- insecure temporary file creation (6a164d84-2f7f-11d9-a9e7-0001020eed82)

FreeBSD : postgresql81-server -- SET ROLE privilege escalation (0b2b4b4d-a07c-11da-be0a-000c6ec775d9)

FreeBSD : PostgresSQL -- ALTER ... DEPENDS ON EXTENSION is missing authorization checks (d331f691-71f4-11ea-8bb5-6cc21735f730)

FreeBSD : PostgresSQL -- TYPE in pg\_temp execute arbitrary SQL during `SECURITY DEFINER` execution (9de4c1c1-b9ee-11e9-82aa-6cc21735f730)

FreeBSD : postnuke -- admin section SQL injection (35f2679f-52d7-11db-8f1a-000a48049292)

FreeBSD : postnuke -- multiple vulnerabilities (0274a9f1-0759-11da-bc08-0001020eed82)

FreeBSD : postnuke -- SQL injection vulnerabilities (f3eec2b5-8cd8-11d9-8066-000a95bc6fae)

FreeBSD : postnuke -- XSS (XSS) vulnerabilities (7e580822-8cd8-11d9-8c81-000a95bc6fae)

FreeBSD : potrace -- multiple memory failure (f4eb9a25-fde0-11e6-9ad0-b8aeed92ecc4)

FreeBSD : pound remotely exploitable vulnerability (fb521119-9bc4-11d8-9366-0020ed76ef5a)

FreeBSD : poweradmin -- multiple XSS vulnerabilities (f7809d9e-6af0-11e2-8e32-080027d768d3)

FreeBSD : powerdns -- denial of service (55c43f5b-5190-11e5-9ad8-14dae9d210b8)

FreeBSD : powerdns -- Denial of Service (56665ccb-8723-11e5-9b13-14dae9d210b8)

FreeBSD : PowerDNS -- Denial of Service Vulnerability (3338f87c-3d5f-11e1-a00a-000c6eb41cf7)

FreeBSD : powerdns -- DoS vulnerability (5a5422fd-7e1a-11d9-a9e7-0001020eed82)

FreeBSD : PowerDNS -- Insufficient validation in the HTTP remote backend (6001cfc6-9f0f-4fae-9b4f-9b8fae001425)

FreeBSD : powerdns -- Label decompression bug can cause crashes or CPU spikes (64e6006e-f009-11e4-98c6-000c292ee6b8)

FreeBSD : PowerDNS -- LDAP backend fails to escape all queries (43a7b0a7-f9bc-11d9-b473-00061bc2ad93)

FreeBSD : powerdns -- Multiple vulnerabilities (0aee2f13-ec1d-11e8-8c92-6805ca2fa271)

FreeBSD : powerdns -- multiple vulnerabilities (1c21f6a3-9415-11e9-95ec-6805ca2fa271)

FreeBSD : powerdns -- multiple vulnerabilities (e3200958-dd6c-11e6-ae1b-002590263bf5)

FreeBSD : powerdns-recursor -- Crafted query can cause a denial of service (f6d6308a-f2ec-11e8-b005-6805ca2fa271)

FreeBSD : powerdns-recursor -- DNS cache poisoning (b21790a5-02fb-11dd-bd06-0017319806e7)

FreeBSD : powerdns-recursor -- insufficient validation of DNSSEC signatures (24a82876-002e-11e8-9a95-0cc47a02c232)

FreeBSD : powerdns-recursor -- multiple vulnerabilities (40d92cc5-1e2b-11e9-bef6-6805ca2fa271)

FreeBSD : powerdns-recursor -- multiple vulnerabilities (dd8f2394-fd08-11de-b425-00215c6a37bb)

FreeBSD : powerdns-recursor -- Multiple vulnerabilities (e9aa0e4c-ea8b-11e8-a5b7-00e04c1ea73d)

FreeBSD : ppxp -- local root exploit (641e8609-cab5-11d9-9aed-000e0c2e438a)

FreeBSD : privoxy -- malicious server spoofing as proxy vulnerability (ad82b0e9-c3d6-11e5-b5fe-002590263bf5)

FreeBSD : privoxy -- multiple vulnerabilities (89d4ed09-c3d7-11e5-b5fe-002590263bf5)

FreeBSD : privoxy -- multiple vulnerabilities (a763a0e7-c3d9-11e5-b5fe-002590263bf5)

FreeBSD : privoxy -- multiple vulnerabilities (d9e1b569-c3d8-11e5-b5fe-002590263bf5)

FreeBSD : procmail -- Heap-based buffer overflow (288f7cee-ced6-11e7-8ae9-0050569f0b83)

FreeBSD : proftpd -- arbitrary code execution vulnerability with chroot (022a4c77-2da4-11e1-b356-00215c6a37bb)

FreeBSD : proftpd -- arbitrary code execution vulnerability with chroot (d0034536-ff24-11e4-a072-d050996490d0)

FreeBSD : proftpd -- Compromised source packages backdoor (ed7fa1b4-ff59-11df-9759-080027284eaa)

FreeBSD : proftpd -- format string vulnerabilities (c28f4705-043f-11da-bc08-0001020eed82)

FreeBSD : proftpd -- Long Command Processing Vulnerability (0f51f2c9-8956-11dd-a6fe-0030843d3802)

FreeBSD : proftpd -- multiple sql injection vulnerabilities (ca0841ff-1254-11de-a964-0030843d3802)

FreeBSD : proftpd -- remote code execution vulnerabilities (3f851b22-89fb-11db-a937-003048116330)

FreeBSD : proftpd -- remote code execution vulnerability (533d20e7-f71f-11df-9ae1-000bcdf0a03b)

FreeBSD : proftpd -- Remote Code Execution Vulnerability (cca97f5f-7435-11db-91de-0008743bf21a)

FreeBSD : proftpd -- user chroot escape vulnerability (770d7e91-72af-11e7-998a-08606e47f965)

FreeBSD : proftpd -- vulnerability in mod\_tls (a733b5ca-06eb-11e6-817f-3085a9a4510d)

FreeBSD : ProFTPD ASCII translation bug resulting in remote root compromise (cf0fb426-3f96-11d8-b096-0020ed76ef5a)

FreeBSD : proftpd IP address access control list breakage (cb6c6c29-9c4f-11d8-9366-0020ed76ef5a)

FreeBSD : prosody -- multiple vulnerabilities (842cd117-ba54-11e5-9728-002590263bf5)

FreeBSD : prosody -- user impersonation vulnerability (50394bc9-c5fa-11e5-96a5-d93b343d1ff7)

FreeBSD : proxychains-ng -- current path as the first directory for the library search path (9471ec47-05a2-11e5-8fda-002590263bf5)

FreeBSD : proxytunnel -- format string vulnerability (50744596-368f-11d9-a9e7-0001020eed82)

FreeBSD : ProZilla -- server response buffer overflow vulnerabilities (1a32e8ee-3edb-11d9-8699-00065be4b5b6)

FreeBSD : pspp -- multiple vulnerabilities (6876b163-8708-11e7-8568-e8e0b747a45a)

FreeBSD : Pubcookie Login Server -- XSS vulnerability (115a1389-858e-11e0-a76c-000743057ca2)

FreeBSD : pubcookie-login-server -- XSS vulnerability (855cd9fa-c452-11da-8bff-000ae42e9b93)

FreeBSD : punbb -- NULL byte injection vulnerability (e79876e4-5061-11db-a5ae-00508d6a62df)

FreeBSD : puppet -- multiple vulnerabilities (101f0aae-52d1-11e2-87fe-f4ce46b9ace8)

FreeBSD : puppet -- multiple vulnerabilities (2b2f6092-0694-11e3-9e8e-000c29f6ae42)

FreeBSD : puppet -- multiple vulnerabilities (3a6960ef-c8a8-11e1-9924-001fd0af1a4c)

FreeBSD : puppet -- Multiple Vulnerabilities (607d2108-a0e4-423a-bf78-846f2a8f01b0)

FreeBSD : puppet -- Unauthenticated Remote Code Execution Vulnerability (b162b218-c547-4ba2-ae31-6fdcb61bc763)

FreeBSD : puppet-agent MCollective plugin -- Remote Code Execution vulnerability (df502a2f-61f6-11e6-a461-643150d3111d)

FreeBSD : puppet26 -- multiple vulnerabilities (04042f95-14b8-4382-a8b9-b30e365776cf)

FreeBSD : puppet27 and puppet -- multiple vulnerabilities (cda566a0-2df0-4eb0-b70e-ed7a6fb0ab3c)

FreeBSD : puppet6 -- Arbitrary Catalog Retrieval (77687355-52aa-11ea-b115-643150d3111d)

FreeBSD : puppetserver and puppetdb -- Puppet Server and PuppetDB may leak sensitive information via metrics API (36def7ba-6d2b-11ea-b115-643150d3111d)

FreeBSD : pure-ftpd (2410)

FreeBSD : pureftpd -- multiple vulnerabilities (1495f931-8522-11e0-a1c1-00215c6a37bb)

FreeBSD : putty (1624)

FreeBSD : PuTTY - old-style scp downloads may allow remote code execution (7f0fbb30-e462-11e5-a3f3-080027ef73ec)

FreeBSD : putty -- buffer overflow vulnerability in ssh2 support (19518d22-2d05-11d9-8943-0050fc56d258)

FreeBSD : PuTTY -- fails to scrub private keys from memory after use (92fc2e2b-c383-11e4-8ef7-080027ef73ec)

FreeBSD : PuTTY -- Four security holes in versions before 0.63 (4b448a96-ff73-11e2-b28d-080027ef73ec)

FreeBSD : PuTTY -- integer overflow permits memory overwrite by forwarded ssh-agent connections (9b973e97-0a99-11e7-ace7-080027ef73ec)

FreeBSD : PuTTY -- memory corruption in terminal emulator's erase character handling (0cb0afd9-86b8-11e5-bf60-080027ef73ec)

FreeBSD : PuTTY -- Password vulnerability (bbd5f486-24f1-11e1-95bc-080027ef73ec)

FreeBSD : putty -- pscp/psftp heap corruption vulnerabilities (a413ed94-836e-11d9-a9e7-0001020eed82)

FreeBSD : PuTTY -- security fixes in new release (46e1ece5-48bd-11e9-9c40-080027ac955c)

FreeBSD : PuTTY 0.72 -- buffer overflow in SSH-1 and integer overflow in SSH client (5914705c-ab03-11e9-a4f9-080027ac955c)

FreeBSD : py-amf -- input sanitization errors (1fbd6db1-a4e4-11e5-b864-14dae9d210b8)

FreeBSD : py-asyncssh -- Allows bypass of authentication (0e8f496a-b498-11e8-bdcf-74d435e60b7c)

FreeBSD : py-bleach -- unsanitized character entities (e97a8852-32dd-4291-ba4d-92711daff056)

FreeBSD : py-cryptography -- tag forgery vulnerability (9e2d0dcf-9926-11e8-a92d-0050562a4d7b)

FreeBSD : py-cryptography -- vulnerable HKDF key generation (e5dcb942-ba6f-11e6-b1cf-14dae9d210b8)

FreeBSD : py-django -- denial of service vulnerability (d2c2952d-85a1-11dc-bfff-003048705d5a)

FreeBSD : py-djblets -- Self-XSS vulnerability (df328fac-f942-11e5-92ce-002590263bf5)

FreeBSD : py-foolscap -- local file inclusion (09fff0d9-4126-11e5-9f01-14dae9d210b8)

FreeBSD : py-graphite-web -- Multiple vulnerabilities (e1f99d59-81aa-4662-bf62-c1076f5016c8)

FreeBSD : py-gunicorn -- CWE-113 vulnerability (a3e24de7-3f0c-11e9-87d1-00012e582166)

FreeBSD : py-imaging, py-pillow -- Buffer overflow in FLI decoding code (6ea60e00-cf13-11e5-805c-5453ed2e2b49)

FreeBSD : py-imaging, py-pillow -- Buffer overflow in PCD decoder (a8de962a-cf15-11e5-805c-5453ed2e2b49)

FreeBSD : py-matrix-synapse -- incomplete cleanup of 3rd-party-IDs on user deactivation (9c36d41c-11df-11ea-9b6d-901b0e934d69)

FreeBSD : py-matrix-synapse -- missing signature checks on some federation APIs (42675046-fa70-11e9-ba4e-901b0e934d69)

FreeBSD : py-matrix-synapse -- multiple vulnerabilities (38d2df4d-b143-11e9-87e7-901b0e934d69)

FreeBSD : py-matrix-synapse -- multiple vulnerabilities (ed8cbad5-21a8-11ea-9b6d-901b0e934d69)

FreeBSD : py-matrix-synapse -- undisclosed vulnerability (383931ba-1818-11e9-92ea-448a5b29e8a9)

FreeBSD : py-matrix-synapse -- users of single-sign-on are vulnerable to phishing (1afe9552-5ee3-11ea-9b6d-901b0e934d69)

FreeBSD : py-pillow -- Buffer overflow in TIFF decoding code (53252879-cf11-11e5-805c-5453ed2e2b49)

FreeBSD : py-pillow -- Integer overflow in Resample.c (0519db18-cf15-11e5-805c-5453ed2e2b49)

FreeBSD : py-pylons -- Path traversal bug (f5c58fc1-49c0-11dd-b0ba-00163e000016)

FreeBSD : py-rsa -- Bleichenbacher'06 signature forgery vulnerability (e78bfc9d-cb1e-11e5-b251-0050562a4d7b)

FreeBSD : py-salt -- potential shell injection vulnerabilities (865863af-fb5e-11e4-8fda-002590263bf5)

FreeBSD : py-yaml -- arbitrary code execution (f6ea18bb-65b9-11e9-8b31-002590045d9c)

FreeBSD : pyblosxom -- atom flavor multiple XML injection vulnerabilities (b07f3254-f83a-11dd-85a4-ea653f0746ab)

FreeBSD : pycrypto -- ARC2 module buffer overflow (5a021595-fba9-11dd-86f3-0030843d3802)

FreeBSD : pycrypto -- PRNG reseed race condition (c0f122e2-3897-11e3-a084-3c970e169bc2)

FreeBSD : pycrypto -- vulnerable ElGamal key generation (f45c0049-be72-11e1-a284-0023ae8e59f0)

FreeBSD : pygments -- shell injection vulnerability (5f276780-b6ce-11e5-9731-5453ed2e2b49)

FreeBSD : Python -- buffer overflow in socket.recvfrom\_into() (8e5e6d42-a0fa-11e3-b09a-080027f2d077)

FreeBSD : python -- buffer overrun in repr() for unicode strings (fe83eb5b-55e1-11db-a5ae-00508d6a62df)

FreeBSD : Python -- DoS via malformed XML-RPC / HTTP POST request (b4f8be9e-56b2-11e1-9fb7-003067b2972c)

FreeBSD : Python -- HTTP Header Injection in Python urllib (a61374fc-3a4d-11e6-a671-60a44ce6887b)

FreeBSD : Python -- Integer overflow in zipimport module (1d0f6852-33d8-11e6-a671-60a44ce6887b)

FreeBSD : python -- Integer Signedness Error in zlib Module (ec41c3e2-129c-11dd-bab7-0016179b2dd5)

FreeBSD : python -- multiple vulnerabilities (0dccaa28-7f3c-11dd-8de5-0030843d3802)

FreeBSD : Python -- NULL pointer dereference vulnerability (d74371d2-4fee-11e9-a5cd-1df8a848de3d)

FreeBSD : python -- possible integer overflow vulnerability (0fe70bcd-2ce3-46c9-a64b-4a7da097db07)

FreeBSD : python -- SimpleXMLRPCServer.py allows unrestricted traversal (6afa87d3-764b-11d9-b0e7-0000e249a0a2)

FreeBSD : Python -- smtplib StartTLS stripping vulnerability (8d5368ef-40fe-11e6-b2ec-b499baebfeaf)

FreeBSD : python 2.7 -- multiple vulnerabilities (8719b935-8bae-41ad-92ba-3c826f651219)

FreeBSD : Python 2.7 -- multiple vulnerabilities (9164f51e-ae20-11e7-a633-009c02a2ab30)

FreeBSD : python 3.6 -- multiple vulnerabilities (18ed9650-a1d6-11e9-9b17-fcaa147e860e)

FreeBSD : python 3.7 -- multiple vulnerabilities (9b7491fb-f253-11e9-a50c-000c29c4dc65)

FreeBSD : python 3.7 -- multiple vulnerabilities (a449c604-a43a-11e9-b422-fcaa147e860e)

FreeBSD : qemu -- 'drive\_init()' Disk Format Security Bypass (8950ac62-1d30-11dd-9388-0211060005df)

FreeBSD : qemu -- buffer overflow vulnerability in virtio-serial message exchanges (21e5abe3-b0c6-11e5-8d13-bc5ff45d0f28)

FreeBSD : qemu -- buffer overflow vulnerability in VNC (2b3b4c27-b0c7-11e5-8d13-bc5ff45d0f28)

FreeBSD : qemu -- code execution on host machine (aea8d90e-b0c1-11e5-8d13-bc5ff45d0f28)

FreeBSD : qemu -- denial of service vulnerabilities in eepro100 NIC support (b56fe6bb-b1b1-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerabilities in NE2000 NIC support (6aa3322f-b150-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability (a228c7a0-ba66-11e6-b1cf-14dae9d210b8)

FreeBSD : qemu -- denial of service vulnerability in e1000 NIC support (10bf8eed-b14d-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in Human Monitor Interface support (62ab8707-b1bc-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in IDE disk/CD/DVD-ROM emulation (bbc97005-b14e-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in MegaRAID SAS HBA emulation (b3f9f8ef-b1bb-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in MSI-X support (3fb06284-b1b7-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in Q35 chipset emulation (152acff3-b1bd-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in Rocker switch emulation (1384f2fd-b1be-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in USB EHCI emulation support (60cb2055-b1b8-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in virtio-net support (42cbd1e8-b152-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in VMWARE VMXNET3 NIC support (9ad8993e-b1ba-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in VNC (67feba97-b1b5-11e5-9728-002590263bf5)

FreeBSD : qemu -- denial of service vulnerability in VNC (8a560bcf-b14b-11e5-9728-002590263bf5)

FreeBSD : qemu -- Heap overflow in Cirrus emulation (07bb3bd2-a920-11dd-8503-0211060005df)

FreeBSD : qemu -- Heap overflow in QEMU PCNET controller, allowing guest to host escape (CVE-2015-3209) (acd5d037-1c33-11e5-be9c-6805ca1d3bb1)

FreeBSD : qemu -- several vulnerabilities (0ac89b39-f829-11db-b55c-000e0c6d38a9)

FreeBSD : qemu -- stack buffer overflow while parsing SCSI commands (a267cd6c-b0c4-11e5-8d13-bc5ff45d0f28)

FreeBSD : qemu -- Translation Block Local Denial of Service Vulnerability (30f5ca1d-a90b-11dc-bf13-0211060005df)

FreeBSD : qemu -- unchecked block read/write vulnerability (9cfbca7f-efb7-11dc-be01-0211060005df)

FreeBSD : qemu and xen-tools -- denial of service vulnerabilities in AMD PC-Net II NIC support (405446f4-b1b3-11e5-9728-002590263bf5)

FreeBSD : qemu, xen and VirtualBox OSE -- possible VM escape and code execution ('VENOM') (2780e442-fc59-11e4-b18b-6805ca1d3bb1) (Venom)

FreeBSD : qemu, xen-tools -- QEMU heap overflow flaw with certain ATAPI commands (da451130-365d-11e5-a4a5-002590263bf5)

FreeBSD : qemu, xen-tools -- QEMU leak of uninitialized heap memory in rtl8139 device model (f06f20dc-4347-11e5-93ad-002590263bf5)

FreeBSD : qemu, xen-tools -- use-after-free in QEMU/Xen block unplug protocol (ee99899d-4347-11e5-93ad-002590263bf5)

FreeBSD : qpopper -- multiple privilege escalation vulnerabilities (eb29a575-3381-11da-8340-000e0c2e438a)

FreeBSD : qpopper format string vulnerability (ebdf65c7-2ca6-11d8-9355-0020ed76ef5a)

FreeBSD : qt (2419)

FreeBSD : qt -- image loader vulnerabilities (ebffe27a-f48c-11d8-9837-000c41e2cdad)

FreeBSD : qt4-gui, qt5-gui -- DoS vulnerability in the BMP image handler (c9c3374d-c2c1-11e4-b236-5453ed2e2b49)

FreeBSD : qt4-imageformats, qt4-gui, qt5-gui -- Multiple Vulnerabilities in Qt Image Format Handling (5713bfda-e27d-11e4-b2ce-5453ed2e2b49)

FreeBSD : qt4-imageformats, qt5-gui -- DoS vulnerability in the GIF image handler (904d78b8-0f7e-11e4-8b71-5453ed2e2b49)

FreeBSD : qt4-xml -- XML Entity Expansion Denial of Service (89709e58-d497-11e3-a3d5-5453ed2e2b49)

FreeBSD : quagga -- BGP OPEN denial of service vulnerability (1e14d46f-af1f-11e1-b242-00215af774f0)

FreeBSD : quagga -- Denial of Service (2748fdde-3a3c-11de-bbc5-00e0815b8da8)

FreeBSD : quagga -- multiple vulnerabilities (42a2c82a-75b9-11e1-89b4-001ec9578670)

FreeBSD : quagga -- multiple vulnerabilities (ab9be2c8-ef91-11e0-ad5a-00215c6a37bb)

FreeBSD : quagga -- several security issues (e15a22ce-f16f-446b-9ca7-6859350c2e75)

FreeBSD : quagga -- stack based buffer overflow vulnerability (70c44cd0-e717-11e5-85be-14dae9d210b8)

FreeBSD : quagga -- stack overflow and DoS vulnerabilities (167953a4-b01c-11df-9a98-0015587e2cc1)

FreeBSD : quagga -- two DoS vulnerabilities (b2a40507-5c88-11e0-9e85-00215af774f0)

FreeBSD : quake2 -- multiple critical vulnerabilities (2c25e762-6bb9-11d9-93db-000a95bc6fae)

FreeBSD : quassel -- multiple vulnerabilities (499f6b41-58db-4f98-b8e7-da8c18985eda)

FreeBSD : quassel -- remote denial of service (7d64d00c-43e3-11e6-ab34-002590263bf5)

FreeBSD : quassel -- remote denial of service (9e7306b9-a5c3-11e5-b864-14dae9d210b8)

FreeBSD : Quassel IRC -- SQL injection vulnerability (49d9c28c-fbad-11e4-b0fb-00269ee29e57)

FreeBSD : Quassel IRC -- SQL injection vulnerability (f969bad7-46fc-11e3-b6ee-00269ee29e57)

FreeBSD : qutebrowser -- Remote code execution due to CSRF (bd6cf187-8710-11e8-833d-18a6f7016652)

FreeBSD : RabbitMQ -- Authentication vulnerability (6aa956fb-d97f-11e6-a071-001e67f15f5a)

FreeBSD : rabbitmq -- Security issues in management plugin (8469d41c-a960-11e4-b18e-bcaec55be5e5)

FreeBSD : rack -- information leak / session hijack vulnerability (66e4dc99-28b3-11ea-8dde-08002728f74c)

FreeBSD : racoon (2128)

FreeBSD : racoon -- improper certificate handling (2328adef-157c-11d9-8402-000d93664d5c)

FreeBSD : racoon -- remote denial-of-service (3b260179-e464-460d-bf9f-d5cda6204020)

FreeBSD : racoon fails to verify signature during Phase 1 (d8769838-8814-11d8-90d1-0020ed76ef5a)

FreeBSD : racoon remote denial of service vulnerability (IKE Generic Payload Header) (40fcf20f-8891-11d8-90d1-0020ed76ef5a)

FreeBSD : racoon remote denial of service vulnerability (ISAKMP header length field) (ccd698df-8e20-11d8-90d1-0020ed76ef5a)

FreeBSD : racoon security association deletion vulnerability (739bb51d-7e82-11d8-9645-0020ed76ef5a)

FreeBSD : radicale -- multiple vulnerabilities (ff824eea-c69c-11e5-96d6-14dae9d210b8)

FreeBSD : Rails -- Action View vulnerabilities (1396a74a-4997-11e9-b5f1-83edb3f89ba1)

FreeBSD : Rails -- Active Job vulnerability (f96044a2-7df9-414b-9f6b-6e5b85d06c86)

FreeBSD : rails -- multiple vulnerabilities (5a016dd0-8aa8-490e-a596-55f4cc17e4ef)

FreeBSD : rails -- multiple vulnerabilities (6a806960-3016-44ed-8575-8614a7cb57c7)

FreeBSD : rails -- multiple vulnerabilities (bb0ef21d-0e1b-461b-bc3d-9cba39948888)

FreeBSD : Rails 4 -- Possible XSS Vulnerability in Action View (43f1c867-654a-11e6-8286-00248c0c745d)

FreeBSD : Rails 4 -- Unsafe Query Generation Risk in Active Record (7e61cf44-6549-11e6-8286-00248c0c745d)

FreeBSD : rails-html-sanitizer -- possible XSS vulnerability (81946ace-6961-4488-a164-22d58ebc8d66)

FreeBSD : raptor/raptor2 -- XXE in RDF/XML File Interpretation (60f81af3-7690-11e1-9423-00235a5f2c9a)

FreeBSD : rar -- password prompt buffer overflow vulnerability (94234e00-be8a-11db-b2ec-000c6ec775d9)

FreeBSD : razor-agents -- denial of service vulnerability (85069fb6-e15b-11d9-83cf-0010dc5df42d)

FreeBSD : rdesktop - critical - Remote Code Execution (3e2c9b63-223c-4575-af5c-816acb14e445)

FreeBSD : RDoc -- multiple jQuery vulnerabilities (ed8d5535-ca78-11e9-980b-999ff59c22ea)

FreeBSD : realplayer -- arbitrary file deletion and other vulnerabilities (02274fd9-6bc5-11d9-8edb-000a95bc6fae)

FreeBSD : realplayer -- remote heap overflow (c73305ae-8cd7-11d9-9873-000a95bc6fae)

FreeBSD : redis -- EVAL Lua Sandbox Escape (838fa84a-0e25-11e5-90e4-d050996490d0)

FreeBSD : redis -- sensitive information leak through command history file (fa175f30-8c75-11e6-924a-60a44ce6887b)

FreeBSD : redmine -- CSRF protection bypass (ae377aeb-9ed4-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- information leak vulnerability (21bc4d71-9ed8-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- information leak vulnerability (49def4b7-9ed6-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- multiple vulnerabilities (0e0385d1-9ed5-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- multiple vulnerabilities (584c506d-0e98-11e0-b59b-0050569b2d21)

FreeBSD : redmine -- multiple vulnerabilities (ba61ce15-8a7b-11df-87ec-0050569b2d21)

FreeBSD : redmine -- multiple vulnerabilities (be63533c-9ed7-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- multiple vulnerabilities (fcc39d22-5777-11df-bf33-001a92771ec2)

FreeBSD : redmine -- open redirect vulnerability (3ec2e0bc-9ed7-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- open redirect vulnerability (c2efcd46-9ed5-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- potential XSS vulnerability (939a7086-9ed6-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- XSS vulnerability (66ba5931-9ed5-11e5-8f5c-002590263bf5)

FreeBSD : redmine -- XSS vulnerability (cf96cd8d-48fb-11e0-98a6-0050569b2d21)

FreeBSD : remind -- buffer overflow with malicious reminder file input (b55ecf12-5d98-11e5-9909-002590263bf5)

FreeBSD : Remote code injection in phpMyAdmin (0d4c31ac-cb91-11d8-8898-000d6111a684)

FreeBSD : Remote Denial of Service of HTTP server and client (1f738bda-c6ac-11d8-8898-000d6111a684)

FreeBSD : Remote-Code-Execution vulnerability in mysql and its variants CVE 2016-6662 (b64a7389-7c27-11e6-8aaa-5404a68ad561)

FreeBSD : Remote-Code-Execution vulnerability in mysql and its variants CVE 2016-6662 (dc596a17-7a9e-11e6-b034-f0def167eeea)

FreeBSD : rest-client -- plaintext password disclosure (ffe2d86c-07d9-11e5-9a28-001e67150279)

FreeBSD : rest-client -- session fixation vulnerability (83a7a720-07d8-11e5-9a28-001e67150279)

FreeBSD : ricochet -- information disclosure (d71831ef-e6f8-11e5-85be-14dae9d210b8)

FreeBSD : ripMIME -- decoding bug allowing content filter bypass (85e19dff-e606-11d8-9b0a-000347a4fa7d)

FreeBSD : rkhunter -- insecure temporary file creation (f14ad681-5b88-11dc-812d-0011098b2f36)

FreeBSD : rlpr (1489)

FreeBSD : rockdodger -- buffer overflows (2b4d5288-447e-11d9-9ebb-000854d03344)

FreeBSD : Roundcube -- arbitrary command execution (125f5958-b611-11e6-a9a5-b499baebfeaf)

FreeBSD : roundcube -- arbitrary file disclosure vulnerability (a592e991-a919-11e2-ade0-8c705af55518)

FreeBSD : roundcube -- arbitrary password resets (bce47c89-4d3f-11e7-8080-a4badb2f4699)

FreeBSD : roundcube -- file disclosure vulnerability (f622608c-c53c-11e7-a633-009c02a2ab30)

FreeBSD : roundcube -- IMAP command injection vulnerability (48894ca9-3e6f-11e8-92f0-f0def167eeea)

FreeBSD : roundcube -- multiple vulnerabilities (038a5808-24b3-11e5-b0c8-bf4d8935d4fa)

FreeBSD : roundcube -- remote execution of arbitrary code (8f483746-d45d-11dd-84ec-001fc66e7203)

FreeBSD : roundcube -- webmail script insertion and php code injection (35c0b572-125a-11de-a964-0030843d3802)

FreeBSD : roundcube -- XSS in HTML email messages (c906e0a4-efa6-11e1-8fbf-001b77d09812)

FreeBSD : roundcube -- XSS vulnerability (4ae68e7c-dda4-11e0-a906-00215c6a37bb)

FreeBSD : roundcube -- XSS vulnerability (97e86d10-2ea7-11e6-ae88-002590263bf5)

FreeBSD : roundup (1608)

FreeBSD : rpm4 -- regression in -setperms, -setugids and -restore (f8fe2905-0918-11e9-a550-00262d164c21)

FreeBSD : rsnapshot -- local privilege escalation (8c5ad0cf-ba37-11d9-837d-000e0c2e438a)

FreeBSD : rssh & scponly -- arbitrary command execution (f11b219a-44b6-11d9-ae2f-021106004fd6)

FreeBSD : rssh - multiple vulnerabilities (d193aa9f-3f8c-11e9-9a24-6805ca0b38e8)

FreeBSD : rssh -- arbitrary command execution (65b25acc-e63b-11e1-b81c-001b77d09812)

FreeBSD : rssh -- configuration restrictions bypass (a4598875-ec91-11e1-8bd8-0022156e8794)

FreeBSD : rssh -- file name disclosure bug (a4815970-c5cc-11d8-8898-000d6111a684)

FreeBSD : rssh -- format string vulnerability (1f826757-26be-11d9-ad2d-0050fc56d258)

FreeBSD : rssh -- privilege escalation vulnerability (e34d0c2e-9efb-11da-b410-000e0c2e438a)

FreeBSD : rsync -- incremental recursion memory corruption vulnerability (9a777c23-b310-11e0-832d-00215c6a37bb)

FreeBSD : rsync -- multiple vulnerabilities (72fff788-e561-11e7-8097-0800271d4b9c)

FreeBSD : rsync -- off by one stack overflow (af8e3a0c-5009-11dc-8a43-003048705d5a)

FreeBSD : rsync -- path sanitizing vulnerability (2689f4cb-ec4c-11d8-9440-000347a4fa7d)

FreeBSD : rsync buffer overflow in server mode (5729b8ed-5d75-11d8-80e3-0020ed76ef5a)

FreeBSD : rsync path traversal issue (73ea0706-9c57-11d8-9366-0020ed76ef5a)

FreeBSD : rsyslog -- remote syslog PRI vulnerability (8e0e86ff-48b5-11e4-ab80-000c29f6ae42)

FreeBSD : RT -- multiple vulnerabilities (3a429192-c36a-11e2-97a9-6805ca0b3d42)

FreeBSD : RT -- Multiple Vulnerabilities (4b738d54-2427-11e2-9817-c8600054b392)

FreeBSD : rt -- multiple vulnerabilities (bf171509-68dd-11e0-afe6-0003ba02bf30)

FreeBSD : RT -- Multiple Vulnerabilities (e0a969e4-a512-11e1-90b4-e0cb4e266481)

FreeBSD : rt -- Remote DoS, Information disclosure and Session Hijackingvulnerabilities (d08f6002-c588-11e4-8495-6805ca0b3d42)

FreeBSD : rt -- Session fixation vulnerability (714c1406-e4cf-11de-883a-003048590f9e)

FreeBSD : RT -- two XSS vulnerabilities (83b38a2c-413e-11e5-bfcf-6805ca0b3d42)

FreeBSD : rt -- XSS via jQuery (416ca0f4-3fe0-11e9-bbdd-6805ca0b3d42)

FreeBSD : rt and dependent modules -- multiple security vulnerabilities (7a92e958-5207-11e7-8d7c-6805ca0b3d42)

FreeBSD : rt42 -- denial-of-service attack via the email gateway (d1dfc4c7-8791-11e3-a371-6805ca0b3d42)

FreeBSD : rt42 -- vulnerabilities related to shellshock (81e2b308-4a6c-11e4-b711-6805ca0b3d42)

FreeBSD : ruby (2119)

FreeBSD : ruby -- $SAFE escaping vulnerability about Exception#to\_s/NameError#to\_s (2a093853-2495-11e2-b0c7-000d601460a4)

FreeBSD : ruby -- arbitrary command execution on XMLRPC server (594eb447-e398-11d9-a8bd-000cf18bbe54)

FreeBSD : ruby -- BigDecimal denial of service vulnerability (62e0fbe5-5798-11de-bb78-001cc0377035)

FreeBSD : ruby -- CGI DoS (d656296b-33ff-11d9-a9e7-0001020eed82)

FreeBSD : ruby -- cgi.rb library Denial of Service (a8674c14-83d7-11db-88d5-0012f06707f0)

FreeBSD : ruby -- cgi.rb library Denial of Service (ab8dbe98-6be4-11db-ae91-0012f06707f0)

FreeBSD : ruby -- Command injection vulnerability in Net::FTP (dd644964-e10e-11e7-8097-0800271d4b9c)

FreeBSD : Ruby -- Denial of Service and Unsafe Object Creation Vulnerability in JSON (c79eb109-a754-45d7-b552-a42099eb2265)

FreeBSD : ruby -- DNS spoofing vulnerability (959d384d-6b59-11dd-9d79-001fc61c2a55)

FreeBSD : ruby -- DoS vulnerability in REXML (844cf3f5-9259-4b3e-ac9e-13ca17333ed7)

FreeBSD : ruby -- DoS vulnerability in WEBrick (f7ba20aa-6b5a-11dd-9d79-001fc61c2a55)

FreeBSD : ruby -- Hash-flooding DoS vulnerability for ruby 1.9 (5e647ca3-2aea-11e2-b745-001fd0af1a4c)

FreeBSD : ruby -- Heap Overflow in Floating Point Parsing (cc9043cf-7f7a-426e-b2cc-8d1980618113)

FreeBSD : ruby -- heap overflow vulnerability (eab8c3bd-e50c-11de-9cd0-001a926c7637)

FreeBSD : ruby -- Hostname check bypassing vulnerability in SSL client (ebd877b9-7ef4-4375-b1fd-c67780581898)

FreeBSD : ruby -- multiple integer and buffer overflow vulnerabilities (53802164-3f7e-11dd-90ea-0019666436c2)

FreeBSD : ruby -- multiple vulnerabilities (76562594-1f19-11db-b7d4-0008743bf21a)

FreeBSD : ruby -- multiple vulnerabilities (95b01379-9d52-11e7-a25c-471bafc3262f)

FreeBSD : ruby -- multiple vulnerabilities (afc60484-0652-440e-b01a-5ef814747f06)

FreeBSD : ruby -- multiple vulnerabilities (eb69bcf2-18ef-4aa2-bb0c-83b263364089)

FreeBSD : ruby -- multiple vulnerabilities (f7fcb75c-e537-11e9-863e-b9b7af01ba9e)

FreeBSD : ruby -- multiple vulnerabilities in safe level (c329712a-6b5b-11dd-9d79-001fc61c2a55)

FreeBSD : ruby -- Object taint bypassing in DL and Fiddle in Ruby (79789daa-8af8-4e21-a47f-e8a645752bdb)

FreeBSD : Ruby -- OpenSSL Hostname Verification Vulnerability (d4379f59-3e9b-49eb-933b-61de4d0b0fdb)

FreeBSD : ruby -- Unintentional file creation caused by inserting an illegal NUL character (3decc87d-2498-11e2-b0c7-000d601460a4)

FreeBSD : Ruby -- unsafe tainted string vulnerability (3b50881d-1860-4721-aab1-503290e23f6c)

FreeBSD : ruby -- UTF-7 encoding XSS vulnerability in WEBrick (34e0316a-aa91-11df-8c2e-001517289bf8)

FreeBSD : ruby -- vulnerability in the safe level settings (1daea60a-4719-11da-b5c6-0004614cc33d)

FreeBSD : Ruby -- XSS exploit of RDoc documentation generated by rdoc (d3e96508-056b-4259-88ad-50dc8d1978a6)

FreeBSD : Ruby Activemodel Gem -- Circumvention of attr\_protected (beab40bf-c1ca-4d2b-ad46-2f14bac8a968)

FreeBSD : Ruby insecure file permissions in the CGI session management (e811aaf1-f015-11d8-876f-00902714cc7c)

FreeBSD : Ruby Rack Gem -- Multiple Issues (fcfdabb7-f14d-4e61-a7d5-cfefb4b99b15)

FreeBSD : ruby-gems -- Algorithmic Complexity Vulnerability (54237182-9635-4a8b-92d7-33bfaeed84cd)

FreeBSD : ruby-gems -- Algorithmic Complexity Vulnerability (742eb9e4-e3cb-4f5a-b94e-0e9a39420600)

FreeBSD : ruby-saml -- XML signature wrapping attack (3fcd52b2-4510-11e6-a15f-00248c0c745d)

FreeBSD : rubygem-actionpack -- Denial of Service (ae2fa87c-4bca-4138-8be1-67ce2a19b3a8)

FreeBSD : rubygem-activerecord -- multiple vulnerabilities (748aa89f-d529-11e1-82ab-001fd0af1a4c)

FreeBSD : rubygem-bson -- DoS and possible injection (f5225b23-192d-11e5-a1cf-002590263bf5)

FreeBSD : rubygem-doorkeeper -- token revocation vulnerability (e309a2c7-598b-4fa6-a398-bc72fbd1d167)

FreeBSD : rubygem-dragonfly -- arbitrary code execution (aa7764af-0b5e-4ddc-bc65-38ad697a484f)

FreeBSD : rubygem-geminabox -- XSS & CSRF vulnerabilities (2bffdf2f-9d45-11e7-a25c-471bafc3262f)

FreeBSD : rubygem-geminabox -- XSS vulnerabilities (27b38d85-c891-11e7-a7bd-cd1209e563f2)

FreeBSD : rubygem-json -- Unsafe Objection Creation Vulnerability in JSON (Additional fix) (40194e1c-6d89-11ea-8082-80ee73419af3)

FreeBSD : rubygem-mail -- multiple vulnerabilities (3d55b961-9a2e-11e1-a2ef-001fd0af1a4c)

FreeBSD : rubygem-mail -- Remote Arbitrary Shell Command Injection Vulnerability (1cae628c-3569-11e0-8e81-0022190034c0)

FreeBSD : rubygem-paperclip -- validation bypass vulnerability (0f154810-16e4-11e5-a1cf-002590263bf5)

FreeBSD : rubygem-passenger -- arbitrary file read vulnerability (8cf25a29-e063-11e7-9b2c-001e672571bc)

FreeBSD : rubygem-rails -- evaluation of ruby code (90064567-28b1-11db-844d-000c6ec775d9)

FreeBSD : rubygem-rails -- JSON XSS vulnerability (44fb0302-9d38-11dc-9114-001c2514716c)

FreeBSD : rubygem-rails -- multiple vulnerabilities (31db9a18-e289-11e1-a57d-080027a27dbf)

FreeBSD : rubygem-rails -- multiple vulnerabilities (be77eff6-ca91-11e0-aea3-00215c6a37bb)

FreeBSD : rubygem-rails -- multiple vulnerabilities (ca5d3272-59e3-11e2-853b-00262d5ed8ee)

FreeBSD : rubygem-rails -- multiple vulnerabilities (db0c4b00-a24c-11e2-9601-000d601460a4)

FreeBSD : rubygem-rails -- multiple vulnerabilities (eb8a8978-8dd5-49ce-87f4-49667b2166dd)

FreeBSD : rubygem-rails -- session-fixation vulnerability (30acb8ae-9d46-11dc-9114-001c2514716c)

FreeBSD : rubygem-rails -- SQL injection vulnerability (8e8b8b94-7f1d-11dd-a66a-0019666436c2)

FreeBSD : rubygem-rails -- SQL injection vulnerability (b4051b52-58fa-11e2-853b-00262d5ed8ee)

FreeBSD : rubygem-redcarpet -- XSS vulnerability (c368155a-fa83-11e4-bc58-001e67150279)

FreeBSD : rubygem-ruby\_parser -- insecure tmp file usage (e1aa3bdd-839a-4a77-8617-cca439a8f9fc)

FreeBSD : rubygems -- deserialization vulnerability (2c8bd00d-ada2-11e7-82af-8dbff7d75206)

FreeBSD : RubyGems -- multiple vulnerabilities (27b12d04-4722-11e9-8b7c-b5e01141761f)

FreeBSD : rubygems -- multiple vulnerabilities (3f6de636-8cdb-11e7-9c71-f0def1fd7ea2)

FreeBSD : rubygems -- request hijacking vulnerability (a0089e18-fc9e-11e4-bc58-001e67150279)

FreeBSD : Rust -- violation of Rust's safety guarantees (37528379-76a8-11e9-a4fd-00012e582166)

FreeBSD : rxvt-unicode -- buffer overflow vulnerability (d4bd4046-93a6-11d9-8378-000bdb1444a4)

FreeBSD : rxvt-unicode -- restore permissions on tty devices (c2fdb3bc-7d72-11da-b96e-000fb586ba73)

FreeBSD : SA-04:01.mksnap\_ff

FreeBSD : SA-04:02.shmat

FreeBSD : SA-04:03.jail

FreeBSD : SA-04:04.tcp

FreeBSD : SA-04:06.ipv6 : setsockopt()

FreeBSD : SA-04:10.cvs

FreeBSD : SA-04:11.msync

FreeBSD : SA-04:12.jailroute

FreeBSD : SA-04:13.linux

FreeBSD : SA-04:15.syscons

FreeBSD : SA-04:16.fetch

FreeBSD : SA-05:02.sendfile

FreeBSD : salt -- code execution (0652005e-ca96-11e5-96d6-14dae9d210b8)

FreeBSD : Salt -- information disclosure (e6b974ab-9d35-11e5-8f5c-002590263bf5)

FreeBSD : salt -- Insecure configuration of PAM external authentication service (6d25c306-f3bb-11e5-92ce-002590263bf5)

FreeBSD : salt -- Maliciously crafted minion IDs can cause unwanted directory traversals on the Salt-master (3531141d-a708-477c-954a-2a0549e49ca9)

FreeBSD : Salt -- multiple vulnerabilities (3934cc60-f0fa-4eca-be09-c8bd7ae42871)

FreeBSD : salt -- multiple vulnerabilities (4f7c6af3-6a2c-4ead-8453-04e509688d45)

FreeBSD : salt -- multiple vulnerabilities (50127e44-7b88-4ade-8e12-5d57320823f1)

FreeBSD : salt -- salt-api vulnerability (8c98e643-6008-11ea-af63-38d547003487)

FreeBSD : sam2p -- multiple issues (43a1b8f9-3451-4f3c-b4fc-730c0f5876c1)

FreeBSD : samba (2336)

FreeBSD : samba -- 'root' credential remote code execution (baf37cd2-8351-11e1-894e-00215c6a37bb)

FreeBSD : samba -- ACLs are not checked on opening an alternate data stream on a file or directory (a4f08579-516c-11e3-9b62-000c292e4fd8)

FreeBSD : samba -- buffer overflow vulnerability (ffcbd42d-a8c5-11dc-bec2-02e0185f8d72)

FreeBSD : samba -- client side SMB2/3 required signing can be downgraded (4729c849-4897-11e6-b704-000c292e4fd8)

FreeBSD : samba -- combination of parameters and permissions can allow user to escape from the share path definition (145a3e17-cea2-11e9-81e2-005056a311d1)

FreeBSD : Samba -- Denial of service - memory corruption (bfdbc7ec-9c3f-11e0-9bec-6c626dd55a41)

FreeBSD : samba -- denial of service vulnerability (e21c7c7a-0116-11e3-9e83-3c970e169bc2)

FreeBSD : samba -- Elevation of privilege to Active Directory Domain Controller (d4f45676-9d33-11e4-8275-000c292e4fd8)

FreeBSD : samba -- Exposure of machine account credentials in winbind log files (92fd40eb-c458-11da-9c79-00123ffe8333)

FreeBSD : samba -- format string bug in afsacl.so VFS plugin (57ae52f7-b9cc-11db-bf0f-0013720b182d)

FreeBSD : samba -- incorrect permission checks vulnerability (0fa15e08-92ec-11e1-a94a-00215c6a37bb)

FreeBSD : samba -- integer overflow vulnerability (3b3676be-52e1-11d9-a9e7-0001020eed82)

FreeBSD : samba -- memory exhaustion DoS in smbd (b168ddea-105a-11db-ac96-000c6ec775d9)

FreeBSD : samba -- multiple vulnerabilities (03e48bf5-a96d-11e3-a556-3c970e169bc2)

FreeBSD : samba -- multiple vulnerabilities (1edae47e-1cdd-11ea-8c2a-08002743b791)

FreeBSD : samba -- multiple vulnerabilities (3546a833-03ea-11dc-a51d-0019b95d4f14)

FreeBSD : samba -- multiple vulnerabilities (50a1bbc9-fb80-11e9-9e70-005056a311d1)

FreeBSD : samba -- multiple vulnerabilities (54976998-f248-11e8-81e2-005056a311d1)

FreeBSD : samba -- multiple vulnerabilities (5f0dd349-40a2-11ea-8d8c-005056a311d1)

FreeBSD : samba -- multiple vulnerabilities (613e45d1-6154-11e3-9b62-000c292e4fd8)

FreeBSD : samba -- multiple vulnerabilities (6ad309d9-fb03-11e3-bebd-000c2980a9f3)

FreeBSD : samba -- multiple vulnerabilities (793a0072-7822-11e9-81e2-005056a311d1)

FreeBSD : samba -- multiple vulnerabilities (a636fc26-00d9-11e6-b704-000c292e4fd8) (Badlock)

FreeBSD : samba -- multiple vulnerabilities (a63b15f9-97ff-11dc-9e48-0016179b2dd5)

FreeBSD : samba -- multiple vulnerabilities (c4e9a427-9fc2-11e8-802a-000c29a1e3ec)

FreeBSD : samba -- multiple vulnerabilities (e4bc323f-cc73-11e6-b704-000c292e4fd8)

FreeBSD : samba -- multiple vulnerabilities (ef434839-a6a4-11e5-8275-000c292e4fd8)

FreeBSD : samba -- multiple vulnerabilities (fb26f78a-26a9-11e8-a1c2-00505689d4ae)

FreeBSD : samba -- nss\_info plugin privilege escalation vulnerability (2bc96f18-683f-11dc-82b6-02e0185f8d72)

FreeBSD : samba -- Orpheus Lyre mutual authentication validation bypass (85851e4f-67d9-11e7-bc37-00505689d4ae) (Orpheus' Lyre)

FreeBSD : samba -- potential Denial of Service bug in smbd (f235fe7a-b9ca-11db-bf0f-0013720b182d)

FreeBSD : samba -- potential leakage of arbitrary memory contents (1583640d-be20-11dd-a578-0030843d3802)

FreeBSD : samba -- potential remote DoS vulnerability (ba13dc13-340d-11d9-ac1b-000d614f7fad)

FreeBSD : samba -- Private key in key.pem world readable (479efd57-516e-11e3-9b62-000c292e4fd8)

FreeBSD : samba -- remote code execution (89ff45e3-1a57-11e4-bebd-000c2980a9f3)

FreeBSD : samba -- remote code execution vulnerability (6f4d96c0-4062-11e7-b291-b499baebfeaf) (SambaCry)

FreeBSD : samba -- remote file disclosure (de16b056-132e-11d9-bc4a-000c41e2cdad)

FreeBSD : samba -- symlink race allows access outside share definition (2826317b-10ec-11e7-944e-000c292e4fd8)

FreeBSD : samba -- Unexpected code execution in smbd (996c219c-bbb1-11e4-88ae-d050992ecde8)

FreeBSD : Samba -- XSS and request forgery vulnerabilities (56f4b3a6-c82c-11e0-a498-00215c6a37bb)

FreeBSD : Samba 3.0.x password initialization bug (3388eff9-5d6e-11d8-80e3-0020ed76ef5a)

FreeBSD : samba3 DoS attack (a711de5c-05fa-11d9-a9b2-00061bc2ad93)

FreeBSD : Sanitize -- XSS vulnerability (39a30e0a-0c34-431b-9dce-b87cab02412a)

FreeBSD : scorched3d (1561)

FreeBSD : scponly -- local privilege escalation exploits (b5a49db7-72fc-11da-9827-021106004fd6)

FreeBSD : screen -- combined UTF-8 characters vulnerability (b318dc8c-6756-11db-83c3-000c6ec775d9)

FreeBSD : screen -- stack overflow (98092444-5645-11e5-9ad8-14dae9d210b8)

FreeBSD : SDL2\_image -- multiple vulnerabilities (3394bc2b-9da4-11e9-951e-14dae9d5a9d2)

FreeBSD : sdl\_image -- buffer overflow vulnerabilities (b1bcab7d-1880-11dd-a914-0016179b2dd5)

FreeBSD : security/cfs -- buffer overflow (e55f948f-d729-11e0-abd1-0017f22d6707)

FreeBSD : security/ossec-hids-\* -- root escalation via syscheck feature (c470db07-1098-11e5-b6a8-002590263bf5)

FreeBSD : security/ossec-hids-\* -- root escalation via temp files (36858e78-3963-11e4-ad84-000c29f6ae42)

FreeBSD : sendmail -- race condition vulnerability (08ac7b8b-bb30-11da-b2fb-000e0c2e438a)

FreeBSD : Serendipity -- multiple vulnerabilities (01018916-c47c-11e8-8b07-00e04c1ea73d)

FreeBSD : serendipity -- multiple XSS vulnerabilities (9c133aa0-12bd-11dd-bab7-0016179b2dd5)

FreeBSD : serendipity -- XSS (3ba87032-7fbd-11e9-8a5f-c85b76ce9b5a)

FreeBSD : Serendipity -- XSS Vulnerabilities (96ed277b-60e0-11db-ad2d-0016179b2dd5)

FreeBSD : serf -- SSL Certificate Null Byte Poisoning (69048656-2187-11e4-802c-20cf30e32f6d)

FreeBSD : seti@home remotely exploitable buffer overflow (0e154a9c-5d7a-11d8-80e3-0020ed76ef5a)

FreeBSD : Several remotely exploitable buffer overflows in gaim (6fd02439-5d70-11d8-80e3-0020ed76ef5a)

FreeBSD : Several Security Defects in the Bouncy Castle Crypto APIs (89cf8cd2-0698-11e7-aa3f-001b216d295b)

FreeBSD : Several Security Defects in the Bouncy Castle Crypto APIs (fe93803c-883f-11e8-9f0c-001b216d295b)

FreeBSD : Several vulnerabilities found in IcedTea-Web (55b498e2-e56c-11e1-bbd5-001c25e46b1d)

FreeBSD : Several vulnerabilities found in PHP (1e232a0c-eb57-11e4-b595-4061861086c1)

FreeBSD : Several vulnerabilities found in PHP (742563d4-d776-11e4-b595-4061861086c1)

FreeBSD : Several vulnerabilities found in PHPNuke (33ab4a47-bfc1-11d8-b00e-000347a4fa7d)

FreeBSD : Several vulnerabilities in libav (2f75141c-da1d-11e4-8d32-5404a68ad561)

FreeBSD : sge -- local root exploit in bundled rsh executable (57a0242d-8c4e-11da-8ddf-000ae42e9b93)

FreeBSD : shadowsocks-libev -- command injection via shell metacharacters (3746de31-0a1a-11e8-83e7-485b3931c969)

FreeBSD : sharutils -- buffer overflows (26c9e8c6-1c99-11d9-814e-0001020eed82)

FreeBSD : sharutils -- unshar insecure temporary file creation (5f003a08-ba3c-11d9-837d-000e0c2e438a)

FreeBSD : shibboleth-sp -- crashes on malformed date/time content (4f8665d0-0465-11e9-b77a-6cc21735f730)

FreeBSD : shibboleth-sp -- DoS vulnerability (b202e4ce-3114-11e5-aa32-0026551a22dc)

FreeBSD : shibboleth-sp -- vulnerable to forged user attribute data (22438240-1bd0-11e8-a2ec-6cc21735f730)

FreeBSD : shibboleth-sp -- vulnerable to forged user attribute data (3dbe9492-f7b8-11e7-a12d-6cc21735f730)

FreeBSD : shibboleth2-sp -- 'Dynamic' metadata provider plugin issue (b4b7ec7d-ca27-11e7-a12d-6cc21735f730)

FreeBSD : shotwell -- failure to encrypt authentication (5a9b3d70-48e2-4267-b196-83064cb14fe0)

FreeBSD : shotwell -- not verifying certificates (448047e9-030e-4ce4-910b-f21a3ad5d9a0)

FreeBSD : shoutcast -- XSS, information exposure (67dbe99f-0f09-11db-94f8-00e029485e38)

FreeBSD : shtool -- insecure temporary file creation (6596bb80-d026-11d9-9aed-000e0c2e438a)

FreeBSD : shutter -- arbitrary code execution (d45ad7ae-5d56-11e5-9ad8-14dae9d210b8)

FreeBSD : sieve-connect -- TLS hostname verification was not occurring (a2ff483f-a5c6-11e2-9601-000d601460a4)

FreeBSD : silc -- pkcs\_decode buffer overflow (ff304c35-fb5b-11dc-91c1-00e0815b8da8)

FreeBSD : silc-client -- Format string vulnerability (4e306850-811f-11de-8a67-000c29a67389)

FreeBSD : silc-toolkit -- Format string vulnerabilities (24aa9970-9ccd-11de-af10-000c29a67389)

FreeBSD : sinatra -- XSS vulnerability (ca05d9da-ac1d-4113-8a05-ffe9cd0d6160)

FreeBSD : sircd -- remote operator privilege escalation vulnerability (e92d8f6b-a1c0-11db-9ddc-0011098b2f36)

FreeBSD : sircd -- remote reverse DNS buffer overflow (1374b96c-a1c2-11db-9ddc-0011098b2f36)

FreeBSD : skype -- multiple buffer overflow vulnerabilities (70fc13d9-4ab4-11da-932d-00055d790c25)

FreeBSD : slim -- insecure PATH assignment (68c7187a-abd2-11df-9be6-0015587e2cc1)

FreeBSD : slim -- local disclosure of X authority magic cookie (80f13884-4d4c-11de-8811-0030843d3802)

FreeBSD : slixmpp -- improper access control (526d9642-3ae7-11e9-a669-8c164582fbac)

FreeBSD : slurm -- insecure handling of user\_name and gid fields (3a66cb69-716f-11e8-be54-3085a9a47796)

FreeBSD : slurm-wlm -- SQL Injection attacks against SlurmDBD (b3e04661-2a0a-11e8-9e63-3085a9a47796)

FreeBSD : smart\_proxy\_dynflow -- authentication bypass vulnerability (2d6de6a8-fb78-4149-aeda-77fc8f140f06)

FreeBSD : smarty3 -- shell injection in math (6e4e35c3-5fd1-11e7-9def-b499baebfeaf)

FreeBSD : smbd -- buffer-overrun vulnerability (f3d3f621-38d8-11d9-8fff-000c6e8f12ef)

FreeBSD : smbftpd -- format string vulnerability (b2571f88-a867-11dc-a6f0-00a0cce0781e)

FreeBSD : smtpproxy (1408)

FreeBSD : snort -- Back Orifice preprocessor buffer overflow vulnerability (97d45e95-3ffc-11da-a263-0001020eed82)

FreeBSD : snort -- DCE/RPC preprocessor vulnerability (afdf500f-c1f6-11db-95c5-000c6ec775d9)

FreeBSD : socat -- buffer overflow with data from command line (a4c9e12d-88b7-11e3-8ada-10bf48e1088e)

FreeBSD : socat -- diffie hellman parameter was not prime (a52a7172-c92e-11e5-96d6-14dae9d210b8)

FreeBSD : socat -- FD leak (6d87c2e9-c64d-11e2-9c22-50465d9ff992)

FreeBSD : socat -- format string vulnerability (f3017ce1-32a4-11d9-a9e7-0001020eed82)

FreeBSD : socat -- Heap-based buffer overflow (6601127c-9e09-11e1-b5e0-000c299b62e1)

FreeBSD : solr -- Code execution via entity expansion (e837390d-0ceb-46b8-9b32-29c1195f5dc7)

FreeBSD : Solr -- multiple vulnerabilities (e59cb761-5ad8-11ea-abb7-001b217b3468)

FreeBSD : sox -- input sanitization errors (92cda470-30cb-11e5-a4a5-002590263bf5)

FreeBSD : sox -- memory corruption vulnerabilities (9dd761ff-30cb-11e5-a4a5-002590263bf5)

FreeBSD : SoX buffer overflows when handling .WAV files (3e4ffe76-e0d4-11d8-9b0a-000347a4fa7d)

FreeBSD : spamass-milter -- remote command execution vulnerability (7132c842-58e2-11df-8d80-0015587e2cc1)

FreeBSD : spamassassin -- Apache SpamAssassin Nefarious rule configuration (.cf) files can be configured to run system commands with warnings (e3404a6e-4364-11ea-b643-206a8a720317)

FreeBSD : SpamAssassin -- denial-of-service in tokenize\_headers (0d3a5148-f512-11d8-9837-000c41e2cdad)

FreeBSD : spamassassin -- multiple vulnerabilities (613193a0-c1b4-11e8-ae2d-54e1ad3d6335)

FreeBSD : spamassassin -- multiple vulnerabilities (70111759-1dae-11ea-966a-206a8a720317)

FreeBSD : spamassassin -- Nefarious rule configuration files can run system commands (c86bfee3-4441-11ea-8be3-54e1ad3d6335)

FreeBSD : spamdyke -- Buffer Overflow Vulnerabilities (7d2336c2-4607-11e1-9f47-00e0815b8da8)

FreeBSD : spamdyke -- open relay (555ac165-2bee-11dd-bbdc-00e0815b8da8)

FreeBSD : spamdyke -- STARTTLS Plaintext Injection Vulnerability (a47af810-3a17-11e1-a1be-00e0815b8da8)

FreeBSD : SQL injection vulnerability in phpnuke (75770425-67a2-11d8-80e3-0020ed76ef5a)

FreeBSD : sql-ledger -- multiple vulnerabilities (0679deeb-8eaf-11db-abc9-0003476f14d3)

FreeBSD : sql-ledger -- security bypass vulnerability (8e02441d-d39c-11db-a6da-0003476f14d3)

FreeBSD : SQLite -- Corrupt DB can cause a NULL pointer dereference (6d52bda1-2e54-11e8-a68f-485b3931c969)

FreeBSD : SQLite -- Corrupt DB can cause a NULL pointer dereference (c1630aa3-7970-11e8-8634-dcfe074bd614)

FreeBSD : sqlite -- multiple vulnerabilities (dec3164f-3121-45ef-af18-bb113ac5082f)

FreeBSD : sqlite3 -- heap-buffer overflow (9245681c-7c3c-11e7-b5af-a4badb2f4699)

FreeBSD : SQLite3 -- Tempdir Selection Vulnerability (546deeea-3fc6-11e6-a671-60a44ce6887b)

FreeBSD : sqlite3 -- use after free (36b905ad-7fbb-11e9-8a5f-c85b76ce9b5a)

FreeBSD : squid (1901)

FreeBSD : squid -- Buffer overflow in SNMP processing (d3324c55-3f11-11e4-ad16-001999f8d30b)

FreeBSD : squid -- buffer overflow in WCCP recvfrom() call (23fb5a04-722b-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- buffer overflow vulnerability in gopherToHTML (184ab9e0-64cd-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- client-first SSL-bump does not correctly validate X509 server certificate (b6da24da-23f7-11e5-a4a5-002590263bf5)

FreeBSD : squid -- confusing results on empty acl declarations (a30e5e44-5440-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- correct handling of oversized HTTP reply headers (bfda39de-7467-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- denial of service (30a04ab4-ed7b-11e2-8643-8c705af55518)

FreeBSD : squid -- denial of service (c37de843-488e-11e2-a5c9-0019996bc1f7)

FreeBSD : Squid -- Denial of Service Vulnerability (6eb580d7-a29c-11dc-8919-001c2514716c)

FreeBSD : squid -- Denial of Service vulnerability in DNS handling (296ecb59-0f6b-11df-8bab-0019996bc1f7)

FreeBSD : squid -- Denial of Service vulnerability in HTCP (81d9dc0c-1988-11df-8e66-0019996bc1f7)

FreeBSD : squid -- Denial of service vulnerability in request handling (e4dac715-c818-11df-a92c-0015587e2cc1)

FreeBSD : squid -- Denial Of Service Vulnerability in sslConnectTimeout (4e210d72-1c5c-11da-92ce-0048543d60ce)

FreeBSD : squid -- denial of service with forged WCCP messages (5fe7e27a-64cb-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- denial-of-service vulnerabilities (5bf1a715-cc57-440f-b0a5-6406961c54a7)

FreeBSD : squid -- DNS lookup spoofing vulnerability (7e97b288-c7ca-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- DoS on failed PUT/POST requests vulnerability (8dbf7894-a9a8-11d9-a788-0001020eed82)

FreeBSD : squid -- FTP server response handling denial of service (1c3142a3-4ab2-11da-932d-00055d790c25)

FreeBSD : squid -- HTTP response splitting cache pollution attack (4e4bd2c2-6bd5-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- Improper Protection of Alternate Path with CONNECT requests (150d1538-23fa-11e5-a4a5-002590263bf5)

FreeBSD : squid -- multiple vulnerabilities (25e5205b-1447-11e6-9ead-6805ca0b3d42)

FreeBSD : squid -- multiple vulnerabilities (297117ba-f92d-11e5-92ce-002590263bf5)

FreeBSD : squid -- multiple vulnerabilities (41f8af15-c8b9-11e6-ae1b-002590263bf5)

FreeBSD : squid -- multiple vulnerabilities (e05bfc92-0763-11e6-94fa-002590263bf5)

FreeBSD : squid -- no sanity check of usernames in squid\_ldap\_auth (7a921e9e-68b1-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- NTLM authentication denial-of-service vulnerability (064225c5-1f53-11d9-836a-0090962cff2a)

FreeBSD : squid -- possible abuse of cachemgr.cgi (a395397c-c7c8-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- possible cache-poisoning via malformed HTTP responses (b4d94fa0-6e38-11d9-9e1e-c296ac722cb3)

FreeBSD : squid -- possible denial of service condition regarding NTLM authentication (44e7764c-2614-11da-9e1e-c296ac722cb3)

FreeBSD : squid -- Possible Denial Of Service Vulnerability in store.c (0c0dc409-1c5e-11da-92ce-0048543d60ce)

FreeBSD : squid -- possible information disclosure (f0db930b-496b-11d9-bf86-0050569f0001)

FreeBSD : squid -- remote denial of service vulnerability (9c2460a4-f6b1-11dd-94d9-0030843d3802)

FreeBSD : squid -- remote DoS in HTTP response processing (660ebbf5-daeb-11e5-b2bd-002590263bf5)

FreeBSD : squid -- several remote denial of service vulnerabilities (e1156e90-7ad6-11de-b26a-0048543d60ce)

FreeBSD : squid -- SNMP module denial-of-service vulnerability (65e99f52-1c5f-11d9-bc4a-000c41e2cdad)

FreeBSD : squid -- SSL/TLS processing remote DoS (56562efb-d5e4-11e5-b2bd-002590263bf5)

FreeBSD : squid -- TLS/SSL parser denial of service vulnerability (d3a98c2d-5da1-11e5-9909-002590263bf5)

FreeBSD : Squid -- TRACE method handling denial of service (c27bc173-d7aa-11db-b141-0016179b2dd5)

FreeBSD : squid -- Vulnerable to Denial of Service attack (d5b6d151-1887-11e8-94f7-9c5c8e75236a)

FreeBSD : squid -- Vulnerable to HTTP Digest Authentication (620685d6-0aa3-11ea-9673-4c72b94353b5)

FreeBSD : squid ACL bypass due to URL decoding bug (705e003a-7f36-11d8-9645-0020ed76ef5a)

FreeBSD : squidclamav -- Denial of Service (8defa0f9-ee8a-11e1-8bd8-0022156e8794)

FreeBSD : squidclamav -- XSS in default virus warning pages (ce680f0a-eea6-11e1-8bd8-0022156e8794)

FreeBSD : squidGuard -- multiple vulnerabilities (692ab645-bf5d-11de-849b-00151797c2d4)

FreeBSD : squirrelmail -- \_$POST variable handling allows for various attacks (7d52081f-2795-11da-bc01-000e0c2e438a)

FreeBSD : squirrelmail -- multiple vulnerabilities (af9018b6-a4f5-11da-bb41-0011433a9404)

FreeBSD : SquirrelMail -- Plug-ins compromise (0d0237d0-7f68-11de-984d-0011098ad87f)

FreeBSD : squirrelmail -- plugin.php local file inclusion vulnerability (00784d6e-f4ce-11da-87a1-000c6ec775d9)

FreeBSD : SquirrelMail -- post-authentication access privileges (928d5c59-2a5a-11e8-a712-0025908740c2)

FreeBSD : SquirrelMail -- post-authentication remote code execution (e1de77e8-c45e-48d7-8866-5a6f943046de)

FreeBSD : squirrelmail -- random variable overwrite vulnerability (21b7c550-2a22-11db-a6e2-000e0c2e438a)

FreeBSD : squirrelmail -- Session hijacking vulnerability (a0afb4b9-89a1-11dd-a65b-00163e000016)

FreeBSD : squirrelmail -- Several XSS vulnerabilities (e879ca68-e01b-11d9-a8bd-000cf18bbe54)

FreeBSD : squirrelmail -- XSS and remote code injection vulnerabilities (79630c0c-8dcc-45d0-9908-4087fe1d618c)

FreeBSD : squirrelmail -- XSS in HTML filter (0e575ed3-0764-11dc-a80b-0016179b2dd5)

FreeBSD : squirrelmail -- XSS vulnerability (7fbfe159-3438-11d9-a9e7-0001020eed82)

FreeBSD : squirrelmail -- XSS vulnerability (d1ce8a4f-c235-11dd-8cbc-00163e000016)

FreeBSD : sqwebmail (2248)

FreeBSD : SSH.COM SFTP server -- format string vulnerability (594ad3c5-a39b-11da-926c-0800209adf0e)

FreeBSD : SSLtelnet (2263)

FreeBSD : star (1802)

FreeBSD : streamripper -- multiple buffer overflows (4d4caee0-b939-11dd-a578-0030843d3802)

FreeBSD : strongswan - Insufficient input validation in RSASSA-PSS signature parser (6a449a37-1570-11e8-8e00-000c294a5758)

FreeBSD : strongswan -- authentication bypass vulnerability in the eap-mschapv2 plugin (3eb0ccc2-8c6a-11e5-8519-005056ac623e)

FreeBSD : strongswan -- Denial-of-service and potential remote code execution vulnerability (55363e65-0e71-11e5-8027-00167671dd1d)

FreeBSD : strongswan -- Denial-of-service vulnerability in the x509 plugin (c7e8e955-6c61-11e7-9b01-2047478f2f70)

FreeBSD : strongSwan -- ECDSA signature verification issue (6ff570cb-b418-11e2-b279-20cf30e32f6d)

FreeBSD : strongswan -- Fix Denial-of-Service Vulnerability strongSwan (CVE-2018-10811, CVE-2018-5388) (7fc3e827-64a5-11e8-aedb-00224d821998)

FreeBSD : strongswan -- Information Leak Vulnerability (10d14955-0e45-11e5-b6a8-002590263bf5)

FreeBSD : strongswan -- multiple DoS vulnerabilities (efa663eb-8754-11e3-9a47-00163e1ed244)

FreeBSD : strongswan -- multiple vulnerabilities (e6ccaf8a-6c63-11e7-9b01-2047478f2f70)

FreeBSD : strongswan -- Remote Authentication Bypass (6fb521b0-d388-11e3-a790-000c2980a9f3)

FreeBSD : stunnel -- heap corruption vulnerability (cdeb34e6-d00d-11e0-987e-00215c6a37bb)

FreeBSD : stunnel -- Remote Code Execution (c97219b6-843d-11e2-b131-000c299b62e1)

FreeBSD : subversion (1638)

FreeBSD : subversion -- Arbitrary code execution vulnerability (6e80bd9b-7e9b-11e7-abfe-90e2baa3bafc)

FreeBSD : subversion -- DoS vulnerabilities (8e887b71-d769-11e4-b1c2-20cf30e32f6d)

FreeBSD : subversion -- DoS vulnerabilities (f5561ade-846c-11e4-b7a7-20cf30e32f6d)

FreeBSD : subversion -- heap overflow vulnerability (bce1f76d-82d0-11de-88ea-001a4d49522b)

FreeBSD : subversion -- mod\_dav\_svn vulnerability (1839f78c-9f2b-11e3-980f-20cf30e32f6d)

FreeBSD : subversion -- multiple DoS (71612099-1e93-11e0-a587-001b77d09812)

FreeBSD : subversion -- multiple vulnerabilities (57bb5e3d-3c4f-11e5-a4d4-001e8c75030d)

FreeBSD : Subversion -- multiple vulnerabilities (b6beb137-9dc0-11e2-882f-20cf30e32f6d)

FreeBSD : subversion -- multiple vulnerabilities (c8174b63-0d3a-11e6-b06e-d43d7eed0ce2)

FreeBSD : subversion -- multiple vulnerabilities (daadef86-a366-11e5-8b40-20cf30e32f6d)

FreeBSD : Subversion -- multiple vulnerabilities (e27a1af3-8d21-11e0-a45d-001e8c75030d)

FreeBSD : subversion -- multiple vulnerabilities (e3244a7b-5603-11e3-878d-20cf30e32f6d)

FreeBSD : subversion -- remote HTTP DoS vulnerability (e27ca763-4721-11e0-bdc4-001e8c75030d)

FreeBSD : subversion -- remotely triggerable 'Assertion failed' DoS vulnerability or read overflow. (2ae24334-f2e6-11e2-8346-001e8c75030d)

FreeBSD : subversion -- several vulnerabilities (83a418cc-2182-11e4-802c-20cf30e32f6d)

FreeBSD : subversion -- Unrestricted XML entity expansion in mod\_dontdothat and Subversionclients using http(s) (ac256985-b6a9-11e6-a3bf-206a8a720317)

FreeBSD : subversion -- WebDAV fails to protect metadata (184f5d0b-0fe8-11d9-8a8a-000c41e2cdad)

FreeBSD : subversion date parsing vulnerability (5d36ef32-a9cf-11d8-9c6d-0020ed76ef5a)

FreeBSD : subversion- (2287)

FreeBSD : sudo -- arbitrary command execution (1b725079-9ef6-11da-b410-000e0c2e438a)

FreeBSD : sudo -- Authentication bypass when clock is reset (764344fb-8214-11e2-9273-902b343deec9)

FreeBSD : sudo -- certain authorized users could run commands as any user (13d6d997-f455-11dd-8516-001b77d09812)

FreeBSD : sudo -- environmental variable CDPATH is not cleared (045944a0-6bca-11d9-aaa6-000a95bc6fae)

FreeBSD : sudo -- Flaw in Runas group matching (67b514c3-ba8f-11df-8f6e-000c29a67389)

FreeBSD : sudo -- format string vulnerability (7c920bb7-4b5f-11e1-9f47-00e0815b8da8)

FreeBSD : sudo -- local privilege escalation (908f4cf2-1e8b-11e0-a587-001b77d09812)

FreeBSD : sudo -- local race condition vulnerability (3bf157fa-e1c6-11d9-b875-0001020eed82)

FreeBSD : sudo -- netmask vulnerability (b3435b68-9ee8-11e1-997c-002354ed89bc)

FreeBSD : sudo -- Potential bypass of Runas user restrictions (3a1474ba-f646-11e9-b0af-b888e347c638)

FreeBSD : sudo -- Potential bypass of Runas user restrictions (b4e5f782-442d-11ea-9ba9-206a8a720317)

FreeBSD : sudo -- Potential bypass of sudo\_noexec.so via wordexp() (2e4fbc9a-9d23-11e6-a298-14dae9d210b8)

FreeBSD : sudo -- Potential bypass of tty\_tickets constraints (82cfd919-8213-11e2-9273-902b343deec9)

FreeBSD : sudo -- potential privilege escalation via symlink misconfiguration (2e8cdd36-c3cc-11e5-b5fe-002590263bf5)

FreeBSD : sudo -- privilege escalation with bash scripts (bdd1537b-354c-11d9-a9e7-0001020eed82)

FreeBSD : sudo -- Privilege escalation with sudoedit (018a84d0-2548-11df-b4a3-00e0815b8da8)

FreeBSD : sudo -- Privilege escalation with sudoedit (1a9f678d-48ca-11df-85f8-000c29a67389)

FreeBSD : sudo -- Secure path vulnerability (d42e5b66-6ea0-11df-9c8d-00e0815b8da8)

FreeBSD : sudo -- sudoedit information disclosure (a268ef4a-0b35-11d9-8a8a-000c41e2cdad)

FreeBSD : sudoscript -- signal delivery vulnerability (85edfb6a-43a5-11d9-a9e7-0001020eed82)

FreeBSD : sudosh -- buffer overflow (8675efd5-e22c-11e1-a808-002354ed89bc)

FreeBSD : sugarcrm -- multiple vulnerabilities (3b776502-f601-44e0-87cd-b63f1b9ae42a)

FreeBSD : sup (1455)

FreeBSD : sup -- format string vulnerability (2c5757f4-88bf-11d9-8720-0007e900f87b)

FreeBSD : super (2496)

FreeBSD : Supervisord -- An authenticated client can run arbitrary shell commands via malicious XML-RPC requests (c9460380-81e3-11e7-93af-005056925db4)

FreeBSD : suphp -- multiple local privilege escalation vulnerabilities (fb672330-02db-11dd-bd06-0017319806e7)

FreeBSD : suPHP -- Privilege escalation (2fbfd455-f2d0-11e2-8a46-000d601460a4)

FreeBSD : surf -- private information disclosure (039d057e-544e-11e1-9fb7-003067b2972c)

FreeBSD : suricata -- buffer over-read (3b903bf3-7f94-11e9-8a5f-c85b76ce9b5a)

FreeBSD : suricata -- TLS/DER Parser Bug (DoS) (fe910ed6-f88d-11e4-9ae3-0050562a4d7b)

FreeBSD : svnserve is vulnerable to a local privilege escalation vulnerability via symlink attack. (f8a913cc-1322-11e3-8ffa-20cf30e32f6d)

FreeBSD : swfdec -- exposure of sensitive information (5ef12755-1c6c-11dd-851d-0016d325a0ed)

FreeBSD : sylpheed -- buffer overflow in header processing (f8536143-9bc4-11d9-b8b3-000a95bc6fae)

FreeBSD : sylpheed -- MIME-encoded file name buffer overflow vulnerability (b1e8c810-01d0-11da-bc08-0001020eed82)

FreeBSD : sympa (1653)

FreeBSD : sympa -- buffer overflow in 'queue' (0d9ba03b-0dbb-42b4-ae0f-60e27af78e22)

FreeBSD : sympa -- Multiple Security Bypass Vulnerabilities (78c39232-a345-11e1-9d81-d0df9acfd7e5)

FreeBSD : sympa -- Remote attackers can read arbitrary files (451a6c79-c92b-11e4-a835-000c292ee6b8)

FreeBSD : syslog-ng2 -- startup directory leakage in the chroot environment (75f2382e-b586-11dd-95f9-00e0815b8da8)

FreeBSD : tarsnap -- buffer overflow and local DoS (2fe40238-480f-11e5-adde-14dae9d210b8)

FreeBSD : tarsnap -- cryptographic nonce reuse (2c2d4e83-2370-11e0-a91b-00e0815b8da8)

FreeBSD : tcl/tk -- buffer overflow in ReadImage function (a058d6fa-7325-11dc-ae10-0016179b2dd5)

FreeBSD : tcpdump -- infinite loops in protocol decoding (9fae0f1f-df82-11d9-b875-0001020eed82)

FreeBSD : tcpdump -- multiple vulnerabilities (eb03d642-6724-472d-b038-f2bf074e1fc8)

FreeBSD : tcpdump ISAKMP payload handling remote denial-of-service (f8551668-de09-4d7b-9720-f1360929df07)

FreeBSD : tdiary -- injection vulnerability (fefd93d8-8af5-11db-9d01-0016179b2dd5)

FreeBSD : tdiary -- XSS vulnerability (666b8c9e-8212-11db-851e-0016179b2dd5)

FreeBSD : Teamspeak Server -- Directory Traversal Vulnerability (4b68d917-e705-11dd-afcd-00e0815b8da8)

FreeBSD : TeamSpeak Server 3 -- Multiple vulnerabilities including Remote Code Execution (f7dd2d09-625e-11e6-828b-fcaa14edc6a6)

FreeBSD : teeworlds -- Remote code execution (81fc7705-b002-11e6-b20a-14dae9d5a9d2)

FreeBSD : telepathy-gabble -- TLS verification bypass (a3c2dee5-cdb9-11e2-b9ce-080027019be0)

FreeBSD : Template::Toolkit -- Directory traversal on write (2bab995f-36d4-11ea-9dad-002590acae31)

FreeBSD : testdisk -- buffer overflow with malicious disk image (c67069dc-0986-11e5-bb90-002590263bf5)

FreeBSD : The Bouncy Castle Crypto APIs: CVE-2017-13098 ('ROBOT') (6a131fbf-ec76-11e7-aa65-001b216d295b)

FreeBSD : The GIMP -- Use after Free vulnerability (6fb8a90f-c9d5-4d14-b940-aed3d63c2edc)

FreeBSD : thunderbird -- javascript execution (61349f77-c620-11da-b2fb-000e0c2e438a)

FreeBSD : tidy -- heap-buffer-overflow (bd1ab7a5-0e01-11e5-9976-a0f3c100ae18)

FreeBSD : tiff -- buffer overflow (0ab66088-4aa5-11e6-a7bd-14dae9d210b8)

FreeBSD : tiff -- buffer overflow (c17fe91d-4aa6-11e6-a7bd-14dae9d210b8)

FreeBSD : tiff -- buffer overflow vulnerability (313da7dc-763b-11df-bcce-0018f3e2eb82)

FreeBSD : tiff -- buffer overflow vulnerability (68222076-010b-11da-bc08-0001020eed82)

FreeBSD : tiff -- denial of service (42ecf370-4aa4-11e6-a7bd-14dae9d210b8)

FreeBSD : tiff -- directory entry count integer overflow vulnerability (fc7e6a42-6012-11d9-a9e7-0001020eed82)

FreeBSD : tiff -- divide-by-zero denial-of-service (b58ff497-6977-11d9-ae49-000c41e2cdad)

FreeBSD : tiff -- multiple integer overflows (3897a2f8-1d57-11d9-bc4a-000c41e2cdad)

FreeBSD : tiff -- Multiple integer overflows (8816bf3a-7929-11df-bcce-0018f3e2eb82)

FreeBSD : tiff -- multiple vulnerabilities (2a96e498-3234-4950-a9ad-419bc84a839d)

FreeBSD : tiff -- multiple vulnerabilities (b38e8150-0535-11e8-96ab-0800271d4b9c)

FreeBSD : tiff -- multiple vulnerabilities (fb74eacc-ec8a-11e6-bc8a-0011d823eebd)

FreeBSD : tiff -- out-of-bounds read in CIE Lab image format (b65e4914-b3bc-11e5-8255-5453ed2e2b49)

FreeBSD : tiff -- out-of-bounds read in tif\_getimage.c (bd349f7a-b3b9-11e5-8255-5453ed2e2b49)

FreeBSD : tiff -- RLE decoder heap overflows (f6680c03-0bd8-11d9-8a8a-000c41e2cdad)

FreeBSD : tiff -- tiffdump integer overflow vulnerability (8f86d8b5-6025-11d9-a9e7-0001020eed82)

FreeBSD : tikiwiki -- multiple vulnerabilities (20a4eb11-8ea3-11dc-a396-0016179b2dd5)

FreeBSD : tikiwiki -- multiple vulnerabilities (e4c62abd-5065-11db-a5ae-00508d6a62df)

FreeBSD : TiMidity++ -- Multiple vulnerabilities (d37407bd-5c5f-11ea-bb2a-8c164582fbac)

FreeBSD : tin -- buffer overflow vulnerabilities (19a92df1-548d-11db-8f1a-000a48049292)

FreeBSD : tinc -- Buffer overflow (a4eb38ea-cc06-11e8-ada4-408d5cf35399)

FreeBSD : tinc -- Buffer overflow (aeb962f6-ab8d-11e2-b3f5-003067c2616f)

FreeBSD : tinyproxy -- ACL lists ineffective when range is configured (b9281fb9-61b2-11e0-b1ce-0019d1a7ece2)

FreeBSD : tkdiff -- temporary file symlink privilege escalation (93ba13f8-5c41-11db-a5ae-00508d6a62df)

FreeBSD : tnftp -- mget does not check for directory escapes (f92e1bbc-5e18-11d9-839a-0050da134090)

FreeBSD : tnftpd -- Remote root Exploit (e969e6cb-8911-11db-9d01-0016179b2dd5)

FreeBSD : tnftpd -- remotely exploitable vulnerability (c4b025bb-f05d-11d8-9837-000c41e2cdad)

FreeBSD : tomcat -- authentication weaknesses (152e4c7e-2a2e-11e2-99c7-00a0d181e71d)

FreeBSD : tomcat -- bypass of CSRF prevention filter (953911fe-51ef-11e2-8e34-0022156e8794)

FreeBSD : tomcat -- bypass of security constraints (f599dfc4-3ec2-11e2-8ae1-001a8056d0b5)

FreeBSD : tomcat -- denial of service (134acaa2-51ef-11e2-8e34-0022156e8794)

FreeBSD : tomcat -- Denial of Service (4ca26574-2a2c-11e2-99c7-00a0d181e71d)

FreeBSD : tomcat -- Denial of Service (7f5ccb1d-439b-11e1-bc16-0023ae8e59f0)

FreeBSD : tomcat -- information disclosure vulnerability (3383e706-4fc3-11df-83fb-0015587e2cc1)

FreeBSD : tomcat -- information disclosure vulnerability (e5ec2767-d529-11e6-ae1b-002590263bf5)

FreeBSD : tomcat -- multiple vulnerabilities (0b9af110-d529-11e6-ae1b-002590263bf5)

FreeBSD : tomcat -- multiple vulnerabilities (1f1124fe-de5c-11e5-8fa8-14dae9d210b8)

FreeBSD : tomcat -- multiple vulnerabilities (25e0593d-13c0-11e5-9afb-3c970e169bc2)

FreeBSD : tomcat -- multiple vulnerabilities (3ae106e2-d521-11e6-ae1b-002590263bf5)

FreeBSD : tomcat -- multiple vulnerabilities (7bbc3016-de63-11e5-8fa8-14dae9d210b8)

FreeBSD : tomcat -- multiple vulnerabilities (81fc1076-1286-11e4-bebd-000c2980a9f3)

FreeBSD : tomcat -- multiple vulnerabilities (872623af-39ec-11dc-b8cc-000fea449b8a)

FreeBSD : tomcat -- Remote Code Execution (c0dae634-4820-4505-850d-b1c975d0f67d)

FreeBSD : tomcat -- Security constraints ignored or applied too late (55c4233e-1844-11e8-a712-0025908740c2)

FreeBSD : tomcat -- Tomcat Manager XSS (26a08c77-32da-4dd7-a884-a76fc49aa824)

FreeBSD : tomcat -- XSS vulnerability (553ec4ed-38d6-11e0-94b1-000c29ba66d2)

FreeBSD : tomcat -- XSS vulnerability in sample applications (ab2575d6-39f0-11dc-b8cc-000fea449b8a)

FreeBSD : tor -- diffie-hellman handshake flaw (5fde5c30-0f4e-11da-bc01-000e0c2e438a)

FreeBSD : tor -- guard discovery (80af2677-d6c0-11e2-8f5e-001966155bea)

FreeBSD : tor -- information disclosure (691ed622-e499-11d9-a8bd-000cf18bbe54)

FreeBSD : tor -- malicious tor server can locate a hidden service (d38e1810-9ef7-11da-b410-000e0c2e438a)

FreeBSD : tor -- multiple vulnerabilities (78f5606b-f9d1-11dd-b79c-0030843d3802)

FreeBSD : tor -- remote code execution and crash (38bdf10e-2293-11e0-bfa4-001676740879)

FreeBSD : tor -- remote crash and potential remote code execution (4bd33bc5-0cd6-11e0-bfa4-001676740879)

FreeBSD : Tor -- remote denial of service (c1dc55dc-9556-11e6-b154-3065ec8fd3ec)

FreeBSD : tor -- remote DoS and loss of anonymity (8e2e6ad8-1720-11d9-9fb9-00902788733b)

FreeBSD : tor -- security regression (0b9f4b5e-5d82-11e7-85df-14dae9d5a9d2)

FreeBSD : tor -- traffic confirmation attack (31c09848-1829-11e4-bf04-60a44c524f57)

FreeBSD : tor -- unspecified memory corruption vulnerability (100a9ed2-ee56-11dd-ab4f-0030843d3802)

FreeBSD : tor -- Use-after-free in onion service v2 (36ef8753-d86f-11e7-ad28-0025908740c2)

FreeBSD : tor-devel -- DNS resolution vulnerability (f59dda75-5ff4-11de-a13e-00e0815b8da8)

FreeBSD : torcs -- untrusted local library loading (e7fd27b2-3ae9-11e1-8b5c-00262d5ed8ee)

FreeBSD : torrentflux -- User-Agent XSS Vulnerability (72f21372-55e4-11db-a5ae-00508d6a62df)

FreeBSD : tptest -- pwd Remote Stack Buffer Overflow (5486669e-ea9f-11de-bd9c-00215c6a37bb)

FreeBSD : trac -- file upload/download vulnerability (b02c1d80-e1bb-11d9-b875-0001020eed82)

FreeBSD : trac -- potential DOS vulnerability (c89a3ebb-ae07-11dd-b4b2-001f3c8eabeb)

FreeBSD : trac -- reStructuredText breach of privacy and denial of service vulnerability (b0d61f73-0e11-11db-a47b-000c2957fdf1)

FreeBSD : trac -- search module SQL injection vulnerability (7289187b-66a5-11da-99f6-00123ffe8333)

FreeBSD : trac -- Wiki Macro Script Insertion Vulnerability (400d9d22-d6c5-11da-a14b-00123ffe8333)

FreeBSD : trac -- XSS vulnerability (e546c7ce-ce46-11db-bc24-0016179b2dd5)

FreeBSD : traefik -- Denial of service in HTTP/2 (41f4baac-bf77-11e9-8d2f-5404a68ad561) (Ping Flood) (Reset Flood)

FreeBSD : trafficserver -- unspecified vulnerability (6318b303-3507-11e4-b76c-0011d823eebd)

FreeBSD : transmission-daemon -- vulnerable to dns rebinding attacks (3e5b8bd3-0c32-452f-a60e-beab7b762351)

FreeBSD : turba -- XSS vulnerabilities in several of the address book name and contact data fields (eeebd55d-6a88-11da-b96e-000fb586ba73)

FreeBSD : turnserver -- multiple vulnerabilities (181beef6-2482-11e9-b4a3-00155d006b02)

FreeBSD : turnserver -- SQL injection vulnerability (543b5939-2067-11e5-a4a5-002590263bf5)

FreeBSD : twiki -- Arbitrary code execution in session files (9227dcaf-827f-11dd-9cd7-0050568452ac)

FreeBSD : twiki -- arbitrary shell command execution (b4af3ede-36e9-11d9-a9e7-0001020eed82)

FreeBSD : twiki -- multiple file extensions file upload vulnerability (a876df84-0fef-11db-ac96-000c6ec775d9)

FreeBSD : twiki -- multiple vulnerabilities (f98dea27-d687-11dd-abd1-0050568452ac)

FreeBSD : twiki -- remote Perl code execution (21ce1840-6107-11e4-9e84-0022156e8794)

FreeBSD : typespeed -- arbitrary code execution (2c4f4688-298b-11dc-a197-0011098b2f36)

FreeBSD : typo -- XSS (67516177-88ec-11e1-9a10-0023ae8e59f0)

FreeBSD : typo3 -- email header injection (62b8f253-12d9-11dc-a35c-001485ab073e)

FreeBSD : typo3 -- Missing access check in Extbase (3caf4e6c-4cef-11e6-a15f-00248c0c745d)

FreeBSD : typo3 -- Multiple vulernabilities in TYPO3 Core (48bcb4b2-e708-11e1-a59d-000d601460a4)

FreeBSD : typo3 -- multiple vulnerabilities (1c9178aa-2709-11ea-9673-4c72b94353b5)

FreeBSD : typo3 -- multiple vulnerabilities (5d8c0876-2716-11e9-9446-b7f8544ce15c)

FreeBSD : TYPO3 -- multiple vulnerabilities (5e35cfba-9994-11e9-b07f-df5abf8b84d6)

FreeBSD : typo3 -- multiple vulnerabilities (653606e9-f6ac-11dd-94d9-0030843d3802)

FreeBSD : typo3 -- multiple vulnerabilities (a0d77bc8-c6a7-11e5-96d6-14dae9d210b8)

FreeBSD : typo3 -- multiple vulnerabilities (bab29816-ff93-11e8-b05b-00e04c1ea73d)

FreeBSD : typo3 -- multiple vulnerabilities (ef013039-89cd-11e8-84e9-00e04c1ea73d)

FreeBSD : typo3 -- multiple vulnerabilities in TYPO3 Core (6693bad2-ca50-11de-8ee8-00215c6a37bb)

FreeBSD : typo3 -- Multiple vulnerabilities in TYPO3 Core (79818ef9-2d10-11e2-9160-00262d5ed8ee)

FreeBSD : typo3 -- Multiple vulnerabilities in TYPO3 Core (b9a347ac-8671-11e2-b73c-0019d18c446a)

FreeBSD : typo3 -- Multiple vulnerabilities in TYPO3 Core (e6839625-fdfa-11e2-9430-20cf30e32f6d)

FreeBSD : typo3 -- Remote Code Execution (3c957a3e-2978-11e1-89b4-001ec9578670)

FreeBSD : typo3 -- XSS and information disclosure (cc47fafe-f823-11dd-94d9-0030843d3802)

FreeBSD : typo3 -- XSS Vulnerability in TYPO3 Core (c28ee9cd-916e-4dcf-8ed3-e97e5846db6c)

FreeBSD : uim -- privilege escalation vulnerability (1e606080-3293-11da-ac91-020039488e34)

FreeBSD : uim -- privilege escalation vulnerability (fb03b1c6-8a8a-11d9-81f7-02023f003c9f)

FreeBSD : unace -- multiple vulnerabilities (1d3a2737-7eb7-11d9-acf7-000854d03344)

FreeBSD : unarj -- directory traversal vulnerability (1f922de0-3fe5-11d9-a9e7-0001020eed82)

FreeBSD : unarj -- long filename buffer overflow (a163baff-3fe1-11d9-a9e7-0001020eed82)

FreeBSD : Unbound -- an empty error packet handling assertion failure (dc96ac1f-86b1-11e0-9e85-00215af774f0)

FreeBSD : unbound -- can be tricked into following an endless series of delegations, this consumes a lot of resources (10d73529-7f4b-11e4-af66-00215af774f0)

FreeBSD : unbound -- denial of service vulnerabilities from nonstandard redirection and denial of existence (7ba65bfd-2a40-11e1-b96e-00215af774f0)

FreeBSD : unbound -- parsing vulnerability (108a4be3-e612-11e9-9963-5f1753e0aca0)

FreeBSD : unbound -- parsing vulnerability (ffc80e58-0dcb-11ea-9673-4c72b94353b5)

FreeBSD : unbound -- vulnerability in the processing of wildcard synthesized NSEC records (8d3bae09-fd28-11e7-95f2-005056925db4)

FreeBSD : unit -- heap memory buffer overflow (c95836a0-2b3b-11e9-9838-8c164567ca3c)

FreeBSD : unreal -- denial of service (0ecc1f55-45d0-11e5-adde-14dae9d210b8)

FreeBSD : unrtf -- buffer overflow vulnerability (f2d5e56e-67eb-11d9-a9e7-0001020eed82)

FreeBSD : unzip -- heap based buffer overflow in iconv patch (3680b234-b6f0-11e4-b7cc-d050992ecde8)

FreeBSD : unzip -- input sanitization errors (d9360908-9d52-11e4-87fd-10bf48e1088e)

FreeBSD : unzip -- multiple vulnerabilities (86c3c66e-b2f5-11e5-863a-b499baebfeaf)

FreeBSD : unzip -- out of boundary access issues in test\_compr\_eb (e543c6f8-abf2-11e4-8ac7-d050992ecde8)

FreeBSD : unzip -- permission race vulnerability (9750cf22-216d-11da-bc01-000e0c2e438a)

FreeBSD : unzoo -- Directory Traversal Vulnerability (5a945904-73b1-11db-91d2-0002a5c2f4ef)

FreeBSD : up-imapproxy -- multiple vulnerabilities (927743d4-5ca9-11d9-a9e7-0001020eed82)

FreeBSD : upnp -- multiple vulnerabilities (244c8288-cc4a-11e6-a475-bcaec524bf84)

FreeBSD : upnp -- multiple vulnerabilities (2ea6ce3d-6afd-11e2-9d4e-bcaec524bf84)

FreeBSD : urban -- stack overflow vulnerabilities (08df5d46-1baf-11da-8038-0040f42d58c6)

FreeBSD : URI handler vulnerabilities in several browsers (df333ede-a8ce-11d8-9c6d-0020ed76ef5a)

FreeBSD : uriparser -- Multiple vulnerabilities (3563fae5-f60c-11e8-b513-5404a68ad561)

FreeBSD : uriparser -- Out-of-bounds read (924bd4f8-11e7-11e9-9fe8-5404a68ad561)

FreeBSD : urllib3 -- certificate verification failure (c5c6e293-9cc7-11e6-823f-b8aeed92ecc4)

FreeBSD : urllib3 -- multiple vulnerabilities (87270ba5-03d3-11ea-b81f-3085a9a95629)

FreeBSD : Use-After-Free Vulnerability in pcsc-lite (c218873d-d444-11e6-84ef-f0def167eeea)

FreeBSD : usermin (2070)

FreeBSD : uudeview buffer overflows (6c7661ff-7912-11d8-9645-0020ed76ef5a)

FreeBSD : uwsgi -- a stack-based buffer overflow (a8f25565-109e-11e8-8d41-97657151f8c2)

FreeBSD : Varnish -- Denial of service vulnerability (88a77ad8-77b1-11e7-b5af-a4badb2f4699)

FreeBSD : varnish -- DoS vulnerability in Varnish HTTP cache (d9dbe6e8-84da-11e3-98bd-080027f2d077)

FreeBSD : varnish -- information disclosure vulnerability (17133e7e-d764-11e7-b5af-a4badb2f4699)

FreeBSD : varnish -- Information Disclosure Vulnerability (2d4076eb-f679-11e9-a87f-a4badb2f4699)

FreeBSD : varnish -- Varnish HTTP Request Parsing Denial of Service (bcee3989-d106-4f60-948f-835375634710)

FreeBSD : verlihub -- insecure temporary file usage and arbitrary command execution (58997463-e012-11dd-a765-0030843d3802)

FreeBSD : viewcvs -- information leakage (323784cf-48a6-11d9-a9e7-0001020eed82)

FreeBSD : ViewVC -- user-reachable override of cvsdb row limit (7af2fb85-8584-11e0-96b7-00300582f9fc)

FreeBSD : vim -- arbitrary command execution (c11629d3-c8ad-11e6-ae1b-002590263bf5)

FreeBSD : vim -- Command Format String Vulnerability (1ed03222-3c65-11dc-b3d3-0016179b2dd5)

FreeBSD : vim -- multiple vulnerabilities in the netrw module (0e1e3789-d87f-11dd-8ecd-00163e000016)

FreeBSD : vim -- Vim Shell Command Injection Vulnerabilities (30866e6c-3c6d-11dd-98c9-00163e000016)

FreeBSD : vim -- vulnerabilities in modeline handling (bd9fc2bf-5ffe-11d9-a11a-000a95bc6fae)

FreeBSD : vim -- vulnerabilities in modeline handling: glob, expand (81f127a8-0038-11da-86bc-000e0c2e438a)

FreeBSD : Vim/NeoVim -- Security vulnerability (bbdb9713-8e09-11e9-87bc-002590acae31)

FreeBSD : vim6 -- heap-based overflow while parsing shell metacharacters (f866d2af-bbba-11df-8a8d-0008743bf21a)

FreeBSD : vinagre -- format string vulnerability (214e8e07-d369-11dd-b800-001b77d09812)

FreeBSD : virtualbox -- privilege escalation (ebeed063-b328-11de-b6a5-0030843d3802)

FreeBSD : VirtualBox -- undisclosed vulnerabilities (7d40edd1-901e-11e6-a590-14dae9d210b8)

FreeBSD : virtualbox-ose -- local vulnerability (81f1fdc2-7ec7-11e3-a6c6-00163e1ed244)

FreeBSD : vlc -- arbitrary code execution in Real RTSP and MMS support (62f36dfd-ff56-11e1-8821-001b2134ef46)

FreeBSD : vlc -- arbitrary code execution in the RealMedia processor (acf80afa-c3ef-11dd-a721-0030843d3802)

FreeBSD : vlc -- arbitrary pointer dereference vulnerability (a0a4e24c-4760-11e5-9391-3c970e169bc2)

FreeBSD : vlc -- Buffer overflow vulnerability (f2144530-936f-11e9-8fc4-5404a68ad561)

FreeBSD : vlc -- cue processing stack overflow (4b09378e-addb-11dd-a578-0030843d3802)

FreeBSD : vlc -- Double free in Matroska demuxer (5b218581-9372-11e9-8fc4-5404a68ad561)

FreeBSD : vlc -- format string vulnerability and integer overflow (7128fb45-2633-11dc-94da-0016179b2dd5)

FreeBSD : VLC -- Heap corruption in MP4 demultiplexer (6a4bfe75-692a-11e0-bce7-001eecdd401a)

FreeBSD : vlc -- Insufficient input validation in MKV demuxer (f9258873-2ee2-11e0-afcd-0015f2db7bde)

FreeBSD : vlc -- invalid id3v2 tags may lead to invalid memory dereferencing (e7d91a3c-a7c9-11df-870c-00242b513d7c)

FreeBSD : vlc -- multiple vulnerabilities (795442e7-c355-11e9-8224-5404a68ad561)

FreeBSD : VLC -- Possibly remote code execution via crafted file (6d402857-2fba-11e6-9f31-5404a68ad561)

FreeBSD : vlc -- remote code execution via crafted subtitles (ec6aeb8e-41e4-11e7-aa00-5404a68ad561)

FreeBSD : vlc -- stack overflow in MPA, AVI and ASF demuxer (3149ab1c-c8b9-11de-b87b-0011098ad87f)

FreeBSD : vlc -- unintended code execution with specially crafted data (752ce039-5242-11df-9139-00242b513d7c)

FreeBSD : vlc -- Use after free vulnerability (dc57ad48-ecbb-439b-a4d0-5869be47684e)

FreeBSD : vnc -- authentication bypass vulnerability (4645b98c-e46e-11da-9ae7-00123fcc6e5c)

FreeBSD : vorbis-tools -- Speex header processing vulnerability (633716fa-1f8f-11dd-b143-0211d880e350)

FreeBSD : vorbis-tools, opus-tools -- multiple vulnerabilities (a35f415d-572a-11e5-b0a4-f8b156b6dcc8)

FreeBSD : vpopmail-devel (1879)

FreeBSD : vte -- Classic terminal title set+query attack (9a8fecef-92c0-11df-b140-0015f2db7bde)

FreeBSD : vtiger -- multiple remote file inclusion vulnerabilities (2c8a84d9-5bee-11db-a5ae-00508d6a62df)

FreeBSD : Vulnerabilities in Curl (e4bc70fc-5a2f-11e6-a1bc-589cfc0654e1)

FreeBSD : Vulnerabilities in H.323 implementations (27c331d5-64c7-11d8-80e3-0020ed76ef5a)

FreeBSD : Vulnerability in HWP document filter (b13af778-f4fc-11e4-a95d-ac9e174be3af)

FreeBSD : w3m - multiple vulnerabilities (e72d5bf5-07a0-11e8-8248-0021ccb9e74d)

FreeBSD : w3m -- format string vulnerability (9347d82d-9a66-11db-b271-000e35248ad7)

FreeBSD : w3m -- multiple vulnerabilities (eafa3aec-211b-4dd4-9b8a-a664a3f0917a)

FreeBSD : wavpack -- multiple invalid memory reads (f1075415-f5e9-11e6-a4e2-5404a68ad561)

FreeBSD : wavpack -- multiple vulnerabilities (50210bc1-54ef-11e8-95d9-9c5c8e75236a)

FreeBSD : web browsers -- window injection vulnerabilities (b0911985-6e2a-11d9-9557-000a95bc6fae)

FreeBSD : WebCalendar -- 'noSet' variable overwrite vulnerability (72999d57-d6f6-11db-961b-005056847b26)

FreeBSD : WebCalendar -- information disclosure vulnerability (09c92f3a-fd49-11da-995c-605724cdf281)

FreeBSD : WebCalendar -- multiple vulnerabilities (18dffa02-946a-11e1-be9d-000c29cc39d3)

FreeBSD : WebCalendar -- Persistent XSS (2b20fd5f-552e-11e1-9fb7-003067b2972c)

FreeBSD : WebCalendar -- remote file inclusion vulnerability (60f8fe7b-3cfb-11da-baa2-0004614cc33d)

FreeBSD : WebCalendar -- unauthorized access vulnerability (07ead557-a220-11da-b410-000e0c2e438a)

FreeBSD : webkit -- UI spoof (1091d2d1-cb2e-11e5-b14b-bcaec565249c)

FreeBSD : webkit-gtk -- Multiple vulnabilities (e3aacd6d-3d01-434c-9330-bc9efd40350f)

FreeBSD : WebKit-gtk -- Multiple vulnerabilities (e9ccdb28-9802-11e4-9d9c-bcaec565249c)

FreeBSD : Webkit-gtk2 -- Multiple Vulnabilities (e5090d2a-dbbe-11df-82f8-0015f2db7bde)

FreeBSD : webkit-gtk2 -- Multiple vulnerabilities (06a12e26-142e-11e0-bea2-0015f2db7bde)

FreeBSD : webkit-gtk2 -- Multiple vulnerabilities (19419b3b-92bd-11df-b140-0015f2db7bde)

FreeBSD : webkit-gtk2 -- Multiple vulnerabilities (9bcfd7b6-bcda-11df-9a6a-0015f2db7bde)

FreeBSD : webkit-gtk2 -- Multiple vurnabilities. (35ecdcbe-3501-11e0-afcd-0015f2db7bde)

FreeBSD : webkit-gtk3 -- Multiple vulnerabilities (1cb0af4e-d641-4f99-9432-297a89447a97)

FreeBSD : webkit-gtk3 -- Multiple vulnerabilities (dc8cff4c-4063-11ea-8a94-3497f6939fdd)

FreeBSD : webkit2-gtk3 -- multiple vulnerabilities (0f66b901-715c-11e7-ad1f-bcaec565249c)

FreeBSD : webkit2-gtk3 -- multiple vulnerabilities (1ce95bc7-3278-11e8-b527-00012e582166) (Spectre)

FreeBSD : webkit2-gtk3 -- Multiple vulnerabilities (3dd46e05-9fb0-11e9-bf65-00012e582166)

FreeBSD : webkit2-gtk3 -- Multiple vulnerabilities (3e748551-c732-45f6-bd88-928da16f23a8)

FreeBSD : webkit2-gtk3 -- Multiple vulnerabilities (92243b6a-5775-4aea-8727-a938058df5ba)

FreeBSD : webkit2-gtk3 -- Multiple vulnerabilities (e45c3669-caf2-11e9-851a-dcf3aaa3f3ff)

FreeBSD : webmin (2132)

FreeBSD : webmin -- insecure temporary file creation at installation time (ae7b7f65-05c7-11d9-b45d-000c41e2cdad)

FreeBSD : webmin -- potential XSS attack via real name field (ec89dc70-2515-11e2-8eda-000a5e1e33c6)

FreeBSD : webmin -- unauthenticated remote code execution (ece65d3b-c20c-11e9-8af4-bcaec55be5e5)

FreeBSD : webmin -- XSS vulnerability (12b7286f-16a2-11dc-b803-0016179b2dd5)

FreeBSD : webmin, usermin -- arbitrary file disclosure vulnerability (227475c2-09cb-11db-9156-000e0c2e438a)

FreeBSD : websvn -- information disclosure (f69e1f09-e39b-11e5-9f77-5453ed2e2b49)

FreeBSD : websvn -- multiple vulnerabilities (71597e3e-f6b8-11dd-94d9-0030843d3802)

FreeBSD : websvn -- reflected XSS (12d1b5a6-e39d-11e5-9f77-5453ed2e2b49)

FreeBSD : weechat -- Arbitrary shell command execution via scripts (81826d12-317a-11e2-9186-406186f3d89d)

FreeBSD : weechat -- crash in logger plugin (b63421b6-a1e0-11e7-ac58-b499baebfeaf)

FreeBSD : weechat -- Crash or freeze when decoding IRC colors in strings (e02c572f-2af0-11e2-bb44-003067b2972c)

FreeBSD : weechat -- multiple vulnerabilities (81433129-2916-11e7-ad3e-00e04c1ea73d)

FreeBSD : WeeChat -- Multiple vulnerabilities (8e3f1812-54d9-11ea-8d49-d4c9ef517024)

FreeBSD : weex -- remote format string vulnerability (d4c70df5-335d-11da-9c70-0040f42d58c6)

FreeBSD : wemux -- read-only can be bypassed (777d7b9e-ab02-11e3-841e-60a44c524f57)

FreeBSD : wesnoth -- Code Injection vulnerability (bad59128-c188-11e8-9d40-f0def10dca57)

FreeBSD : wesnoth -- disclosure of .pbl files with lowercase, uppercase, and mixed-case extension (2a8b7d21-1ecc-11e5-a4a5-002590263bf5)

FreeBSD : Wesnoth -- Remote information disclosure (ba326a36-5f02-452d-a215-31e7b06d5edf)

FreeBSD : wget -- Access List Bypass / Race Condition (479c5b91-b6cc-11e6-a04e-3417eb99b9a0)

FreeBSD : wget -- cookie injection vulnerability (7b5a8e3b-52cc-11e8-8c7a-9c5c8e75236a)

FreeBSD : wget -- Heap overflow in HTTP protocol handling (d77ceb8c-bb13-11e7-8357-3065ec6f3643)

FreeBSD : wget -- HTTP to FTP redirection file name confusion vulnerability (6df56c60-3738-11e6-a671-60a44ce6887b)

FreeBSD : wget -- multiple HTTP client download filename vulnerability (d754b7d2-b6a7-11df-826c-e464a695cb21)

FreeBSD : wget -- multiple vulnerabilities (06f142ff-4df3-11d9-a9e7-0001020eed82)

FreeBSD : wget -- path traversal vulnerability in recursive FTP mode (ee7b4f9d-66c8-11e4-9ae1-e8e0b722a85e)

FreeBSD : wget -- security flaw in caching credentials passed as a part of the URL (a737eb11-5cfc-11e9-ab87-8cec4bf8fcfb)

FreeBSD : wget -- Stack overflow in HTTP protocol handling (09849e71-bb12-11e7-8357-3065ec6f3643)

FreeBSD : win32-codecs -- multiple vulnerabilities (24f6b1eb-43d5-11db-81e1-000e0c2e438a)

FreeBSD : wine -- information disclosure due to insecure temporary file handling (48a59c96-9c6e-11d9-a040-000a95bc6fae)

FreeBSD : wireshark -- denial of service in DRDA dissector (5415f1b3-f33d-11e1-8bd8-0022156e8794)

FreeBSD : wireshark -- DOCSIS dissector denial of service (28022228-5a0e-11df-942d-0015587e2cc1)

FreeBSD : Wireshark -- DoS in the BER-based dissectors (b2eaa7c2-e64a-11df-bc65-0022156e8794)

FreeBSD : wireshark -- LWRES vulnerability (bb0a8795-15dc-11df-bf0a-002170daae37)

FreeBSD : wireshark -- Multiple problems (7fadc049-2ba0-11dc-9377-0016179b2dd5)

FreeBSD : wireshark -- multiple security issues (4684a426-774d-4390-aa19-b8dd481c4c94)

FreeBSD : wireshark -- multiple security issues (4b228e69-22e1-4019-afd0-8aa716d0ec0b)

FreeBSD : wireshark -- multiple security issues (c5ab620f-4576-4ad5-b51f-93e4fec9cd0e)

FreeBSD : wireshark -- multiple vulnerabilities (313e9557-41e8-11e6-ab34-002590263bf5)

FreeBSD : Wireshark -- Multiple vulnerabilities (3ebb2dc8-4609-11e1-9f47-00e0815b8da8)

FreeBSD : wireshark -- multiple vulnerabilities (42c2c422-df55-11e5-b2bd-002590263bf5)

FreeBSD : wireshark -- multiple vulnerabilities (45117749-df55-11e5-b2bd-002590263bf5)

FreeBSD : Wireshark -- Multiple vulnerabilities (4cdfe875-e8d6-11e1-bea0-002354ed89bc)

FreeBSD : wireshark -- multiple vulnerabilities (610101ea-5b6a-11e6-b334-002590263bf5)

FreeBSD : wireshark -- multiple vulnerabilities (7e36c369-10c0-11e6-94fa-002590263bf5)

FreeBSD : wireshark -- multiple vulnerabilities (7fff2b16-b0ee-11e6-86b8-589cfc054129)

FreeBSD : wireshark -- multiple vulnerabilities (8a835235-ae84-11dc-a5f9-001a4d49522b)

FreeBSD : wireshark -- multiple vulnerabilities (9bdd8eb5-564a-11e5-9ad8-14dae9d210b8)

FreeBSD : wireshark -- multiple vulnerabilities (a13500d0-0570-11e5-aab1-d050996490d0)

FreeBSD : Wireshark -- Multiple Vulnerabilities (a7706414-1be7-11e2-9aad-902b343deec9)

FreeBSD : wireshark -- multiple vulnerabilities (defce068-39aa-11de-a493-001b77d09812)

FreeBSD : wireshark -- multiple vulnerabilities (f6f19735-9245-4918-8a60-87948ebb4907)

FreeBSD : wireshark -- Pcapng file parser crash (24e4d383-7b3e-11e5-a250-68b599b52a02)

FreeBSD : wireshark -- PCNFSD Dissector Denial of Service Vulnerability (a2d4a330-4d54-11de-8811-0030843d3802)

FreeBSD : wireshark -- SMTP Processing Denial of Service Vulnerability (baece347-c489-11dd-a721-0030843d3802)

FreeBSD : wolfssl -- DDoS amplification in DTLS (3d1372e1-7822-4fd8-b56e-5ee832afbd96)

FreeBSD : wolfssl -- leakage of private key information (331eabb3-85b1-466a-a2af-66ac864d395a)

FreeBSD : wordpress -- 2 XSS vulnerabilities (d86890da-f498-11e4-99aa-bcaec565249c)

FreeBSD : wordpress -- full path disclosure (e0b342a1-d2ae-11da-a672-000e0c2e438a)

FreeBSD : wordpress -- header rss feed script insertion vulnerability (622bc638-be27-11dd-a578-0030843d3802)

FreeBSD : wordpress -- multiple issues (15ee0e93-4bbb-11e9-9ba0-4c72b94353b5)

FreeBSD : wordpress -- multiple issues (459df1ba-051c-11ea-9673-4c72b94353b5)

FreeBSD : wordpress -- multiple issues (4740174c-82bb-11e8-a29a-00e04c1ea73d)

FreeBSD : wordpress -- multiple issues (4b98613c-0078-11e9-b05b-00e04c1ea73d)

FreeBSD : wordpress -- multiple issues (7b97b32e-27c4-11ea-9673-4c72b94353b5)

FreeBSD : wordpress -- multiple issues (8a9f86de-d080-11e9-9051-4c72b94353b5)

FreeBSD : wordpress -- multiple issues (a2589511-d6ba-11e7-88dd-00e04c1ea73d)

FreeBSD : wordpress -- multiple issues (a48d4478-e23f-4085-8ae4-6b3a7b6f016b)

FreeBSD : wordpress -- multiple issues (be38245e-44d9-11e8-a292-00e04c1ea73d)

FreeBSD : wordpress -- multiple issues (c04dc18f-fcde-11e7-bdf6-00e04c1ea73d)

FreeBSD : wordpress -- multiple issues (cee3d12f-bf41-11e7-bced-00e04c1ea73d)

FreeBSD : wordpress -- multiple unspecified privilege escalation bugs (30149157-f926-11e1-95cd-001fd0af1a4c)

FreeBSD : wordpress -- multiple vulnerabilities (043d3a78-f245-4938-9bc7-3d0d35dd94bf)

FreeBSD : wordpress -- multiple vulnerabilities (049332d2-f6e1-11e2-82f3-000c29ee3065)

FreeBSD : wordpress -- multiple vulnerabilities (0640198a-d117-11de-b667-0030843d3802)

FreeBSD : wordpress -- multiple vulnerabilities (14ea4458-e5cd-11e6-b56d-38d547003487)

FreeBSD : wordpress -- multiple vulnerabilities (3686917b-164d-11e6-94fa-002590263bf5)

FreeBSD : wordpress -- multiple vulnerabilities (505904d3-ea95-11e4-beaf-bcaec565249c)

FreeBSD : wordpress -- multiple vulnerabilities (54e50cd9-c1a8-11e6-ae1b-002590263bf5)

FreeBSD : wordpress -- multiple vulnerabilities (559e00b7-6a4d-11e2-b6b0-10bf48230856)

FreeBSD : wordpress -- multiple vulnerabilities (5e135178-8aeb-11e4-801f-0022156e8794)

FreeBSD : wordpress -- multiple vulnerabilities (82752070-0349-11e7-b48d-00e04c1ea73d)

FreeBSD : wordpress -- multiple vulnerabilities (a4955b32-ed84-11d9-8310-0001020eed82)

FreeBSD : Wordpress -- multiple vulnerabilities (a5bb7ea0-3e58-11e7-94a2-00e04c1ea73d)

FreeBSD : wordpress -- multiple vulnerabilities (b180d1fb-dac6-11e6-ae1b-002590263bf5)

FreeBSD : wordpress -- multiple vulnerabilities (b384cc5b-8d56-11e1-8d7b-003067b2972c)

FreeBSD : wordpress -- multiple vulnerabilities (bfcc23b6-3b27-11e6-8e82-002590263bf5)

FreeBSD : wordpress -- multiple vulnerabilities (dca0a345-ed81-11d9-8310-0001020eed82)

FreeBSD : wordpress -- multiple vulnerabilities (f4ce64c2-5bd4-11e5-9040-3c970e169bc2)

FreeBSD : wordpress -- multiple vulnerabilities (fef03980-e4c6-11e5-b2bd-002590263bf5)

FreeBSD : wordpress -- Multiple vulnerability (ac5ec8e3-3c6c-11e5-b921-00a0986f28c4)

FreeBSD : wordpress -- remote admin password reset vulnerability (2430e9c3-8741-11de-938e-003048590f9e)

FreeBSD : wordpress -- remote privilege escalation (884fced7-7f1c-11dd-a66a-0019666436c2)

FreeBSD : wordpress -- remote sql injection vulnerability (63347ee7-6841-11dc-82b6-02e0185f8d72)

FreeBSD : wordpress -- snoopy '\_httpsrequest()' shell command execution vulnerability (3a4a3e9c-a1fe-11dd-81be-001c2514716c)

FreeBSD : wordpress -- SQL injection vulnerability (8c93e997-30e0-11e0-b300-485d605f4717)

FreeBSD : wordpress -- unmoderated comments disclosure (6a31cbe3-1695-11dc-a197-0011098b2f36)

FreeBSD : wordpress -- XMLRPC SQL Injection (0838733d-1698-11dc-a197-0011098b2f36)

FreeBSD : wordpress -- XSS (a467d0f9-8875-11dc-b3ba-0016179b2dd5)

FreeBSD : wordpress -- XSS in administration panel (12b7b4cf-1d53-11d9-814e-0001020eed82)

FreeBSD : WordPress -- XSS vulnerability (810df820-3664-11e1-8fe3-00215c6a37bb)

FreeBSD : wordpress -- XSS vulnerability (ba4f9b19-ed9d-11e4-9118-bcaec565249c)

FreeBSD : wordpress -- XSS vulnerability (c80b27a2-3165-11e5-8a1d-14dae9d210b8)

FreeBSD : wordpress -- XSS vulnerability (fb754341-c3e2-11e5-b5fe-002590263bf5)

FreeBSD : WPA packet number reuse with replayed messages and key reinstallation (d670a953-b2a1-11e7-a633-009c02a2ab30) (KRACK)

FreeBSD : wpa\_supplicant -- P2P SSID processing vulnerability (cb9d2fcd-eb47-11e4-b03e-002590263bf5)

FreeBSD : wpa\_supplicant -- unauthenticated encrypted EAPOL-Key data (6bedc863-9fbe-11e8-945f-206a8a720317)

FreeBSD : wpa\_supplicant -- WPS\_NFC option payload length validation vulnerability (c93c9395-25e1-11e5-a4a5-002590263bf5)

FreeBSD : wu-ftpd -- remote globbing DoS vulnerability (ef410571-a541-11d9-a788-0001020eed82)

FreeBSD : wu-ftpd ftpaccess `restricted-uid'/`restricted-gid' directive may be bypassed (3b7c7f6c-7102-11d8-873f-0020ed76ef5a)

FreeBSD : wv (1892)

FreeBSD : wv -- Multiple Integer Overflow Vulnerabilities (d29dc506-8aa6-11db-bd0d-00123ffe8333)

FreeBSD : wv2 -- Integer Overflow Vulnerability (b9044cc2-8aa5-11db-bd0d-00123ffe8333)

FreeBSD : www/chromium -- multiple vulnerabilities (2092a45b-e2f6-11e1-a8ca-00262d5ed8ee)

FreeBSD : www/chromium -- multiple vulnerabilities (36a415c8-3867-11e4-b522-00262d5ed8ee)

FreeBSD : www/chromium -- multiple vulnerabilities (a70966a1-ac22-11e3-8d04-00262d5ed8ee)

FreeBSD : www/chromium -- multiple vulnerabilities (d46ed7b8-1912-11e5-9fdf-00262d5ed8ee)

FreeBSD : www/chromium --multiple vulnerabilities (24cefa4b-a940-11e3-91f2-00262d5ed8ee)

FreeBSD : www/mod\_dav\_svn -- Malicious SVN clients can crash mod\_dav\_svn. (4af3241d-1f0c-11e9-b4bd-d43d7eed0ce2)

FreeBSD : www/mod\_security -- NULL pointer dereference DoS (9dfb63b8-8f36-11e2-b34d-000c2957946c)

FreeBSD : www/py-bleach -- multiple vulnerabilities (3d19c776-68e7-11ea-91db-0050562a4d7b)

FreeBSD : www/py-requests -- Information disclosure vulnerability (50ad9a9a-1e28-11e9-98d7-0050562a4d7b)

FreeBSD : www/varnish6 -- Denial of Service (ce231189-ce56-11e9-9fa0-0050569f0b83)

FreeBSD : wzdftpd -- remote DoS (e0070221-2dd8-11d9-a9e7-0001020eed82)

FreeBSD : X.org libraries -- multiple vulnerabilities (1cf65085-a760-41d2-9251-943e1af62eb8)

FreeBSD : X11 server -- pixmap allocation vulnerability (a863aa74-24be-11da-8882-000e0c33c2dc)

FreeBSD : X11 Session -- SDDM allows unauthorised unlocking (f00acdec-b59f-11e8-805d-001e2a3f778d)

FreeBSD : x11vnc -- authentication bypass vulnerability (9dda3ff1-2b02-11db-a6e2-000e0c2e438a)

FreeBSD : xapian-omega -- XSS vulnerability (b46f3a1e-a052-11de-a649-000c2955660f)

FreeBSD : xchat remotely exploitable buffer overflow (Socks5) (8338a20f-9573-11d8-9366-0020ed76ef5a)

FreeBSD : xdelta3 -- buffer overflow vulnerability (f1bf28c5-d447-11e5-b2bd-002590263bf5)

FreeBSD : xdm -- remote denial of service (d905b219-c1ca-11e9-8c46-0c9d925bbbc0)

FreeBSD : xen-kernel -- arm: vgic-v2: GICD\_SGIR is not properly emulated (785c86b1-27d6-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- arm: vgic: incorrect rate limiting of guest triggered logging (912cb7f7-27df-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- broken check in memory\_exchange() permits PV guest breakout (90becf7c-1acf-11e7-970f-002590263bf5)

FreeBSD : xen-kernel -- Certain domctl operations may be abused to lock up the host (103a47d5-27e7-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- CPU lockup during exception delivery (2cabfbab-8bfb-11e5-bd18-002590263bf5)

FreeBSD : xen-kernel -- CR0.TS and CR0.EM not always honored for x86 HVM guests (4d7cf654-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- GNTTABOP\_swap\_grant\_ref operation misbehavior (80e846ff-27eb-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- guest 32-bit ELF symbol table load leaking host data (5555120d-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- Hypervisor memory corruption due to x86 emulator flaw (83a28417-27e3-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- information leak in legacy x86 FPU/XMM initialization (e839ca04-b40d-11e5-9728-002590263bf5)

FreeBSD : xen-kernel -- Information leak through version information hypercall (ef9d041e-27e2-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- Information leak through XEN\_DOMCTL\_gettscinfo (ce658051-27ea-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- Information leak via internal x86 system device emulation (5023f559-27e2-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- ioreq handling possibly susceptible to multiple read issue (6aa2d135-b40e-11e5-9728-002590263bf5)

FreeBSD : xen-kernel -- leak of main per-domain vcpu pointer array (fc1f8795-881d-11e5-ab94-002590263bf5)

FreeBSD : xen-kernel -- leak of per-domain profiling-related vcpu pointer array (e3792855-881f-11e5-ab94-002590263bf5)

FreeBSD : xen-kernel -- Long latency populate-on-demand operation is not preemptible (83350009-881e-11e5-ab94-002590263bf5)

FreeBSD : xen-kernel -- multiple vulnerabilities (da70d472-af59-11e7-ace2-f8b156b439c5)

FreeBSD : xen-kernel -- PV superpage functionality missing sanity checks (7ed7c36f-ddaf-11e5-b2bd-002590263bf5)

FreeBSD : xen-kernel -- some pmu and profiling hypercalls log without rate limiting (e4848ca4-8820-11e5-ab94-002590263bf5)

FreeBSD : xen-kernel -- Uncontrolled creation of large page mappings by PV guests (3d9f6260-881d-11e5-ab94-002590263bf5)

FreeBSD : xen-kernel -- use after free in FIFO event channel code (4bf57137-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- VMX: guest user mode may crash guest with non-canonical RIP (81f9d6a4-ddaf-11e5-b2bd-002590263bf5)

FreeBSD : xen-kernel -- VMX: intercept issue with INVLPG on non-canonical address (80adc394-ddaf-11e5-b2bd-002590263bf5)

FreeBSD : xen-kernel -- vulnerability in the iret hypercall handler (8c31b288-27ec-11e5-a4a5-002590263bf5)

FreeBSD : xen-kernel -- x86 64-bit bit test instruction emulation broken (56f0f11e-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86 CMPXCHG8B emulation fails to ignore operand size override (80a897a2-c1a6-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86 HVM: Overflow of sh\_ctxt->seg\_reg[] (4aae54be-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86 null segments not always treated as unusable (50ac2e96-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86 PV guests may be able to mask interrupts (3ae078ca-c7eb-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86 segment base write emulation lacking canonical address checks (53dbd096-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86 shadow pagetables: address width overflow (d51ced72-4212-11e6-942d-bc5ff45d0f28)

FreeBSD : xen-kernel -- x86 software guest page walk PS bit handling flaw (e43b210a-4212-11e6-942d-bc5ff45d0f28)

FreeBSD : xen-kernel -- x86 task switch to VM86 mode mis-handled (523bb0b7-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86: Disallow L3 recursive pagetable for 32-bit PV guests (45ca25b5-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86: Mishandling of instruction pointer truncation during emulation (49211361-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86: Mishandling of SYSCALL singlestep during emulation (942433db-c661-11e6-ae1b-002590263bf5)

FreeBSD : xen-kernel -- x86: Missing SMAP whitelisting in 32-bit exception / event delivery (04cf89e3-5854-11e6-b334-002590263bf5)

FreeBSD : xen-kernel -- x86: Privilege escalation in PV guests (032aa524-5854-11e6-b334-002590263bf5) (Bunker Buster)

FreeBSD : xen-kernel -- XENMEM\_exchange error handling issues (bcad3faa-b40c-11e5-9728-002590263bf5)

FreeBSD : xen-kernel and xen-tools -- Long latency MMIO mapping operations are not preemptible (d40c66cb-27e4-11e5-a4a5-002590263bf5)

FreeBSD : xen-tools -- Cirrus VGA Heap overflow via display refresh (af19ecd0-0f6a-11e7-970f-002590263bf5)

FreeBSD : xen-tools -- cirrus\_bitblt\_cputovideo does not check if memory region is safe (8cbd9c08-f8b9-11e6-ae1b-002590263bf5)

FreeBSD : xen-tools -- delimiter injection vulnerabilities in pygrub (59f79c99-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-tools -- Guest triggerable qemu MSI-X pass-through error messages (cbe1a0f9-27e9-11e5-a4a5-002590263bf5)

FreeBSD : xen-tools -- HVM qemu unexpectedly enabling emulated VGA graphics backends (0d732fd1-27e0-11e5-a4a5-002590263bf5)

FreeBSD : xen-tools -- libxl fails to honour readonly flag on disks with qemu-xen (301b04d7-881c-11e5-ab94-002590263bf5)

FreeBSD : xen-tools -- libxl leak of pv kernel and initrd on error (5d1d4473-b40d-11e5-9728-002590263bf5)

FreeBSD : xen-tools -- oob access in cirrus bitblt copy (a73aba9a-effe-11e6-ae1b-002590263bf5)

FreeBSD : xen-tools -- PCI MSI mask bits inadvertently exposed to guests (4db8a0f4-27e9-11e5-a4a5-002590263bf5)

FreeBSD : xen-tools -- populate-on-demand balloon size inaccuracy can crash guests (c0e76d33-8821-11e5-ab94-002590263bf5)

FreeBSD : xen-tools -- Potential unintended writes to host MSI message data field via qemu (af38cfec-27e7-11e5-a4a5-002590263bf5)

FreeBSD : xen-tools -- qemu incautious about shared ring processing (58685e23-ba4d-11e6-ae1b-002590263bf5)

FreeBSD : xen-tools -- QEMU: Banked access to VGA memory (VBE) uses inconsistent bounds checks (e6ce6f50-4212-11e6-942d-bc5ff45d0f28)

FreeBSD : xen-tools -- Unmediated PCI command register access in qemu (79f401cd-27e6-11e5-a4a5-002590263bf5)

FreeBSD : xen-tools -- Unmediated PCI register access in qemu (3d657340-27ea-11e5-a4a5-002590263bf5)

FreeBSD : xen-tools -- Unrestricted qemu logging (e800cd4b-4212-11e6-942d-bc5ff45d0f28)

FreeBSD : xen-tools -- Unsanitised driver domain input in libxl device handling (e589ae90-4212-11e6-942d-bc5ff45d0f28)

FreeBSD : xen-tools -- Unsanitised guest input in libxl device handling code (e2fca11b-4212-11e6-942d-bc5ff45d0f28)

FreeBSD : xen-tools -- virtio: unbounded memory allocation issue (06574c62-5854-11e6-b334-002590263bf5)

FreeBSD : xen-tools -- xenstore denial of service via repeated update (47873d72-14eb-11e7-970f-002590263bf5)

FreeBSD : xen-tools -- xl command line config handling stack overflow (f1deed23-27ec-11e5-a4a5-002590263bf5)

FreeBSD : xerces-c2 -- Attribute blowup denial-of-service (76301302-1d59-11d9-814e-0001020eed82)

FreeBSD : xerces-c3 -- Parser Crashes on Malformed Input (a7f2e9c6-de20-11e5-8458-6cc21735f730)

FreeBSD : xercesi-c3 -- multiple vulnerabilities (cb09a7aa-5344-11e6-a7bd-14dae9d210b8)

FreeBSD : xfce -- multiple vulnerabilities (024edd06-c933-11dc-810c-0016179b2dd5)

FreeBSD : XFree86 opens a chooserFd TCP socket even when DisplayManager.requestPort is 0 (ff00f2ce-c54c-11d8-b708-00061bc2ad93)

FreeBSD : xfs -- multiple vulnerabilities (a5f667db-7596-11dc-8b7a-0019b944b34e)

FreeBSD : xine -- multiple remote string vulnerabilities (8d4ae57d-d2ab-11da-a672-000e0c2e438a)

FreeBSD : xine-lib arbitrary file overwrite (e50b04e8-9c55-11d8-9366-0020ed76ef5a)

FreeBSD : xinetd -- attackers can bypass access restrictions if tcpmux-servers service enabled (e11955ca-187c-11e2-be36-00215af774f0)

FreeBSD : xinetd -- ignores user and group directives for TCPMUX services (5c34664f-2c2b-11e3-87c2-00215af774f0)

FreeBSD : xli -- integer overflows in image size calculations (bfbbd505-3bd6-409c-8c67-445d3635cf4b)

FreeBSD : xloadimage -- arbitrary command execution when handling compressed files (310d0087-0fde-4929-a41f-96f17c5adffe)

FreeBSD : xloadimage -- buffer overflow in FACES image handling (8c1da77d-d3e9-11d9-8ffb-00061bc2ad93)

FreeBSD : xloadimage -- buffer overflows in NIFF image title handling (2f0cb4bb-416d-11da-99fe-000854d03344)

FreeBSD : xlockmore -- local exploit (57652765-18aa-11e2-8382-00a0d181e71d)

FreeBSD : xml-security-c -- crashes on malformed KeyInfo content (5786185a-9a43-11e8-b34b-6cc21735f730)

FreeBSD : xmms -- Integer Overflow And Underflow Vulnerabilities (20e23b65-a52e-11e3-ae3a-00224d7c32a2)

FreeBSD : xorg -- multiple vulnerabilities (800e8bd5-3acb-11dd-8842-001302a18722)

FreeBSD : xorg -- multiple vulnerabilities (fe2b6597-c9a4-11dc-8da8-0008a18a9961)

FreeBSD : xorg -- protocol handling issues in X Window System client libraries (2eebebff-cd3b-11e2-8f09-001b38c3836c)

FreeBSD : Xorg server -- two vulnerabilities in X server lock handling code (8441957c-f9b4-11e0-a78a-bcaec565249c)

FreeBSD : xorg-server -- Information leak in the XkbSetGeometry request of X servers. (54a69cf7-b2ef-11e4-b1f1-bcaec565249c)

FreeBSD : xorg-server -- Multiple Issues (ab881a74-c016-4e6d-9f7d-68c8e7cedafb)

FreeBSD : xorg-server -- multiple vulnabilities (4f8ffb9c-f388-4fbd-b90f-b3131559d888)

FreeBSD : xorg-server -- multiple vulnabilities (7274e0cc-575f-41bc-8619-14a41b3c2ad0)

FreeBSD : xorg-server -- privilege escalation (61534682-b8f4-11da-8e62-000e0c33c2dc)

FreeBSD : xorg-server -- use-after-free (9a57c607-3cab-11e3-b4d9-bcaec565249c)

FreeBSD : xpcd -- buffer overflow (d337b206-200f-11dc-a197-0011098b2f36)

FreeBSD : xpdf -- buffer overflow vulnerability (e3e266e9-5473-11d9-a9e7-0001020eed82)

FreeBSD : xpdf -- disk fill DoS vulnerability (24eee285-09c7-11da-bc08-0001020eed82)

FreeBSD : xpdf -- integer overflow vulnerabilities (ad2f3337-26bf-11d9-9289-000c41e2cdad)

FreeBSD : xpdf -- makeFileKey2() buffer overflow vulnerability (f755545e-6fcd-11d9-abec-00061bd2d56f)

FreeBSD : xpdf -- multiple remote Stream.CC vulnerabilities (2747fc39-915b-11dc-9239-001c2514716c)

FreeBSD : Xpdf -- Multiple Vulnerabilities (791e8f79-e7d1-11e9-8b31-206a8a720317)

FreeBSD : Xpdf -- Multiple Vulnerabilities (8581189c-bd5f-11de-8709-0017a4cccfc6)

FreeBSD : xpdf -- multiple vulnerabilities (a21037d5-2c38-11de-ab3b-0017a4cccfc6)

FreeBSD : xpdf -- stack based buffer overflow (0e43a14d-3f3f-11dc-a79a-0016179b2dd5)

FreeBSD : xpm -- image decoding vulnerabilities (ef253f8b-0727-11d9-b45d-000c41e2cdad)

FreeBSD : xrdb -- root hole via rogue hostname (2eccb24f-61c0-11e0-b199-0015f2db7bde)

FreeBSD : xrdp -- local user can cause a denial of service (a66f9be2-d519-11e7-9866-c85b763a2f96)

FreeBSD : xscreensaver - lock bypass (4b9393b8-7c0c-11e5-a010-080027ddead3)

FreeBSD : xserver -- multiple issue with X client request handling (27b9b2f0-8081-11e4-b4ca-bcaec565249c)

FreeBSD : xshisen -- local buffer overflows (56971fa6-641c-11d9-a097-000854d03344)

FreeBSD : XSS issue in MantisBT (a83f25df-d775-11e0-8bf1-003067b2972c)

FreeBSD : xterm -- DECRQSS remote command execution vulnerability (d5e1aac8-db0b-11dd-ae30-001cc0377035)

FreeBSD : xtrlock -- X display locking bypass (f7e8d2ca-410e-40b2-8748-3abd021e44a9)

FreeBSD : xv (1551)

FreeBSD : xv -- exploitable buffer overflows (fffacc93-16cb-11d9-bc4a-000c41e2cdad)

FreeBSD : xv -- filename handling format string vulnerability (a4bd3039-9a48-11d9-a256-0001020eed82)

FreeBSD : xview -- multiple buffer overflows in xv\_parse\_one (ae6ec9b8-2f43-4d02-8129-c6a3a53ef09d)

FreeBSD : Xymon -- buffer overrun (1c7cfd05-aaee-11e4-83b4-14dae9d210b8)

FreeBSD : xymon-server -- multiple vulnerabilities (10e1d580-d174-11e9-a87f-a4badb2f4699)

FreeBSD : xymon-server -- multiple vulnerabilities (1cecd5e0-c372-11e5-96d6-14dae9d210b8)

FreeBSD : yamt -- arbitrary command execution vulnerability (d4a7054a-6d96-11d9-a9e7-0001020eed82)

FreeBSD : yamt -- buffer overflow and directory traversal issues (99b5cfa5-d3d2-11d9-8ffb-00061bc2ad93)

FreeBSD : yii -- Remote arbitrary PHP code execution (5a35bc56-7027-11e4-a4a3-001999f8d30b)

FreeBSD : YUI JavaScript library -- JavaScript injection exploits in Flash components (aa4f86af-3172-11e2-ad21-20cf30e32f6d)

FreeBSD : YUI JavaScript library -- JavaScript injection exploits in Flash components (d560b346-08a2-11e0-bcca-0050568452ac)

FreeBSD : zabbix -- php frontend multiple vulnerabilities (03140526-1250-11de-a964-0030843d3802)

FreeBSD : Zabbix -- Remote code execution (5df8bd95-8290-11e7-93af-005056925db4)

FreeBSD : zabbix -- shell command injection vulnerability (44d0f8dc-6607-11e3-bb11-0025900931f8)

FreeBSD : zabbix-frontend -- multiple XSS vulnerabilities (048c77df-3211-11e1-9583-14dae938ec40)

FreeBSD : zebra/quagga denial of service vulnerability (cad045c0-81a5-11d8-9645-0020ed76ef5a)

FreeBSD : zeek -- potential denial of service issues (4ae135f7-85cd-4c32-ad94-358271b31f7f)

FreeBSD : zeek -- Remote crash vulnerability (f59c4c53-c55f-43fe-9920-82b9d1ea9c3d)

FreeBSD : Zend Framework -- Local File Inclusion vulnerability in Zend\_View::render() (cf495fd4-fdcd-11dd-9a86-0050568452ac)

FreeBSD : Zend Framework -- multiple vulnerabilities (c9263916-006f-11df-94cb-0050568452ac)

FreeBSD : Zend Framework -- Multiple vulnerabilities via XXE injection (ec34d0c2-1799-11e2-b4ab-000c29033c32)

FreeBSD : Zend Framework -- potential SQL injection when using PDO\_MySql (34e8ccf5-7d71-11e0-9d83-000c29cc39d3)

FreeBSD : Zend Framework -- security issues in bundled Dojo library (8ad1c404-3e78-11df-a5a1-0050568452ac)

FreeBSD : ZendFramework1 -- SQL injection vulnerability (d3324fdb-6bf0-11e5-bc5e-00505699053e)

FreeBSD : zenphoto -- multiple vulnerabilities (5c399624-2bef-11e5-86ff-14dae9d210b8)

FreeBSD : zenphoto -- XSS vulnerability (1a818749-d646-11dc-8959-000bcdc1757a)

FreeBSD : zgv -- exploitable heap overflows (249a8c42-6973-11d9-ae49-000c41e2cdad)

FreeBSD : zgv, xzgv -- heap overflow vulnerability (a813a219-d2d4-11da-a672-000e0c2e438a)

FreeBSD : zhcon -- unauthorized file access (d371b627-6ed5-11d9-bd18-000a95bc6fae)

FreeBSD : zinf -- potential buffer overflow playlist support (30cf9485-1c2c-11d9-9ecb-000c6e8f12ef)

FreeBSD : zip -- long path buffer overflow (40549bbf-43b5-11d9-a9e7-0001020eed82)

FreeBSD : ziproxy -- atypical huge picture files vulnerability (b43004b8-6a53-11df-bc7b-0245fb008c0b)

FreeBSD : ziproxy -- multiple vulnerability (872ae5be-29c0-11de-bdeb-0030843d3802)

FreeBSD : ziproxy -- security vulnerability in PNG decoder (25673e6e-786b-11df-a921-0245fb008c0b)

FreeBSD : zlib -- buffer overflow vulnerability (837b9fb2-0595-11da-86bc-000e0c2e438a)

FreeBSD : zlib -- buffer overflow vulnerability (8efe93e2-ee62-11d9-8310-0001020eed82)

FreeBSD : znc -- Denial of Service (b22d6d4c-53b9-11e9-9310-28d244aee256)

FreeBSD : znc -- multiple vulnerabilities (c6d1a8a6-8a91-11e8-be4d-005056925db4)

FreeBSD : znc -- NULL pointer dereference in webadmin module (19751e06-c798-11e2-a373-000c29833058)

FreeBSD : znc -- privilege escalation (6f15730d-94ea-11e9-a83e-641c67a117d8)

FreeBSD : zoo -- stack based buffer overflow (d9307a41-c4d7-11da-b2fb-000e0c2e438a)

FreeBSD : zookeeper -- Denial Of Service (af61b271-9e47-4db0-a0f6-29fb032236a3)

FreeBSD : zope -- expose RestructuredText functionality to untrusted users (d2b80c7c-3aae-11da-9484-00123ffe8333)

FreeBSD : zope -- information disclosure vulnerability (5f2a0c40-1322-11db-bd23-000475abc56f)

FreeBSD : zope -- restructuredText 'csv\_table' Information Disclosure (65a8f773-4a37-11db-a4cc-000a48049292)

FreeBSD : zope -- XSS vulnerability (34414a1e-e377-11db-b8ab-000c76189c4c)

FreeBSD : zziplib - multiple vulnerabilities (7764b219-8148-11e8-aa4d-000e0cd7b374)

FreeBSD < 10 qls\_eioctl function Unauthorized Disclosure of Information

FreeBSD < 10.3-RELEASE-p19 / 11.0 < 11.0-RELEASE-p10 ipfilter Kernel Module Packet Fragment DoS (FreeBSD-SA-17:04.ipfilter)

FreeBSD < 10.3-RELEASE-p21 / 11.0 < 11.0-RELEASE-p12 / 11.1 < 11.1-RELEASE-p1 OpenSSH Password Length DoS (FreeBSD-SA-17:06.openssh)

FreeBSD < 11.2-RELEASE-p5 Multiple vulnerabilities in NFS server code (FreeBSD-SA-18:03.nfs)

FreeBSD Ports : FreeRADIUS < 1.0.1

# Firewalls

3Proxy HTTP Proxy Crafted Transparent Request Remote Overflow

602LAN SUITE Open Telnet Proxy

AnalogX Proxy SOCKS4a DNS Hostname Handling Remote Overflow

Arkoon Appliance Detection

Axent Raptor Firewall Zero Length IP Remote DoS

BenHur Firewall Source Port 20 ACL Restriction Bypass

Blue Coat ProxySG 4.x OpenSSL Security Bypass

Blue Coat ProxySG 6.2.x < 6.2.16.4 / 6.5.x < 6.5.7.5 / 6.6.x < 6.6.2.1 Multiple OpenSSL Vulnerabilities

Blue Coat ProxySG 6.2.x OpenSSL Security Bypass

Blue Coat ProxySG 6.4.x OpenSSL Security Bypass

Blue Coat ProxySG 6.5.x / 6.2.x / 5.5 OpenSSL Vulnerability (FREAK)

Blue Coat ProxySG 6.5.x < 6.5.9.8 / 6.6.x < 6.6.4.1 Multiple OpenSSL Vulnerabilities

Blue Coat ProxySG 6.5.x Multiple OpenSSL Vulnerabilities

Blue Coat ProxySG Console Management Detection

Blue Coat ProxySG Core File Information Disclosure

Blue Coat ProxySG Heartbeat Information Disclosure (Heartbleed)

Blue Coat ProxySG Local User Modification Race Condition

Blue Coat ProxySG Recursive HTTP Pipeline Pre-Fetch Remote DoS

Blue Coat ProxySG Unspecified XSS

CCProxy Application Proxy Detection

Cerbere HTTP Proxy Server Host: Header Remote DoS

Check Point FireWall-1 4.x Multiple Vulnerabilities (OF, FS)

Check Point FireWall-1 HTTP Client Authentication Detection

Check Point FireWall-1 ICA Service Detection

Check Point FireWall-1 Identification

Check Point FireWall-1 Open Web Administration

Check Point FireWall-1 Spoofed UDP Packet Remote DoS

Check Point FireWall-1 Telnet Client Authentication Detection

Check Point FireWall-1 UDP Port 0 DoS

Check Point FireWall-1/VPN-1 Syslog Daemon Remote Overflow DoS

Check Point Gaia Operating Bash Code Injection (sk102673)(SHELLSHOCK)

Check Point Gaia Operating Remote Heap Buffer Overflow (sk104443)(GHOST)

Check Point Gaia Operating Security and Stability Update (sk100431)

Check Point Gaia Operating System < R77.20 Multiple NTP Client Vulnerabilities (sk103825)

Check Point Gaia Operating System Administrator password truncation (sk155172)

Check Point Gaia Operating System Administrator password truncation (sk156192)

Check Point Gaia Operating System Detection

Check Point Gaia Operating System DoS (sk115596)

Check Point Gaia Operating System HTTP evasion protection failure (sk98814)

Check Point Gaia Operating System Malicious URL Detection issue (sk111740)

Check Point Gaia Operating System Multiple Vulnerabilities (sk106499)

Check Point Gaia Operating System Open Interfaces With Default Password (sk145612)

Check Point Gaia Operating System Privilege Escalation

Check Point Gaia Operating System SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (sk103683) (POODLE)

Check Point Gaia Operating System Threat Emulation Email Scan Bypass (sk96269)

Check Point Gaia Operating System VM escape and code execution (sk106060)(VENOM)

Check Point Local Privilege Escalation

Check Point SecuRemote Hostname Information Disclosure

Check Point Security Gateway Denial of Service (sk161812)

Checkpoint Gaia Portal WebUI Detection

Cisco ASA 5500 Series Adaptive Security Appliance NTLMv1 Authentication Bypass (cisco-sa-20100217-asa)

Cisco PIX Firewall Mailguard Feature SMTP Content Filter Bypass

Default Password (zebra) for Zebra

DeleGate < 8.11 Multiple Unspecified Overflows

DeleGate DNS Response Message DoS

DeleGate Multiple Function Remote Overflows

DeleGate Proxy Server < 9.7.5 Multiple Vulnerabilities

Finjan SurfinGate Proxy FHTTP Command Admin Functions Authentication Bypass

FireEye Operating System Detection

FireEye Operating System Multiple Vulnerabilities

FireEye Operating System Multiple Vulnerabilities (AX < 7.7.7 / EX < 8.0.1)

FireEye Operating System Multiple Vulnerabilities (SB001)

Firewall Detection

Firewall Detection (2) (deprecated)

Firewall Rule Enumeration

Firewall UDP Packet Source Port 53 Ruleset Bypass

Fortinet Device Detection

Fortinet FortiGate 5.2.0 < 5.6.11 / 6.0.x < 6.0.5 Cross-Site Scripting (FG-IR-19-034)

Fortinet FortiGate 5.2.x >= 5.2.12 / 5.4.6 - 5.4.7 / 5.6.1 - 5.6.3 Information Disclosure (FG-IR-18-325)

Fortinet FortiGate 5.x < 5.6.6 / 6.x < 6.0.2 Private IP and Hostname Information Disclosure (FG-IR-18-085)

Fortinet FortiGate < 5.2 / 5.2.x <= 5.2.11 / 5.4.x <= 5.4.5 / 5.6.x <= 5.6.2 Multiple Vulnerabilities (FG-IR-17-196) (KRACK)

Fortinet FortiGate < 5.4.11 / 5.6.x < 5.6.8 / 6.x < 6.0.3 RCE (FG-IR-18-230)

Fortinet FortiGate < 5.6.6 / 6.0.x < 6.0.1 Plain Text Credentials (FG-IR-18-027)

Fortinet FortiGate < 5.6.8 / 6.x < 6.0.3 LDAP Credential Disclosure (FG-IR-18-157)

Fortinet FortiGate < 6.2.1 Information Disclosure (FG-IR-19-037)

Fortinet FortiGate <= 5.2.x / 5.4.x < 5.4.9 / 5.6.x < 5.6.3 Multiple Vulnerabilities (FG-IR-17-231, FG-IR-17-245 and FG-IR-17-172)

Fortinet FortiGate <= 5.4.x / 5.6.x < 5.6.11 / 6.x < 6.2.0 Admin Privilege Escalation (FG-IR-17-053)

Fortinet FortiManager 5.0.x < 5.0.11 / 5.2.x < 5.2.2 Multiple Vulnerabilities (FG-IR-15-011)

Fortinet FortiManager < 6.0.2 Information Disclosure Vulnerability (FG-IR-18-016)

Fortinet FortiManager Unencrypted Password Vulnerability (FG-IR-18-051)

Fortinet FortiOS 4.1.x < 4.1.11 / 4.2.x < 4.2.13 / 4.3.x < 4.3.9 Web Interface Cookie Parser RCE (EGREGIOUSBLUNDER)

Fortinet FortiOS 4.3.x < 4.3.19 TLS and IPSEC Information Disclosure

Fortinet FortiOS 5.0.x / 5.2.x < 5.2.11 'global-label' Parameter XSS (FG-IR-17-057)

Fortinet FortiOS 5.0.x < 5.0.1 Multiple DoS

Fortinet FortiOS 5.0.x < 5.0.12 / 5.2.x < 5.2.4 Weak Ciphers (FG-IR-15-021)

Fortinet FortiOS 5.0.x < 5.0.2 Multiple Vulnerabilities

Fortinet FortiOS 5.0.x < 5.0.4 Empty Device Group Firewall Bypass

Fortinet FortiOS 5.0.x < 5.0.5 FortiToken Security Bypass

Fortinet FortiOS 5.0.x < 5.0.8 Packet Handling DoS

Fortinet FortiOS 5.0.x < 5.0.9 Telnet / SSH Username XSS

Fortinet FortiOS 5.2.3 ZebOS Shell Remote Command Execution (FG-IR-15-020)

Fortinet FortiOS 5.2.x / 5.3.x / 5.4.x < 5.4.5 Multiple XSS (FG-IR-17-127)

Fortinet FortiOS 5.2.x < 5.2.10 / 5.4.1 < 5.4.2 Local Password Hash Disclosure (FG-IR-16-050)

Fortinet FortiOS 5.2.x < 5.2.11 srcintf XSS (FG-IR-17-017)

Fortinet FortiOS 5.2.x < 5.2.12 / 5.4.x < 5.4.6 / 5.6.x < 5.6.1 Multiple Vulnerabilities (FG-IR-17-104)

Fortinet FortiOS 5.2.x < 5.2.23 / 5.4.x < 5.4.6 / 5.6.x < 5.6.1 Web Proxy Disclaimer Response Page Reflected XSS (FG-IR-17-168)

Fortinet FortiOS 5.2.x < 5.2.3 Multiple XSS

Fortinet FortiOS 5.2.x < 5.2.6 ICMP Redirect Response DoS

Fortinet FortiOS 5.4.1 < 5.4.11 / 5.6.x < 5.6.9 / 6.0.x < 6.0.5 SSL VPN Security Bypass (FG-IR-18-389)

Fortinet FortiOS 5.4.1 < 5.4.4 Multiple Vulnerabilities

Fortinet FortiOS 5.4.6 <= 5.4.12 / 5.6.3 < 5.6.8 / 6.0.x < 6.0.5 SSL VPN Directory Traversal (FG-IR-18-384)

Fortinet FortiOS 5.4.x < 5.4.6 / 5.6.x < 5.6.1 XSS (CVE-2017-3131)

Fortinet FortiOS 5.4.x < 5.4.6 / 5.6.x < 5.6.1 XSS (FG-IR-17-113)

Fortinet FortiOS 5.4.x < 5.4.6 Denial of Service (FG-IR-17-206)

Fortinet FortiOS 5.6.0 < 5.6.8 / 6.0.x < 6.0.5 multiple pre-auth XSS vulnerabilities on SSL VPN (FG-IR-18-383)

Fortinet FortiOS 5.6.0 Remote Code Execution (FG-IR-18-018)

Fortinet FortiOS 5.x < 5.0.3 Security Bypass

Fortinet FortiOS 5.x < 5.0.6 XSS

Fortinet FortiOS 5.x < 5.4.2 Flow-mode Detection Bypass

Fortinet FortiOS 5.x < 5.4.8 / 5.6.x < 5.6.3 HTTP Host Header XSS(FG-IR-17-262)

Fortinet FortiOS 5.x >= 5.4.0 / 6.x < 6.0.9 / 6.2.x < 6.2.2 URL Redirection Vulnerability (FG-IR-19-179)

Fortinet FortiOS < 4.3.13 / 5.0.3 Multiple XSRF

Fortinet FortiOS < 4.3.13 SSL-VPN TLS MAC Spoofing

Fortinet FortiOS < 4.3.16 / 5.x < 5.0.8 Multiple Vulnerabilities (FG-IR-14-006)

Fortinet FortiOS < 5.2 / 5.4.x < 5.4.6 / 5.6.x < 5.6.1 SSL / TLS Renegotiation Handshakes MitM Plaintext Data Injection (FG-IR-17-137)

Fortinet FortiOS < 5.2.15, 5.4.0 < 6.0.5 SSL VPN web portal Host Header Redirection (FG-IR-19-002)

Fortinet FortiOS < 5.6.10 / 6.0 < 6.0.7 / 6.2.x < 6.2.1 Vulnerable Encryption (FG-IR-19-007)

Fortinet FortiOS < 5.6.11 / 6.0.0 < 6.0.7 / 6.2.0 < 6.2.2 Information Disclosure (FG-IR-19-134)

Fortinet FortiOS < 5.6.11, 6.0.x < 6.0.5 SSL VPN Heap Buffer Overflow (FG-IR-18-388)

Fortinet FortiOS < 6.0.7 / 6.2.x < 6.2.2 Multiple Vulnerabilities (FG-IR-19-184, FG-IR-19-236)

Fortinet FortiOS < 6.0.7 Information Disclosure MitM (FG-IR-18-100)

Fortinet FortiOS < 6.2.3 Multiple Vulnerabilities (FG-IR-19-217)

Fortinet FortiOS <= 5.4 / 5.6.x < 5.6.8 / 6.0.x < 6.0.5 SSL VPN Web Portal login redir XSS (FG-IR-17-242)

Fortinet FortiOS <= 5.4, 5.6.x < 5.6.8, 6.0.x < 6.0.5 SSL VPN Buffer Overflow (FG-IR-18-387)

Fortinet FortiOS Redirect Parameter Multiple Vulnerabilities

Fortinet FortiOS SSL VPN Directory Traversal Vulnerability (FG-IR-18-384) (Direct Check)

FortiOS DRBG unsufficient entropy (FG-IR-19-186)

Halon Security Router Detection

Host Logical Network Segregation Weakness

HTTP Proxy Arbitrary Site/Port Relaying

HTTP Proxy CONNECT Request Relaying

HTTP Proxy Open gopher:// Request Relaying

HTTP Proxy Open Relay Detection

HTTP Proxy POST Request Relaying

IBM Tivoli Firewall Toolbox (TFST) Unspecified Remote Overflow

IP Forwarding Enabled

ISS BlackICE / RealSecure Large ICMP Ping Packet Overflow DoS

Juniper NetScreen Security Manager (NSM) guiSrv/devSrv Crafted String Remote DoS

Juniper ScreenOS 5.4 < 5.4.0r28 / 6.2 < 6.2.0r18 / 6.3 < 6.3.0r16 Malformed ICMP Echo Request DoS (JSA10604)

Juniper ScreenOS 5.4.x < 5.4.0r12 / 6.1.x / 6.2.x < 6.2.0r2 'about.html' Information Disclosure

Juniper ScreenOS 6.2.0r15 < 6.2.0r19 / 6.3.0r12 < 6.3.0r21 Multiple Vulnerabilities (JSA10713)

Juniper ScreenOS 6.3 < 6.3.0r17 DNS Lookup DoS

Juniper ScreenOS 6.3 < 6.3.0r17 DoS

Juniper ScreenOS 6.3 < 6.3.0r17 IPv6 Packet DoS

Juniper ScreenOS 6.3 SSG-5 and SSG-20 (KRACK)

Juniper ScreenOS 6.3.0r20 SSH ssh-pka SSH Negotiation RCE (JSA10712)

Juniper ScreenOS 6.3.x < 6.3.0r21 Malformed SSL/TLS Packet DoS (JSA10732)

Juniper ScreenOS 6.3.x < 6.3.0r22 Multiple Vulnerabilities in OpenSSL (JSA10733)

Juniper ScreenOS 6.3.x < 6.3.0r23 Multiple Vulnerabilities in OpenSSL (JSA10759) (DROWN)

Juniper ScreenOS 6.3.x < 6.3.0r24 Multiple XSS (JSA10782)

Juniper ScreenOS 6.3.x < 6.3.0r24 SSL Death Alert (JSA10808)

Juniper ScreenOS 6.3.x < 6.3.0r4 Firewall Private Address Information Disclosure

Juniper ScreenOS < 6.3.0r20 L2TP DoS (JSA10704)

Juniper ScreenOS < 6.3.0r25 Etherleak Vulnerability (JSA10841)

Juniper ScreenOS < 6.3.0r26 Stored Cross Site Scripting Vulnerability (JSA10894)

Juniper ScreenOS Device Detection

Junos OS 12.1X46 SRX 210, 240, 650 series firewalls (KRACK)

Kerio Personal Firewall Administrator Authentication Handshake Packet Remote Buffer Overflow

Kerio WinRoute Firewall HTTP/HTTPS Management Detection

L2TP Network Server Detection

McAfee Firewall Enterprise Detection

McAfee Firewall Enterprise DoS (SB10052)

McAfee Firewall Enterprise DoS (SB10126)

McAfee Firewall Enterprise IGMP Packet Integer Overflow DoS (SB10107)

McAfee Firewall Enterprise OpenSSL Information Disclosure (SB10071) (Heartbleed)

McAfee Firewall Enterprise OpenSSL Multiple Vulnerabilities (SB10102) (FREAK)

McAfee Next Generation Firewall Detection

Misconfigured SOCKS filtering

ModSecurity < 2.1.1 POST Data Null Byte Filter Bypass

ModSecurity < 2.5.9 Multipart Request Header Name DoS

ModSecurity < 2.7.0 Multipart Request Parsing Filter Bypass

ModSecurity < 2.7.3 XML External Entity (XXE) Data Parsing Arbitrary File Disclosure

ModSecurity < 2.7.4 forceRequestBodyVariable Action Handling DoS

ModSecurity < 2.7.6 Chunked Header Filter Bypass

ModSecurity Version

Multiple BSD ipfw / ip6fw ECE Bit Filtering Evasion

Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances (cisco-sa-20100217-asa)

NEC SOCKS4 Module Username Handling Remote Overflow

NetAsq IPS-Firewalls Detection

Novell BorderManager Port 2000 Telnet DoS

OTRS WebUI Detection

Palo Alto Networks PAN-OS Firewall/Panorama Web UI Detection

Palo Alto Networks PAN-OS Firewall/Panorama WebUI Default Credentials

Palo Alto Networks PAN-OS Version Detection

pfSense 2.3.x < 2.3.5-p1 / 2.4.x < 2.4.2-p1 Multiple Vulnerabilities (SA-17\_10 / SA-17\_11)

pfSense 2.3.x < 2.3.5-p2 / 2.4.x < 2.4.3-p1 Multiple Vulnerabilities (SA-18\_04 / SA-18\_05)

pfSense 2.3.x <= 2.3.5-p2 / 2.4.x < 2.4.4 Multiple Vulnerabilities (SA-18\_06 / SA-18\_07 / SA-18\_08)

pfSense < 2.1.1 Multiple Vulnerabilities (SA-14\_02 / SA-14\_03)

pfSense < 2.1.4 Multiple Vulnerabilities ( SA-14\_07 )

pfSense < 2.2.3 Multiple Vulnerabilities (SA-15\_07) (Logjam)

pfSense < 2.2.4 Multiple Vulnerabilities (SA-15\_07)

pfSense < 2.2.5 Multiple Vulnerabilities (SA-15\_08)

pfSense < 2.2.6 Multiple Vulnerabilities (SA-15\_09 / SA-15\_10 / SA-15\_11)

pfSense < 2.3 Multiple Vulnerabilities (SA-16\_01 - SA-16\_02)

pfSense < 2.3.1 Multiple Vulnerabilities (SA-16\_03 / SA-16-04)

pfSense < 2.3.1-p5 Multiple Vulnerabilities (SA-16\_07 / SA-16\_08)

pfSense < 2.3.3 Multiple Vulnerabilities (SA-17\_01 - SA-17\_03)

pfSense < 2.3.4 Multiple Vulnerabilities (SA-17\_04)

pfSense < 2.3.5 Multiple Vulnerabilities (KRACK)

pfSense < 2.4.2 Multiple Vulnerabilities (SA-17\_07)

pfSense < 2.4.3 Multiple Vulnerabilities (SA-18\_01 / SA-18\_02 / SA-18\_03) (Meltdown) (Spectre)

pfSense Unsupported Version Detection

pfSense Web Interface Detection

Privoxy < 3.0.21 Multiple Information Disclosure Vulnerabilities

Privoxy < 3.0.22 Multiple Vulnerabilities

Privoxy < 3.0.23 Multiple DoS Vulnerabilities

Privoxy Detection

Raptor Firewall 6.5 HTTP Proxy Detection

Reverse NAT/Intercepting Proxy Detection

SecurityGateway < 1.0.2 Administration Interface username Field Remote Overflow

SOCKS4 Server Recursive Connection Remote DoS

SOCKS5 Server Recursive Connection Remote DoS

SonicWall SonicOS Firewall Multiple Management Vulnerabilities (URGENT/11)

Source Routed Packet Weakness

Squid %xx URL Encoding ACL Bypass

Squid 2.x / 3.x < 3.1.22 / 3.2.4 / 3.3.0.2 cachemgr.cgi DoS

Squid 2.x / 3.x < 3.1.23 / 3.2.6 / 3.3.0.3 cachemgr.cgi DoS

Squid 2.x / 3.x < 3.5.17 / 4.x < 4.0.9 cachemgr.cgi RCE

Squid 3.0.STABLE16 / 3.10.11

Squid 3.1 < 3.x < 3.5.23 / 4.x < 4.0.17 Information Disclosure Vulnerability (SQUID-2016:11)

Squid 3.1.12.1 <= 3.1.x <= 3.1.23 / 3.2.0.4 <= 3.2.x / 3.3.x / 3.4.x / 3.5.x <= 3.5.28 / 4.x < 4.4 Cross-Site Scripting Vulnerability (SQUID-2018:4)

Squid 3.1.12.2 <= 3.1.x <= 3.1.23 / 3.2.0.8 <= 3.2.x <= 3.2.14 / 3.3.x / 3.4.x / 3.5.x <= 3.5.27 / 4.x < 4.0.13 Denial of Service Vulnerability (SQUID-2018:3)

Squid 3.1.6 DNS Reply Denial of Service

Squid 3.1.x < 3.1.16 / 3.2.x < 3.2.0.13 DNS Replies CName Record Parsing Remote DoS

Squid 3.1.x < 3.3.12 / 3.4.4 HTTPS Request Handling DoS

Squid 3.2 < 3.5.4 Incorrect X509 Server Certificate Validation Vulnerability

Squid 3.2.0.10 <= 3.2.x / 3.3.x / 3.4.x / 3.5.x <= 3.5.28 / 4.x < 4.4 Denial of Service Vulnerability (SQUID-2018:5)

Squid 3.2.0.11 < 3.x < 3.5.18 / 4.x < 4.0.10 Cache Poisoning Vulnerability (SQUID-2016:7)

Squid 3.2.x < 3.2.13 / 3.3.x < 3.3.8 Port Handling DoS

Squid 3.5.13 / 4.0.4 / 4.0.5 Server Connection Error Handling DoS

Squid 3.5.x < 3.5.23 / 4.x < 4.0.17 Information Disclosure Vulnerability (SQUID-2016:10)

Squid 3.5.x < 3.5.9 Multiple DoS

Squid 3.x < 3.0.STABLE26 / 3.1.15 / 3.2.0.11 Gopher Buffer Overflow

Squid 3.x < 3.2.12 / 3.3.x < 3.3.7 idnsALookup HTTP Request DoS

Squid 3.x < 3.2.9 / 3.3.3 strHdrAcptLangGetItem Malformed Accept-Language Denial of Service

Squid 3.x < 3.3.13 / 3.4.7 Request Processing DoS

Squid 3.x < 3.4.8 Multiple Vulnerabilities

Squid 3.x < 3.5.15 / 4.x < 4.0.7 Multiple DoS

Squid 3.x < 3.5.17 / 4.x < 4.0.9 Esi.cc Multiple Vulnerabilities

Squid 3.x < 3.5.18 / 4.x < 4.0.10 Multiple Denial of Service Vulnerabilities (SQUID-2016:9)

Squid 3.x < 3.5.28 / 4.x < 4.0.23 Multiple Denial of Service Vulnerabilities (SQUID-2018:1) (SQUID-2018:2)

Squid < 2.5.STABLE8 Malformed Host Name Error Message Information Disclosure

Squid < 2.5.STABLE8 Multiple Vulnerabilities

Squid < 2.6.STABLE12 src/client\_side.c clientProcessRequest() function TRACE Request DoS

Squid < 2.6.STABLE18 Cache Update Reply Unspecified DoS

Squid < 2.6.STABLE7 Multiple Remote DoS

Squid < 2.7.STABLE6 / 3.0.STABLE13 / 3.1.0.5 HTTP Version Number Request Remote DoS

Squid < 3.0.STABLE19 / 3.1.0.14 / 2.6.STABLE23 strListGetItem Function Remote DoS

Squid < 3.0.STABLE23 / 3.1.0.16

Squid < 3.0.STABLE24 / 2.7.STABLE8 / 2.6.STABLE24

Squid < 3.1.0.10 HTTP Header Injection Vulnerability

Squid < 3.1.8 / 3.2.0.2 NULL Pointer Dereference Denial of Service

Squid < 3.5.18 Host Header Handling Same-Origin Protection / Content Filtering Bypass (SQUID-2016:8)

Squid < 3.5.6 Squid Cache Peer CONNECT Remote Access Bypass

Squid Crafted NTLM Authentication Header DoS

Squid FTP URL Special Character Handling Remote Overflow

Squid mkdir-only PUT Request Remote DoS

Squid NTLM Component fakeauth Multiple Remote DoS

Squid ntlm\_check\_auth Function NTLM Authentication Helper Password Handling Remote Overflow

Squid Proxy Version Detection

Squid Set-Cookie Header Cross-session Information Disclosure

Squid SNMP Module asn\_parse\_header() Function Remote DoS

Squid Unsupported Version Detection

StoneGate Firewall Client Authentication Detection

Symantec (Blue Coat) ProxySG 6.5.x < 6.5.10.6 / 6.6.x < 6.6.5.8 / 6.7.x < 6.7.1.2 Impromper User Authorization Vulnerability

Symantec (Blue Coat) ProxySG SGOS Version

Symantec Firewall Malformed TCP Packet Options Remote DoS

Symantec ProxySG 6.5 / 6.6 / 6.7 < 6.7.4.1 OpenSSL Denial of Service Vulnerability (SA1462)

Symantec ProxySG 6.5 < 6.5.10.15 / 6.6 < 6.7.4.2 XSS and Information Disclosure Vulnerabilities (SA1472)

Symantec ProxySG 6.5 < 6.5.10.6 / 6.6 < 6.6.5.13 / 6.7 < 6.7.3.1 Multiple Vulnerabilities (SA155)

Symantec ProxySG 6.5 < 6.5.10.8 / 6.6 < 6.6.5.14 / 6.7.3 < 6.7.3.7 / 6.7.4 < 6.7.4.1 Multiple Vulnerabilities (SA162)

TCP/IP SYN+FIN Packet Filtering Weakness

tinyProxy Long Connect Request Overflow

Trend Micro InterScan Web Security Virtual Appliance Device Detection

Trend Micro IWSVA 6.5 < 6.5 Build 1737 Multiple Vulnerabilities

Trend Micro IWSVA 6.5 < 6.5 Build 1746 Multiple Vulnerabilities

Trend Micro IWSVA < 6.0 Build 1244 Information Disclosure

UMN Gopherd Unauthorized FTP Proxy

Unsupported IPSO Firewall

Unsupported ScreenOS Operating System

Web Application Firewall Detection

WinProxy < 6.1a HTTP Proxy Multiple Vulnerabilities

WinProxy < 6.1a Multiple Vulnerabilities (credentialed check)

ZoneAlarm Personal Firewall UDP Source Port 67 Bypass

ZoneAlarm Pro Configuration File/Directory Permission Weakness DoS

ZoneAlarm VSMON.exe Local Privilege Escalation

# Fedora Local Security Checks

# F5 Networks Local Security Checks

F5 Networks BIG-IP : Apache vulnerability (K42644206)

F5 Networks BIG-IP : BIG-IP AFM SQL injection vulnerability (K21121741)

F5 Networks BIG-IP : NTP vulnerability (K03331206)

F5 Networks BIG-IP : NTP vulnerability (K82644737)

F5 Networks BIG-IP : PHP vulnerability (K64412100)

F5 Networks BIG-IP : Apache Axis vulnerability (SOL16821)

F5 Networks BIG-IP : Apache Commons FileUpload vulnerability (K15189)

F5 Networks BIG-IP : Apache HTTP Expect header handling (SOL6669)

F5 Networks BIG-IP : Apache HTTP server vulnerabilities (SOL15889)

F5 Networks BIG-IP : Apache HTTP server vulnerability (SOL15901)

F5 Networks BIG-IP : Apache HTTP server vulnerability (SOL17189)

F5 Networks BIG-IP : Apache HTTP server vulnerability (SOL17201)

F5 Networks BIG-IP : Apache HTTPD vulnerability (K23332326)

F5 Networks BIG-IP : Apache HTTPD vulnerability (K34125394)

F5 Networks BIG-IP : Apache HTTPD vulnerability (K75429050)

F5 Networks BIG-IP : Apache HTTPD vulnerability (K83043359)

F5 Networks BIG-IP : Apache HTTPD vulnerability (SOL16907)

F5 Networks BIG-IP : Apache Portable Runtime vulnerability (K52319810)

F5 Networks BIG-IP : Apache Range header vulnerability (K13114)

F5 Networks BIG-IP : Apache Struts 2 vulnerability (K23432135)

F5 Networks BIG-IP : Apache Tomcat 6.x vulnerabilities (K58084500)

F5 Networks BIG-IP : Apache Tomcat 6.x vulnerability (K18174924)

F5 Networks BIG-IP : Apache Tomcat 6.x vulnerability (K30971148)

F5 Networks BIG-IP : Apache Tomcat 6.x vulnerability (K34341852)

F5 Networks BIG-IP : Apache Tomcat information disclosure vulnerability (SOL9110)

F5 Networks BIG-IP : Apache Tomcat vulnerability (K50116122)

F5 Networks BIG-IP : Apache Tomcat vulnerability (K73008537)

F5 Networks BIG-IP : Apache Tomcat vulnerability (SOL15426)

F5 Networks BIG-IP : Apache Tomcat vulnerability (SOL15428)

F5 Networks BIG-IP : Apache Tomcat vulnerability (SOL15432)

F5 Networks BIG-IP : Apache Tomcat vulnerability (SOL16344)

F5 Networks BIG-IP : Apache Tomcat vulnerability (SOL17123)

F5 Networks BIG-IP : Apache vulnerability (K00373024)

F5 Networks BIG-IP : Apache vulnerability (K16863)

F5 Networks BIG-IP : Apache vulnerability (K65355492)

F5 Networks BIG-IP : Apache vulnerability (SOL15273)

F5 Networks BIG-IP : Apache vulnerability (SOL15877)

F5 Networks BIG-IP : Apache vulnerability (SOL15902)

F5 Networks BIG-IP : Apache vulnerability (SOL15920)

F5 Networks BIG-IP : Apache vulnerability (SOL17251)

F5 Networks BIG-IP : Apache Xerces vulnerability (K04253390)

F5 Networks BIG-IP : Apache Xerces vulnerability (K70191975)

F5 Networks BIG-IP : Appliance mode tmsh access vulnerability (K02043709)

F5 Networks BIG-IP : Appliance mode tmsh vulnerability (K82814400)

F5 Networks BIG-IP : Appliance mode tmsh vulnerability (K87659521)

F5 Networks BIG-IP : Appliance mode vulnerability (K46524395)

F5 Networks BIG-IP : ASM < 11.6.0 Response Body XSS

F5 Networks BIG-IP : ASM Cloud Security Services authentication vulnerability (K59957337)

F5 Networks BIG-IP : BADoS vulnerability (K62201098)

F5 Networks BIG-IP : Bash vulnerability (K73705133)

F5 Networks BIG-IP : BDF parsing vulnerability (K15095307)

F5 Networks BIG-IP : BIG-IP file validation vulnerability (K12401251)

F5 Networks BIG-IP : BIG-IP AAM DCDB vulnerability (K54843525)

F5 Networks BIG-IP : BIG-IP AAM security vulnerability (K25359902)

F5 Networks BIG-IP : BIG-IP AFM and PEM TMUI XSS vulnerability (K61002104)

F5 Networks BIG-IP : BIG-IP AFM vulnerability (K20682450)

F5 Networks BIG-IP : BIG-IP Analytics generates predictable session cookies (SOL14334)

F5 Networks BIG-IP : BIG-IP Analytics vulnerability (K31152411)

F5 Networks BIG-IP : BIG-IP AOM password sync vulnerability (SOL05272632)

F5 Networks BIG-IP : BIG-IP APM access logs vulnerability (K31925518)

F5 Networks BIG-IP : BIG-IP APM apd vulnerability (K61705126)

F5 Networks BIG-IP : BIG-IP APM clickjacking vulnerability (SOL14700)

F5 Networks BIG-IP : BIG-IP APM client for Linux and macOS vulnerability (K12130880)

F5 Networks BIG-IP : BIG-IP APM client for Linux and macOS vulnerability (K52171282)

F5 Networks BIG-IP : BIG-IP APM client for Linux and macOS vulnerability (K54431371)

F5 Networks BIG-IP : BIG-IP APM client for Windows vulnerability (K10015187)

F5 Networks BIG-IP : BIG-IP APM CRL vulnerability (K34652116)

F5 Networks BIG-IP : BIG-IP APM DTLS vulnerability (K97241515)

F5 Networks BIG-IP : BIG-IP APM Edge Client logging vulnerability (K23876153)

F5 Networks BIG-IP : BIG-IP APM Edge Client vulnerability (K51220077)

F5 Networks BIG-IP : BIG-IP APM logging disclosure vulnerability (K37890841)

F5 Networks BIG-IP : BIG-IP APM logging disclosure vulnerability (K45432295)

F5 Networks BIG-IP : BIG-IP APM OAuth failure response message vulnerability (K27617652)

F5 Networks BIG-IP : BIG-IP APM per-request policy object vulnerability (K27391542)

F5 Networks BIG-IP : BIG-IP APM portal access vulnerability (K52206731)

F5 Networks BIG-IP : BIG-IP APM Portal Access vulnerability (K54358225)

F5 Networks BIG-IP : BIG-IP APM Portal Access vulnerability (K73183618)

F5 Networks BIG-IP : BIG-IP APM redirect vulnerability (K66171422)

F5 Networks BIG-IP : BIG-IP APM redirect vulnerability (K87141725)

F5 Networks BIG-IP : BIG-IP APM SAML IdP vulnerability (K05018525)

F5 Networks BIG-IP : BIG-IP APM SSO vulnerability (K26738102)

F5 Networks BIG-IP : BIG-IP APM SSO vulnerability (SOL82679059)

F5 Networks BIG-IP : BIG-IP APM VPN vulnerability (K20087443)

F5 Networks BIG-IP : BIG-IP APM vulnerability (K23024812)

F5 Networks BIG-IP : BIG-IP APM XSS vulnerability (K31424926)

F5 Networks BIG-IP : BIG-IP APM XSS vulnerability (K32840424)

F5 Networks BIG-IP : BIG-IP APM XSS vulnerability (K43523962)

F5 Networks BIG-IP : BIG-IP Appliance mode vulnerability (K11330536)

F5 Networks BIG-IP : BIG-IP Appliance mode vulnerability (K73522927)

F5 Networks BIG-IP : BIG-IP ARM BGP vulnerability (K17264695)

F5 Networks BIG-IP : BIG-IP ASM and BIG-IP AFM/BIG-IP Analytics vulnerability (K23520761)

F5 Networks BIG-IP : BIG-IP ASM and BIG-IQ/Enterprise Manager/F5 iWorkflow device authentication and trust vulnerability (K26462555)

F5 Networks BIG-IP : BIG-IP ASM and PSM remote buffer overflow exploit (SOL10417)

F5 Networks BIG-IP : BIG-IP ASM data processing vulnerability (K38243073)

F5 Networks BIG-IP : BIG-IP ASM memory exhaustion vulnerability (K40452417)

F5 Networks BIG-IP : BIG-IP ASM Virtual Edition may run out of memory under certain DoS conditions (K15341)

F5 Networks BIG-IP : BIG-IP ASM vulnerability (K04280042)

F5 Networks BIG-IP : BIG-IP ASM vulnerability (K12403422)

F5 Networks BIG-IP : BIG-IP ASM vulnerability (K75432956)

F5 Networks BIG-IP : BIG-IP ASM vulnerability (SOL17119920)

F5 Networks BIG-IP : BIG-IP ASM XSS vulnerability (K14812883)

F5 Networks BIG-IP : BIG-IP ASM XSS vulnerability (SOL16081)

F5 Networks BIG-IP : BIG-IP Automatic Update Check and ASM Automatic Signature Update man-in-the-middle vulnerability (K16090)

F5 Networks BIG-IP : BIG-IP AWS vulnerability (K01054113)

F5 Networks BIG-IP : BIG-IP Azure cloud vulnerability (K61757346)

F5 Networks BIG-IP : BIG-IP BIND vulnerability (K98528405)

F5 Networks BIG-IP : BIG-IP Client SSL vulnerability (K43121447)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K00363258)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K17253)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K20222812)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K23734425)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K29280193)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K44603900)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K46401178)

F5 Networks BIG-IP : BIG-IP Configuration utility vulnerability (K50254952)

F5 Networks BIG-IP : BIG-IP DHCPv6 vulnerability (K36228121)

F5 Networks BIG-IP : BIG-IP directory traversal vulnerability (SOL16121)

F5 Networks BIG-IP : BIG-IP DNS Cache vulnerability (K48224824)

F5 Networks BIG-IP : BIG-IP Edge and FirePass client information leakage vulnerability (SOL14969)

F5 Networks BIG-IP : BIG-IP Edge Client for macOS vulnerability (K49827114)

F5 Networks BIG-IP : BIG-IP FastL4 profile vulnerability (K36300805)

F5 Networks BIG-IP : BIG-IP FastL4 TMM vulnerability (K65615624)

F5 Networks BIG-IP : BIG-IP file validation vulnerability (K49580002)

F5 Networks BIG-IP : BIG-IP FIX profile vulnerability (K82781208)

F5 Networks BIG-IP : BIG-IP FTP profile vulnerability (K15759349)

F5 Networks BIG-IP : BIG-IP HSB vulnerability (K26455071)

F5 Networks BIG-IP : BIG-IP HTTP profile vulnerability (K19501795)

F5 Networks BIG-IP : BIG-IP HTTP profile vulnerability (K70275209)

F5 Networks BIG-IP : BIG-IP HTTP/2 vulnerability (K81557381)

F5 Networks BIG-IP : BIG-IP HTTP/3 QUIC vulnerability (K61367237)

F5 Networks BIG-IP : BIG-IP iControl and tmsh vulnerability (K77313277)

F5 Networks BIG-IP : BIG-IP IPsec IKE peer listener vulnerability (K10133477)

F5 Networks BIG-IP : BIG-IP IPsec tunnel endpoint vulnerability (K05263202)

F5 Networks BIG-IP : BIG-IP last hop kernel module vulnerability (K00032124)

F5 Networks BIG-IP : BIG-IP management interface vulnerability (SOL9875)

F5 Networks BIG-IP : BIG-IP management vulnerability (K55792317)

F5 Networks BIG-IP : BIG-IP mcpd vulnerability (K87920510)

F5 Networks BIG-IP : BIG-IP MRF Diameter vulnerability (K55812535)

F5 Networks BIG-IP : BIG-IP PEM vulnerability (K10329515)

F5 Networks BIG-IP : BIG-IP PEM vulnerability (K54562183)

F5 Networks BIG-IP : BIG-IP Resource Administrator vulnerability (K07702240)

F5 Networks BIG-IP : BIG-IP Resource Administrator vulnerability (K38941195)

F5 Networks BIG-IP : BIG-IP REST vulnerability (K12685114)

F5 Networks BIG-IP : BIG-IP restjavad vulnerability (K01049383)

F5 Networks BIG-IP : BIG-IP Secure Vault vulnerability (K18535734)

F5 Networks BIG-IP : BIG-IP SNMP vulnerability (K42027747)

F5 Networks BIG-IP : BIG-IP SNMPD vulnerability (K12139752)

F5 Networks BIG-IP : BIG-IP snmpd vulnerability (K35209601)

F5 Networks BIG-IP : BIG-IP SOCKS proxy vulnerability (K55225440)

F5 Networks BIG-IP : BIG-IP SPDY and HTTP/2 profile vulnerability (K01587042)

F5 Networks BIG-IP : BIG-IP SSL profile vulnerability (K53931245)

F5 Networks BIG-IP : BIG-IP SSL vulnerability (K21905460) (ROBOT)

F5 Networks BIG-IP : BIG-IP SSL vulnerability (K48042976)

F5 Networks BIG-IP : BIG-IP system vulnerability (K51754851)

F5 Networks BIG-IP : BIG-IP TMM AWS vulnerability (K00025388)

F5 Networks BIG-IP : BIG-IP TMM Ram Cache vulnerability (K22113131)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K04897373)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K19361245)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K39225055)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K50046200)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K62712037)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K76328112)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K77671456)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K91026261)

F5 Networks BIG-IP : BIG-IP TMM vulnerability (K92411323)

F5 Networks BIG-IP : BIG-IP tmsh vulnerability (K01067037)

F5 Networks BIG-IP : BIG-IP tmsh vulnerability (K36814487)

F5 Networks BIG-IP : BIG-IP TMUI vulnerability (K23566124)

F5 Networks BIG-IP : BIG-IP TMUI XSS vulnerability (K00432398)

F5 Networks BIG-IP : BIG-IP TMUI XSS vulnerability (K22441651)

F5 Networks BIG-IP : BIG-IP TMUI XSS vulnerability (K79902360)

F5 Networks BIG-IP : BIG-IP URL classification vulnerability (K42465020)

F5 Networks BIG-IP : BIG-IP virtual server TCP sequence numbers vulnerability (K68401558)

F5 Networks BIG-IP : BIG-IP virtual server with HTTP Explicit Proxy and/or SOCKS vulnerability (K02692210)

F5 Networks BIG-IP : BIG-IP virtual server with HTTP Explicit Proxy and/or SOCKS vulnerability (K35520031)

F5 Networks BIG-IP : BIG-IP virtual servers with Client SSL and HTTP/2 or SPDY configured vulnerability (K22541983)

F5 Networks BIG-IP : BIG-IP vulnerability (K25607522)

F5 Networks BIG-IP : BIG-IQ / BIG-IP privilege escalation vulnerability (K15229)

F5 Networks BIG-IP : big3d vulnerability (K82038789)

F5 Networks BIG-IP : BIND 9 vulnerabilities - Dereferencing freed fetch context and DNSSEC Validation (SOL7053)

F5 Networks BIG-IP : BIND 9 vulnerability (SOL11503)

F5 Networks BIG-IP : BIND 9 vulnerability (SOL9754)

F5 Networks BIG-IP : BIND 9.3.0 denial of service vulnerability (SOL4351)

F5 Networks BIG-IP : BIND 9: Multiple DoS vulnerabilities (SOL6612)

F5 Networks BIG-IP : BIND denial-of-service attack (SOL14201)

F5 Networks BIG-IP : BIND DNS cache poisoning vulnerability (SOL8938)

F5 Networks BIG-IP : BIND DNSSEC vulnerability (SOL17025)

F5 Networks BIG-IP : BIND vulnerability (K00040234)

F5 Networks BIG-IP : BIND vulnerability (K01713115)

F5 Networks BIG-IP : BIND vulnerability (K02138183)

F5 Networks BIG-IP : BIND vulnerability (K02230327)

F5 Networks BIG-IP : BIND vulnerability (K08613310)

F5 Networks BIG-IP : BIND vulnerability (K10092301)

F5 Networks BIG-IP : BIND vulnerability (K14386)

F5 Networks BIG-IP : BIND vulnerability (K15840535)

F5 Networks BIG-IP : BIND vulnerability (K16356)

F5 Networks BIG-IP : BIND vulnerability (K16909)

F5 Networks BIG-IP : BIND vulnerability (K17181)

F5 Networks BIG-IP : BIND vulnerability (K18829561)

F5 Networks BIG-IP : BIND vulnerability (K25244852)

F5 Networks BIG-IP : BIND vulnerability (K34250741)

F5 Networks BIG-IP : BIND vulnerability (K35322517)

F5 Networks BIG-IP : BIND vulnerability (K40181790)

F5 Networks BIG-IP : BIND vulnerability (K53445000)

F5 Networks BIG-IP : BIND vulnerability (K59448931)

F5 Networks BIG-IP : BIND vulnerability (K62012529)

F5 Networks BIG-IP : BIND vulnerability (K74009656)

F5 Networks BIG-IP : BIND vulnerability (K80533167)

F5 Networks BIG-IP : BIND vulnerability (K86272821)

F5 Networks BIG-IP : BIND vulnerability (SOL01471335)

F5 Networks BIG-IP : BIND vulnerability (SOL10366)

F5 Networks BIG-IP : BIND vulnerability (SOL12985)

F5 Networks BIG-IP : BIND vulnerability (SOL12986)

F5 Networks BIG-IP : BIND vulnerability (SOL13660)

F5 Networks BIG-IP : BIND vulnerability (SOL14204)

F5 Networks BIG-IP : BIND vulnerability (SOL14316)

F5 Networks BIG-IP : BIND vulnerability (SOL14601)

F5 Networks BIG-IP : BIND vulnerability (SOL14613)

F5 Networks BIG-IP : BIND vulnerability (SOL15172)

F5 Networks BIG-IP : BIND vulnerability (SOL15481)

F5 Networks BIG-IP : BIND vulnerability (SOL15748)

F5 Networks BIG-IP : BIND vulnerability (SOL15787)

F5 Networks BIG-IP : BIND vulnerability (SOL15927)

F5 Networks BIG-IP : BIND vulnerability (SOL16912)

F5 Networks BIG-IP : BIND vulnerability (SOL17227)

F5 Networks BIG-IP : Boost memory allocator vulnerability (K16946)

F5 Networks BIG-IP : Bootstrap vulnerability (K24383845)

F5 Networks BIG-IP : bzip2 vulnerability (SOL15878)

F5 Networks BIG-IP : bzip2 vulnerability (SOL9592)

F5 Networks BIG-IP : CGNAT/PPTP vulnerability (K47527163)

F5 Networks BIG-IP : Client-side component flaw (SOL14468)

F5 Networks BIG-IP : ConfigSync IP Rsync full file system access vulnerability (K15236)

F5 Networks BIG-IP : ConfigSync mcpd vulnerability (K62279530)

F5 Networks BIG-IP : ConfigSync vulnerability (K05123525)

F5 Networks BIG-IP : Configuration utility CSRF vulnerability (K61045143)

F5 Networks BIG-IP : Configuration utility CSRF vulnerability (SOL21485342)

F5 Networks BIG-IP : Configuration utility login vulnerability (SOL4369)

F5 Networks BIG-IP : CRIME vulnerability via the SPDY protocol (K14059)

F5 Networks BIG-IP : CRIME vulnerability via TLS 1.2 protocol (K14054)

F5 Networks BIG-IP : cURL and libcurl vulnerability (K01006862)

F5 Networks BIG-IP : cURL and libcurl vulnerability (K16704)

F5 Networks BIG-IP : cURL and libcurl vulnerability (K16707)

F5 Networks BIG-IP : cURL and libcurl vulnerability (K46123931)

F5 Networks BIG-IP : cURL and libcurl vulnerability (K84940705)

F5 Networks BIG-IP : cURL and libcurl vulnerability (K85235351)

F5 Networks BIG-IP : cURL buffer overflow vulnerability (SOL4447)

F5 Networks BIG-IP : cURL vulnerability (SOL15875)

F5 Networks BIG-IP : Custom monitor privilege escalation vulnerability (K00265182)

F5 Networks BIG-IP : D-Bus vulnerability (SOL17256)

F5 Networks BIG-IP : Datastor kernel vulnerability (K17407)

F5 Networks BIG-IP : Denial of service vulnerability in GnuPG (SOL6535)

F5 Networks BIG-IP : DHCP client vulnerability (K08306700)

F5 Networks BIG-IP : DHCP Client vulnerability (SOL13219)

F5 Networks BIG-IP : Directory Traversal and File Deletion (ID 363027)

F5 Networks BIG-IP : DNS Express vulnerability (K45435121)

F5 Networks BIG-IP : DNS vulnerability (K24401914)

F5 Networks BIG-IP : DNSSEC BIND vulnerability (SOL10898)

F5 Networks BIG-IP : Excess resource consumption due to low MSS values vulnerability (K35421172) (SACK Slowness)

F5 Networks BIG-IP : Expat vulnerabilities (K15905)

F5 Networks BIG-IP : Expat vulnerabilities (K16949)

F5 Networks BIG-IP : Expat vulnerability (K52320548)

F5 Networks BIG-IP : Expat XML library vulnerability (K15104541)

F5 Networks BIG-IP : Expat XML library vulnerability (K50459349)

F5 Networks BIG-IP : Expat XML library vulnerability (K70938105)

F5 Networks BIG-IP : Expat XML parser vulnerability (K65460334)

F5 Networks BIG-IP : F5 BIG-IP TMM vulnerability (K31404801)

F5 Networks BIG-IP : F5 iRules vulnerability (K30215839)

F5 Networks BIG-IP : F5 management sshd vulnerability (K92140924)

F5 Networks BIG-IP : F5 Path MTU Discovery vulnerability (K22843911)

F5 Networks BIG-IP : F5 TCP IPv6 vulnerability (K46535047)

F5 Networks BIG-IP : F5 TCP vulnerability (K06223540)

F5 Networks BIG-IP : F5 TLS vulnerability (K05121675) (Ticketbleed)

F5 Networks BIG-IP : F5 TMM vulnerability (K43945001)

F5 Networks BIG-IP : F5 tmsh vulnerability (K40378764)

F5 Networks BIG-IP : F5 TMUI and iControl Rest vulnerability (K64855220)

F5 Networks BIG-IP : file vulnerability (SOL16875)

F5 Networks BIG-IP : GeoIP vulnerability (K23124150)

F5 Networks BIG-IP : GHOST: glibc gethostbyname buffer overflow vulnerability (K16057) (GHOST)

F5 Networks BIG-IP : glibc vulnerability (K06493172)

F5 Networks BIG-IP : glibc vulnerability (K16365)

F5 Networks BIG-IP : glibc vulnerability (K16472)

F5 Networks BIG-IP : glibc vulnerability (K20486351) (Stack Clash)

F5 Networks BIG-IP : glibc vulnerability (K23946311)

F5 Networks BIG-IP : glibc vulnerability (K31211252)

F5 Networks BIG-IP : glibc vulnerability (K47098834)

F5 Networks BIG-IP : glibc vulnerability (K51079478)

F5 Networks BIG-IP : glibc vulnerability (K55001100)

F5 Networks BIG-IP : glibc vulnerability (SOL09408132)

F5 Networks BIG-IP : GNU Binutils vulnerability (K13534168)

F5 Networks BIG-IP : GNU C Library (glibc) vulnerability (K29241247)

F5 Networks BIG-IP : GNU C Library (glibc) vulnerability (SOL16010)

F5 Networks BIG-IP : GNU C Library (glibc) vulnerability (SOL16342)

F5 Networks BIG-IP : GNU C Library (glibc) vulnerability (SOL16364)

F5 Networks BIG-IP : GNU C library strxfrm/strcoll overflow vulnerabilities (K16416)

F5 Networks BIG-IP : GNU C Library vulnerability (SOL15885)

F5 Networks BIG-IP : GNU C Library vulnerability (SOL16435)

F5 Networks BIG-IP : GnuPG vulnerability (K11785283)

F5 Networks BIG-IP : GnuPG vulnerability (K21284031)

F5 Networks BIG-IP : GnuPG vulnerability (K50413110)

F5 Networks BIG-IP : GnuPG vulnerability (K75253136)

F5 Networks BIG-IP : GnuPG vulnerability (SOL40131068)

F5 Networks BIG-IP : GnuTLS RSA PKCS signature vulnerability (K17327)

F5 Networks BIG-IP : GnuTLS vulnerability (K53330207)

F5 Networks BIG-IP : GnuTLS vulnerability (K54022413)

F5 Networks BIG-IP : GnuTLS vulnerability (SOL15637)

F5 Networks BIG-IP : GraphicsMagick vulnerability (K82747025)

F5 Networks BIG-IP : Grep vulnerability (K42891424)

F5 Networks BIG-IP : Grep vulnerability (K69662152)

F5 Networks BIG-IP : GRUB2 vulnerability (SOL25901386)

F5 Networks BIG-IP : Hosts may generate weak RSA keys under low entropy conditions (SOL13607)

F5 Networks BIG-IP : HTTP cookie vulnerability (SOL15406)

F5 Networks BIG-IP : HTTP/2 ALPN vulnerability (K94563344)

F5 Networks BIG-IP : HTTP/2 Ping Flood vulnerability (K98053339) (Ping Flood)

F5 Networks BIG-IP : HTTP/2 Reset Flood vulnerability (K01988340) (Reset Flood)

F5 Networks BIG-IP : HTTP/2 Settings Flood vulnerability (K50233772) (Settings Flood)

F5 Networks BIG-IP : HTTPS monitor vulnerability (K05112543)

F5 Networks BIG-IP : iCall privilege escalation vulnerability (K16728)

F5 Networks BIG-IP : icclib vulnerabilities (SOL9990)

F5 Networks BIG-IP : ICMP packet processing vulnerability (SOL17047)

F5 Networks BIG-IP : iControl REST and tmsh vulnerability (K20541896)

F5 Networks BIG-IP : iControl REST vulnerability (K20445457)

F5 Networks BIG-IP : iControl REST vulnerability (K22317030)

F5 Networks BIG-IP : iControl REST vulnerability (K22384173)

F5 Networks BIG-IP : iControl REST vulnerability (K24465120)

F5 Networks BIG-IP : iControl REST vulnerability (K29149494)

F5 Networks BIG-IP : iControl REST vulnerability (K41107914)

F5 Networks BIG-IP : iControl REST vulnerability (K44885536)

F5 Networks BIG-IP : iControl REST vulnerability (K53990093)

F5 Networks BIG-IP : iControl REST vulnerability (K67825238)

F5 Networks BIG-IP : iControl REST vulnerability (K99998454)

F5 Networks BIG-IP : iControl vulnerability (K15220)

F5 Networks BIG-IP : iControl vulnerability (K47284724)

F5 Networks BIG-IP : ImageMagick vulnerabilities (K30403302)

F5 Networks BIG-IP : ImageMagick vulnerability (K03151140) (ImageTragick)

F5 Networks BIG-IP : ImageMagick vulnerability (K03512441)

F5 Networks BIG-IP : ImageMagick vulnerability (K10550253)

F5 Networks BIG-IP : ImageMagick vulnerability (K20336394)

F5 Networks BIG-IP : ImageMagick vulnerability (K25102203)

F5 Networks BIG-IP : ImageMagick vulnerability (K29154575)

F5 Networks BIG-IP : ImageMagick vulnerability (K61974123)

F5 Networks BIG-IP : ImageMagick vulnerability (K68785753)

F5 Networks BIG-IP : Inadequate validation for TCP segments (SOL4743)

F5 Networks BIG-IP : Insufficient validation of ICMP error messages (K23440942)

F5 Networks BIG-IP : Insufficient validation of ICMP error messages (SOL4583)

F5 Networks BIG-IP : Intel SPI Flash vulnerability (K19855851)

F5 Networks BIG-IP : IP Intelligence Feed List vulnerability (K11464209)

F5 Networks BIG-IP : IPsec vulnerability (K05013313)

F5 Networks BIG-IP : IPv6 fragmentation vulnerability (K57211290)

F5 Networks BIG-IP : IPv6 Neighbor Discovery Protocol (NDP) vulnerability (SOL9528)

F5 Networks BIG-IP : iRulesLX debug NodeJS vulnerability (K75532331)

F5 Networks BIG-IP : ISC DHCP 4.x vulnerability (K57500018)

F5 Networks BIG-IP : Java commons-collections library vulnerability (K30518307)

F5 Networks BIG-IP : Java Runtime Environment vulnerability (SOL16872)

F5 Networks BIG-IP : Java SE vulnerabilities (SOL17079)

F5 Networks BIG-IP : Java vulnerabilities (K48802597)

F5 Networks BIG-IP : Java vulnerabilities (K50118123)

F5 Networks BIG-IP : jQuery vulnerability (K62532311)

F5 Networks BIG-IP : Kerberos vulnerability (K15553)

F5 Networks BIG-IP : Kernel vulnerability (K62442245)

F5 Networks BIG-IP : Lazy FP state restore vulnerability (K21344224)

F5 Networks BIG-IP : libarchive vulnerability (K13074505)

F5 Networks BIG-IP : libarchive vulnerability (K24036027)

F5 Networks BIG-IP : libarchive vulnerability (K35246595)

F5 Networks BIG-IP : libarchive vulnerability (K35263486)

F5 Networks BIG-IP : libarchive vulnerability (K52697522)

F5 Networks BIG-IP : libcurl vulnerability (K10196624)

F5 Networks BIG-IP : libcurl vulnerability (K26899353)

F5 Networks BIG-IP : libcurl vulnerability (K44503763)

F5 Networks BIG-IP : libcurl vulnerability (K52828640)

F5 Networks BIG-IP : libgd vulnerability (K71581599)

F5 Networks BIG-IP : libjpeg vulnerability (K59503294)

F5 Networks BIG-IP : libjpeg-turbo vulnerability (K62655427)

F5 Networks BIG-IP : libpng out-of-bounds read vulnerability (SOL21057235)

F5 Networks BIG-IP : Libpng vulnerability (K81903701)

F5 Networks BIG-IP : Libpng vulnerability (SOL15881)

F5 Networks BIG-IP : Libpng vulnerability (SOL76930736)

F5 Networks BIG-IP : libpng vulnerability (SOL9988)

F5 Networks BIG-IP : libssh vulnerability (K57255643)

F5 Networks BIG-IP : libssh2 vulnerability (K21531693)

F5 Networks BIG-IP : libtar vulnerability (K16015326)

F5 Networks BIG-IP : LibTIFF vulnerabilities (K34527393)

F5 Networks BIG-IP : LibTIFF vulnerabilities (K89096577)

F5 Networks BIG-IP : Libtiff vulnerabilities (SOL15863)

F5 Networks BIG-IP : LibTIFF vulnerability (K11220361)

F5 Networks BIG-IP : LibTIFF vulnerability (K24923910)

F5 Networks BIG-IP : LibTIFF vulnerability (K38871451)

F5 Networks BIG-IP : libtirpc vulnerability (K19157044)

F5 Networks BIG-IP : libxml2 vulnerabilities (K24322529)

F5 Networks BIG-IP : libxml2 vulnerabilities (K54225343)

F5 Networks BIG-IP : libxml2 vulnerability (K04450715)

F5 Networks BIG-IP : libxml2 vulnerability (K14338030)

F5 Networks BIG-IP : libxml2 vulnerability (K14614344)

F5 Networks BIG-IP : libxml2 vulnerability (K16712298)

F5 Networks BIG-IP : libxml2 vulnerability (K26422113)

F5 Networks BIG-IP : libxml2 vulnerability (K45439210)

F5 Networks BIG-IP : libxml2 vulnerability (K48220300)

F5 Networks BIG-IP : libxml2 vulnerability (K71926235)

F5 Networks BIG-IP : libxml2 vulnerability (SOL15872)

F5 Networks BIG-IP : Linux file utility vulnerabilities (K16347)

F5 Networks BIG-IP : Linux kernel driver vulnerabilities (K15912)

F5 Networks BIG-IP : Linux kernel KVM subsystem vulnerability (K11186236)

F5 Networks BIG-IP : Linux kernel KVM subsystem vulnerability (K13145361)

F5 Networks BIG-IP : Linux kernel SCTP vulnerabilities (K15910)

F5 Networks BIG-IP : Linux kernel SCTP vulnerability (K16016)

F5 Networks BIG-IP : Linux kernel SCTP vulnerability (K16025)

F5 Networks BIG-IP : Linux kernel SCTP vulnerability (K17242)

F5 Networks BIG-IP : Linux kernel SCTP vulnerability (K37510383)

F5 Networks BIG-IP : Linux kernel TCP ISN vulnerability (K15301)

F5 Networks BIG-IP : Linux kernel tcp\_rcv\_state\_process vulnerability (SOL15304)

F5 Networks BIG-IP : Linux kernel TTY vulnerability (K15319)

F5 Networks BIG-IP : Linux kernel vulnerabilities (K31026324)

F5 Networks BIG-IP : Linux kernel vulnerabilities (K62700573)

F5 Networks BIG-IP : Linux kernel vulnerability (K05513373)

F5 Networks BIG-IP : Linux kernel vulnerability (K24578092)

F5 Networks BIG-IP : Linux kernel vulnerability (K54610514)

F5 Networks BIG-IP : Linux kernel vulnerability (K02236463)

F5 Networks BIG-IP : Linux kernel vulnerability (K02613439)

F5 Networks BIG-IP : Linux kernel vulnerability (K08440897)

F5 Networks BIG-IP : Linux kernel vulnerability (K14445)

F5 Networks BIG-IP : Linux kernel vulnerability (K15317)

F5 Networks BIG-IP : Linux kernel vulnerability (K15526101)

F5 Networks BIG-IP : Linux kernel vulnerability (K17132)

F5 Networks BIG-IP : Linux kernel vulnerability (K17241)

F5 Networks BIG-IP : Linux kernel vulnerability (K17246)

F5 Networks BIG-IP : Linux kernel vulnerability (K17307)

F5 Networks BIG-IP : Linux kernel vulnerability (K17309)

F5 Networks BIG-IP : Linux kernel vulnerability (K17326)

F5 Networks BIG-IP : Linux kernel vulnerability (K17403481)

F5 Networks BIG-IP : Linux kernel vulnerability (K17462)

F5 Networks BIG-IP : Linux kernel vulnerability (K18015201)

F5 Networks BIG-IP : Linux kernel vulnerability (K20022580)

F5 Networks BIG-IP : Linux kernel vulnerability (K20934447)

F5 Networks BIG-IP : Linux kernel vulnerability (K21632201)

F5 Networks BIG-IP : Linux kernel vulnerability (K22012502)

F5 Networks BIG-IP : Linux kernel vulnerability (K23030550)

F5 Networks BIG-IP : Linux kernel vulnerability (K27673650)

F5 Networks BIG-IP : Linux kernel vulnerability (K28056114)

F5 Networks BIG-IP : Linux kernel vulnerability (K28241423)

F5 Networks BIG-IP : Linux kernel vulnerability (K31300371)

F5 Networks BIG-IP : Linux kernel vulnerability (K31603170)

F5 Networks BIG-IP : Linux kernel vulnerability (K41739114)

F5 Networks BIG-IP : Linux kernel vulnerability (K42142782)

F5 Networks BIG-IP : Linux kernel vulnerability (K43322910)

F5 Networks BIG-IP : Linux kernel vulnerability (K51931024) (Stack Clash)

F5 Networks BIG-IP : Linux kernel vulnerability (K55672042)

F5 Networks BIG-IP : Linux kernel vulnerability (K60104355)

F5 Networks BIG-IP : Linux kernel vulnerability (K60742457)

F5 Networks BIG-IP : Linux kernel vulnerability (K61223103)

F5 Networks BIG-IP : Linux kernel vulnerability (K61429540)

F5 Networks BIG-IP : Linux kernel vulnerability (K68852819)

F5 Networks BIG-IP : Linux kernel vulnerability (K74374841)

F5 Networks BIG-IP : Linux kernel vulnerability (K74413297)

F5 Networks BIG-IP : Linux kernel vulnerability (K80440915)

F5 Networks BIG-IP : Linux kernel vulnerability (K81211720)

F5 Networks BIG-IP : Linux kernel vulnerability (K82508682)

F5 Networks BIG-IP : Linux kernel vulnerability (K84024430)

F5 Networks BIG-IP : Linux kernel vulnerability (K90230486)

F5 Networks BIG-IP : Linux kernel vulnerability (K90803619)

F5 Networks BIG-IP : Linux kernel vulnerability (K93472064)

F5 Networks BIG-IP : Linux kernel vulnerability (K94105604)

F5 Networks BIG-IP : Linux kernel vulnerability (K94735334)

F5 Networks BIG-IP : Linux kernel vulnerability (K95343321)

F5 Networks BIG-IP : Linux kernel vulnerability (K95345942)

F5 Networks BIG-IP : Linux kernel vulnerability (K98102572)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL15685)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL15699)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL15732)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL15746)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL15797)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL15852)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL15984)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL16122)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL16471)

F5 Networks BIG-IP : Linux Kernel vulnerability (SOL16473)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL16479)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL17199)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL17237)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL17458)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL17543)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL17551)

F5 Networks BIG-IP : Linux kernel vulnerability (SOL51518670)

F5 Networks BIG-IP : Linux libuser vulnerability (SOL05770600)

F5 Networks BIG-IP : Linux privilege-escalation vulnerability (K10558632) (Dirty COW)

F5 Networks BIG-IP : Linux RPM vulnerability (SOL16383)

F5 Networks BIG-IP : Linux SACK Panic vulnerability (K78234183) (SACK Panic)

F5 Networks BIG-IP : Linux SACK Slowness vulnerability (K26618426) (SACK Slowness)

F5 Networks BIG-IP : Linux TCP stack vulnerability (K46514822)

F5 Networks BIG-IP : list.jsp XSS vulnerability (SOL15296)

F5 Networks BIG-IP : Local OpenSSL vulnerabilities (SOL6734)

F5 Networks BIG-IP : logrotate vulnerability (SOL16869)

F5 Networks BIG-IP : logrotate vulnerability (SOL16871)

F5 Networks BIG-IP : LZO vulnerability (K95698826)

F5 Networks BIG-IP : Mailx vulnerabilities (K16945)

F5 Networks BIG-IP : Martian address filtering vulnerability (K45644893)

F5 Networks BIG-IP : MCPD vulnerability (K52180214)

F5 Networks BIG-IP : MCPQ vulnerability (SOL16196)

F5 Networks BIG-IP : MD2 Message-Digest Algorithm vulnerability (SOL15663)

F5 Networks BIG-IP : MFC vulnerability (K93417064)

F5 Networks BIG-IP : MIT Kerberos 5 vulnerability (K15547)

F5 Networks BIG-IP : MIT Kerberos 5 vulnerability (K15552)

F5 Networks BIG-IP : Mozilla NSS vulnerabilities (SOL31372672)

F5 Networks BIG-IP : Mozilla NSS vulnerability (K15479471)

F5 Networks BIG-IP : Mozilla NSS vulnerability (K15955144)

F5 Networks BIG-IP : Mozilla NSS vulnerability (K20145801)

F5 Networks BIG-IP : Mozilla NSS vulnerability (K91100352)

F5 Networks BIG-IP : MQTT vulnerability (K26583415)

F5 Networks BIG-IP : Multiple DNS vulnerabilities (SOL6365)

F5 Networks BIG-IP : Multiple FreeType vulnerabilities (K16900)

F5 Networks BIG-IP : Multiple GNU Bash vulnerabilities (SOL15629) (Shellshock)

F5 Networks BIG-IP : Multiple LibTIFF vulnerabilities (K16715)

F5 Networks BIG-IP : Multiple LibTIFF vulnerabilities (K35155453)

F5 Networks BIG-IP : Multiple libXML2 vulnerabilities (K61570943)

F5 Networks BIG-IP : Multiple Mozilla NSS vulnerabilities (K16716)

F5 Networks BIG-IP : Multiple MySQL vulnerabilities (K14410)

F5 Networks BIG-IP : Multiple MySQL vulnerabilities (K16389)

F5 Networks BIG-IP : Multiple PCRE vulnerabilities (K20225390)

F5 Networks BIG-IP : Multiple PHP CDF vulnerabilities (SOL16954)

F5 Networks BIG-IP : Multiple PHP vulnerabilities (K13519)

F5 Networks BIG-IP : Multiple PHP vulnerabilities (K17061)

F5 Networks BIG-IP : Multiple PHP vulnerabilities (SOL7859)

F5 Networks BIG-IP : Multiple QEMU vulnerabilities (K63519101)

F5 Networks BIG-IP : Multiple unzip vulnerabilities (SOL16480)

F5 Networks BIG-IP : Multiple Wireshark (tshark) vulnerabilities (K01837042)

F5 Networks BIG-IP : Multiple Wireshark vulnerabilities (K15868)

F5 Networks BIG-IP : Multiple Wireshark vulnerabilities (K16940)

F5 Networks BIG-IP : Multiple Wireshark vulnerabilities (K34035645)

F5 Networks BIG-IP : MySQL Server vulnerability (SOL14907)

F5 Networks BIG-IP : MySQL vulnerabilities (SOL8178)

F5 Networks BIG-IP : MySQL vulnerability (K16845) (BACKRONYM)

F5 Networks BIG-IP : MySQL vulnerability (K44611310)

F5 Networks BIG-IP : MySQL vulnerability (K53729441)

F5 Networks BIG-IP : MySQL vulnerability (K73828041)

F5 Networks BIG-IP : NAT64 vulnerability (K64743453)

F5 Networks BIG-IP : Net-SNMP vulnerability (K15883)

F5 Networks BIG-IP : NET-SNMP vulnerability (K16476)

F5 Networks BIG-IP : Netscape reuse cipher change bug (SOL10674)

F5 Networks BIG-IP : Node.js vulnerability (K23134279)

F5 Networks BIG-IP : Node.js vulnerability (K27228191)

F5 Networks BIG-IP : Node.js vulnerability (SOL17238)

F5 Networks BIG-IP : NodeJS vulnerability (K15311661)

F5 Networks BIG-IP : NodeJS vulnerability (K37111863)

F5 Networks BIG-IP : NodeJS vulnerability (K63025104)

F5 Networks BIG-IP : NTP input validation vulnerability (K43205719)

F5 Networks BIG-IP : NTP vulnerabilities (K00329831)

F5 Networks BIG-IP : NTP vulnerabilities (K02360853)

F5 Networks BIG-IP : NTP vulnerabilities (K06288381)

F5 Networks BIG-IP : NTP vulnerabilities (K17530)

F5 Networks BIG-IP : NTP vulnerability (K01324833)

F5 Networks BIG-IP : NTP vulnerability (K02951273)

F5 Networks BIG-IP : NTP vulnerability (K05046514)

F5 Networks BIG-IP : NTP vulnerability (K07082049)

F5 Networks BIG-IP : NTP vulnerability (K10600056)

F5 Networks BIG-IP : NTP vulnerability (K11251130)

F5 Networks BIG-IP : NTP vulnerability (K16393)

F5 Networks BIG-IP : NTP vulnerability (K16505)

F5 Networks BIG-IP : NTP vulnerability (K16506)

F5 Networks BIG-IP : NTP vulnerability (K17114)

F5 Networks BIG-IP : NTP vulnerability (K17515)

F5 Networks BIG-IP : NTP vulnerability (K17516)

F5 Networks BIG-IP : NTP vulnerability (K17517)

F5 Networks BIG-IP : NTP vulnerability (K17525)

F5 Networks BIG-IP : NTP vulnerability (K17528)

F5 Networks BIG-IP : NTP vulnerability (K17529)

F5 Networks BIG-IP : NTP vulnerability (K17566)

F5 Networks BIG-IP : NTP vulnerability (K20804323)

F5 Networks BIG-IP : NTP vulnerability (K24613253)

F5 Networks BIG-IP : NTP vulnerability (K31310492)

F5 Networks BIG-IP : NTP vulnerability (K32262483)

F5 Networks BIG-IP : NTP vulnerability (K51444934)

F5 Networks BIG-IP : NTP vulnerability (K55405388)

F5 Networks BIG-IP : NTP vulnerability (K63675293)

F5 Networks BIG-IP : NTP vulnerability (K64505405)

F5 Networks BIG-IP : NTP vulnerability (K71245322)

F5 Networks BIG-IP : NTP vulnerability (K96670746)

F5 Networks BIG-IP : NTP vulnerability (K99254031)

F5 Networks BIG-IP : NTP vulnerability (SOL10905)

F5 Networks BIG-IP : NTP vulnerability (SOL15934)

F5 Networks BIG-IP : NTP vulnerability (SOL15935)

F5 Networks BIG-IP : NTP vulnerability (SOL15936)

F5 Networks BIG-IP : NTP vulnerability (SOL16392)

F5 Networks BIG-IP : NTP vulnerability (SOL17518)

F5 Networks BIG-IP : OpenJDK vulnerability (K17175)

F5 Networks BIG-IP : OpenJDK vulnerability (SOL17171)

F5 Networks BIG-IP : OpenJDK vulnerability (SOL17173)

F5 Networks BIG-IP : OpenJDK vulnerability (SOL17381)

F5 Networks BIG-IP : OpenSSH vulnerabilities (K15780)

F5 Networks BIG-IP : OpenSSH vulnerabilities (K17263)

F5 Networks BIG-IP : OpenSSH vulnerabilities (SOL6736)

F5 Networks BIG-IP : OpenSSH vulnerability (K14609)

F5 Networks BIG-IP : OpenSSH vulnerability (K14741)

F5 Networks BIG-IP : OpenSSH vulnerability (K14845276)

F5 Networks BIG-IP : OpenSSH vulnerability (K17113)

F5 Networks BIG-IP : OpenSSH vulnerability (K17461)

F5 Networks BIG-IP : OpenSSH vulnerability (K20911042)

F5 Networks BIG-IP : OpenSSH vulnerability (K24324390)

F5 Networks BIG-IP : OpenSSH vulnerability (K31440025)

F5 Networks BIG-IP : OpenSSH vulnerability (K31510510)

F5 Networks BIG-IP : OpenSSH vulnerability (K32485746)

F5 Networks BIG-IP : OpenSSH vulnerability (K62201745)

F5 Networks BIG-IP : OpenSSH vulnerability (K64292204)

F5 Networks BIG-IP : OpenSSH vulnerability (SOL15156)

F5 Networks BIG-IP : OpenSSL and Intel processor SMT side-channel vulnerability (PortSmash) (K49711130)

F5 Networks BIG-IP : OpenSSL DTLS Buffer vulnerability (SOL15348)

F5 Networks BIG-IP : OpenSSL DTLS SRTP Memory Leak (SOL15722)

F5 Networks BIG-IP : OpenSSL OCSP vulnerability (SOL14261)

F5 Networks BIG-IP : OpenSSL signature vulnerability (SOL6623)

F5 Networks BIG-IP : OpenSSL SSL\_get\_shared\_ciphers vulnerability (SOL8106)

F5 Networks BIG-IP : OpenSSL vulnerabilities (SOL95463126) (DROWN)

F5 Networks BIG-IP : OpenSSL vulnerability (K16321)

F5 Networks BIG-IP : OpenSSL vulnerability (K16323)

F5 Networks BIG-IP : OpenSSL vulnerability (K01276005)

F5 Networks BIG-IP : OpenSSL vulnerability (K02652550)

F5 Networks BIG-IP : OpenSSL vulnerability (K12824341)

F5 Networks BIG-IP : OpenSSL vulnerability (K13167034)

F5 Networks BIG-IP : OpenSSL vulnerability (K14363514)

F5 Networks BIG-IP : OpenSSL vulnerability (K15158)

F5 Networks BIG-IP : OpenSSL vulnerability (K15159) (Heartbleed)

F5 Networks BIG-IP : OpenSSL vulnerability (K15325)

F5 Networks BIG-IP : OpenSSL vulnerability (K15328)

F5 Networks BIG-IP : OpenSSL vulnerability (K15356)

F5 Networks BIG-IP : OpenSSL vulnerability (K16317)

F5 Networks BIG-IP : OpenSSL vulnerability (K16914)

F5 Networks BIG-IP : OpenSSL vulnerability (K17248)

F5 Networks BIG-IP : OpenSSL vulnerability (K17382)

F5 Networks BIG-IP : OpenSSL vulnerability (K21665601)

F5 Networks BIG-IP : OpenSSL vulnerability (K22334603)

F5 Networks BIG-IP : OpenSSL vulnerability (K23196136) (DROWN)

F5 Networks BIG-IP : OpenSSL vulnerability (K23230229)

F5 Networks BIG-IP : OpenSSL vulnerability (K23512141)

F5 Networks BIG-IP : OpenSSL vulnerability (K23873366)

F5 Networks BIG-IP : OpenSSL vulnerability (K36488941)

F5 Networks BIG-IP : OpenSSL vulnerability (K37526132)

F5 Networks BIG-IP : OpenSSL vulnerability (K40524634)

F5 Networks BIG-IP : OpenSSL vulnerability (K43570545)

F5 Networks BIG-IP : OpenSSL vulnerability (K44512851)

F5 Networks BIG-IP : OpenSSL vulnerability (K51920288)

F5 Networks BIG-IP : OpenSSL vulnerability (K52349521)

F5 Networks BIG-IP : OpenSSL vulnerability (K53084033)

F5 Networks BIG-IP : OpenSSL vulnerability (K54211024)

F5 Networks BIG-IP : OpenSSL vulnerability (K55540723)

F5 Networks BIG-IP : OpenSSL vulnerability (K59298921)

F5 Networks BIG-IP : OpenSSL vulnerability (K75152412)

F5 Networks BIG-IP : OpenSSL vulnerability (K79215841)

F5 Networks BIG-IP : OpenSSL vulnerability (K86772626)

F5 Networks BIG-IP : OpenSSL vulnerability (K90492697)

F5 Networks BIG-IP : OpenSSL vulnerability (K93122894)

F5 Networks BIG-IP : OpenSSL vulnerability (K93600123)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL11533)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15147)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15343)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15388)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15401)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15404)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15461)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15568)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL15723)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL16123)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL16126)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL16135)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL16139) (FREAK)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL16285)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL16302)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL16913)

F5 Networks BIG-IP : OpenSSL vulnerability (SOL8108)

F5 Networks BIG-IP : Oracle Java SE vulnerability (K15217245)

F5 Networks BIG-IP : Oracle Java SE vulnerability (K33924005)

F5 Networks BIG-IP : Oracle Java SE vulnerability (K44923228)

F5 Networks BIG-IP : Oracle Java SE vulnerability (K70321874)

F5 Networks BIG-IP : Oracle Java SE vulnerability (K73112451)

F5 Networks BIG-IP : Oracle Java SE vulnerability (K81223200)

F5 Networks BIG-IP : Oracle Java vulnerability (K05016441)

F5 Networks BIG-IP : Oracle Java vulnerability (K25075696)

F5 Networks BIG-IP : OS Kernel and SMM mode L1 Terminal Fault vulnerability (K95275140) (Foreshadow)

F5 Networks BIG-IP : Out-of-bounds memory vulnerability with the BIG-IP APM system (SOL43552605)

F5 Networks BIG-IP : PAM vulnerability (SOL17494)

F5 Networks BIG-IP : pam\_ldap password policy control vulnerability (SOL5725)

F5 Networks BIG-IP : pam\_ldap vulnerability (SOL6634)

F5 Networks BIG-IP : Path MTU discovery vulnerability (K15792)

F5 Networks BIG-IP : PCRE library vulnerability (K16983)

F5 Networks BIG-IP : PCRE library vulnerability (K17331)

F5 Networks BIG-IP : pcregrep in PCRE vulnerability (K05428062)

F5 Networks BIG-IP : Perl vulnerabilities (K15867)

F5 Networks BIG-IP : perl-XML-Twig vulnerability (K08383757)

F5 Networks BIG-IP : PHP vulnerabilities (K17028)

F5 Networks BIG-IP : PHP vulnerabilities (K51390683)

F5 Networks BIG-IP : PHP vulnerabilities (SOL16993)

F5 Networks BIG-IP : PHP vulnerabilities (SOL17377)

F5 Networks BIG-IP : PHP vulnerability (K03534020)

F5 Networks BIG-IP : PHP vulnerability (K13588)

F5 Networks BIG-IP : PHP vulnerability (K17049)

F5 Networks BIG-IP : PHP vulnerability (K17127)

F5 Networks BIG-IP : PHP vulnerability (K30363030)

F5 Networks BIG-IP : PHP vulnerability (K35232053)

F5 Networks BIG-IP : PHP vulnerability (K35240323)

F5 Networks BIG-IP : PHP vulnerability (K42065024)

F5 Networks BIG-IP : PHP vulnerability (K43267483)

F5 Networks BIG-IP : PHP vulnerability (K43449212)

F5 Networks BIG-IP : PHP vulnerability (K54308010)

F5 Networks BIG-IP : PHP vulnerability (K54924436)

F5 Networks BIG-IP : PHP vulnerability (K75543432)

F5 Networks BIG-IP : PHP vulnerability (K91084571)

F5 Networks BIG-IP : PHP vulnerability (K95432245)

F5 Networks BIG-IP : PHP vulnerability (SOL12650)

F5 Networks BIG-IP : PHP vulnerability (SOL14574)

F5 Networks BIG-IP : PHP vulnerability (SOL15169)

F5 Networks BIG-IP : PHP vulnerability (SOL15876)

F5 Networks BIG-IP : PHP vulnerability (SOL16826)

F5 Networks BIG-IP : PHP vulnerability (SOL17313)

F5 Networks BIG-IP : PHP vulnerability (SOL63712424)

F5 Networks BIG-IP : PHP vulnerability (SOL9761)

F5 Networks BIG-IP : PHPMailer vulnerability (K73926196)

F5 Networks BIG-IP : PHPMailer vulnerability (K74977440)

F5 Networks BIG-IP : PKCS #7 vulnerability (SOL16898)

F5 Networks BIG-IP : pl\_tree.php XSS vulnerability (SOL15939)

F5 Networks BIG-IP : Potential protocol version rollback vulnerability in OpenSSL (SOL5533)

F5 Networks BIG-IP : Privilege escalation vulnerability (K75136237)

F5 Networks BIG-IP : Python and Jython vulnerability (K53192206)

F5 Networks BIG-IP : Python and Jython vulnerability (K78825687)

F5 Networks BIG-IP : Python vulnerability (K16398)

F5 Networks BIG-IP : QEMU vulnerability (K75248350)

F5 Networks BIG-IP : QEMU vulnerability (SOL13405416)

F5 Networks BIG-IP : QEMU vulnerability (SOL16620) (Venom)

F5 Networks BIG-IP : QEMU vulnerability (SOL51841514)

F5 Networks BIG-IP : RADIUS authentication vulnerability (K62750376)

F5 Networks BIG-IP : Reflected XSS vulnerability (K44462254)

F5 Networks BIG-IP : Reflected XSS vulnerability in an undisclosed Configuration utility page (K41704442)

F5 Networks BIG-IP : Remote vulnerability in the mod\_jk2 Apache module (SOL7886)

F5 Networks BIG-IP : RESOLV::lookup iRule command vulnerability (K52638558)

F5 Networks BIG-IP : REST Framework vulnerability (K11818407)

F5 Networks BIG-IP : REST Framework vulnerability (K89509323)

F5 Networks BIG-IP : Rsync sender.c vulnerability (SOL15548)

F5 Networks BIG-IP : Rsync vulnerability (SOL15549)

F5 Networks BIG-IP : SafeNet External Network HSM script vulnerability (K74759095)

F5 Networks BIG-IP : Samba vulnerabilities (K37603172) (Badlock)

F5 Networks BIG-IP : Samba vulnerabilities (K53313971)

F5 Networks BIG-IP : SCP vulnerability (K54336216)

F5 Networks BIG-IP : Side-channel processor vulnerabilities (K91229003) (Meltdown) (Spectre)

F5 Networks BIG-IP : Side-channel processor vulnerability (K54252492)

F5 Networks BIG-IP : SLOTH: TLS 1.2 handshake vulnerability (K02201365) (SLOTH)

F5 Networks BIG-IP : Slowloris denial-of-service attack vulnerability (K12636)

F5 Networks BIG-IP : SNMP vulnerability (K17315)

F5 Networks BIG-IP : SNMP vulnerability (K17378)

F5 Networks BIG-IP : SNMP vulnerability (K27400151)

F5 Networks BIG-IP : SNMP vulnerability (K40443301)

F5 Networks BIG-IP : SNMPv3 HMAC verification vulnerability (SOL8939)

F5 Networks BIG-IP : SNTP vulnerability (K60352002)

F5 Networks BIG-IP : SOAP parser vulnerability (SOL15879)

F5 Networks BIG-IP : Socat vulnerabilities (K14919)

F5 Networks BIG-IP : SOCKS proxy vulnerability (K30201296)

F5 Networks BIG-IP : Sockstress DoS tool vulnerability (SOL10509)

F5 Networks BIG-IP : SQL injection vulnerability (K39428424)

F5 Networks BIG-IP : SQL injection vulnerability from an authenticated source (SOL14154)

F5 Networks BIG-IP : SQLite vulnerability (K16950)

F5 Networks BIG-IP : SSH vulnerability (K13600)

F5 Networks BIG-IP : SSHD session.c vulnerability (K93532943)

F5 Networks BIG-IP : SSL acceleration card timing vulnerability (K15500)

F5 Networks BIG-IP : SSL decryption vulnerabilities (SOL4944)

F5 Networks BIG-IP : SSL Forward Proxy vulnerability (K20134942)

F5 Networks BIG-IP : SSL forward proxy vulnerability (K45325728)

F5 Networks BIG-IP : SSL forward proxy vulnerability (K64552448)

F5 Networks BIG-IP : SSL Renegotiation vulnerability (SOL10737)

F5 Networks BIG-IP : SSL/TLS RC4 vulnerability (K16864) (Bar Mitzvah)

F5 Networks BIG-IP : SSL\_MODE\_RELEASE\_BUFFERS vulnerability (K15329)

F5 Networks BIG-IP : ssldump vulnerability (K46121888)

F5 Networks BIG-IP : SUSE coreutils vulnerabilities (SOL16859)

F5 Networks BIG-IP : systemd vulnerabilities (K06044762)

F5 Networks BIG-IP : TCP vulnerability (K35358312)

F5 Networks BIG-IP : tcpdump vulnerabilities (K04225025)

F5 Networks BIG-IP : tcpdump vulnerabilities (K31997425)

F5 Networks BIG-IP : tcpdump vulnerabilities (K39512927)

F5 Networks BIG-IP : tcpdump vulnerabilities (K49144112)

F5 Networks BIG-IP : tcpdump vulnerabilities (K55129614)

F5 Networks BIG-IP : tcpdump vulnerabilities (K72403108)

F5 Networks BIG-IP : tcpdump vulnerabilities (K77384526)

F5 Networks BIG-IP : tcpdump vulnerabilities (K94010578)

F5 Networks BIG-IP : tcpdump vulnerabilities (K94778122)

F5 Networks BIG-IP : The BIG-IP APM access policy logout page may be vulnerable to XSS cookie tampering (SOL14712)

F5 Networks BIG-IP : The BIG-IP ASM web management interface XSS vulnerability (SOL8406)

F5 Networks BIG-IP : TLS 1.3 vulnerability (K34450231)

F5 Networks BIG-IP : TLS in Mozilla NSS vulnerability (K15630)

F5 Networks BIG-IP : TLS vulnerability (K02714910)

F5 Networks BIG-IP : TLS vulnerability (K16674) (Logjam)

F5 Networks BIG-IP : TLS vulnerability (SOL15564)

F5 Networks BIG-IP : TLS/DTLS 'Lucky 13' vulnerability (K14190)

F5 Networks BIG-IP : TLS/SSL RC4 vulnerability (K14638)

F5 Networks BIG-IP : TLS1.x padding vulnerability (K15882)

F5 Networks BIG-IP : TMM DIAMETER vulnerability (K54130510)

F5 Networks BIG-IP : TMM FastL4 vulnerability (K53183580)

F5 Networks BIG-IP : TMM SSL profile vulnerability (K54167061)

F5 Networks BIG-IP : TMM SSL/TLS profile vulnerability (K21154730)

F5 Networks BIG-IP : TMM SSL/TLS virtual server vulnerability (K39508724)

F5 Networks BIG-IP : TMM SSO plugin vulnerability (K95444512)

F5 Networks BIG-IP : TMM TLS virtual server vulnerability (K10065173) (POODLE)

F5 Networks BIG-IP : TMM vulnerability (K17155)

F5 Networks BIG-IP : TMM vulnerability (K06045217)

F5 Networks BIG-IP : TMM vulnerability (K06747393)

F5 Networks BIG-IP : TMM vulnerability (K07127032)

F5 Networks BIG-IP : TMM vulnerability (K07369970)

F5 Networks BIG-IP : TMM vulnerability (K10002335)

F5 Networks BIG-IP : TMM vulnerability (K10930474)

F5 Networks BIG-IP : TMM vulnerability (K11447758)

F5 Networks BIG-IP : TMM vulnerability (K12044607)

F5 Networks BIG-IP : TMM vulnerability (K13053402)

F5 Networks BIG-IP : TMM vulnerability (K13421245)

F5 Networks BIG-IP : TMM vulnerability (K14632915)

F5 Networks BIG-IP : TMM vulnerability (K16248201)

F5 Networks BIG-IP : TMM vulnerability (K19430431)

F5 Networks BIG-IP : TMM vulnerability (K19784568)

F5 Networks BIG-IP : TMM vulnerability (K22216037)

F5 Networks BIG-IP : TMM vulnerability (K23328310)

F5 Networks BIG-IP : TMM vulnerability (K23860356)

F5 Networks BIG-IP : TMM vulnerability (K25033460)

F5 Networks BIG-IP : TMM vulnerability (K25573437)

F5 Networks BIG-IP : TMM vulnerability (K27044729)

F5 Networks BIG-IP : TMM vulnerability (K33211839)

F5 Networks BIG-IP : TMM vulnerability (K33500120)

F5 Networks BIG-IP : TMM vulnerability (K34514540)

F5 Networks BIG-IP : TMM vulnerability (K37404773)

F5 Networks BIG-IP : TMM vulnerability (K43625118)

F5 Networks BIG-IP : TMM vulnerability (K45611803)

F5 Networks BIG-IP : TMM vulnerability (K46940010)

F5 Networks BIG-IP : TMM vulnerability (K52167636)

F5 Networks BIG-IP : TMM vulnerability (K55101404)

F5 Networks BIG-IP : TMM vulnerability (K55102452)

F5 Networks BIG-IP : TMM vulnerability (K64208870)

F5 Networks BIG-IP : TMM vulnerability (K71282001)

F5 Networks BIG-IP : TMM vulnerability (K72335002)

F5 Networks BIG-IP : TMM vulnerability (K72442354)

F5 Networks BIG-IP : TMM vulnerability (K81137982)

F5 Networks BIG-IP : TMM vulnerability (K82851041)

F5 Networks BIG-IP : TMM vulnerability (K87416818)

F5 Networks BIG-IP : TMM vulnerability (K92002212)

F5 Networks BIG-IP : TMM vulnerability (K94105051)

F5 Networks BIG-IP : TMM vulnerability (K95117754)

F5 Networks BIG-IP : TMM vulnerability (K95434410)

F5 Networks BIG-IP : TMM vulnerability (SOL13233)

F5 Networks BIG-IP : TMM WebSocket vulnerability (K11718033)

F5 Networks BIG-IP : TMM with HTTP/2 vulnerability (K45320419)

F5 Networks BIG-IP : TMM with LRO vulnerability (K07550539)

F5 Networks BIG-IP : TMOS Shell vulnerability (K37442533)

F5 Networks BIG-IP : TMOS vulnerability (K03126093)

F5 Networks BIG-IP : TMOS vulnerability (K49440608)

F5 Networks BIG-IP : TMOS vulnerability: Password changes for local users may not be preserved unless the configuration is explicitly saved (K37250780)

F5 Networks BIG-IP : tmsh utility vulnerability (K28003839)

F5 Networks BIG-IP : TMUI vulnerability (K30500703)

F5 Networks BIG-IP : TMUI vulnerability (K61620494)

F5 Networks BIG-IP : Unbound vulnerability (SOL15931)

F5 Networks BIG-IP : vCMP Cavium Nitrox SSL hardware accelerator vulnerability (K52521791)

F5 Networks BIG-IP : vCMP DoS vulnerability (K17386)

F5 Networks BIG-IP : vCMP vulnerability (K01413496)

F5 Networks BIG-IP : vCMP vulnerability (K03165684)

F5 Networks BIG-IP : vCMP vulnerability (K05765031)

F5 Networks BIG-IP : vCMP vulnerability (K64721111)

F5 Networks BIG-IP : Vim vulnerability (K22183127)

F5 Networks BIG-IP : Virtual Machine Manager L1 Terminal Fault vulnerability (K31300402) (Foreshadow)

F5 Networks BIG-IP : Websocket profile vulnerability (K51351360)

F5 Networks BIG-IP : XML Entity Injection vulnerabilities (K15605)

F5 Networks BIG-IP : XML External Entity Injection (XXE) from authenticated source vulnerability (K14138)

F5 Networks BIG-IP : XML vulnerability (K03244804)

F5 Networks BIG-IP : XSS vulnerabilities in BIG-IP Configuration utility (SOL8280)

F5 Networks BIG-IP : XSS vulnerability (SOL13838)

F5 Networks BIG-IP : XSS vulnerability in Apache mod\_imap (SOL8186)

F5 Networks BIG-IP : XSS vulnerability in BIG-IP ASM Web Scraping feature (SOL12953)

F5 Networks BIG-IP : XSS vulnerability in echo.jsp (SOL15532)

F5 Networks BIG-IP : XSS vulnerability in the BIG-IP and Enterprise Manager Configuration utilities (K16838)

F5 Networks BIG-IP : XSS vulnerability in the BIG-IP and Enterprise Manager Configuration utilities (K97285349)

F5 Networks BIG-IP : XSS vulnerability in undisclosed TMUI page (K04524282)

F5 Networks BIG-IP : XSS vulnerability in undisclosed TMUI page (K21042153)

F5 Networks BIG-IP : XSS vulnerability viewing logs from the Console section of the web management interface (SOL8599)

F5 Networks BIG-IP : XSS vulnerability viewing logs from the web management interface (SOL8602)

# DNS

DNS Sender Policy Framework (SPF) Enabled

DNS Server BIND version Directive Remote Version Detection

DNS Server Cache Snooping Remote Information Disclosure

DNS Server Detection

DNS Server DNSSEC Aware Resolver

DNS Server Dynamic Update Record Injection

DNS Server Fingerprinting

DNS Server hostname.bind Map Hostname Disclosure

DNS Server Recursive Query Cache Poisoning Weakness

DNS Server Spoofed Request Amplification DDoS

DNS Server UDP Query Limitation

DNS Server Version Detection

DNS Server Zone Transfer Information Disclosure (AXFR)

Dns2TCP Service Detection

dnsmasq 2.25 DHCP Request Denial of Service (CVE-2008-3214)

dnsmasq 2.73rc6 < 2.73rc8 extract\_name() Function RCE

dnsmasq < 2.21.0 Multiple Remote Vulnerabilities

dnsmasq < 2.45 Multiple Remote DoS

dnsmasq < 2.50 Multiple Remote TFTP Vulnerabilities

dnsmasq < 2.63test1 libvirtd TCP Network Packet Parsing Response DNS Amplification DoS

dnsmasq < 2.66test2 libvirtd TCP Network Packet Parsing Response DNS Amplification DoS

dnsmasq < 2.73rc4 setup\_reply() Function Return Value Checking Information Disclosure

dnsmasq < 2.76 Empty Address Denial of Service (CVE-2015-8899)

dnsmasq < 2.78 Multiple Remote Vulnerabilities

DNSSEC NSEC Records

ISC BIND 9 'RRSIG' Record Type Remote DoS

ISC BIND 9 9.4-ESV < 9.4-ESV-R4, 9.6.2 < 9.6.2-P3, 9.6-ESV < 9.6-ESV-R3, 9.7.x < 9.7.2-P3 Multiple Vulnerabilities

ISC BIND 9 9.7.2 < 9.7.2-P2 Multiple Vulnerabilities

ISC BIND 9 < 9.9.10-P2 / 9.9.10-S3 / 9.10.5-P2 / 9.10.5-S3 / 9.11.1-P2 Multiple Vulnerabilities

ISC BIND 9 < 9.9.11-P1 / 9.9.11-S2 / 9.10.6-P1 / 9.10.6-S2 / 9.11.2-P1 / 9.12.0rc2 Multiple Vulnerabilities

ISC BIND 9 < 9.9.9-P5 / 9.9.9-S7 / 9.10.4-P5 / 9.11.0-P2 Multiple DoS

ISC BIND 9 < 9.9.9-P6 / 9.9.9-S8 / 9.10.4-P6 / 9.11.0-P3 DNS64 and RPZ DoS

ISC BIND 9 < 9.9.9-P8 / 9.9.9-S10 / 9.9.10rc3 / 9.10.4-P8 / 9.10.5rc3 / 9.11.0-P5 / 9.11.1r3 Multiple Vunlerabilities

ISC BIND 9 Denial of Service Vulnerability (CVE-2018-5743)

ISC BIND 9 DNS RDATA Handling DoS

ISC BIND 9 DNS64 Handling DoS

ISC BIND 9 DNS64 Handling DoS (CVE-2012-5689)

ISC BIND 9 DNSSEC Cache Poisoning

ISC BIND 9 DNSSEC NSEC/NSEC3 Bogus NXDOMAIN Responses

ISC BIND 9 Dynamic Update Handling Remote DoS (intrusive check)

ISC BIND 9 EDNS Processing DoS

ISC BIND 9 EVP\_VerifyFinal() / DSA\_do\_verify() SSL/TLS Signature Validation Weakness

ISC BIND 9 for Windows UDP Client Handler Remote DoS

ISC BIND 9 Large RRSIG RRsets Negative Caching Remote DoS

ISC BIND 9 libdns Regular Expression Handling DoS

ISC BIND 9 localnets ACL Security Bypass

ISC BIND 9 Multiple Denial of Service Vulnerabilities

ISC BIND 9 Multiple DoS

ISC BIND 9 Multiple DoS

ISC BIND 9 Multiple DoS Vulnerabilities

ISC BIND 9 Multiple Remote DoS

ISC BIND 9 NSEC3-Signed Zone Handling DoS

ISC BIND 9 Query.c Logging Resolver Denial of Service

ISC BIND 9 RDATA Section Handling DoS

ISC BIND 9 Recursive Resolver Malformed Zone DoS

ISC BIND 9 Recursive Response DNAME Record Handling DoS

ISC BIND 9 Recursive Server prefetch DoS

ISC BIND 9 resolver.c Multiple DNS Cookie Packet Handling DoS

ISC BIND 9 Unspecified Packet Processing Remote DoS

ISC BIND 9 Zero-Length RDATA Section Denial of Service / Information Disclosure

ISC BIND 9.0.x < 9.9.7-P3 / 9.10.x < 9.10.2-P4 Multiple DoS

ISC BIND 9.10.2 < 9.10.2rc2 Multiple Vulnerabilities

ISC BIND 9.10.5-S1 < 9.11.5-S6 Assertion Failure Vulnerability

ISC BIND 9.10.5-S1 <= 9.11.6-S1 EDNS Client Subnet RRSIG Denial of Service

ISC BIND 9.10.x < 9.10.1-P2 DNSSEC Validation DoS

ISC BIND 9.11.0 / 9.11.x < 9.11.13 / 9.11.x < 9.11.13-S1 / 9.12.x < 9.12.5-P2 / 9.14.x < 9.14.8 / 9.15 / 9.15.x < 9.15.6 Vulnerability

ISC BIND 9.12.x < 9.12.1-P1 Multiple Vulnerabilities

ISC BIND 9.12.x < 9.12.4-P1, 9.13.x < 9.14.1 Denial of Service Vulnerability

ISC BIND 9.14.x < 9.14.7 / 9.15.x < 9.15.5 Multiple Vulnerabilities

ISC BIND 9.3.0 < 9.9.8-P3 / 9.9.x-Sx < 9.9.8-S4 / 9.10.x < 9.10.3-P3 Multiple DoS

ISC BIND 9.7.0.x < 9.9.6-P2 DNSSEC Validation DoS

ISC BIND 9.7.1-9.7.2-P3 IXFR / DDNS Update Combined with High Query Rate DoS

ISC BIND 9.7.x < 9.9.7-P1 / 9.10.x < 9.10.2-P2 Resolver DNSSEC Validation DoS

ISC BIND 9.7.x < 9.9.7-P2 / 9.10.x < 9.10.2-P3 TKEY Query Handling Remote DoS

ISC BIND 9.9.6-S2 DNSSEC Validation DoS

ISC BIND 9.9.7.x < 9.9.7rc2 Multiple Vulnerabilities

ISC BIND 9.9.8 < 9.9.8-P2 / 9.10.3 < 9.10.3-P2 Socket Error Handling DoS

ISC BIND 9.9.8-Sx < 9.9.8-S5 REQUIRE Assertion DoS

ISC BIND 9.9.x < 9.9.9-P3 / 9.10.x < 9.10.4-P3 / 9.11.x < 9.11.0rc3 buffer.c Query Response DoS

ISC BIND 9.x < 9.9.8-P2 / 9.10.x < 9.10.3-P2 Response Parsing Class Attribute Handling DoS

ISC BIND 9.x < 9.9.9-P2 / 9.10.x < 9.10.4-P2 / 9.11.0a3 < 9.11.0b2 lwres Query DoS

ISC BIND 9.x < 9.9.9-P3 Options Sections DoS

ISC BIND 9.x AUTHORS Map Remote Version Disclosure

ISC BIND 9.x.x < 9.11.5 / 9.12.x < 9.12.3 Policy-Bypass Record Update Vulnerability

ISC BIND 9.x.x < 9.9.10-P1 / 9.10.x < 9.10.5-P1 / 9.11.x < 9.11.1-P1 Multiple Vulnerabilities

ISC BIND 9.x.x < 9.9.13-P1 / 9.10.x < 9.10.8-P1 / 9.11.x < 9.11.4-P1 / 9.12.x < 9.12.2-P1 deny-answer-aliases DoS Vulnerability

ISC BIND < 4.9.11 stub resolver (libresolv.a) DNS Response Overflow

ISC BIND < 4.9.5 DNS Resolver Functions Remote Overflow

ISC BIND < 4.9.7 / 8.1.2 Inverse-Query Remote Overflow

ISC BIND < 4.9.7-REL / 8.2.2-P5 Multiple Remote Vulnerabilities

ISC BIND < 4.9.8 / 8.2.3 Multiple Remote Overflows

ISC BIND < 8.2.2-P7 Compressed ZXFR Name Service Query DoS

ISC BIND < 8.3.4 Multiple Remote Vulnerabilities

ISC BIND < 8.3.7 / 8.4.3 Negative Record Cache Poisoning

ISC BIND < 8.4.6 q\_usedns Array Remote Overflow DoS

ISC BIND < 9.2.1 rdataset Parameter Malformed DNS Packet DoS

ISC BIND < 9.2.2 DNS Resolver Functions Remote Overflow

ISC BIND < 9.3.1 Validator Self Checking Remote DoS

ISC BIND < 9.4.1 / 9.5.0a4 query.c query\_addsoa Function Recursive Query DoS

ISC BIND Allow-Recursion Vulnerability

ISC BIND Assertion Error Resource Record RDATA Query Parsing Remote DoS

ISC BIND Assertion Failure Vulnerability

ISC BIND Assertion Failure Vulnerability

ISC BIND Assertion Failure Vulnerability (DoS)

ISC BIND Assertion Failure Vulnerability (DoS)

ISC BIND Cache Update Policy Deleted Domain Name Resolving Weakness

ISC BIND Crafted ANY Request Response Multiple RRsets DoS

ISC BIND Dynamic Update Message Handling Remote DoS

ISC BIND Dynamic Updates Unauthorized Resource Record Manipulation

ISC BIND Memory Leak DoS Vulnerability

ISC BIND Multiple Vulnerabilities

ISC BIND named SIG Resource Server Response RR Overflow

ISC BIND Race Condition Vulnerability (CVE-2019-6471)

ISC BIND Response Policy Zones (RPZ) DNAME / CNAME Parsing Remote DoS

ISC BIND Response Policy Zones RRSIG Query Assertion Failure DoS

ISC BIND Unsupported Version Detection

ISC BIND Zone Data Denial of Service

Knot DNS 1.5.2 Incremental Zone Transfer (IXFR) DoS

Knot DNS 1.6.x < 1.6.6 / 2.0.x < 2.0.2 NAPTR Record DoS

Knot DNS 2.4.x < 2.4.4 / 2.5.x < 2.5.2 TSIG Authentication Bypass Vulnerability (CVE-2017-11104)

Knot DNS < 1.4.5 TSIG Signature Spoofing

Knot DNS < 1.6.3 Multiple Vulnerabilities

Knot DNS Server Version Detection

MaraDNS 0.5.x < 0.5.31 / 0.9.x < 0.9.01 Compression Code Remote DoS

MaraDNS 1.2.12.06 / 1.3.05 Wildcard Resource Record Remote DoS

MaraDNS 1.2.x < 1.2.12.05 / 1.3.x < 1.3.03 IPv6 Memory Leak Remote DoS

MaraDNS 1.2.x < 1.2.12.06 / 1.3.x < 1.3.05 Invalid DNS Packet Fields Remote DoS

MaraDNS 1.3.03 to 1.3.07.10 / 1.4.x < 1.4.03 NULL Pointer Dereference Local DoS (Linux)

MaraDNS 2.0.x < 2.0.05 Hash Collision Zone File Record Local DoS

MaraDNS < 1.0.41 / 1.2.x < 1.2.12.08 / 1.3.x < 1.3.07.04 CNAME Record Resource Rotation Remote DoS

MaraDNS < 1.3.07.11 / 1.4.x < 1.4.06 / 2.0.x < 2.0.02 compress\_add\_dlabel\_points Function Buffer Overflow

MaraDNS < 1.3.07.14 / 1.4.x < 1.4.10 Hash Collision Form Parameter Remote DoS

MaraDNS < 1.3.07.15 / 1.4.x < 1.4.12 / 2.0.x < 2.0.06 Persistent Ghost Domain Caching

MaraDNS < 1.4.14 / 2.0.x < 2.0.09 Deadwood Out-of-Bounds DoS

MaraDNS < 2.0.13 Multiple Vulnerabilities

MaraDNS Server Version Detection

Microsoft DNS Server Inverse Query Buffer Over-Read

Microsoft DNS Server Version Detection

MS07-029: Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (935966) (uncredentialed check)

MS07-062: Vulnerability in DNS Could Allow Spoofing (941672) (uncredentialed check)

MS08-037: Vulnerabilities in DNS Could Allow Spoofing (951746) (uncredentialed check)

MS09-008: Vulnerabilities in DNS Server Could Allow Spoofing (961063) (uncredentialed check)

MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)

MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)

Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Multiple Vendor DNS Response Flooding Denial Of Service

NSD packet.c Off-By-One Remote Overflow

NSD query\_add\_optional() Function NULL Pointer Dereference Malformed DNS Packet Parsing Remote DoS

NSD version Directive Remote Version Disclosure

PowerDNS < 2.9.17 Multiple DoS

PowerDNS < 2.9.18 Multiple Vulnerabilities

PowerDNS Authoritative < 4.0.5 Read Only Configuration Bypass (CVE-2017-15091)

PowerDNS Authoritative Server 3.4.4 / 3.4.5 / 3.4.6 Process Packet Handling DoS

PowerDNS Authoritative Server 3.4.x < 3.4.6 distributor.hh Packet Handling DoS

PowerDNS Authoritative Server 3.x < 3.4.5 Label Decompression Self-Referential Name Handling DoS

PowerDNS Authoritative Server < 2.9.21.2 CH HINFO Query Handling DoS

PowerDNS Authoritative Server < 2.9.22.5 / 3.0.1 Response Packet Parsing DoS

PowerDNS Authoritative Server Malformed Query Cache Poisoning Weakness

PowerDNS Recursor 3.3.x / 3.4.x / 3.5 RC1 Cache Update Policy Deleted Domain Name Resolving Weakness

PowerDNS Recursor 3.6.0 Packet Sequence Handling DoS

PowerDNS Recursor 3.x < 3.0.1 EDNS0 DoS

PowerDNS Recursor 3.x < 3.1.4 Multiple Vulnerabilities

PowerDNS Recursor 3.x < 3.1.6 DNS Predictable Transaction ID (TRXID) Cache Poisoning

PowerDNS Recursor 3.x < 3.1.7.2 Multiple Vulnerabilities

PowerDNS Recursor 3.x < 3.6.2 Recursive Referral Handling DoS

PowerDNS Recursor 3.x < 3.7.3 Label Decompression DoS

PowerDNS Recursor 4.0.x < 4.0.7 Multiple Vulnerabilities

PowerDNS Recursor 4.0.x < 4.0.8 CNAME Parser DoS (CVE-2017-15120)

PowerDNS Recursor 4.1.0 DNSSEC Signature Validation Spoofing Vulnerability (CVE-2018-1000003)

PowerDNS Recursor < 4.0.7 API Configuration Injection Vulnerability (CVE-2017-15093)

PowerDNS Unsupported Version Detection

PowerDNS Version Detection

SheerDNS < 1.0.1 Multiple Vulnerabilities

Unbound < 1.3.4 NSEC3 Signature Verification DNS Spoofing Vulnerability (CVE-2009-3602)

Unbound < 1.4.10 daemon/worker.c DNS Request Error Handling DoS

Unbound < 1.4.11 Cache Update Policy Deleted Domain Name Resolving Weakness

Unbound < 1.4.14 / 1.4.13p2 Multiple DoS

Unbound < 1.4.3 'sock\_list' Structure Allocation Remote Denial Of Service Vulnerability (CVE-2010-0969)

Unbound < 1.4.4 Unbound Signed Zone Query Response DNSSEC Outage DoS

Unbound < 1.5.1 Delegation Handling Recursive Referral Handling Resource Exhaustion DoS

Unbound < 1.5.2 Upstream Server Trust Anchor Unspecified DNSSEC Validation Weakness

Unbound < 1.5.9 daemon/remote.c Diffie-Hellman Key Exchange Value Small Subgroup Confinement Attack Vulnerability

Unbound < 1.6.3 use-caps-for-id Option qname Handling Denial of Service

Unbound < 1.6.4 parse\_edns\_options Heap Buffer Overflow

Unbound < 1.6.8 Wildcard Synthesized NSEC Records Handling Remote Validation Weakness

Unbound DNS Resolver Remote Version Detection

Unsupported Microsoft DNS Server Detection

WindowsNT DNS Server Character Saturation DoS

# Denial of Service

+ + + ATH0 Modem Hang Up String Remote DoS

3Com HiPer Access Router Card (HiperARC) IAC Packet Flood DoS

3com RAS 1500 / Wyse Winterm Malformed Packet Remote DoS

Allegro Software RomPager 2.10 Malformed Authentication Request DoS

Apache Struts 2 ClassLoader Manipulation Incomplete Fix for Security Bypass

Apache Struts ClassLoader Manipulation

AppSocket Half-open Connection Remote DoS

Ascend MAX / Pipeline Router Discard Port Malformed Packet DoS

Asterisk IAX2 (IAX) POKE Request Saturation Resource Exhaustion Remote DoS

Asterisk IAX2 Call Number Exhaustion DoS

Asterisk IAX2 FWDOWNL Request Spoofing Remote DoS

Asterisk IAX2 Multiple Method Handshake Spoofing DoS

Asterisk Multiple Channel Drivers Denial of Service (AST-2011-008 / AST-2011-009 / AST-2011-010)

Asterisk Multiple Denial of Service Vulnerabilities (AST-2011-003 / AST-2011-004)

Asterisk Multiple Vulnerabilities (AST-2011-005 / AST-2011-006)

Asterisk SIP Channel Driver Denial of Service (AST-2011-007)

Asterisk SIP Channel Driver Uninitialized Variable Request Parsing DoS (AST-2011-012)

AVM KEN! ISDN Proxy Server Malformed Request Remote DoS

BlackBerry Enterprise Server Crafted SRP Packet Remote DoS

BNBT EasyTracker Malformed GET Request Remote DoS

CA Multiple Products Message Queuing Multiple Remote DoS

Cajun Switch Negative Integer Handling Remote DoS

Cassandra NNTP Server Login Name Remote Overflow DoS

Chargen UDP Service Remote DoS

Dropbear SSH Authorization-pending Connection Saturation DoS

Eicon Technology Diva LAN ISDN Modem login.htm Long password Field DoS

Ekiga < 4.0.0 Invalid UTF-8 Character Connection Data Parsing DoS

Ekiga < 4.0.1 ptlib XML Expansion Recursion DoS

F-Secure Policy Manager Server fsmsh.dll module DoS

FreeBSD nfsd Malformed NFS Mount Request Remote DoS

GameSpy 3D Based Games Spoofed UDP Response Amplification DDoS

GameSpy SDK Malformed \query\ Request Overflow DoS

Helix RealServer HTTP GET Request DoS

Helix Universal Server Remote Integer Handling DoS

IBM Lotus Domino < 7.0.2 FP3 Unspecified DoS

IBM Tivoli Directory Server LDAP Packet Handling DoS

IPSEC Server ISAKMP Implementation Malformed IKE Request Remote DoS

ipsec-tools KAME racoon Daemon ISAKMP Header Parsing Remote DoS

ISC DHCP Server supersede\_lease() Function DHCPDISCOVER Packet DoS

Jabber Studio jabberd SASL Negotiation Remote DoS

JBoss Remoting RemoteMessageChannel DoS (intrusive check)

Kame Racoon Invalid Cookie Handling Remote DoS

Kerio MailServer < 6.0.10 Multiple Mail Handling DoS

Kerio MailServer < 6.3.1 Long LDAP Query DoS

Kerio MailServer IMAP Server Crafted LOGIN Command DoS

Kerio MailServer Webmail Malformed Email Handling Resource Exhaustion DoS

l2tpd Malformed Data Remote DoS

LANDesk idsintkm.dll Multiple Port Connection Remote DoS

Libssh ssh\_packet\_kexinit() Double-free Memory DoS

Linux 2.1.89 - 2.2.3 IP Fragmenting Functionality 0 Length Fragment Handling Remote DoS

Linux 2.4 NFSv3 knfsd Malformed GETATTR Request Remote DoS

Linux 2.6 Netfilter TCP Option Matching DoS

Linux Kernel Netfilter \*\_conntrack\_proto\_sctp.c sctp\_new Function Unknown Chunk Type Remote DoS

Linux SCTP ECNE Chunk Handling Remote DoS

Linux SCTP Functionality Multiple Remote DoS

Linux SCTP ICMP Packet Handling Null Dereference Remote DoS

Livingston PortMaster ComOS Malformed Packet Remote DoS

Lotus Domino /./ Request Database Locking DoS

Lotus Domino LDAP Server Crafted Packet Remote DoS

LSH lshd parse\_kexinit() Function Malformed Key Exchange Message Remote DoS

Mac OS X Directory Service Connection Saturation Remote DoS

Macromedia Flash Media Server Administration Service Crafted Packet Remote DoS

MailEnable IMAP Connection Saturation Remote DoS (ME-10042)

Marconi ASX-1000 Switches Multiple Interface Malformed Packet DoS

memcached No Newline Memory Consumption DoS

Multiple IRC Client Non-registered User parse\_client\_queued Saturation DoS

Multiple Vendor Out Of Band Data DoS (WinNuke)

NAI PGP Certificate Server Unresolvable IP DoS

Network Block Device (NBD) Server Request Handling Remote Overflow

Network Service Long Line Handling Remote DoS

Network Service Malformed Data Remote DoS

NIPrint LPD-LPR Print Server String Handling Remote Overflow

Novell eDirectory < 8.8.5 ftf1/8.7.3.10 ftf2 NULL Base DN DoS

Novell eDirectory Host Environment Service (dhost.exe) HTTP Connection Header DoS

Openfire < 3.5.0 ConnectionManagerImpl.java Queue Handling Remote DoS

OpenLDAP SASL authcid Name BIND Request DoS

OpenSSH < 3.6.1p2 Multiple Vulnerabilities

OpenSSH < 5.9 Multiple DoS

OpenSSH LoginGraceTime / MaxStartups DoS

OpenSSH With OpenPAM DoS

Palo Alto Networks PAN-OS Management Interface API Remote DoS (PAN-SA-2016-0008)

Palo Alto Networks PAN-OS Management Interface Remote DoS (PAN-SA-2016-0027)

Quagga / Zebra Malformed Telnet Command Denial of Service

RealServer Long ramgen Request Remote DoS

RealServer Malformed viewsource Directory Request DoS

RealServer Port 7070 Malformed Input DoS

Rendezvous < 8.0.0 Crafted Packet Remote DoS

Samba < 3.0.7 Multiple Remote DoS

Samba smbd FindNextPrintChangeNotify() Request Remote DoS

Solaris 10 ICMP Packet Handling DoS

Solaris ^D Character Remote Telnet Service DoS

Splunk Enterprise 6.x < 6.0.1 Malformed Packet DoS

Sun Java System Directory Server 6.x < 6.3.1 LDAP JDBC Backend DoS

Sun ONE Directory Server LDAP Malformed Packet DoS

SuSE Linux in.identd Request Saturation DoS

TCP/IP 'Chorusing' Windows DoS

TCP/IP ACK Packet Saturation Remote DoS (stream.c)

TCP/IP Fragmentation DoS (nestea)

TCP/IP IGMP Overlap Remote DoS (pimp)

TCP/IP IP Fragment Re-Assembly Remote DoS (teardrop)

TCP/IP IP Fragmentation Remote DoS (bonk)

TCP/IP IP Fragmentation Remote DoS (jolt2)

TCP/IP Multicast Address Handling Remote DoS (spank.c)

TCP/IP Ping of Death Remote DoS (jolt)

TCP/IP Sequence Prediction Blind Reset Spoofing DoS

TCP/IP SYN Loopback Request Remote DoS (land.c)

up-imapproxy IMAP Proxy IMAP\_Line\_Read() Function Literal Size DoS

Ventrilo Server Malformed Status Query Remote DoS

Veritas Storage Foundation Multiple Service Remote DoS (SYM08-004)

Zebedee Malformed Protocol Option Header Port 0 Remote DoS

# Default Unix Accounts

Default Password '00000000' for 'root' Account

Default Password '1111' for 'admin' Account

Default Password '1111' for 'root' Account

Default Password '1111111' for 'admin' Account

Default Password '1234' for 'admin' Account

Default Password '1234' for 'administrator' Account

Default Password '1234' for 'root' Account

Default Password '12345' for 'admin' Account

Default Password '12345' for 'guest' Account

Default Password '12345' for 'root' Account

Default Password '123456' for 'admin' Account

Default Password '123456' for 'root' Account

Default Password '4321' for 'admin' Account

Default Password '54321' for 'admin' Account

Default Password '54321' for 'root' Account

Default Password '5SaP9I26' for 'remotessh' Account

Default Password '666666' for '666666' Account

Default Password '666666' for 'root' Account

Default Password '7ujMko0admin' for 'admin' Account

Default Password '7ujMko0admin' for 'root' Account

Default Password '7ujMko0vizxv' for 'root' Account

Default Password '888888' for '888888' Account

Default Password '888888' for 'root' Account

Default Password 'admin123' for 'admin' Account

Default Password 'admin1234' for 'admin' Account

Default Password 'adminIWSS85' for 'admin' Account

Default Password 'adminIWSS85' for 'root' Account

Default Password 'anko' for 'root' Account

Default Password 'cat1029' for 'Wproot' Account

Default Password 'dreambox' for 'root' Account

Default Password 'f\*\*\*\*r' for 'mother' Account

Default Password 'hi3518' for 'root' Account

Default Password 'ikwb' for 'root' Account

Default Password 'juantech' for 'root' Account

Default Password 'jvbzd' for 'root' Account

Default Password 'klv123' for 'root' Account

Default Password 'klv1234' for 'root' Account

Default Password 'meinsm' for 'admin' Account

Default Password 'meinsm' for 'Administrator' Account

Default Password 'P@ssw0rd' for 'admin' Account

Default Password 'padmin' for 'padmin' Account

Default Password 'pass' for 'admin' Account

Default Password 'pass' for 'root' Account

Default Password 'password' for 'admin1' Account

Default Password 'QwestM0dem' for 'admin' Account

Default Password 'realtek' for 'root' Account

Default Password 'service' for 'service' Account

Default Password 'smcadmin' for 'admin' Account

Default Password 'St0r@ge!' for 'administrator' Account

Default Password 'supervisor' for 'supervisor' Account

Default Password 'support' for 'support' Account

Default Password 'system' for 'root' Account

Default Password 'tech' for 'tech' Account

Default Password 'ubnt' for 'ubnt' Account

Default Password 'user' for 'root' Account

Default Password 'vizxv' for 'root' Account

Default Password 'xc3511' for 'root' Account

Default Password 'xmhdipc' for 'root' Account

Default Password 'zlxx.' for 'root' Account

Default Password 'Zte521' for 'root' Account

Default Password ('!2345Asdfg') for 'root' Account

Default Password ('scpuser') for 'scpuser' Account

Default Password (0p3nm35h) for 'root' Account

Default Password (123456) for 'nexthink' Account

Default Password (12345678) for 'root' Account on MacOS X Server

Default Password (abc123) for 'admin' Account

Default Password (abc123) for 'root' Account

Default Password (admin) for 'admin' Account

Default Password (admin) for 'root' Account

Default Password (alien) for 'root' Account

Default Password (alpine) for 'mobile' Account

Default Password (alpine) for 'root' Account

Default Password (arcsight) for 'root' Account

Default Password (arkeia) for 'root' Account

Default Password (artica) for 'root' Account

Default Password (badg3r5) for 'HPSupport' Account

Default Password (bank) for 'bank' Account

Default Password (centreon) for 'root' Account

Default Password (CenturyL1nk) for 'admin' Account

Default Password (changeme) for 'splunkadmin' Account

Default Password (changemenow) for 'root' Account

Default Password (cliuser) for 'cliuser' Account

Default Password (D13HH[) for 'root' Account

Default Password (D13hh[) for 'root' Account

Default password (dasdec1) for 'root' account

Default Password (db2as) for 'db2as' Account

Default Password (db2fenc1) for 'db2fenc1' Account

Default Password (db2inst) for 'db2inst1' Account

Default Password (debug) for 'super' Account

Default Password (debug) for 'user' Account

Default Password (default) for 'root' Account

Default Password (dottie) for 'root' Account

Default Password (f00b@r) for 'root' Account

Default Password (facepunch) for 'chronos' Account

Default Password (forgot) for 'super' Account

Default Password (forgot) for 'user' Account

Default Password (gforge) for 'root' Account

Default Password (glftpd) for 'glftpd' Account

Default Password (guest) for 'guest' Account

Default Password (ibmdb2) for 'db2as' Account

Default Password (ibmdb2) for 'db2fenc1' Account

Default Password (ibmdb2) for 'db2inst1' Account

Default Password (infoblox) for 'admin' Account

Default Password (informix) for 'informix' Account

Default Password (ironport) for 'admin' Account

Default Password (ironport) for 'enablediag' Account

Default Password (lrkr0x) for 'gamez' Account

Default Password (m) for 'root' Account

Default Password (manager) for 'system' Account

Default Password (merlin) for 'mg3500' Account

Default Password (nagiosxi) for 'root' Account

Default Password (nas4free) for 'root' Account

Default Password (nasadmin) for 'nasadmin' Account

Default Password (nasadmin) for 'root' Account

Default Password (netoptics) for 'admin' Account

Default Password (nsroot) for 'nsroot' Account

Default Password (openelec) for 'root' Account

Default Password (openvpnas) for 'root' Account

Default Password (oracle) for 'oracle' Account

Default Password (passw0rd) for 'superuser' Account

Default Password (password) for 'admin' Account

Default Password (password) for 'admin' Account on Broadcom BCM96338 ADSL Router

Default Password (password) for 'cmc' Account

Default Password (password) for 'emcupdate' Account

Default Password (password) for 'root' Account

Default Password (patrol) for 'patrol' Account

Default Password (profense) for 'operator' Account

Default Password (public) for 'public' Account

Default Password (rain) for 'root' Account

Default Password (raspberry) for 'pi' Account

Default Password (raspi) for 'root' Account

Default Password (root) for 'root' Account

Default Password (rootme) for 'root' Account

Default Password (satori) for 'rewt' Account

Default Password (sq!us3r) for 'dbadmin' Account

Default Password (swift) for 'swift' Account

Default Password (synnet) for 'debug' Account

Default Password (TANDBERG) for 'root' Account

Default Password (testpass123) for 'root' Account

Default Password (toor) for 'root' Account

Default Password (trans) for 'trans' Account

Default Password (ucspe) for 'ucspe' Account

Default Password (user) for 'user' Account

Default Password (vmware) for 'root' Account

Default Password (wank) for 'wank' Account

Default Password (wh00t!) for 'root' Account

Juniper ScreenOS SSH / Telnet Authentication Backdoor

NetApp OnTap OS Default Credentials

pfSense Default SSH Credentials

Remote Authentication Message Check

Unpassworded '4Dgifts' Account

Unpassworded 'backdoor' Account

Unpassworded 'date' Account

Unpassworded 'demos' Account

Unpassworded 'EZsetup' Account

Unpassworded 'friday' Account

Unpassworded 'guest' Account

Unpassworded 'hax0r' Account

Unpassworded 'help' Account

Unpassworded 'jack' Account

Unpassworded 'jill' Account

Unpassworded 'lp' Account

Unpassworded 'mpi' Account

Unpassworded 'OutOfBox' Account

Unpassworded 'r00t' account

Unpassworded 'root' Account

Unpassworded 'StoogR' Account

Unpassworded 'sync' Account

Unpassworded 'toor' Account

Unpassworded 'tutor' Account

Unprotected 'admin' Account

# Debian Local Security Checks

Debian DLA-100-1 : mutt security update

Debian DLA-1000-1 : imagemagick security update

Debian DLA-1001-1 : exim4 security update (Stack Clash)

Debian DLA-1002-1 : smb4k security update

Debian DLA-1003-1 : unrar-nonfree security update

Debian DLA-1004-1 : drupal7 security update

Debian DLA-1005-1 : mercurial security update

Debian DLA-1006-1 : libarchive security update

Debian DLA-1007-1 : icedove/thunderbird security update

Debian DLA-1008-1 : libxml2 security update

Debian DLA-1009-1 : apache2 security update

Debian DLA-101-1 : jasper security update

Debian DLA-1010-1 : vorbis-tools security update

Debian DLA-1011-1 : sudo security update

Debian DLA-1012-1 : puppet security update

Debian DLA-1013-1 : graphite2 security update

Debian DLA-1014-1 : libclamunrar security update

Debian DLA-1015-1 : libgcrypt11 security update

Debian DLA-1016-1 : radare2 security update

Debian DLA-1017-1 : mpg123 security update

Debian DLA-1018-1 : sqlite3 security update

Debian DLA-1019-1 : phpldapadmin security update

Debian DLA-102-1 : tcpdump security update

Debian DLA-1020-1 : jetty security update

Debian DLA-1021-1 : jetty8 security update

Debian DLA-1022-1 : tiff security update

Debian DLA-1023-1 : tiff3 security update

Debian DLA-1024-1 : nginx security update

Debian DLA-1025-1 : bind9 security update

Debian DLA-1026-1 : xorg-server security update

Debian DLA-1027-1 : heimdal security update (Orpheus' Lyre)

Debian DLA-1028-1 : apache2 security update

Debian DLA-1029-1 : libmtp security update

Debian DLA-103-1 : linux-2.6 security update

Debian DLA-1030-1 : vim security update

Debian DLA-1031-1 : evince security update

Debian DLA-1032-1 : unattended-upgrades regression update

Debian DLA-1033-1 : memcached security update

Debian DLA-1034-1 : php5 security update

Debian DLA-1035-1 : qemu security update

Debian DLA-1036-1 : gsoap security update (Devil's Ivy)

Debian DLA-1037-1 : catdoc security update

Debian DLA-1038-1 : libtasn1-3 security update

Debian DLA-1039-1 : rkhunter security update

Debian DLA-104-1 : pdns-recursor security update

Debian DLA-1040-1 : resiprocate security update

Debian DLA-1041-1 : nasm security update

Debian DLA-1042-1 : libquicktime security update

Debian DLA-1043-1 : mysql-5.5 security update

Debian DLA-1044-1 : ipsec-tools security update

Debian DLA-1045-1 : graphicsmagick security update

Debian DLA-1046-1 : lucene-solr security update

Debian DLA-1047-1 : supervisor security update

Debian DLA-1048-1 : ghostscript security update

Debian DLA-1049-1 : libsndfile security update

Debian DLA-105-1 : graphviz security update

Debian DLA-1051-1 : postgresql-9.1 security update

Debian DLA-1052-1 : subversion security update

Debian DLA-1053-1 : firefox-esr security update

Debian DLA-1054-1 : libgxps security update

Debian DLA-1055-1 : libgd2 security update

Debian DLA-1056-1 : cvs security update

Debian DLA-1057-1 : libraw security update

Debian DLA-1058-1 : krb5 security update

Debian DLA-1059-1 : strongswan security update

Debian DLA-106-1 : getmail4 security update

Debian DLA-1060-1 : libxml2 security update

Debian DLA-1061-1 : newsbeuter security update

Debian DLA-1062-1 : curl security update

Debian DLA-1063-1 : extplorer security update

Debian DLA-1064-1 : freeradius security update

Debian DLA-1065-1 : fontforge security update

Debian DLA-1066-1 : php5 security update

Debian DLA-1067-1 : augeas security update

Debian DLA-1068-1 : git security update

Debian DLA-1069-1 : tenshi security update

Debian DLA-107-1 : unbound security update

Debian DLA-1070-1 : qemu security update

Debian DLA-1071-1 : qemu-kvm security update

Debian DLA-1072-1 : mercurial security update

Debian DLA-1073-1 : openjdk-7 security update

Debian DLA-1074-1 : poppler security update

Debian DLA-1075-1 : wordpress security update

Debian DLA-1076-1 : php5 security update

Debian DLA-1077-1 : faad2 security update

Debian DLA-1078-1 : connman security update

Debian DLA-1079-1 : libdbd-mysql-perl security update

Debian DLA-108-1 : nfs-utils security update

Debian DLA-1080-1 : gnupg security update

Debian DLA-1081-1 : imagemagick security update

Debian DLA-1082-1 : graphicsmagick security update

Debian DLA-1083-1 : openexr security update

Debian DLA-1084-1 : libidn security update

Debian DLA-1085-1 : libidn2-0 security update

Debian DLA-1086-1 : enigmail security update

Debian DLA-1087-2 : icedove/thunderbird regression update

Debian DLA-1088-1 : irssi security update

Debian DLA-1089-1 : irssi security update

Debian DLA-109-1 : libyaml-libyaml-perl security update

Debian DLA-1090-1 : tcpdump security update

Debian DLA-1091-1 : unrar-free security update

Debian DLA-1092-1 : libarchive security update

Debian DLA-1093-1 : tiff security update

Debian DLA-1094-1 : tiff3 security update

Debian DLA-1095-1 : freerdp security update

Debian DLA-1096-1 : wordpress-shibboleth security update

Debian DLA-1097-1 : tcpdump security update

Debian DLA-1098-1 : freexl security update

Debian DLA-1099-1 : linux security update (BlueBorne) (Stack Clash)

Debian DLA-110-1 : libyaml security update

Debian DLA-1100-1 : gdk-pixbuf security update

Debian DLA-1101-1 : emacs23 security update

Debian DLA-1102-1 : apache2 security update (Optionsbleed)

Debian DLA-1103-1 : bluez security update (BlueBorne)

Debian DLA-1104-1 : newsbeuter security update

Debian DLA-1105-1 : clamav security update

Debian DLA-1106-1 : libgd2 security update

Debian DLA-1107-1 : bzr security update

Debian DLA-1108-1 : tomcat7 security update

Debian DLA-1109-1 : libraw security update

Debian DLA-111-1 : cpio security update

Debian DLA-1110-1 : samba security update

Debian DLA-1111-1 : weechat security update

Debian DLA-1112-1 : rubygems security update

Debian DLA-1113-1 : ruby1.8 security update

Debian DLA-1114-1 : ruby1.9.1 security update

Debian DLA-1115-1 : debsecan update

Debian DLA-1116-1 : poppler security update

Debian DLA-1117-1 : opencv security update

Debian DLA-1118-1 : firefox-esr security update

Debian DLA-1119-1 : otrs2 security update

Debian DLA-112-1 : bind9 security update

Debian DLA-1120-1 : git security update

Debian DLA-1121-1 : curl security update

Debian DLA-1122-1 : asterisk security update

Debian DLA-1123-1 : golang security update

Debian DLA-1124-1 : dnsmasq security update

Debian DLA-1125-1 : botan1.10 security update

Debian DLA-1126-1 : libxfont security update

Debian DLA-1127-1 : sam2p security update

Debian DLA-1128-1 : qemu-kvm security update

Debian DLA-1129-1 : qemu security update

Debian DLA-113-1 : bsd-mailx security update

Debian DLA-1131-1 : imagemagick security update

Debian DLA-1132-1 : xen security update

Debian DLA-1133-1 : ming security update

Debian DLA-1134-1 : sdl-image1.2 security update

Debian DLA-1135-1 : db security update

Debian DLA-1136-1 : db4.8 security update

Debian DLA-1137-1 : db4.7 security update

Debian DLA-1138-1 : nss security update

Debian DLA-1139-1 : imagemagick security update

Debian DLA-114-1 : heirloom-mailx security update

Debian DLA-1140-1 : graphicsmagick security update

Debian DLA-1141-1 : mysql-5.5 security update

Debian DLA-1142-1 : libav security update

Debian DLA-1143-1 : curl security update

Debian DLA-1144-1 : git-annex security update

Debian DLA-1145-1 : zoneminder security update

Debian DLA-1146-1 : mosquitto security update

Debian DLA-1147-1 : exiv2 security update

Debian DLA-1148-1 : golang security update

Debian DLA-1149-1 : wget security update

Debian DLA-1150-1 : wpa security update (KRACK)

Debian DLA-1151-2 : wordpress regression update

Debian DLA-1152-1 : quagga security update

Debian DLA-1153-1 : icedove/thunderbird security update

Debian DLA-1154-1 : graphicsmagick security update

Debian DLA-1155-1 : tzdata new upstream version

Debian DLA-1156-1 : libdatetime-timezone-perl new upstream version

Debian DLA-1157-1 : openssl security update

Debian DLA-1158-1 : bchunk security update

Debian DLA-1159-1 : graphicsmagick security update

Debian DLA-116-1 : ntp security update

Debian DLA-1160-1 : wordpress security update

Debian DLA-1161-1 : redis security update

Debian DLA-1162-1 : apr security update

Debian DLA-1163-1 : apr-util security update

Debian DLA-1164-1 : mupdf security update

Debian DLA-1165-1 : libpam4j security update

Debian DLA-1166-2 : tomcat7 regression update

Debian DLA-1167-1 : ruby-yajl security update

Debian DLA-1168-1 : graphicsmagick security update

Debian DLA-1169-1 : postgresql-common security update

Debian DLA-117-1 : qt4-x11 security update

Debian DLA-1170-1 : graphicsmagick security update

Debian DLA-1171-1 : libxml-libxml-perl security update

Debian DLA-1172-1 : firefox-esr security update

Debian DLA-1173-1 : procmail security update

Debian DLA-1174-1 : konversation security update

Debian DLA-1175-1 : lynx-cur security update

Debian DLA-1176-1 : ming security update

Debian DLA-1177-1 : poppler security update

Debian DLA-1178-1 : opensaml2 security update

Debian DLA-1179-1 : shibboleth-sp2 security update

Debian DLA-118-1 : linux-2.6 security update

Debian DLA-1180-1 : libspring-ldap-java security update

Debian DLA-1181-1 : xen security update

Debian DLA-1182-1 : ldns security update

Debian DLA-1183-1 : samba security update

Debian DLA-1184-1 : optipng security update

Debian DLA-1185-1 : sam2p security update

Debian DLA-1186-1 : xorg-server security update

Debian DLA-1187-1 : openjdk-7 security update

Debian DLA-1188-1 : libxml2 security update

Debian DLA-1189-1 : python2.7 security update

Debian DLA-119-1 : subversion security update

Debian DLA-1190-1 : python2.6 security update

Debian DLA-1191-1 : python-werkzeug security update

Debian DLA-1192-1 : libofx security update

Debian DLA-1193-1 : roundcube security update

Debian DLA-1194-1 : libxml2 security update

Debian DLA-1195-1 : curl security update

Debian DLA-1196-1 : optipng security update

Debian DLA-1197-1 : sox security update

Debian DLA-1198-1 : libextractor security update

Debian DLA-1199-1 : thunderbird security update

Debian DLA-120-2 : xorg-server regression update

Debian DLA-1200-1 : linux security update (KRACK)

Debian DLA-1201-1 : libxcursor security update

Debian DLA-1202-1 : firefox-esr security update

Debian DLA-1203-2 : xrdp regression update

Debian DLA-1204-1 : evince security update

Debian DLA-1205-1 : simplesamlphp security update

Debian DLA-1206-1 : tiff security update

Debian DLA-1207-1 : erlang security update (ROBOT)

Debian DLA-1208-1 : reportbug update

Debian DLA-1209-1 : sensible-utils security update

Debian DLA-121-1 : jasper security update

Debian DLA-1210-1 : kildclient security update

Debian DLA-1211-1 : libxml2 security update

Debian DLA-1212-1 : otrs2 security update

Debian DLA-1213-1 : openafs security update

Debian DLA-1214-1 : libreoffice security update

Debian DLA-1215-1 : otrs2 security update

Debian DLA-1216-1 : wordpress security update

Debian DLA-1217-1 : irssi security update

Debian DLA-1218-1 : rsync security update

Debian DLA-1219-1 : enigmail security update

Debian DLA-122-1 : eglibc security update

Debian DLA-1220-1 : gimp security update

Debian DLA-1221-1 : ruby1.9.1 security update

Debian DLA-1222-1 : ruby1.8 security update

Debian DLA-1223-1 : thunderbird security update

Debian DLA-1224-1 : mercurial security update

Debian DLA-1225-1 : asterisk security update

Debian DLA-1226-1 : wireshark security update

Debian DLA-1227-1 : imagemagick security update

Debian DLA-1228-1 : poppler security update

Debian DLA-1229-1 : imagemagick security update

Debian DLA-123-1 : firebird2.5 security update

Debian DLA-1230-1 : xen security update

Debian DLA-1231-1 : graphicsmagick security update

Debian DLA-1232-1 : linux security update (Meltdown)

Debian DLA-1233-1 : gifsicle security update

Debian DLA-1234-2 : gdk-pixbuf regression update

Debian DLA-1235-1 : opencv security update

Debian DLA-1236-1 : plexus-utils security update

Debian DLA-1237-1 : plexus-utils2 security update

Debian DLA-1238-1 : awstats security update

Debian DLA-1239-1 : poco security update

Debian DLA-124-1 : unzip security update

Debian DLA-1240-1 : ming security update

Debian DLA-1241-1 : libkohana2-php security update

Debian DLA-1242-1 : xmltooling security update

Debian DLA-1243-1 : xbmc security update

Debian DLA-1244-1 : ca-certificates update

Debian DLA-1245-1 : graphicsmagick security update

Debian DLA-1246-1 : transmission security update

Debian DLA-1247-1 : rsync security update

Debian DLA-1248-1 : libgd2 security update

Debian DLA-1249-2 : smarty3 regression update

Debian DLA-125-1 : mime-support security update

Debian DLA-1250-1 : mysql-5.5 security update

Debian DLA-1251-1 : php5 security update

Debian DLA-1252-1 : couchdb security update

Debian DLA-1253-1 : openocd security update

Debian DLA-1254-1 : lucene-solr security update

Debian DLA-1255-1 : bind9 security update

Debian DLA-1256-1 : firefox-esr security update

Debian DLA-1257-1 : openssh security update

Debian DLA-1258-1 : wireshark security update

Debian DLA-1259-1 : tiff security update

Debian DLA-126-1 : ettercap security update

Debian DLA-1260-1 : tiff3 security update

Debian DLA-1261-1 : clamav security update

Debian DLA-1262-1 : thunderbird security update

Debian DLA-1263-1 : curl security update

Debian DLA-1264-1 : unbound security update

Debian DLA-1265-1 : krb5 security update

Debian DLA-1266-1 : squid3 security update

Debian DLA-1267-1 : squid security update

Debian DLA-1268-1 : p7zip security update

Debian DLA-1269-1 : dokuwiki security update

Debian DLA-127-1 : pyyaml security update

Debian DLA-1270-1 : xen security update

Debian DLA-1271-1 : postgresql-9.1 security update

Debian DLA-1272-1 : mailman security update

Debian DLA-1273-1 : simplesamlphp security update

Debian DLA-1274-1 : exim4 security update

Debian DLA-1275-1 : uwsgi security update

Debian DLA-1276-1 : tomcat-native security update

Debian DLA-1277-1 : audacity security update

Debian DLA-1278-1 : librsvg security update

Debian DLA-1279-1 : clamav security update

Debian DLA-128-1 : sox security update

Debian DLA-1280-1 : pound security update

Debian DLA-1281-1 : advancecomp security update

Debian DLA-1282-1 : graphicsmagick security update

Debian DLA-1283-2 : python-crypto security update

Debian DLA-1284-1 : leptonlib security update

Debian DLA-1285-1 : bind9 security update

Debian DLA-1286-1 : quagga security update

Debian DLA-1287-1 : zziplib security update

Debian DLA-1288-1 : cups security update

Debian DLA-1289-1 : irssi security update

Debian DLA-129-1 : polarssl security update

Debian DLA-1290-1 : libvpx security update

Debian DLA-1291-1 : tzdata new upstream version

Debian DLA-1292-1 : libdatetime-timezone-perl new upstream version

Debian DLA-1293-1 : imagemagick security update

Debian DLA-1294-1 : golang security update

Debian DLA-1295-1 : drupal7 security update

Debian DLA-1296-1 : xmltooling security update

Debian DLA-1297-1 : freexl security update

Debian DLA-1298-1 : simplesamlphp security update

Debian DLA-1299-1 : libjgraphx-java security update

Debian DLA-130-1 : firebird2.1 security update

Debian DLA-1300-1 : xen security update

Debian DLA-1301-1 : tomcat7 security update

Debian DLA-1302-1 : leptonlib security update

Debian DLA-1303-1 : python-django security update

Debian DLA-1304-1 : zsh security update

Debian DLA-1305-1 : ming security update

Debian DLA-1306-1 : vips security update

Debian DLA-1307-1 : clamav security update

Debian DLA-1308-1 : firefox-esr security update

Debian DLA-1309-1 : curl security update

Debian DLA-131-1 : file security update

Debian DLA-1310-1 : exempi security update

Debian DLA-1311-1 : adminer security update

Debian DLA-1312-1 : libvorbisidec security update

Debian DLA-1313-1 : isc-dhcp security update

Debian DLA-1314-1 : simplesamlphp security update

Debian DLA-1315-1 : libvirt security update

Debian DLA-1316-1 : freeplane security update

Debian DLA-1318-1 : irssi security update

Debian DLA-1319-1 : firefox-esr security update

Debian DLA-132-1 : openssl security update (FREAK)

Debian DLA-1320-1 : samba security update

Debian DLA-1321-1 : firefox-esr security update

Debian DLA-1322-1 : graphicsmagick security update

Debian DLA-1323-1 : tzdata security update

Debian DLA-1324-1 : libdatetime-timezone-perl security update

Debian DLA-1325-1 : drupal7 security update (Drupalgeddon 2)

Debian DLA-1326-1 : php5 security update

Debian DLA-1327-1 : thunderbird security update

Debian DLA-1328-1 : xerces-c security update

Debian DLA-1329-1 : memcached security update

Debian DLA-133-1 : unrtf security update

Debian DLA-1330-1 : openssl security update

Debian DLA-1331-1 : mercurial security update

Debian DLA-1332-1 : libvncserver security update

Debian DLA-1333-1 : dovecot security update

Debian DLA-1334-1 : mosquitto security update

Debian DLA-1335-1 : zsh security update

Debian DLA-1336-1 : rubygems security update

Debian DLA-1337-1 : jruby security update

Debian DLA-1338-1 : beep security update

Debian DLA-1339-1 : openjdk-7 security update

Debian DLA-134-1 : curl security update

Debian DLA-1340-1 : sam2p security update

Debian DLA-1341-1 : sdl-image1.2 security update

Debian DLA-1342-1 : ldap-account-manager security update

Debian DLA-1343-1 : ming security update

Debian DLA-1344-1 : squirrelmail security update

Debian DLA-1345-1 : perl security update

Debian DLA-1346-1 : tiff security update

Debian DLA-1347-1 : tiff3 security update

Debian DLA-1348-1 : patch security update

Debian DLA-1349-1 : linux-tools security update

Debian DLA-135-1 : ia32-libs security update

Debian DLA-1350-1 : qemu-kvm security update

Debian DLA-1351-1 : qemu security update

Debian DLA-1352-1 : jruby security update

Debian DLA-1353-1 : wireshark security update

Debian DLA-1354-1 : opencv security update

Debian DLA-1355-1 : mysql-5.5 security update

Debian DLA-1356-1 : libreoffice security update

Debian DLA-1357-1 : gunicorn security update

Debian DLA-1358-1 : ruby1.9.1 security update

Debian DLA-1359-1 : ruby1.8 security update

Debian DLA-136-1 : websvn security update

Debian DLA-1360-1 : lucene-solr security update

Debian DLA-1361-1 : psensor security update

Debian DLA-1362-1 : gcc-4.9-backport new package

Debian DLA-1363-1 : ghostscript security update

Debian DLA-1364-1 : openslp-dfsg security update

Debian DLA-1365-1 : drupal7 security update (Drupalgeddon 2)

Debian DLA-1366-1 : wordpress security update

Debian DLA-1367-1 : slurm-llnl security update

Debian DLA-1368-1 : libvorbis security update

Debian DLA-1369-1 : linux security update (Spectre)

Debian DLA-137-1 : libevent security update

Debian DLA-1370-1 : quassel security update

Debian DLA-1371-1 : tzdata new upstream release

Debian DLA-1372-1 : libdatetime-timezone-perl new upstream release

Debian DLA-1373-1 : php5 security update

Debian DLA-1374-1 : firebird2.5 security update

Debian DLA-1375-1 : wget security update

Debian DLA-1376-1 : firefox-esr security update

Debian DLA-1377-1 : tiff security update

Debian DLA-1378-1 : tiff3 security update

Debian DLA-1379-1 : curl security update

Debian DLA-138-1 : jasper security update

Debian DLA-1380-1 : libmad security update

Debian DLA-1381-1 : imagemagick security update

Debian DLA-1382-1 : thunderbird security update

Debian DLA-1383-1 : xen security update

Debian DLA-1384-1 : xdg-utils security update

Debian DLA-1385-1 : batik security update

Debian DLA-1386-1 : ming security update

Debian DLA-1387-1 : cups security update

Debian DLA-1388-1 : wireshark security update

Debian DLA-1389-1 : apache2 security update

Debian DLA-139-1 : eglibc security update (GHOST)

Debian DLA-1390-1 : procps security update

Debian DLA-1391-1 : tiff security update

Debian DLA-1392-1 : linux security update

Debian DLA-1394-1 : imagemagick security update

Debian DLA-1395-1 : php-horde-image security update

Debian DLA-1397-1 : php5 security update

Debian DLA-1398-1 : php-horde-crypt security update

Debian DLA-1399-1 : ruby-passenger security update

Debian DLA-140-1 : rpm security update

Debian DLA-1400-2 : tomcat7 regression update

Debian DLA-1401-1 : graphicsmagick security update

Debian DLA-1402-1 : exiv2 security update

Debian DLA-1403-1 : zendframework security update

Debian DLA-1404-1 : lava-server security update

Debian DLA-1405-1 : libgcrypt20 security update

Debian DLA-1406-1 : firefox-esr security update

Debian DLA-1407-1 : mariadb-10.0 security update

Debian DLA-1408-1 : simplesamlphp security update

Debian DLA-1409-1 : mosquitto security update

Debian DLA-141-1 : libksba security update

Debian DLA-1410-1 : python-pysaml2 security update

Debian DLA-1411-1 : tiff security update

Debian DLA-1412-1 : cups security update

Debian DLA-1413-1 : dokuwiki security update

Debian DLA-1414-2 : mercurial regression update

Debian DLA-1415-1 : phpmyadmin security update

Debian DLA-1416-1 : libsoup2.4 security update

Debian DLA-1417-1 : ca-certificates security update

Debian DLA-1418-1 : bouncycastle security update

Debian DLA-1419-1 : ruby-sprockets security update

Debian DLA-142-1 : privoxy security update

Debian DLA-1420-1 : cinnamon security update

Debian DLA-1421-1 : ruby2.1 security update

Debian DLA-1422-2 : linux security update (Spectre)

Debian DLA-1423-1 : linux-4.9 new package (Spectre)

Debian DLA-1424-1 : linux-latest-4.9 new package

Debian DLA-1425-1 : thunderbird security update

Debian DLA-1426-1 : cups security update

Debian DLA-1427-1 : znc security update

Debian DLA-1428-1 : 389-ds-base security update

Debian DLA-1429-1 : sssd security update

Debian DLA-143-1 : python-django security update

Debian DLA-1430-1 : taglib security update

Debian DLA-1431-1 : ant security update

Debian DLA-1432-1 : gpac security update

Debian DLA-1433-1 : openjpeg2 security update

Debian DLA-1434-1 : linux-base update

Debian DLA-1435-1 : dnsmasq regression update

Debian DLA-1436-1 : gosa security update

Debian DLA-1437-2 : slurm-llnl regression update

Debian DLA-1438-1 : opencv security update

Debian DLA-1439-1 : resiprocate security update

Debian DLA-144-1 : polarssl security update

Debian DLA-1440-1 : libarchive-zip-perl security update

Debian DLA-1441-1 : sympa security update

Debian DLA-1442-2 : mailman regression update

Debian DLA-1443-1 : evolution-data-server security update

Debian DLA-1444-1 : vim-syntastic security update

Debian DLA-1445-3 : busybox regression update

Debian DLA-1446-1 : intel-microcode security update (Spectre)

Debian DLA-1447-1 : libidn security update

Debian DLA-1448-1 : policykit-1 security update

Debian DLA-1449-1 : openssl security update

Debian DLA-145-1 : php5 security update

Debian DLA-1450-1 : tomcat8 security update

Debian DLA-1451-1 : wireshark security update

Debian DLA-1452-1 : wordpress security update

Debian DLA-1453-1 : tomcat7 security update

Debian DLA-1454-1 : network-manager-vpnc security update

Debian DLA-1455-1 : mutt security update

Debian DLA-1456-1 : graphicsmagick security update

Debian DLA-1457-1 : ant security update

Debian DLA-1458-1 : xml-security-c security update

Debian DLA-1459-1 : cgit security update

Debian DLA-146-1 : krb5 security update

Debian DLA-1460-1 : libmspack security update

Debian DLA-1461-1 : clamav security update

Debian DLA-1462-1 : wpa security update

Debian DLA-1463-1 : sam2p security update

Debian DLA-1464-1 : postgresql-9.4 security update

Debian DLA-1465-1 : blender security update

Debian DLA-1466-1 : linux-4.9 security update

Debian DLA-1467-1 : ruby-zip security update

Debian DLA-1468-1 : fuse security update

Debian DLA-1469-1 : libxcursor security update

Debian DLA-147-1 : wpasupplicant security update

Debian DLA-1470-1 : confuse security update

Debian DLA-1471-1 : kamailio security update

Debian DLA-1472-1 : libcgroup security update

Debian DLA-1473-1 : otrs2 security update

Debian DLA-1474-1 : openssh security update

Debian DLA-1475-1 : tomcat-native security update

Debian DLA-1476-1 : dropbear security update

Debian DLA-1477-1 : libgit2 security update

Debian DLA-1478-1 : libextractor security update

Debian DLA-1479-1 : twitter-bootstrap3 security update

Debian DLA-148-1 : sympa security update

Debian DLA-1480-1 : ruby2.1 security update

Debian DLA-1481-1 : linux-4.9 security update (Foreshadow)

Debian DLA-1482-1 : libx11 security update

Debian DLA-1483-1 : 389-ds-base security update

Debian DLA-1484-1 : squirrelmail security update

Debian DLA-1485-1 : bind9 security update

Debian DLA-1486-1 : spice security update

Debian DLA-1487-1 : libtirpc security update

Debian DLA-1488-1 : mariadb-10.0 security update

Debian DLA-1489-1 : spice-gtk security update

Debian DLA-149-1 : ntp security update

Debian DLA-1490-1 : php5 security update

Debian DLA-1491-1 : tomcat8 security update

Debian DLA-1492-1 : dojo security update

Debian DLA-1493-1 : xen security update

Debian DLA-1494-1 : gdm3 security update

Debian DLA-1495-1 : git-annex security update

Debian DLA-1496-1 : lcms2 security update

Debian DLA-1497-1 : qemu security update (Spectre)

Debian DLA-1498-1 : curl security update

Debian DLA-1499-1 : discount security update

Debian DLA-150-1 : unzip security update

Debian DLA-1500-2 : openssh regression update

Debian DLA-1501-1 : libextractor security update

Debian DLA-1502-1 : mgetty security update

Debian DLA-1503-1 : kamailio security update

Debian DLA-1504-1 : ghostscript security update

Debian DLA-1505-1 : zutils security update

Debian DLA-1506-1 : intel-microcode security update (Foreshadow) (Spectre)

Debian DLA-1507-1 : libapache2-mod-perl2 security update

Debian DLA-1508-1 : suricata security update

Debian DLA-1509-1 : php5 security update

Debian DLA-151-1 : libxml2 security update

Debian DLA-1510-1 : glusterfs security update

Debian DLA-1511-1 : reportbug update

Debian DLA-1512-1 : sympa security update

Debian DLA-1513-1 : openafs security update

Debian DLA-1514-1 : texlive-bin security update

Debian DLA-1515-1 : hylafax security update

Debian DLA-1516-1 : okular security update

Debian DLA-1517-1 : dom4j security update

Debian DLA-1518-1 : polarssl security update

Debian DLA-1519-1 : python2.7 security update

Debian DLA-152-1 : postgresql-8.4 update

Debian DLA-1520-1 : python3.4 security update

Debian DLA-1521-1 : otrs2 security update

Debian DLA-1522-1 : strongswan security update

Debian DLA-1523-1 : asterisk security update

Debian DLA-1524-1 : libxml2 security update

Debian DLA-1525-1 : mosquitto security update

Debian DLA-1526-1 : 389-ds-base security update

Debian DLA-1527-2 : ghostscript regression update

Debian DLA-1528-1 : strongswan security update

Debian DLA-153-1 : e2fsprogs security update

Debian DLA-1530-1 : imagemagick security update

Debian DLA-1531-1 : linux-4.9 security update

Debian DLA-154-1 : nss security update (BEAST)

Debian DLA-1542-1 : dnsruby update

Debian DLA-1544-1 : tomcat7 security update

Debian DLA-1545-1 : tomcat8 security update

Debian DLA-1546-1 : moin security update

Debian DLA-1547-1 : libpdfbox-java security update

Debian DLA-1548-1 : libssh security update

Debian DLA-1549-1 : xen security update

Debian DLA-155-1 : linux-2.6 security update

Debian DLA-1550-1 : drupal7 security update

Debian DLA-1551-1 : exiv2 security update

Debian DLA-1552-1 : ghostscript security update

Debian DLA-1553-1 : clamav security update

Debian DLA-1554-2 : 389-ds-base regression update

Debian DLA-1555-1 : libmspack security update

Debian DLA-1556-1 : paramiko security update

Debian DLA-1557-1 : tiff security update

Debian DLA-1558-1 : ruby2.1 security update

Debian DLA-1559-1 : xen security update

Debian DLA-156-1 : samba security update

Debian DLA-1560-1 : gnutls28 security update

Debian DLA-1561-1 : phpldapadmin security update

Debian DLA-1562-3 : poppler regression update

Debian DLA-1563-1 : tzdata new upstream version

Debian DLA-1564-1 : mono security update

Debian DLA-1565-1 : glusterfs security update

Debian DLA-1566-1 : mysql-5.5 security update

Debian DLA-1567-1 : gthumb security update

Debian DLA-1568-1 : curl security update

Debian DLA-1569-2 : libdatetime-timezone-perl regression update

Debian DLA-157-1 : openjdk-6 security update (POODLE)

Debian DLA-1570-1 : mariadb-10.0 security update

Debian DLA-1571-1 : firefox-esr security update

Debian DLA-1572-1 : nginx security update

Debian DLA-1573-1 : firmware-nonfree security update (KRACK)

Debian DLA-1574-1 : imagemagick security update

Debian DLA-1575-1 : thunderbird security update

Debian DLA-1576-1 : ansible security update

Debian DLA-1577-1 : xen security update

Debian DLA-1578-1 : spamassassin security update

Debian DLA-1579-1 : openjpeg2 security update

Debian DLA-158-1 : request-tracker3.8 security update

Debian DLA-1580-1 : systemd security update

Debian DLA-1581-1 : uriparser security update

Debian DLA-1582-1 : liblivemedia security update

Debian DLA-1583-1 : jasper security update

Debian DLA-1584-1 : ruby-i18n security update

Debian DLA-1585-1 : ruby-rack security update

Debian DLA-1586-1 : openssl security update

Debian DLA-1587-1 : pixman security update

Debian DLA-1588-1 : icecast2 security update

Debian DLA-1589-1 : keepalived security update

Debian DLA-159-1 : cups security update

Debian DLA-1590-1 : openjdk-7 security update

Debian DLA-1591-2 : libphp-phpmailer regression update

Debian DLA-1592-1 : otrs2 security update

Debian DLA-1593-1 : phpbb3 security update

Debian DLA-1594-1 : xml-security-c security update

Debian DLA-1595-1 : gnuplot5 security update

Debian DLA-1596-1 : squid3 security update

Debian DLA-1597-1 : gnuplot security update

Debian DLA-1598-1 : ghostscript security update

Debian DLA-1599-1 : qemu security update

Debian DLA-16-1 : libxml2 security update

Debian DLA-160-1 : sudo security update

Debian DLA-1600-1 : libarchive security update

Debian DLA-1601-1 : perl security update

Debian DLA-1602-1 : nsis security update

Debian DLA-1603-1 : suricata security update

Debian DLA-1604-1 : lxml security update

Debian DLA-1605-1 : firefox-esr security update

Debian DLA-1606-1 : gcc-4.9 bugfix update

Debian DLA-1607-1 : samba security update

Debian DLA-1608-1 : php5 security update

Debian DLA-1609-1 : libapache-mod-jk security update

Debian DLA-161-1 : libgtk2-perl security update

Debian DLA-1610-1 : sleuthkit security update

Debian DLA-1611-2 : libav security update

Debian DLA-1612-1 : libarchive security update

Debian DLA-1613-1 : sqlite3 security update

Debian DLA-1614-1 : openjpeg2 security update

Debian DLA-1615-1 : nagios3 security update

Debian DLA-1616-1 : libextractor security update

Debian DLA-1617-1 : libvncserver security update

Debian DLA-1618-1 : libsndfile security update

Debian DLA-1619-1 : graphicsmagick security update

Debian DLA-162-1 : e2fsprogs security update

Debian DLA-1620-1 : ghostscript security update

Debian DLA-1621-1 : c3p0 security update

Debian DLA-1622-1 : debian-security-support security update

Debian DLA-1623-1 : tar security update

Debian DLA-1624-1 : thunderbird security update

Debian DLA-1625-1 : tzdata new upstream version

Debian DLA-1626-1 : libdatetime-timezone-perl new upstream version

Debian DLA-1627-1 : qtbase-opensource-src security update

Debian DLA-1628-2 : jasper regression update

Debian DLA-1629-1 : python-django security update

Debian DLA-163-1 : bind9 security update

Debian DLA-1630-1 : libav security update

Debian DLA-1631-1 : libcaca security update

Debian DLA-1632-1 : libsndfile security update

Debian DLA-1633-1 : sqlite3 security update

Debian DLA-1634-1 : wireshark security update

Debian DLA-1635-1 : sssd security update

Debian DLA-1636-1 : aria2 security update

Debian DLA-1637-1 : apt security update (amended)

Debian DLA-1638-1 : libjpeg-turbo security update

Debian DLA-1639-1 : systemd security update

Debian DLA-164-1 : unace security update

Debian DLA-1640-1 : tmpreaper security update

Debian DLA-1641-1 : mxml security update

Debian DLA-1642-1 : postgresql-9.4 new minor release

Debian DLA-1643-1 : krb5 security update

Debian DLA-1644-1 : policykit-1 security update

Debian DLA-1645-1 : wireshark security update

Debian DLA-1646-1 : qemu security update

Debian DLA-1647-1 : apache2 security update

Debian DLA-1648-1 : firefox-esr security update

Debian DLA-1649-1 : spice security update

Debian DLA-165-1 : eglibc security update

Debian DLA-1650-1 : rssh security update

Debian DLA-1651-1 : libgd2 security update

Debian DLA-1652-1 : libvncserver security update

Debian DLA-1653-1 : postgis security update

Debian DLA-1654-1 : libav security update

Debian DLA-1655-1 : mariadb-10.0 security update

Debian DLA-1656-1 : agg security update

Debian DLA-1657-1 : debian-security-support enigmail end of life

Debian DLA-1658-1 : phpmyadmin security update

Debian DLA-1659-1 : drupal7 security update

Debian DLA-166-1 : libarchive security update

Debian DLA-1660-2 : rssh regression update

Debian DLA-1661-1 : mumble security update

Debian DLA-1662-1 : libthrift-java security update

Debian DLA-1663-1 : python3.4 security update

Debian DLA-1664-1 : golang security update

Debian DLA-1665-1 : netmask security update

Debian DLA-1666-1 : freerdp security update

Debian DLA-1667-1 : dovecot security update

Debian DLA-1668-1 : libarchive security update

Debian DLA-1669-1 : libreoffice security update

Debian DLA-167-1 : redcloth security update

Debian DLA-1670-1 : ghostscript security update

Debian DLA-1671-1 : coturn security update

Debian DLA-1672-1 : curl security update

Debian DLA-1673-1 : wordpress security update

Debian DLA-1674-1 : php5 security update

Debian DLA-1675-1 : python-gnupg security update

Debian DLA-1676-1 : unbound security update

Debian DLA-1677-1 : firefox-esr security update

Debian DLA-1678-1 : thunderbird security update

Debian DLA-1679-1 : php5 security update

Debian DLA-168-1 : konversation security update

Debian DLA-1680-1 : tiff security update

Debian DLA-1681-1 : gsoap security update

Debian DLA-1682-1 : uriparser security update

Debian DLA-1683-1 : rdesktop security update

Debian DLA-1684-1 : systemd security update

Debian DLA-1685-1 : drupal7 security update

Debian DLA-1686-1 : freedink-dfarc security update

Debian DLA-1687-1 : sox security update

Debian DLA-1688-1 : waagent update

Debian DLA-1689-1 : elfutils security update

Debian DLA-169-1 : axis security update

Debian DLA-1690-1 : liblivemedia security update

Debian DLA-1691-1 : exiv2 security update

Debian DLA-1692-1 : phpmyadmin security update

Debian DLA-1693-1 : gpac security update

Debian DLA-1694-1 : qemu security update

Debian DLA-1695-1 : sox security update

Debian DLA-1696-1 : ceph security update

Debian DLA-1697-1 : bind9 security updat

Debian DLA-1698-2 : file regression update

Debian DLA-1699-1 : ldb security update

Debian DLA-17-1 : tor: new upstream version

Debian DLA-170-1 : mod-gnutls security update

Debian DLA-1700-1 : uw-imap security update

Debian DLA-1701-1 : openssl security update

Debian DLA-1702-1 : advancecomp security update

Debian DLA-1703-1 : jackson-databind security update

Debian DLA-1704-1 : nss security update

Debian DLA-1705-1 : sox security update

Debian DLA-1706-1 : poppler security update

Debian DLA-1707-1 : symfony security update

Debian DLA-1708-1 : zabbix security update

Debian DLA-1709-1 : waagent security update

Debian DLA-171-1 : libssh2 security update

Debian DLA-1710-1 : xmltooling security update

Debian DLA-1711-1 : systemd security update

Debian DLA-1712-1 : libsndfile security update

Debian DLA-1713-2 : libsdl1.2 regression update

Debian DLA-1714-2 : libsdl2 regression update

Debian DLA-1715-1 : linux-4.9 security update (Spectre)

Debian DLA-1716-1 : ikiwiki security update

Debian DLA-1717-1 : rdflib security update

Debian DLA-1718-1 : sqlalchemy security update

Debian DLA-1719-1 : libjpeg-turbo security update

Debian DLA-172-1 : libextlib-ruby security update

Debian DLA-1720-1 : liblivemedia security update

Debian DLA-1721-1 : otrs2 security update

Debian DLA-1722-1 : firefox-esr security update

Debian DLA-1723-1 : cron security update

Debian DLA-1724-1 : ntfs-3g security update

Debian DLA-1725-1 : rsync security update

Debian DLA-1726-1 : bash security update

Debian DLA-1727-1 : firefox-esr security update

Debian DLA-1728-1 : openssh security update

Debian DLA-1729-1 : wireshark security update

Debian DLA-173-1 : putty security update

Debian DLA-1730-4 : libssh2 regression update

Debian DLA-1731-2 : linux regression update (Spectre)

Debian DLA-1732-1 : openjdk-7 security update

Debian DLA-1733-1 : wpa security update

Debian DLA-1734-1 : libraw security update

Debian DLA-1735-1 : ruby2.1 security update

Debian DLA-1736-1 : dovecot security update

Debian DLA-1737-1 : pdns security update

Debian DLA-1738-1 : gpsd security update

Debian DLA-1739-1 : rails security update

Debian DLA-174-1 : tcpdump security update

Debian DLA-1740-1 : libav security update

Debian DLA-1741-1 : php5 security update

Debian DLA-1742-1 : wordpress security update

Debian DLA-1743-1 : thunderbird security update

Debian DLA-1744-1 : tzdata new upstream version

Debian DLA-1745-1 : libdatetime-timezone-perl new upstream version

Debian DLA-1746-1 : drupal7 security update

Debian DLA-1747-1 : firmware-nonfree security update

Debian DLA-1748-1 : apache2 security update

Debian DLA-1749-1 : golang security update

Debian DLA-175-1 : gnupg security update

Debian DLA-1750-1 : roundup security update

Debian DLA-1751-1 : suricata security update

Debian DLA-1752-1 : poppler security update

Debian DLA-1753-3 : proftpd-dfsg regression update

Debian DLA-1754-1 : samba security update

Debian DLA-1755-1 : graphicsmagick security update

Debian DLA-1756-1 : libxslt security update

Debian DLA-1757-1 : cacti security update

Debian DLA-1758-1 : debian-security-support update

Debian DLA-1759-1 : clamav security update

Debian DLA-176-1 : mono security update

Debian DLA-1760-1 : wget security update

Debian DLA-1761-1 : ghostscript security update

Debian DLA-1762-2 : systemd regression update

Debian DLA-1763-1 : putty security update

Debian DLA-1764-1 : mercurial security update

Debian DLA-1765-1 : gpac security update

Debian DLA-1766-1 : evolution security update

Debian DLA-1767-1 : monit security update

Debian DLA-1768-1 : checkstyle security update

Debian DLA-1769-1 : gst-plugins-base0.10 security update

Debian DLA-177-1 : openssl security update

Debian DLA-1770-1 : gst-plugins-base1.0 security update

Debian DLA-1771-1 : linux-4.9 security update

Debian DLA-1772-1 : libvirt security update

Debian DLA-1773-1 : signing-party security update

Debian DLA-1774-1 : otrs2 security update

Debian DLA-1775-1 : phpbb3 security update

Debian DLA-1776-1 : librecad security update

Debian DLA-1777-2 : jquery regression update

Debian DLA-1778-1 : symfony security update

Debian DLA-1779-1 : 389-ds-base security update

Debian DLA-178-1 : tor security update

Debian DLA-1780-1 : firefox-esr new upstream version

Debian DLA-1781-1 : qemu security update

Debian DLA-1782-1 : openjdk-7 security update

Debian DLA-1783-1 : atftp security update

Debian DLA-1784-1 : postgresql-9.4 new minor release

Debian DLA-1785-1 : imagemagick security update

Debian DLA-1786-1 : qt4-x11 security update

Debian DLA-1787-1 : linux-4.9 security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Debian DLA-1788-1 : samba security update

Debian DLA-1789-2 : intel-microcode security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Debian DLA-179-1 : tzdata new upstream version

Debian DLA-1790-1 : lemonldap-ng security update

Debian DLA-1791-1 : faad2 security update

Debian DLA-1792-2 : cups-filters regression update

Debian DLA-1793-1 : dhcpcd5 security update

Debian DLA-1794-1 : libspring-security-2.0-java security update

Debian DLA-1795-1 : graphicsmagick security update

Debian DLA-1796-1 : jruby security update

Debian DLA-1797-1 : drupal7 security update

Debian DLA-1798-1 : jackson-databind security update

Debian DLA-1799-2 : linux security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Debian DLA-18-1 : php5 security update

Debian DLA-180-1 : gnutls26 security update

Debian DLA-1800-1 : firefox-esr security update

Debian DLA-1801-1 : zookeeper security update

Debian DLA-1802-1 : wireshark security update

Debian DLA-1803-1 : php5 security update

Debian DLA-1804-1 : curl security update

Debian DLA-1805-1 : minissdpd security update

Debian DLA-1806-1 : thunderbird security update

Debian DLA-1807-1 : vcftools security update

Debian DLA-1808-1 : sox security update

Debian DLA-1809-1 : libav security update

Debian DLA-181-1 : xerces-c security update

Debian DLA-1810-1 : tomcat7 security update

Debian DLA-1811-1 : miniupnpd security update

Debian DLA-1812-1 : doxygen security update

Debian DLA-1813-1 : php5 security update

Debian DLA-1814-1 : python-django security update

Debian DLA-1815-1 : poppler security update

Debian DLA-1816-1 : otrs2 security update

Debian DLA-1817-1 : libgd2 security update

Debian DLA-1818-1 : dbus security update

Debian DLA-1819-1 : pyxdg security update

Debian DLA-182-1 : batik security update

Debian DLA-1820-1 : thunderbird security update

Debian DLA-1821-1 : phpmyadmin security update

Debian DLA-1822-1 : php-horde-form security update

Debian DLA-1823-1 : linux security update (SACK Panic) (SACK Slowness)

Debian DLA-1824-1 : linux-4.9 security update (SACK Panic) (SACK Slowness)

Debian DLA-1825-1 : kdepim security update

Debian DLA-1826-1 : glib2.0 security update

Debian DLA-1827-1 : gvfs security update

Debian DLA-1828-1 : python-urllib3 security update

Debian DLA-1829-1 : firefox-esr security update

Debian DLA-183-1 : libxfont security update

Debian DLA-1830-1 : znc security update

Debian DLA-1831-1 : jackson-databind security update

Debian DLA-1832-1 : libvirt security update

Debian DLA-1833-2 : bzip2 regression update

Debian DLA-1834-1 : python2.7 security update

Debian DLA-1835-2 : python3.4 regression update

Debian DLA-1836-1 : thunderbird security update

Debian DLA-1837-2 : rdesktop regression update

Debian DLA-1838-1 : mupdf security update

Debian DLA-1839-1 : expat security update

Debian DLA-184-1 : binutils security update

Debian DLA-1840-1 : golang-go.crypto security update

Debian DLA-1841-1 : gpac security update

Debian DLA-1842-1 : python-django security update

Debian DLA-1843-1 : pdns security update

Debian DLA-1844-1 : lemonldap-ng security update

Debian DLA-1845-1 : dosbox security update

Debian DLA-1846-2 : unzip regression update

Debian DLA-1847-1 : squid3 security update

Debian DLA-1848-1 : libspring-security-2.0-java security update

Debian DLA-1849-1 : zeromq3 security update

Debian DLA-185-1 : freetype security update

Debian DLA-1850-1 : redis security update

Debian DLA-1851-1 : openjpeg2 security update

Debian DLA-1852-1 : python3.4 security update

Debian DLA-1853-1 : libspring-java security update

Debian DLA-1854-1 : libonig security update

Debian DLA-1855-1 : exiv2 security update

Debian DLA-1856-1 : patch security update

Debian DLA-1857-1 : nss security update

Debian DLA-1858-1 : squid3 security update

Debian DLA-1859-1 : bind9 security update

Debian DLA-186-1 : mailman security update

Debian DLA-1860-1 : libxslt security update

Debian DLA-1861-1 : libsdl2-image security update

Debian DLA-1862-1 : linux security update

Debian DLA-1863-1 : linux-4.9 security update

Debian DLA-1864-1 : patch security update

Debian DLA-1865-1 : sdl-image1.2 security update

Debian DLA-1866-2 : glib2.0 regression update

Debian DLA-1867-1 : wpa security update

Debian DLA-1868-1 : squirrelmail security update

Debian DLA-1869-1 : firefox-esr security update

Debian DLA-187-1 : tor security update

Debian DLA-1870-1 : thunderbird security update

Debian DLA-1871-1 : vim security update

Debian DLA-1872-1 : python-django security update

Debian DLA-1873-1 : proftpd-dfsg security update

Debian DLA-1874-1 : postgresql-9.4 security update

Debian DLA-1875-1 : fusiondirectory security update

Debian DLA-1876-1 : gosa security update

Debian DLA-1877-1 : otrs2 security update

Debian DLA-1878-1 : php5 security update

Debian DLA-1879-1 : jackson-databind security update

Debian DLA-188-1 : arj security update

Debian DLA-1880-1 : ghostscript security update

Debian DLA-1881-1 : evince security update

Debian DLA-1882-1 : atril security update

Debian DLA-1883-1 : tomcat8 security update (httpoxy)

Debian DLA-1884-1 : linux security update

Debian DLA-1885-1 : linux-4.9 security update

Debian DLA-1886-2 : openjdk-7 regression update

Debian DLA-1887-1 : freetype security update

Debian DLA-1888-1 : imagemagick security update

Debian DLA-1889-1 : python3.4 security update

Debian DLA-189-1 : libgd2 security update

Debian DLA-1890-1 : kde4libs security update

Debian DLA-1891-1 : openldap security update

Debian DLA-1892-1 : flask security update

Debian DLA-1893-1 : cups security update

Debian DLA-1894-1 : libapache2-mod-auth-openidc security

Debian DLA-1895-1 : libmspack security update

Debian DLA-1896-1 : commons-beanutils security update

Debian DLA-1897-1 : tiff security update

Debian DLA-1898-1 : xymon security update

Debian DLA-1899-1 : faad2 security update

Debian DLA-19-1 : postgresql-8.4 update

Debian DLA-190-1 : libgcrypt11 security update

Debian DLA-1900-2 : apache2 regression update

Debian DLA-1901-1 : dovecot security update

Debian DLA-1902-1 : djvulibre security update

Debian DLA-1903-1 : subversion security update

Debian DLA-1904-1 : libextractor security update

Debian DLA-1905-1 : gosa security update

Debian DLA-1906-1 : python2.7 security update

Debian DLA-1907-1 : libav security update

Debian DLA-1908-1 : pump security update

Debian DLA-1909-1 : freetype security update

Debian DLA-191-1 : checkpw security update

Debian DLA-1910-1 : firefox-esr security update

Debian DLA-1911-1 : exim4 security update

Debian DLA-1912-1 : expat security update

Debian DLA-1913-1 : memcached security update

Debian DLA-1914-1 : icedtea-web security update

Debian DLA-1915-1 : ghostscript security update

Debian DLA-1916-1 : opensc security update

Debian DLA-1917-1 : curl security update

Debian DLA-1918-1 : libonig security update

Debian DLA-1919-2 : linux-4.9 security update

Debian DLA-192-1 : ntp security update

Debian DLA-1920-1 : golang-go.crypto security update

Debian DLA-1921-1 : dnsmasq security update

Debian DLA-1922-1 : wpa security update

Debian DLA-1923-1 : ansible security update

Debian DLA-1924-1 : python3.4 security update

Debian DLA-1925-1 : python2.7 security update

Debian DLA-1926-1 : thunderbird security update

Debian DLA-1927-1 : qemu security update

Debian DLA-1928-1 : php5 security update

Debian DLA-1929-1 : php-pecl-http security update

Debian DLA-193-1 : chrony security update

Debian DLA-1930-1 : linux security update

Debian DLA-1931-2 : libgcrypt20 regression update

Debian DLA-1932-1 : openssl security update

Debian DLA-1933-1 : ruby-nokogiri security update

Debian DLA-1934-1 : cimg security update

Debian DLA-1935-1 : e2fsprogs security update

Debian DLA-1936-1 : cups security update

Debian DLA-1937-1 : httpie security update

Debian DLA-1938-1 : file-roller security update

Debian DLA-1939-1 : poppler security update

Debian DLA-194-1 : das-watchdog security update

Debian DLA-1940-1 : linux-4.9 security update

Debian DLA-1941-1 : netty security update

Debian DLA-1942-2 : phpbb3 regression update

Debian DLA-1943-1 : jackson-databind security update

Debian DLA-1944-1 : libapreq2 security update

Debian DLA-1945-1 : openconnect security update

Debian DLA-1946-1 : novnc security update

Debian DLA-1947-1 : libreoffice security update

Debian DLA-1948-1 : ruby-mini-magick security update

Debian DLA-1949-1 : xen security update

Debian DLA-195-1 : libtasn1-3 security update

Debian DLA-1950-1 : openjpeg2 security update

Debian DLA-1951-1 : libtomcrypt security update

Debian DLA-1952-1 : rsyslog security update

Debian DLA-1953-2 : clamav regression update

Debian DLA-1954-1 : lucene-solr security update

Debian DLA-1955-1 : tcpdump security update

Debian DLA-1956-1 : ruby-openid security update

Debian DLA-1957-1 : tzdata new upstream version

Debian DLA-1958-1 : libdatetime-timezone-perl new upstream version

Debian DLA-1959-1 : xtrlock security update

Debian DLA-196-1 : ia32-libs security update

Debian DLA-1960-1 : wordpress security update

Debian DLA-1961-1 : milkytracker security update

Debian DLA-1962-1 : graphite-web security update

Debian DLA-1963-2 : poppler regression update

Debian DLA-1964-1 : sudo security update

Debian DLA-1965-1 : nfs-utils security update

Debian DLA-1966-1 : aspell security update

Debian DLA-1967-1 : libpcap security update

Debian DLA-1968-1 : imagemagick security update

Debian DLA-1969-1 : file security update

Debian DLA-197-1 : libvncserver security update

Debian DLA-1970-1 : php5 security update

Debian DLA-1971-1 : libarchive security update

Debian DLA-1972-1 : mosquitto security update

Debian DLA-1973-1 : libxslt security update

Debian DLA-1974-1 : proftpd-dfsg security update

Debian DLA-1975-1 : spip security update

Debian DLA-1976-1 : imapfilter security update

Debian DLA-1977-1 : libvncserver security update

Debian DLA-1978-1 : python-ecdsa security update

Debian DLA-1979-1 : italc security update

Debian DLA-198-1 : wireshark security update

Debian DLA-1980-1 : wordpress security update

Debian DLA-1981-1 : cpio security update

Debian DLA-1982-1 : openafs security update

Debian DLA-1983-1 : simplesamlphp security update

Debian DLA-1984-1 : gdal security update

Debian DLA-1985-1 : djvulibre security update

Debian DLA-1986-1 : ruby-haml security update

Debian DLA-1987-1 : firefox-esr security update

Debian DLA-1988-1 : ampache security update

Debian DLA-1989-1 : linux security update

Debian DLA-199-1 : libx11 security update

Debian DLA-1990-1 : linux-4.9 security update

Debian DLA-1991-1 : libssh2 security update

Debian DLA-1992-1 : ghostscript security update

Debian DLA-1993-1 : mesa security update

Debian DLA-1994-1 : postgresql-common security update

Debian DLA-1995-1 : angular.js security update

Debian DLA-1996-1 : libapache2-mod-auth-openidc security update

Debian DLA-1997-1 : thunderbird security update

Debian DLA-1998-1 : python-psutil security update

Debian DLA-1999-1 : symfony security update

Debian DLA-20-1 : munin security update

Debian DLA-200-1 : ruby1.9.1 security update

Debian DLA-2000-1 : pam-python security update

Debian DLA-2001-1 : libofx security update

Debian DLA-2002-1 : libice security update

Debian DLA-2003-1 : isc-dhcp security update

Debian DLA-2004-1 : 389-ds-base security update

Debian DLA-2005-1 : tnef security update

Debian DLA-2006-1 : libxdmcp security update

Debian DLA-2007-1 : ruby2.1 security update

Debian DLA-2008-1 : nss security update

Debian DLA-2009-1 : tiff security update

Debian DLA-201-1 : tzdata new upstream version

Debian DLA-2010-1 : bsdiff security update

Debian DLA-2011-1 : xmlrpc-epi security update

Debian DLA-2012-1 : libvpx security update

Debian DLA-2013-1 : libvorbis security update

Debian DLA-2014-1 : vino security update

Debian DLA-2015-1 : nss security update

Debian DLA-2016-1 : ssvnc security update

Debian DLA-2017-2 : asterisk regression update

Debian DLA-2018-1 : proftpd-dfsg security update

Debian DLA-2019-1 : exiv2 security update

Debian DLA-202-1 : wesnoth-1.8 security update

Debian DLA-2020-1 : libonig security update

Debian DLA-2021-1 : libav security update

Debian DLA-2022-1 : librabbitmq security update

Debian DLA-2023-1 : openjdk-7 security update

Debian DLA-2024-1 : phpmyadmin security update

Debian DLA-2025-1 : openslp-dfsg security update

Debian DLA-2026-1 : htmldoc security update

Debian DLA-2027-1 : jruby security update

Debian DLA-2028-1 : squid3 security update

Debian DLA-2029-1 : firefox-esr security update

Debian DLA-203-1 : openldap security update

Debian DLA-2030-1 : jackson-databind security update

Debian DLA-2031-1 : freeimage security update

Debian DLA-2032-1 : cacti security update

Debian DLA-2033-1 : php-horde security update

Debian DLA-2034-1 : davical security update

Debian DLA-2035-1 : libpgf security update

Debian DLA-2036-1 : thunderbird security update

Debian DLA-2037-1 : spamassassin security update

Debian DLA-2038-2 : x2goclient regression update

Debian DLA-2039-1 : libvorbis security update

Debian DLA-204-1 : file security update

Debian DLA-2040-1 : harfbuzz security update

Debian DLA-2041-1 : debian-edu-config security update

Debian DLA-2042-1 : python-django security update

Debian DLA-2043-2 : gdk-pixbuf regression update

Debian DLA-2044-1 : cyrus-sasl2 security update

Debian DLA-2045-1 : tightvnc security update

Debian DLA-2046-1 : opensc security update

Debian DLA-2047-1 : cups security update

Debian DLA-2048-1 : libxml2 security update

Debian DLA-2049-1 : imagemagick security update

Debian DLA-205-1 : ppp security update

Debian DLA-2050-1 : php5 security update

Debian DLA-2051-1 : intel-microcode security update

Debian DLA-2052-1 : libbsd security update

Debian DLA-2053-1 : otrs2 security update

Debian DLA-2054-1 : jhead security update

Debian DLA-2055-1 : igraph security update

Debian DLA-2056-1 : waitress security update

Debian DLA-2057-1 : pillow security update

Debian DLA-2058-1 : nss security update

Debian DLA-2059-1 : git security update

Debian DLA-206-1 : python-django-markupfield security update

Debian DLA-2060-1 : phpmyadmin security update

Debian DLA-2061-1 : firefox-esr security update

Debian DLA-2062-1 : sa-exim security update

Debian DLA-2063-1 : debian-lan-config security update

Debian DLA-2064-1 : ldm security update

Debian DLA-2065-1 : apache-log4j1.2 security update

Debian DLA-2067-1 : wordpress security update

Debian DLA-2068-1 : linux security update

Debian DLA-2069-1 : cacti security update

Debian DLA-207-1 : subversion security update

Debian DLA-2070-1 : ruby-excon security update

Debian DLA-2071-1 : thunderbird security update

Debian DLA-2072-1 : gpac security update

Debian DLA-2073-1 : transfig security update

Debian DLA-2074-1 : python-apt security update

Debian DLA-2075-1 : jsoup security update

Debian DLA-2076-1 : slirp security update

Debian DLA-2077-1 : tomcat7 security update

Debian DLA-2078-1 : libxmlrpc3-java security update

Debian DLA-2079-1 : otrs2 security update

Debian DLA-208-1 : tzdata new upstream version

Debian DLA-2080-1 : iperf3 security update

Debian DLA-2081-1 : openjpeg2 security update

Debian DLA-2082-1 : unzip security update

Debian DLA-2083-1 : hiredis security update

Debian DLA-2084-1 : graphicsmagick security update

Debian DLA-2085-1 : zlib security update

Debian DLA-2086-1 : wget security update

Debian DLA-2087-1 : suricata security update

Debian DLA-2088-1 : libsolv security update

Debian DLA-2089-1 : openjpeg2 security update

Debian DLA-209-1 : jruby security update

Debian DLA-2090-1 : qemu security update

Debian DLA-2091-1 : libjackson-json-java security update

Debian DLA-2092-1 : qtbase-opensource-src security update

Debian DLA-2093-1 : firefox-esr security update

Debian DLA-2094-1 : sudo security update

Debian DLA-2095-1 : storebackup security update

Debian DLA-2096-1 : ruby-rack-cors security update

Debian DLA-2097-1 : ppp security update

Debian DLA-2098-1 : ipmitool security update

Debian DLA-2099-1 : checkstyle security update

Debian DLA-21-1 : fail2ban security update

Debian DLA-210-1 : qt4-x11 security update

Debian DLA-2100-1 : libexif security update

Debian DLA-2101-1 : libemail-address-list-perl security update

Debian DLA-2102-1 : firefox-esr security update

Debian DLA-2103-1 : debian-security-support update: libqb and mysql-5.5 end

Debian DLA-2104-1 : thunderbird security update

Debian DLA-2105-1 : postgresql-9.4 security update

Debian DLA-2106-1 : libgd2 security update

Debian DLA-2107-1 : spamassassin security update

Debian DLA-2108-1 : clamav security update

Debian DLA-2109-1 : netty security update

Debian DLA-211-1 : curl security update

Debian DLA-2110-1 : netty-3.9 security update

Debian DLA-2111-1 : jackson-databind security update

Debian DLA-2112-1 : python-reportlab security update

Debian DLA-2113-1 : cloud-init security update

Debian DLA-2114-1 : linux-4.9 security update

Debian DLA-2115-2 : proftpd-dfsg regression update

Debian DLA-2116-1 : libpam-radius-auth security update

Debian DLA-2117-1 : zsh security update

Debian DLA-2118-1 : otrs2 security update

Debian DLA-2119-1 : python-pysaml2 security update

Debian DLA-212-1 : php5 security update

Debian DLA-2120-1 : rake security update

Debian DLA-2121-1 : libimobiledevice security update

Debian DLA-2122-1 : libusbmuxd security update

Debian DLA-2123-1 : pure-ftpd security update

Debian DLA-2124-1 : php5 security update

Debian DLA-2125-1 : collabtive security update

Debian DLA-2126-1 : gst-plugins-base0.10 security update

Debian DLA-2127-1 : dojo security update

Debian DLA-2128-1 : openjdk-7 security update

Debian DLA-2129-1 : firebird2.5 security update

Debian DLA-213-1 : openjdk-6 security update

Debian DLA-2130-1 : libapache2-mod-auth-openidc security

Debian DLA-2131-2 : rrdtool regression update

Debian DLA-2132-1 : libzypp security update

Debian DLA-2133-1 : tomcat7 security update

Debian DLA-2134-1 : pdfresurrect security update

Debian DLA-2135-1 : jackson-databind security update

Debian DLA-2136-1 : libvpx security update

Debian DLA-2137-1 : sleuthkit security update

Debian DLA-2138-1 : wpa security update

Debian DLA-2139-1 : dojo security update

Debian DLA-214-1 : libxml-libxml-perl security update

Debian DLA-2140-1 : firefox-esr security update

Debian DLA-2141-1 : yubikey-val security update

Debian DLA-2142-1 : slirp security update

Debian DLA-2143-1 : slurm-llnl security update

Debian DLA-2144-1 : qemu security update

Debian DLA-2145-2 : twisted security update

Debian DLA-2146-1 : libvncserver security update

Debian DLA-2147-1 : gdal security update

Debian DLA-2148-1 : amd64-microcode security update (Spectre)

Debian DLA-2149-1 : rails security update

Debian DLA-215-1 : libjson-ruby security update

Debian DLA-2150-1 : thunderbird security update

Debian DLA-2151-1 : icu security update

Debian DLA-2152-1 : graphicsmagick security update

Debian DLA-2153-1 : jackson-databind security update

Debian DLA-2154-1 : phpmyadmin security update

Debian DLA-2155-1 : tomcat8 security update

Debian DLA-2156-1 : e2fsprogs security update

Debian DLA-2157-1 : weechat security update

Debian DLA-2158-1 : ruby2.1 security update

Debian DLA-2159-1 : okular security update

Debian DLA-216-1 : squid security update

Debian DLA-2160-1 : php5 security update

Debian DLA-2161-1 : tika security update

Debian DLA-2162-1 : php-horde-form security update

Debian DLA-2163-1 : tinyproxy security update

Debian DLA-2164-1 : gst-plugins-bad0.10 security update

Debian DLA-2165-1 : apng2gif security update

Debian DLA-2166-1 : libpam-krb5 security update

Debian DLA-2167-1 : python-bleach security update

Debian DLA-2168-1 : libplist security update

Debian DLA-2169-1 : libmtp security update

Debian DLA-2170-1 : firefox-esr security update

Debian DLA-2171-1 : ceph security update

Debian DLA-2172-1 : thunderbird security update

Debian DLA-2173-1 : graphicsmagick security update

Debian DLA-2174-1 : php-horde-data security update

Debian DLA-2175-1 : php-horde-trean security update

Debian DLA-2177-1 : git security update

Debian DLA-218-1 : xorg-server security update

Debian DLA-219-1 : icu security update

Debian DLA-22-1 : cups security update

Debian DLA-220-1 : dpkg security update

Debian DLA-221-1 : tiff security update

Debian DLA-222-1 : commons-httpclient security update

Debian DLA-223-1 : nbd security update

Debian DLA-224-1 : ruby1.8 security update

Debian DLA-225-1 : dnsmasq security update

Debian DLA-226-2 : ntfs-3g regression update

Debian DLA-227-1 : postgresql-8.4 update

Debian DLA-228-1 : exactimage security update

Debian DLA-229-1 : libnokogiri-ruby security update

Debian DLA-23-1 : nss security update

Debian DLA-230-1 : eglibc security update

Debian DLA-231-1 : dulwich security update

Debian DLA-232-1 : tomcat6 security update

Debian DLA-233-1 : clamav security and upstream version update

Debian DLA-234-1 : ipsec-tools security update

Debian DLA-235-1 : ruby1.9.1 security update

Debian DLA-236-1 : wordpress security update

Debian DLA-237-1 : mercurial security update

Debian DLA-238-1 : fuse security update

Debian DLA-239-1 : cups security update

Debian DLA-24-1 : poppler security update

Debian DLA-240-1 : libapache-mod-jk security update

Debian DLA-241-1 : wireshark security update

Debian DLA-242-1 : imagemagick security update

Debian DLA-243-1 : libraw security update

Debian DLA-244-1 : strongswan security update

Debian DLA-245-1 : p7zip security update

Debian DLA-246-2 : linux-2.6 regression update

Debian DLA-247-1 : openssl security update (Logjam)

Debian DLA-248-1 : qemu security update (Venom)

Debian DLA-249-1 : qemu-kvm security update (Venom)

Debian DLA-25-3 : python2.6 regression update

Debian DLA-250-1 : libclamunrar security update

Debian DLA-251-2 : zendframework regression update

Debian DLA-252-1 : postgresql-8.4 update

Debian DLA-253-1 : libwmf security update

Debian DLA-254-1 : librack-ruby security update

Debian DLA-255-1 : cacti security update

Debian DLA-256-1 : t1utils security update

Debian DLA-257-1 : libwmf security update

Debian DLA-258-1 : jqueryui security update

Debian DLA-259-1 : shibboleth-sp2 security update

Debian DLA-26-1 : python-scipy security update

Debian DLA-260-1 : hostapd security update

Debian DLA-261-2 : aptdaemon regression update

Debian DLA-262-1 : libcrypto++ security update

Debian DLA-263-1 : ruby1.9.1 security update

Debian DLA-264-1 : libmodule-signature-perl security update

Debian DLA-265-2 : pykerberos regression update

Debian DLA-266-1 : libxml2 security update

Debian DLA-268-1 : virtualbox-ose security update (Venom)

Debian DLA-269-1 : linux-ftpd-ssl security update

Debian DLA-27-1 : file security update

Debian DLA-270-1 : bind9 security update

Debian DLA-271-1 : libunwind security update

Debian DLA-272-1 : python-django security update

Debian DLA-273-1 : tidy security update

Debian DLA-274-1 : groovy security update

Debian DLA-275-1 : ruby1.9.1 security update

Debian DLA-276-1 : inspircd security update

Debian DLA-277-1 : libidn security update

Debian DLA-278-2 : cacti regression update

Debian DLA-279-1 : python-tornado security update

Debian DLA-28-1 : augeas security update

Debian DLA-280-1 : ghostscript security update

Debian DLA-281-1 : expat security update

Debian DLA-282-1 : lighttpd security update (POODLE)

Debian DLA-283-1 : icu security update

Debian DLA-284-1 : apache2 security update

Debian DLA-285-1 : bind9 security update

Debian DLA-286-1 : squid3 security update

Debian DLA-287-1 : ia32-libs security update

Debian DLA-288-2 : openssh regression update

Debian DLA-289-1 : remind security update

Debian DLA-29-1 : puppet security update

Debian DLA-290-2 : opensaml2 security update

Debian DLA-291-1 : libidn security update

Debian DLA-292-1 : libstruts1.2-java security update

Debian DLA-293-1 : subversion security update

Debian DLA-294-1 : wordpress security update

Debian DLA-295-1 : conntrack security update

Debian DLA-296-1 : extplorer security update

Debian DLA-297-1 : wesnoth-1.8 security update

Debian DLA-298-1 : roundup security update

Debian DLA-299-1 : ruby1.8 security update

Debian DLA-30-1 : acpi-support security update

Debian DLA-300-1 : ruby1.9.1 security update

Debian DLA-301-1 : python-django security update

Debian DLA-302-1 : zendframework security update

Debian DLA-303-1 : openjdk-6 security update (Bar Mitzvah) (Logjam)

Debian DLA-304-1 : openslp-dfsg security update

Debian DLA-305-1 : screen security update

Debian DLA-306-1 : libvdpau security update

Debian DLA-307-1 : php5 security update

Debian DLA-308-1 : bind9 security update

Debian DLA-309-1 : openldap security update

Debian DLA-31-1 : reportbug security update

Debian DLA-310-1 : linux-2.6 security update

Debian DLA-311-1 : rpcbind security update

Debian DLA-312-1 : libtorrent-rasterbar security update

Debian DLA-313-1 : virtualbox-ose security update

Debian DLA-314-1 : cups security update

Debian DLA-315-1 : nss security update

Debian DLA-316-1 : eglibc security update

Debian DLA-317-1 : vorbis-tools security update

Debian DLA-318-1 : flightgear security update

Debian DLA-319-1 : freetype security update

Debian DLA-32-1 : nspr security update

Debian DLA-320-1 : libemail-address-perl security update

Debian DLA-321-1 : wordpress security update

Debian DLA-322-1 : commons-httpclient security update

Debian DLA-323-1 : fuseiso security update

Debian DLA-324-1 : binutils security update

Debian DLA-325-1 : linux-2.6 security update

Debian DLA-326-1 : zendframework security update

Debian DLA-327-1 : freeimage security update

Debian DLA-328-1 : tzdata new upstream version

Debian DLA-329-1 : postgresql-8.4 update

Debian DLA-33-1 : openssl security update

Debian DLA-330-1 : unzip security update

Debian DLA-331-1 : polarssl security update

Debian DLA-332-1 : optipng security update

Debian DLA-333-1 : cakephp security update

Debian DLA-334-2 : libxml2 regression update

Debian DLA-335-1 : ntp security update

Debian DLA-336-1 : phpmyadmin security update

Debian DLA-337-1 : busybox security update

Debian DLA-338-1 : xscreensaver security update

Debian DLA-339-1 : libhtml-scrubber-perl security update

Debian DLA-34-1 : libapache-mod-security security update

Debian DLA-340-1 : krb5 security update

Debian DLA-341-1 : php5 security update

Debian DLA-342-1 : openafs security update

Debian DLA-343-1 : libpng security update

Debian DLA-344-1 : nspr security update

Debian DLA-345-1 : strongswan security update

Debian DLA-346-1 : openjdk-6 security update

Debian DLA-347-1 : putty security update

Debian DLA-348-1 : smokeping security update

Debian DLA-349-1 : python-django security update

Debian DLA-35-1 : lzo2 security update

Debian DLA-350-1 : eglibc security update

Debian DLA-351-1 : redmine security update

Debian DLA-352-1 : libcommons-collections3-java security update

Debian DLA-353-1 : imagemagick security update

Debian DLA-354-1 : nss security update

Debian DLA-355-1 : libxml2 security update

Debian DLA-356-1 : libsndfile security update

Debian DLA-357-1 : libphp-snoopy security update

Debian DLA-358-1 : openssl security update

Debian DLA-36-1 : polarssl security update

Debian DLA-360-1 : linux-2.6 security update

Debian DLA-361-1 : bouncycastle security update

Debian DLA-362-1 : dhcpcd security update

Debian DLA-363-1 : libphp-phpmailer security update

Debian DLA-364-1 : gnutls26 security update

Debian DLA-365-1 : foomatic-filters security update

Debian DLA-366-1 : arts security update

Debian DLA-367-1 : kdelibs security update

Debian DLA-368-1 : grub2 security update

Debian DLA-369-1 : pygments security update

Debian DLA-37-1 : krb5 security update

Debian DLA-370-1 : bind9 security update

Debian DLA-371-1 : foomatic-filters security update

Debian DLA-373-1 : libxml2 security update

Debian DLA-374-3 : cacti regression update

Debian DLA-375-1 : ia32-libs security update

Debian DLA-375-1 : libpng Security Update

Debian DLA-376-1 : mono security update

Debian DLA-378-1 : linux-2.6 security update

Debian DLA-379-1 : samba security update

Debian DLA-380-1 : libvncserver security update

Debian DLA-381-1 : icu security update

Debian DLA-382-1 : sudo security update

Debian DLA-383-1 : claws-mail security update

Debian DLA-384-1 : inspircd security and regression update

Debian DLA-385-2 : isc-dhcp regression update

Debian DLA-386-1 : cacti security update

Debian DLA-387-1 : openssh security update

Debian DLA-388-1 : dwarfutils security update

Debian DLA-389-1 : giflib security update

Debian DLA-39-1 : gpgme1.0 security update

Debian DLA-390-1 : dbconfig-common security update

Debian DLA-391-1 : prosody security update

Debian DLA-392-1 : roundcube security update

Debian DLA-393-1 : srtp security update

Debian DLA-394-1 : passenger security update

Debian DLA-395-1 : librsvg security update

Debian DLA-396-1 : bind9 security update

Debian DLA-397-1 : ecryptfs-utils security update

Debian DLA-398-1 : privoxy security update

Debian DLA-399-1 : foomatic-filters security update

Debian DLA-40-1 : cacti security update

Debian DLA-400-1 : pound security update (BEAST) (POODLE)

Debian DLA-401-1 : imlib2 security update

Debian DLA-402-1 : tiff security update

Debian DLA-403-1 : radicale security update

Debian DLA-404-1 : nginx security update

Debian DLA-405-1 : tiff security update

Debian DLA-406-1 : phpmyadmin security update

Debian DLA-407-1 : prosody security update

Debian DLA-408-1 : gosa security update

Debian DLA-409-1 : mysql-5.5 security update

Debian DLA-41-1 : python-imaging security update

Debian DLA-410-1 : openjdk-6 security update (SLOTH)

Debian DLA-411-2 : eglibc regression update

Debian DLA-412-1 : linux-2.6 security update

Debian DLA-413-1 : gajim security update

Debian DLA-414-1 : chrony security update

Debian DLA-415-1 : cpio security update

Debian DLA-416-1 : eglibc security update

Debian DLA-417-1 : xdelta3 security update

Debian DLA-418-1 : wordpress security update

Debian DLA-419-1 : gtk+2.0 security update

Debian DLA-42-1 : live-config security update

Debian DLA-420-1 : libmatroska security update

Debian DLA-421-1 : openssl security update

Debian DLA-422-1 : python-imaging security update

Debian DLA-423-1 : krb5 security update

Debian DLA-424-1 : didiwiki security update

Debian DLA-425-1 : libssh security update

Debian DLA-426-1 : libssh2 security update

Debian DLA-427-1 : nss security update

Debian DLA-428-1 : websvn security update

Debian DLA-429-1 : pixman security update

Debian DLA-43-1 : eglibc security update

Debian DLA-430-1 : libfcgi security update

Debian DLA-431-1 : libfcgi-perl security update

Debian DLA-432-1 : postgresql-8.4 update

Debian DLA-433-1 : xerces-c security update

Debian DLA-434-1 : gtk+2.0 security update

Debian DLA-435-1 : tomcat6 security update

Debian DLA-436-1 : ia32-libs security update

Debian DLA-437-1 : clamav version update

Debian DLA-438-1 : libebml security update

Debian DLA-439-1 : linux-2.6 security update

Debian DLA-44-1 : libwpd security update

Debian DLA-440-1 : dansguardian package update

Debian DLA-441-1 : pcre3 security update

Debian DLA-442-1 : lxc security update

Debian DLA-443-1 : bsh security update

Debian DLA-444-1 : php5 security update

Debian DLA-445-2 : squid3 regression update

Debian DLA-446-1 : poppler security update

Debian DLA-447-1 : mysql-5.5 security update

Debian DLA-448-1 : subversion security update

Debian DLA-449-2 : botan1.10 regression update

Debian DLA-45-1 : squid3 security update

Debian DLA-450-1 : gdk-pixbuf security update

Debian DLA-451-1 : openjdk-7 security update

Debian DLA-452-1 : smarty3 security update

Debian DLA-453-1 : extplorer security update

Debian DLA-454-1 : minissdpd security update

Debian DLA-455-1 : asterisk security update

Debian DLA-456-1 : openssl security update

Debian DLA-457-1 : mplayer security update

Debian DLA-458-1 : mplayer2 security update

Debian DLA-459-1 : mercurial security update

Debian DLA-46-1 : procmail update

Debian DLA-460-1 : file security update

Debian DLA-461-1 : nagios3 security update

Debian DLA-462-1 : websvn security update

Debian DLA-463-1 : ikiwiki security update

Debian DLA-464-1 : libav security update

Debian DLA-465-1 : debian-security-support update

Debian DLA-466-1 : ocaml security update

Debian DLA-467-1 : xerces-c security update

Debian DLA-468-1 : libuser security update

Debian DLA-469-1 : libgwenhywfar security update

Debian DLA-47-1 : lua5.1 security update

Debian DLA-470-1 : libksba security update

Debian DLA-471-1 : jansson security update

Debian DLA-472-2 : icedove regression update

Debian DLA-473-1 : wpa security update

Debian DLA-474-1 : dosfstools security update

Debian DLA-475-1 : python-tornado security update

Debian DLA-476-1 : libidn security update

Debian DLA-477-1 : librsvg security update

Debian DLA-478-1 : squid3 security update

Debian DLA-479-1 : xen security update

Debian DLA-48-1 : bind9 security update

Debian DLA-480-1 : nss security update

Debian DLA-481-2 : phpmyadmin regression update

Debian DLA-482-1 : libgd2 security update

Debian DLA-483-1 : expat security update

Debian DLA-484-1 : graphicsmagick security update (ImageTragick)

Debian DLA-485-1 : extplorer security update

Debian DLA-486-1 : imagemagick security update (ImageTragick)

Debian DLA-487-1 : debian-security-support - Long term security support update

Debian DLA-488-1 : xymon security update

Debian DLA-489-1 : ruby-mail security update

Debian DLA-49-1 : acpi-support security update

Debian DLA-490-1 : bozohttpd security update

Debian DLA-491-1 : postgresql-9.1 bugfix update

Debian DLA-492-1 : pdns security update

Debian DLA-493-1 : openafs security update

Debian DLA-494-1 : eglibc security update

Debian DLA-495-1 : libtasn1-3 security update

Debian DLA-496-1 : ruby-activerecord-3.2 security update

Debian DLA-497-1 : wireshark security update

Debian DLA-498-1 : ruby-activemodel-3.2 security update

Debian DLA-499-1 : php5 security update

Debian DLA-50-1 : file security update

Debian DLA-500-1 : imagemagick security update

Debian DLA-501-1 : gdk-pixbuf security update

Debian DLA-502-1 : graphicsmagick security update

Debian DLA-503-1 : libxml2 security update

Debian DLA-504-1 : libxstream-java security update

Debian DLA-505-1 : libpdfbox-java security update

Debian DLA-506-1 : dhcpcd5 security update

Debian DLA-507-1 : nss security update (Logjam)

Debian DLA-508-1 : expat security update

Debian DLA-509-1 : samba security update

Debian DLA-51-1 : gnupg2 security update

Debian DLA-510-1 : p7zip security update

Debian DLA-511-1 : libtorrent-rasterbar security update

Debian DLA-512-1 : mantis security update

Debian DLA-513-1 : nspr security update

Debian DLA-514-1 : libxslt security update

Debian DLA-515-1 : libav security update

Debian DLA-516-1 : linux security update

Debian DLA-517-1 : imagemagick security update

Debian DLA-518-1 : mozilla-devscripts security update

Debian DLA-519-1 : icedove security update

Debian DLA-52-1 : ia32-libs security update

Debian DLA-520-1 : horizon security update

Debian DLA-521-1 : firefox-esr security update

Debian DLA-522-1 : python2.7 security update

Debian DLA-523-1 : enigmail security update

Debian DLA-524-1 : squidguard security update

Debian DLA-525-1 : gimp security update

Debian DLA-526-1 : mysql-connector-java security update

Debian DLA-527-1 : nss security update

Debian DLA-528-1 : libcommons-fileupload-java security update

Debian DLA-529-1 : tomcat7 security update

Debian DLA-53-1 : apt security update

Debian DLA-530-1 : java-common security update

Debian DLA-531-1 : spice security update

Debian DLA-532-1 : movabletype-opensource security update

Debian DLA-533-1 : php5 security update

Debian DLA-534-1 : libgd2 security update

Debian DLA-535-1 : xerces-c security update

Debian DLA-536-1 : wget security update

Debian DLA-537-1 : roundcube security update

Debian DLA-538-1 : wireshark security update

Debian DLA-539-1 : qemu-kvm security update

Debian DLA-540-1 : qemu security update

Debian DLA-541-1 : libvirt security update

Debian DLA-542-1 : pidgin security update

Debian DLA-543-1 : sqlite3 security update

Debian DLA-544-1 : tcpreplay security update

Debian DLA-545-1 : icu security update

Debian DLA-546-2 : clamav version update

Debian DLA-547-2 : graphicsmagick regression update

Debian DLA-548-1 : drupal7 security update

Debian DLA-549-1 : ruby-eventmachine security update

Debian DLA-55-1 : nginx security update

Debian DLA-550-1 : drupal7 security update

Debian DLA-551-1 : phpmyadmin security update

Debian DLA-552-1 : binutils security update

Debian DLA-553-1 : apache2 security update (httpoxy)

Debian DLA-554-1 : libarchive security update

Debian DLA-555-1 : python-django security update

Debian DLA-556-1 : squid3 security update

Debian DLA-557-1 : dietlibc security update

Debian DLA-558-1 : squid security update

Debian DLA-559-1 : ntp security update

Debian DLA-56-1 : wordpress security update

Debian DLA-560-2 : cacti regression update

Debian DLA-561-1 : uclibc security update

Debian DLA-562-1 : gosa security update

Debian DLA-563-1 : libgd2 security update

Debian DLA-564-1 : tardiff security update

Debian DLA-565-1 : perl security update

Debian DLA-566-1 : cakephp security update

Debian DLA-567-2 : mysql-5.5 security and regression update

Debian DLA-568-1 : wordpress security update (httpoxy)

Debian DLA-569-1 : xmlrpc-epi security update

Debian DLA-57-1 : libstruts1.2-java security update

Debian DLA-570-1 : kde4libs security update

Debian DLA-571-1 : xen security update (Bunker Buster)

Debian DLA-572-1 : icedove security update

Debian DLA-573-1 : qemu security update

Debian DLA-574-1 : qemu-kvm security update

Debian DLA-575-2 : collectd regression update

Debian DLA-576-1 : libdbd-mysql-perl security update

Debian DLA-577-1 : redis security update

Debian DLA-578-1 : openssh security update

Debian DLA-579-1 : openjdk-7 security update

Debian DLA-58-3 : apt robustness improvements

Debian DLA-581-1 : libreoffice security update

Debian DLA-582-1 : libidn security update

Debian DLA-583-1 : lighttpd security update

Debian DLA-584-1 : libsys-syslog-perl security update

Debian DLA-585-1 : firefox-esr security update

Debian DLA-586-1 : curl security update

Debian DLA-587-1 : fontconfig security update

Debian DLA-588-2 : mongodb security update

Debian DLA-589-1 : mupdf security update

Debian DLA-590-1 : python-django security update

Debian DLA-591-1 : libreoffice security update

Debian DLA-592-1 : postgresql-9.1 security update

Debian DLA-593-1 : nettle security update

Debian DLA-594-1 : openssh security update

Debian DLA-595-1 : wireshark security update

Debian DLA-596-1 : extplorer security update

Debian DLA-597-1 : libupnp security update

Debian DLA-598-1 : suckless-tools security update

Debian DLA-599-1 : cracklib2 security update

Debian DLA-60-1 : icinga security update

Debian DLA-600-1 : libgcrypt11 security update

Debian DLA-601-1 : quagga security update

Debian DLA-602-1 : gnupg security and hardening update

Debian DLA-603-1 : ruby-activesupport-3.2 security update

Debian DLA-604-1 : ruby-actionpack-3.2 security update

Debian DLA-605-1 : eog security update

Debian DLA-606-1 : tiff security update

Debian DLA-608-1 : mailman security update

Debian DLA-609-1 : linux security update

Debian DLA-61-1 : libplack-perl security update

Debian DLA-610-2 : tiff3 regression update

Debian DLA-611-1 : jsch security update

Debian DLA-612-1 : libtomcrypt security update

Debian DLA-613-1 : roundcube security update

Debian DLA-614-1 : xen security update

Debian DLA-615-1 : icu security update

Debian DLA-616-1 : curl security update

Debian DLA-617-1 : libarchive security update

Debian DLA-618-1 : qemu security update

Debian DLA-619-1 : qemu-kvm security update

Debian DLA-62-1 : nss security update

Debian DLA-620-1 : libphp-adodb security update

Debian DLA-621-1 : autotrace security update

Debian DLA-622-1 : tomcat6 security update

Debian DLA-623-1 : tomcat7 security update

Debian DLA-624-1 : mysql-5.5 security update

Debian DLA-625-1 : curl security update

Debian DLA-626-1 : phpmyadmin security update

Debian DLA-627-1 : pdns security update

Debian DLA-628-1 : php5 security update

Debian DLA-629-1 : jackrabbit security update

Debian DLA-63-1 : bash security update

Debian DLA-630-1 : zookeeper security update

Debian DLA-631-1 : unadf security update

Debian DLA-632-1 : wireshark security update

Debian DLA-633-1 : wordpress security update

Debian DLA-634-1 : dropbear security update

Debian DLA-635-1 : dwarfutils security update

Debian DLA-636-2 : firefox-esr regression update

Debian DLA-637-1 : openssl security update

Debian DLA-638-1 : policycoreutils security update

Debian DLA-639-1 : mactelnet security update

Debian DLA-64-1 : curl security update

Debian DLA-640-1 : icedove security update

Debian DLA-641-1 : ruby-activesupport-3.2 security update

Debian DLA-642-1 : ruby-activerecord-3.2 security update

Debian DLA-643-1 : chicken security update

Debian DLA-644-1 : libav security update

Debian DLA-645-1 : bind9 security update

Debian DLA-646-1 : zendframework security update

Debian DLA-648-1 : c-ares security update

Debian DLA-65-1 : python-django security update

Debian DLA-650-1 : mat security update

Debian DLA-651-1 : graphicsmagick security update

Debian DLA-652-1 : qemu security update

Debian DLA-653-1 : qemu-kvm security update

Debian DLA-654-1 : libxfixes security update

Debian DLA-655-1 : mpg123 security update

Debian DLA-656-1 : libdbd-mysql-perl security update

Debian DLA-657-1 : libarchive security update

Debian DLA-658-1 : icedove security update

Debian DLA-66-1 : apache2 security update

Debian DLA-660-1 : libxrandr security update

Debian DLA-661-1 : libarchive security update

Debian DLA-662-1 : quagga security update

Debian DLA-663-1 : tor security update

Debian DLA-664-1 : libxrender security update

Debian DLA-665-1 : libgd2 security update

Debian DLA-666-1 : guile-2.0 security update

Debian DLA-667-1 : libxv security update

Debian DLA-668-1 : libass security update

Debian DLA-669-1 : dwarfutils security update

Debian DLA-67-1 : php5 security update

Debian DLA-670-1 : linux security update (Dirty COW)

Debian DLA-671-1 : libxvmc security update

Debian DLA-672-1 : bind9 security update

Debian DLA-673-1 : kdepimlibs security update

Debian DLA-674-2 : ghostscript regression update

Debian DLA-675-1 : potrace security update

Debian DLA-676-1 : nspr security update

Debian DLA-677-1 : nss security update

Debian DLA-678-1 : qemu security update

Debian DLA-679-1 : qemu-kvm security update

Debian DLA-68-1 : fex security update

Debian DLA-680-2 : bash version number correction

Debian DLA-681-1 : tzdata new upstream version

Debian DLA-682-1 : libdatetime-timezone-perl new upstream version

Debian DLA-683-1 : graphicsmagick security update

Debian DLA-684-2 : libx11 regression update

Debian DLA-685-2 : libxi regression update

Debian DLA-686-1 : libxtst security update

Debian DLA-687-1 : tre security update

Debian DLA-688-1 : cairo security update

Debian DLA-689-1 : qemu-kvm security update

Debian DLA-69-1 : exuberant-ctags security update

Debian DLA-690-1 : tar security update

Debian DLA-691-1 : libxml2 security update

Debian DLA-692-1 : tiff3 security update

Debian DLA-693-2 : tiff regression update

Debian DLA-694-1 : libwmf security update

Debian DLA-695-1 : spip security update

Debian DLA-696-1 : bind9 security update

Debian DLA-697-1 : bsdiff security update

Debian DLA-698-1 : qemu security update

Debian DLA-699-1 : xen security update

Debian DLA-70-1 : tryton-server security update

Debian DLA-700-1 : libxslt security update

Debian DLA-701-1 : memcached security update

Debian DLA-702-1 : tzdata new upstream version

Debian DLA-703-1 : libdatetime-timezone-perl new upstream version

Debian DLA-704-1 : openjdk-7 security update

Debian DLA-705-1 : python-imaging security update

Debian DLA-707-1 : sudo security update

Debian DLA-708-1 : mysql-5.5 security update

Debian DLA-709-1 : postgresql-9.1 update

Debian DLA-71-1 : apache2 security update

Debian DLA-710-1 : akonadi update

Debian DLA-711-1 : curl security update

Debian DLA-712-1 : gst-plugins-bad0.10 security update

Debian DLA-713-1 : sniffit security update

Debian DLA-714-1 : wireshark security update

Debian DLA-715-1 : drupal7 security update

Debian DLA-716-1 : tiff security update

Debian DLA-717-1 : moin security update

Debian DLA-718-1 : vim security update

Debian DLA-72-2 : rsyslog regression update

Debian DLA-720-1 : xen security update

Debian DLA-721-1 : libgc security update

Debian DLA-722-1 : irssi security update

Debian DLA-723-1 : libsoap-lite-perl security update

Debian DLA-724-1 : mcabber security update

Debian DLA-725-1 : tzdata new upstream version

Debian DLA-726-1 : libdatetime-timezone-perl new upstream version

Debian DLA-727-1 : gst-plugins-good0.10 security update

Debian DLA-728-1 : tomcat6 security update

Debian DLA-729-1 : tomcat7 security update

Debian DLA-73-1 : tzdata update

Debian DLA-730-1 : firefox-esr security update

Debian DLA-731-2 : imagemagick regression update

Debian DLA-732-3 : monit regression update

Debian DLA-733-1 : openafs security update

Debian DLA-734-1 : mapserver security update

Debian DLA-735-1 : gst-plugins-base0.10 security update

Debian DLA-736-1 : gst-plugins-bad0.10 security update

Debian DLA-737-1 : roundcube security update

Debian DLA-738-1 : spip security update

Debian DLA-739-1 : jasper security updat

Debian DLA-74-1 : ppp security update

Debian DLA-740-1 : libgsf security update

Debian DLA-741-1 : unzip security update

Debian DLA-742-1 : chrony security update

Debian DLA-743-1 : firefox-esr security update

Debian DLA-744-1 : icu security update

Debian DLA-745-1 : most security update

Debian DLA-746-2 : tomcat6 regression update

Debian DLA-747-1 : libupnp security update

Debian DLA-748-1 : libupnp4 security update

Debian DLA-749-1 : php5 security update (httpoxy)

Debian DLA-75-1 : mysql-5.1 security update

Debian DLA-750-1 : game-music-emu security update

Debian DLA-751-1 : nagios3 security update

Debian DLA-752-1 : icedove security update

Debian DLA-753-1 : tomcat7 security update

Debian DLA-754-1 : tor security update

Debian DLA-755-1 : dcmtk security update

Debian DLA-756-1 : imagemagick security update

Debian DLA-757-1 : phpmyadmin security update

Debian DLA-758-1 : libgd2 security update

Debian DLA-759-1 : nss security update

Debian DLA-76-1 : kde4libs security update

Debian DLA-760-1 : spip security update

Debian DLA-761-2 : python-bottle regression update

Debian DLA-762-1 : exim4 security update

Debian DLA-763-1 : squid3 security update

Debian DLA-764-1 : qemu security update

Debian DLA-765-1 : qemu-kvm security update

Debian DLA-766-1 : libcrypto++ security update

Debian DLA-767-1 : curl security update

Debian DLA-768-1 : pgpdump security update

Debian DLA-769-1 : shutter security update

Debian DLA-77-1 : libtasn1-3 security update

Debian DLA-770-2 : libphp-phpmailer regression update

Debian DLA-771-1 : hdf5 security update

Debian DLA-772-1 : linux security update

Debian DLA-773-4 : python-crypto update

Debian DLA-774-1 : postgresql-common security update

Debian DLA-775-1 : hplip security update

Debian DLA-776-1 : samba security update

Debian DLA-777-1 : libvncserver security update

Debian DLA-778-1 : pcsc-lite security update

Debian DLA-779-1 : tomcat7 security update

Debian DLA-78-1 : torque security update

Debian DLA-780-1 : libav security update

Debian DLA-781-2 : asterisk regression update

Debian DLA-782-1 : icedove security update

Debian DLA-783-1 : xen security update

Debian DLA-784-1 : gcc-mozilla new package

Debian DLA-785-1 : wireless-regdb new upstream version

Debian DLA-786-1 : botan1.10 security update

Debian DLA-787-1 : otrs2 security update

Debian DLA-788-1 : pdns-recursor security update

Debian DLA-789-1 : icoutils security update

Debian DLA-79-1 : dokuwiki security update

Debian DLA-790-1 : mapserver security update

Debian DLA-791-1 : libav security update

Debian DLA-792-1 : libphp-swiftmailer security update

Debian DLA-793-1 : opus security update

Debian DLA-794-1 : groovy security update

Debian DLA-795-1 : tiff security update

Debian DLA-797-1 : mysql-5.5 security update

Debian DLA-798-1 : pdns security update

Debian DLA-799-1 : ming security update

Debian DLA-80-1 : libxml2 security update

Debian DLA-800-1 : firefox-esr security update

Debian DLA-801-1 : libxpm security update

Debian DLA-802-1 : openjdk-7 security update

Debian DLA-803-1 : lcms2 security update

Debian DLA-804-1 : libgd2 security update

Debian DLA-805-1 : bind9 security update

Debian DLA-806-1 : zoneminder security update

Debian DLA-807-1 : imagemagick security update

Debian DLA-808-1 : ruby-archive-tar-minitar security update

Debian DLA-809-1 : tcpdump security update

Debian DLA-81-1 : openssl security update

Debian DLA-810-1 : libarchive security update

Debian DLA-811-1 : libplist security update

Debian DLA-812-1 : ikiwiki security update

Debian DLA-813-1 : wordpress security update

Debian DLA-814-1 : openssl security update

Debian DLA-815-1 : ntfs-3g security update

Debian DLA-816-1 : svgsalamander security update

Debian DLA-817-1 : libphp-phpmailer security update

Debian DLA-818-1 : php5 security update

Debian DLA-819-2 : mysql-5.5 version number correction

Debian DLA-82-1 : wget security update

Debian DLA-820-1 : viewvc security update

Debian DLA-821-1 : openjdk-7 security update

Debian DLA-822-1 : vim security update

Debian DLA-823-2 : tomcat7 regression update

Debian DLA-824-1 : libevent security update

Debian DLA-825-1 : spice security update

Debian DLA-826-1 : wireshark security update

Debian DLA-827-1 : gst-plugins-base0.10 security update

Debian DLA-828-1 : gst-plugins-good0.10 security update

Debian DLA-829-1 : gst-plugins-ugly0.10 security update

Debian DLA-83-1 : ffmpeg update

Debian DLA-830-1 : gst-plugins-bad0.10 security update

Debian DLA-831-1 : gtk-vnc security update

Debian DLA-832-1 : bitlbee security update

Debian DLA-833-1 : linux security update

Debian DLA-834-1 : phpmyadmin security update

Debian DLA-835-1 : cakephp security update

Debian DLA-836-2 : munin regression update

Debian DLA-837-1 : radare2 security update

Debian DLA-838-1 : shadow security update

Debian DLA-839-2 : tnef regression update

Debian DLA-84-1 : curl security update

Debian DLA-840-1 : libplist security update

Debian DLA-841-2 : apache2 regression update

Debian DLA-842-1 : qemu-kvm security update

Debian DLA-843-1 : bind9 security update

Debian DLA-844-1 : libquicktime security update

Debian DLA-845-1 : qemu security update

Debian DLA-846-1 : libzip-ruby security update

Debian DLA-847-1 : texlive-base security update

Debian DLA-848-1 : freetype security update

Debian DLA-849-1 : linux security update

Debian DLA-85-1 : libxml-security-java security update

Debian DLA-850-1 : vim security update

Debian DLA-851-1 : wget security update

Debian DLA-852-1 : firefox-esr security update

Debian DLA-853-1 : pidgin security update

Debian DLA-854-1 : icoutils security update

Debian DLA-855-1 : roundcube security update

Debian DLA-856-1 : tzdata new upstream version

Debian DLA-857-1 : libdatetime-timezone-perl new upstream version

Debian DLA-858-1 : wireshark security update

Debian DLA-859-1 : calibre security update

Debian DLA-86-1 : file security update

Debian DLA-860-1 : wordpress security update

Debian DLA-861-1 : r-base security update

Debian DLA-863-1 : deluge security update

Debian DLA-864-1 : jhead security update

Debian DLA-865-1 : suricata security update

Debian DLA-866-1 : libxslt security update

Debian DLA-867-1 : audiofile security update

Debian DLA-868-1 : imagemagick security update

Debian DLA-869-1 : cgiemail security update

Debian DLA-87-1 : dbus security update

Debian DLA-870-1 : libplist security update

Debian DLA-871-1 : python3.2 security update

Debian DLA-872-1 : xrdp security update

Debian DLA-873-1 : apt-cacher security update

Debian DLA-874-1 : jbig2dec security update

Debian DLA-875-1 : php5 security update

Debian DLA-876-1 : eject security update

Debian DLA-877-1 : tiff security update

Debian DLA-878-1 : libytnef security update

Debian DLA-879-1 : firebird2.5 security update

Debian DLA-88-1 : ruby1.8 security update

Debian DLA-880-1 : tiff3 security update

Debian DLA-881-1 : ejabberd security update

Debian DLA-882-1 : tryton-server security update

Debian DLA-883-1 : curl security update

Debian DLA-884-1 : collectd security update

Debian DLA-885-1 : python-django security update

Debian DLA-886-1 : tzdata new upstream version

Debian DLA-887-1 : libdatetime-timezone-perl new upstream version

Debian DLA-888-1 : logback security update

Debian DLA-889-1 : potrace security update

Debian DLA-89-1 : nss security update

Debian DLA-890-1 : ming security update

Debian DLA-891-1 : libnl security update

Debian DLA-892-1 : libnl3 security update

Debian DLA-893-1 : bouncycastle security update

Debian DLA-894-1 : samba security update

Debian DLA-895-1 : openoffice.org-dictionaries update

Debian DLA-896-1 : icedove/thunderbird security update

Debian DLA-897-1 : qbittorrent security update

Debian DLA-898-1 : libosip2 security update

Debian DLA-899-1 : feh security update

Debian DLA-90-1 : imagemagick security update

Debian DLA-900-1 : freetype security update

Debian DLA-901-1 : radare2 security update

Debian DLA-902-1 : imagemagick security update

Debian DLA-903-1 : hunspell-en-us update

Debian DLA-904-1 : uzbek-wordlist update

Debian DLA-905-1 : ghostscript security update

Debian DLA-906-1 : firefox-esr security update

Debian DLA-907-1 : xen security update

Debian DLA-908-1 : chicken security update

Debian DLA-909-1 : libcroco security update

Debian DLA-91-2 : tomcat6 regression update

Debian DLA-910-1 : libreoffice security update

Debian DLA-911-1 : tiff security update

Debian DLA-912-1 : tiff3 security update

Debian DLA-913-1 : activemq security update

Debian DLA-914-1 : minicom security update

Debian DLA-915-1 : botan1.10 security update

Debian DLA-916-1 : mysql-5.5 security update (Riddle)

Debian DLA-917-1 : rtmpdump security update

Debian DLA-918-1 : freetype security update

Debian DLA-919-1 : weechat security update

Debian DLA-92-1 : tomcat-native security followup update

Debian DLA-920-1 : jasper security update

Debian DLA-921-1 : slurm-llnl security update

Debian DLA-922-1 : linux security update

Debian DLA-923-1 : partclone security update

Debian DLA-924-2 : tomcat7 regression update

Debian DLA-925-1 : kedpm security update

Debian DLA-926-1 : batik security update

Debian DLA-927-1 : fop security update

Debian DLA-928-1 : libsndfile security update

Debian DLA-929-1 : libpodofo security update

Debian DLA-93-1 : libgcrypt11 security update

Debian DLA-930-1 : libxstream-java security update

Debian DLA-931-1 : freetype security update

Debian DLA-932-1 : ghostscript security update

Debian DLA-933-1 : roundcube security update

Debian DLA-934-1 : radicale security update

Debian DLA-935-1 : lxterminal security update

Debian DLA-936-1 : libtirpc security update

Debian DLA-937-1 : rpcbind security update

Debian DLA-938-1 : git security update

Debian DLA-939-1 : qemu-kvm security update

Debian DLA-94-1 : php5 security update

Debian DLA-940-1 : sane-backends security update

Debian DLA-941-1 : squirrelmail security update

Debian DLA-942-1 : jbig2dec security update

Debian DLA-943-1 : deluge security update

Debian DLA-944-1 : openvpn security update

Debian DLA-945-1 : mysql-connector-java security update

Debian DLA-946-1 : nss security update

Debian DLA-947-1 : icu security update

Debian DLA-948-1 : dropbear security update

Debian DLA-949-1 : miniupnpc security update

Debian DLA-95-1 : clamav security update

Debian DLA-950-1 : libtasn1-3 security update

Debian DLA-951-1 : samba security update (SambaCry)

Debian DLA-952-1 : kde4libs security update

Debian DLA-953-1 : graphicsmagick security update

Debian DLA-954-1 : openjdk-7 security update

Debian DLA-955-1 : rzip security update

Debian DLA-956-1 : libsndfile security update

Debian DLA-957-1 : bind9 security update

Debian DLA-958-1 : libonig security update

Debian DLA-959-1 : libical security update

Debian DLA-96-1 : openjdk-6 security update

Debian DLA-960-1 : imagemagick security update

Debian DLA-961-1 : mosquitto security update

Debian DLA-962-1 : tnef security update

Debian DLA-963-1 : exiv2 security update

Debian DLA-964-1 : xen security update

Debian DLA-965-1 : qemu-kvm security update

Debian DLA-966-1 : pngquant security update

Debian DLA-967-1 : gajim security update

Debian DLA-968-1 : libpodofo security update

Debian DLA-969-1 : tiff security update

Debian DLA-97-1 : eglibc security update

Debian DLA-970-1 : sudo security update

Debian DLA-971-1 : nss security update

Debian DLA-972-1 : openldap security update

Debian DLA-973-1 : strongswan security update

Debian DLA-974-1 : picocom security update

Debian DLA-975-1 : wordpress security update

Debian DLA-976-1 : yodl security update

Debian DLA-977-1 : freeradius security update

Debian DLA-978-1 : perl security update

Debian DLA-979-1 : debian-security-support update

Debian DLA-98-1 : openvpn security update

Debian DLA-980-1 : ming security update

Debian DLA-981-1 : apng2gif security update

Debian DLA-982-1 : tor security update

Debian DLA-983-1 : tiff3 security update

Debian DLA-984-1 : tiff security update

Debian DLA-985-1 : libsndfile security update

Debian DLA-986-1 : zookeeper security update

Debian DLA-987-1 : request-tracker4 security update

Debian DLA-988-1 : rt-authen-externalauth security update

Debian DLA-989-1 : jython security update

Debian DLA-99-1 : flac security update

Debian DLA-990-1 : expat security update

Debian DLA-991-1 : firefox-esr security update

Debian DLA-992-1 : eglibc security update (Stack Clash)

Debian DLA-993-2 : linux regression update (Stack Clash)

Debian DLA-994-1 : zziplib security update

Debian DLA-995-1 : swftools security update

Debian DLA-996-1 : tomcat7 security update

Debian DLA-997-1 : libffi security update (Stack Clash)

Debian DLA-998-1 : c-ares security update

Debian DLA-999-1 : openvpn security update

Debian DSA-011-2 : mgetty - insecure tempfile handling

Debian DSA-012-1 : micq - remote buffer overflow

Debian DSA-013 : MySQL - remote buffer overflow

Debian DSA-014-2 : splitvt - buffer overflow and format string attack

Debian DSA-015-1 : sash - broken maintainer script

Debian DSA-016-3 : wu-ftpd - temp file creation and format string

Debian DSA-017-1 : jazip - buffer overflow

Debian DSA-018-1 : tinyproxy - remote nobody exploit

Debian DSA-019-1 : squid - insecure tempfile handling

Debian DSA-020-1 : php4 - remote DOS and remote information leak

Debian DSA-021-1 : apache - insecure tempfile bug, broken mod\_rewrite

Debian DSA-022-1 : exmh - local insecure tempfile creation

Debian DSA-023-1 : inn2 - local tempfile vulnerabilities

Debian DSA-024-1 : cron - local insecure crontab handling

Debian DSA-025-2 : openssh - Missing PAM support

Debian DSA-026-1 : bind - buffer overflows and information leak

Debian DSA-027-1 : OpenSSH - remote exploit

Debian DSA-028-1 : man-db - format string vulnerability

Debian DSA-029-2 : proftpd - remote DOS & potential buffer overflow

Debian DSA-030-2 : xfree86

Debian DSA-031-2 : sudo - buffer overflow

Debian DSA-032-1 : proftpd - proftpd running with incorrect userid, erroneous file removal

Debian DSA-033-1 : analog - buffer overflow

Debian DSA-034-1 : ePerl - remote root exploit

Debian DSA-035-1 : man2html - remote denial of service

Debian DSA-036-1 : Midnight Commander - arbitrary program execution

Debian DSA-037-1 : Athena Widget replacement libraries - insecure tempfile handling

Debian DSA-038-1 : sgml-tools - insecure tempfiles

Debian DSA-039-1 : glibc

Debian DSA-040-1 : slrn - buffer overflow

Debian DSA-041-1 : joe - local exploit

Debian DSA-042-1 : gnuserv

Debian DSA-043-1 : zope

Debian DSA-044-1 : mailx

Debian DSA-045-2 : ntpd - remote root exploit

Debian DSA-046-2 : exuberant-ctags

Debian DSA-047-1 : kernel

Debian DSA-048-3 : samba

Debian DSA-049-1 : cfingerd

Debian DSA-050-1 : sendfile - broken privileges dropping, broken tempfile

Debian DSA-051-1 : netscape - unexpected javascript execution

Debian DSA-052-1 : sendfile - broken dropping of privileges

Debian DSA-053-1 : nedit - insecure temporary file

Debian DSA-054-1 : cron - local root exploit

Debian DSA-055-1 : zope - remote unauthorized access

Debian DSA-056-1 : man-db - local file overwrite

Debian DSA-057-1 : gftp - printf format attack

Debian DSA-058-1 : exim - local printf format attack

Debian DSA-059-1 : man-db - symlink attack

Debian DSA-060-1 : fetchmail - buffer overflow

Debian DSA-061-1 : gnupg - printf format attack

Debian DSA-062-1 : rxvt - buffer overflow

Debian DSA-063-1 : xinetd - change default umask

Debian DSA-064-1 : w3m - buffer overflow

Debian DSA-065-1 : samba - remote file append/creation

Debian DSA-066-1 : cfingerd - remote exploit

Debian DSA-067-1 : apache - Remote exploit

Debian DSA-068-1 : openldap - remote DoS

Debian DSA-069-1 : xloadimage - buffer overflow

Debian DSA-070-1 : netkit-telnet - remote exploit

Debian DSA-071-1 : fetchmail - memory corruption

Debian DSA-072-1 : groff - printf format attack

Debian DSA-073-1 : imp - 3 remote exploits

Debian DSA-074-1 : wmaker - buffer overflow

Debian DSA-075-1 : netkit-telnet-ssl - remote exploit

Debian DSA-076-1 : most - buffer overflow

Debian DSA-077-1 : squid - remote DoS

Debian DSA-078-1 : slrn - remote command invocation

Debian DSA-079-2 : uucp - uucp uid/gid access

Debian DSA-080-1 : htdig - unauthorized gathering of data

Debian DSA-081-1 : w3m - Buffer Overflow

Debian DSA-082-1 : xvt - Buffer Overflow

Debian DSA-083-1 : procmail - insecure signal handling

Debian DSA-084-1 : gftp - Information Retrieval

Debian DSA-085-1 : nvi - Format string vulnerability

Debian DSA-086-1 : ssh-nonfree - remote root exploit

Debian DSA-087-1 : wu-ftpd - remote root exploit

Debian DSA-088-1 : fml - improper character escaping

Debian DSA-089-2 : icecast-server - remote root exploit (and others)

Debian DSA-090-1 : xtel - symlink attack

Debian DSA-091-1 : ssh - influencing login

Debian DSA-092-1 : wmtv - local root exploit

Debian DSA-093-1 : postfix - remote DoS

Debian DSA-094-1 : mailman - XSS hole

Debian DSA-095-1 : gpm - local root vulnerability

Debian DSA-096-2 : mutt - buffer overflow

Debian DSA-097-1 : exim - Uncontrolled program execution

Debian DSA-098-1 : libgtop - format string vulnerability and buffer overflow

Debian DSA-099-1 : xchat - IRC session hijacking

Debian DSA-100-1 : gzip - Potential buffer overflow

Debian DSA-1000-2 : libapreq2-perl - design error

Debian DSA-1001-1 : crossfire - buffer overflow

Debian DSA-1002-1 : webcalendar - several vulnerabilities

Debian DSA-1003-1 : xpvm - insecure temporary file

Debian DSA-1004-1 : vlc - buffer overflow

Debian DSA-1005-1 : xine-lib - buffer overflow

Debian DSA-1006-1 : wzdftpd - missing input sanitising

Debian DSA-1007-1 : drupal - several vulnerabilities

Debian DSA-1008-1 : kdegraphics - buffer overflow

Debian DSA-1009-1 : crossfire - buffer overflow

Debian DSA-101-1 : sudo - Local root exploit

Debian DSA-1010-1 : ilohamail - missing input sanitising

Debian DSA-1011-1 : kernel-patch-vserver - missing attribute support

Debian DSA-1012-1 : unzip - buffer overflow

Debian DSA-1013-1 : snmptrapfmt - insecure temporary file

Debian DSA-1014-1 : firebird2 - buffer overflow

Debian DSA-1015-1 : sendmail - programming error

Debian DSA-1016-1 : evolution - format string vulnerabilities

Debian DSA-1017-1 : kernel-source-2.6.8 - several vulnerabilities

Debian DSA-1018-2 : kernel-source-2.4.27 - several vulnerabilities

Debian DSA-1019-1 : koffice - several vulnerabilities

Debian DSA-102-2 : at - daemon exploit

Debian DSA-1020-1 : flex - buffer overflow

Debian DSA-1021-1 : netpbm-free - insecure program execution

Debian DSA-1022-1 : storebackup - several vulnerabilities

Debian DSA-1023-1 : kaffeine - buffer overflow

Debian DSA-1024-1 : clamav - several vulnerabilities

Debian DSA-1025-1 : dia - programming error

Debian DSA-1026-1 : sash - buffer overflows

Debian DSA-1027-1 : mailman - programming error

Debian DSA-1028-1 : libimager-perl - programming error

Debian DSA-1029-1 : libphp-adodb - several vulnerabilities

Debian DSA-103-1 : glibc - buffer overflow

Debian DSA-1030-1 : moodle - several vulnerabilities

Debian DSA-1031-1 : cacti - several vulnerabilities

Debian DSA-1032-1 : zope-cmfplone - programming error

Debian DSA-1033-1 : horde3 - several vulnerabilities

Debian DSA-1034-1 : horde2 - several vulnerabilities

Debian DSA-1035-1 : fcheck - insecure temporary file

Debian DSA-1036-1 : bsdgames - buffer overflow

Debian DSA-1037-1 : zgv - programming error

Debian DSA-1038-1 : xzgv - programming error

Debian DSA-1039-1 : blender - several vulnerabilities

Debian DSA-104-1 : cipe - DoS attack

Debian DSA-1040-1 : gdm - programming error

Debian DSA-1041-1 : abc2ps - buffer overflows

Debian DSA-1042-1 : cyrus-sasl2 - programming error

Debian DSA-1043-1 : abcmidi - buffer overflows

Debian DSA-1044-1 : mozilla-firefox - several vulnerabilities

Debian DSA-1045-1 : openvpn - design error

Debian DSA-1046-1 : mozilla - several vulnerabilities

Debian DSA-1047-1 : resmgr - programming error

Debian DSA-1048-1 : asterisk - several vulnerabilities

Debian DSA-1049-1 : ethereal - several vulnerabilities

Debian DSA-105-1 : enscript - insecure temporary files

Debian DSA-1050-1 : clamav - buffer overflow

Debian DSA-1051-1 : mozilla-thunderbird - several vulnerabilities

Debian DSA-1052-1 : cgiirc - buffer overflows

Debian DSA-1053-1 : mozilla - programming error

Debian DSA-1054-1 : tiff - several vulnerabilities

Debian DSA-1055-1 : mozilla-firefox - programming error

Debian DSA-1056-1 : webcalendar - verbose error message

Debian DSA-1057-1 : phpldapadmin - missing input sanitising

Debian DSA-1058-1 : awstats - missing input sanitising

Debian DSA-1059-1 : quagga - several vulnerabilities

Debian DSA-106-2 : rsync - remote exploit

Debian DSA-1060-1 : kernel-patch-vserver - programming error

Debian DSA-1061-1 : popfile - missing input sanitising

Debian DSA-1062-1 : kphone - insecure file creation

Debian DSA-1063-1 : phpgroupware - missing input sanitising

Debian DSA-1064-1 : cscope - buffer overflows

Debian DSA-1065-1 : hostapd - missing input sanitising

Debian DSA-1066-1 : phpbb2 - missing input sanitising

Debian DSA-1067-1 : kernel-source-2.4.16 - several vulnerabilities

Debian DSA-1068-1 : fbi - insecure temporary file

Debian DSA-1069-1 : kernel-source-2.4.18 - several vulnerabilities

Debian DSA-107-1 : jgroff - format print vulnerability

Debian DSA-1070-1 : kernel-source-2.4.19 - several vulnerabilities

Debian DSA-1071-1 : mysql - several vulnerabilities

Debian DSA-1072-1 : nagios - buffer overflow

Debian DSA-1073-1 : mysql-dfsg-4.1 - several vulnerabilities

Debian DSA-1074-1 : mpg123 - buffer overflow

Debian DSA-1075-1 : awstats - programming error

Debian DSA-1076-1 : lynx - programming error

Debian DSA-1077-1 : lynx-ssl - programming error

Debian DSA-1078-1 : tiff - out-of-bounds read

Debian DSA-1079-1 : mysql-dfsg - several vulnerabilities

Debian DSA-108-1 : wmtv - symlink vulnerability

Debian DSA-1080-1 : dovecot - programming error

Debian DSA-1081-1 : libextractor - buffer overflow

Debian DSA-1082-1 : kernel-source-2.4.17 - several vulnerabilities

Debian DSA-1083-1 : motor - buffer overflow

Debian DSA-1084-1 : typespeed - buffer overflow

Debian DSA-1085-1 : lynx-cur - several vulnerabilities

Debian DSA-1086-1 : xmcd - design flaw

Debian DSA-1087-1 : postgresql - programming error

Debian DSA-1088-1 : centericq - buffer overflow

Debian DSA-1089-1 : freeradius - several vulnerabilities

Debian DSA-109-1 : faqomatic - XSS vulnerability

Debian DSA-1090-1 : spamassassin - programming error

Debian DSA-1091-1 : tiff - buffer overflows

Debian DSA-1092-1 : mysql-dfsg-4.1 - programming error

Debian DSA-1093-1 : xine - format string

Debian DSA-1094-1 : gforge - missing input sanitising

Debian DSA-1095-1 : freetype - integer overflows

Debian DSA-1096-1 : webcalendar - uninitialised variable

Debian DSA-1097-1 : kernel-source-2.4.27 - several vulnerabilities

Debian DSA-1098-1 : horde3 - missing input sanitising

Debian DSA-1099-1 : horde2 - missing input sanitising

Debian DSA-110-1 : cups - buffer overflow

Debian DSA-1100-1 : wv2 - integer overflow

Debian DSA-1101-1 : courier - programming error

Debian DSA-1102-1 : pinball - design error

Debian DSA-1103-1 : kernel-source-2.6.8 - several vulnerabilities

Debian DSA-1104-2 : openoffice.org - several vulnerabilities

Debian DSA-1105-1 : xine-lib - buffer overflow

Debian DSA-1106-1 : ppp - programming error

Debian DSA-1107-1 : gnupg - integer overflow

Debian DSA-1108-1 : mutt - buffer overflow

Debian DSA-1109-1 : rssh - programming error

Debian DSA-111-1 : ucd-snmp - remote exploit

Debian DSA-1110-1 : samba - missing input sanitising

Debian DSA-1111-2 : kernel-source-2.6.8 - race condition

Debian DSA-1112-1 : mysql-dfsg-4.1 - several vulnerabilities

Debian DSA-1113-1 : zope2.7 - programming error

Debian DSA-1114-1 : hashcash - buffer overflow

Debian DSA-1115-1 : gnupg2 - integer overflow

Debian DSA-1116-1 : gimp - buffer overflow

Debian DSA-1117-1 : libgd2 - insufficient input sanitising

Debian DSA-1118-1 : mozilla - several vulnerabilities

Debian DSA-1119-1 : hiki - design flaw

Debian DSA-112-1 : hanterm - buffer overflow

Debian DSA-1120-1 : mozilla-firefox - several vulnerabilities

Debian DSA-1121-1 : postgrey - format string

Debian DSA-1122-1 : libnet-server-perl - format string

Debian DSA-1123-1 : libdumb - buffer overflow

Debian DSA-1124-1 : fbi - typo

Debian DSA-1125-2 : drupal - several vulnerabilities

Debian DSA-1126-1 : asterisk - buffer overflow

Debian DSA-1127-1 : ethereal - several vulnerabilities

Debian DSA-1128-1 : heartbeat - permission error

Debian DSA-1129-1 : osiris - format string

Debian DSA-113-1 : ncurses - buffer overflow

Debian DSA-1130-1 : sitebar - missing input validation

Debian DSA-1131-1 : apache - buffer overflow

Debian DSA-1132-1 : apache2 - buffer overflow

Debian DSA-1133-1 : mantis - missing input sanitising

Debian DSA-1134-1 : mozilla-thunderbird - several vulnerabilities

Debian DSA-1135-1 : libtunepimp - buffer overflow

Debian DSA-1136-1 : gpdf - wrong input sanitising

Debian DSA-1137-1 : tiff - several vulnerabilities

Debian DSA-1138-1 : cfs - integer overflow

Debian DSA-1139-1 : ruby1.6 - missing privilege checks

Debian DSA-114-1 : gnujsp - unauthorized file access

Debian DSA-1140-1 : gnupg - integer overflow

Debian DSA-1141-1 : gnupg2 - integer overflow

Debian DSA-1142-1 : freeciv - missing boundary checks

Debian DSA-1143-1 : dhcp - programming error

Debian DSA-1144-1 : chmlib - missing input sanitising

Debian DSA-1145-1 : freeradius - several vulnerabilities

Debian DSA-1146-1 : krb5 - programming error

Debian DSA-1147-1 : drupal - missing input sanitising

Debian DSA-1148-1 : gallery - several vulnerabilities

Debian DSA-1149-1 : ncompress - buffer underflow

Debian DSA-115-1 : php - broken boundary check and more

Debian DSA-1150-1 : shadow - programming error

Debian DSA-1151-1 : heartbeat - out-of-bounds read

Debian DSA-1152-1 : trac - missing input sanitising

Debian DSA-1153-1 : clamav - buffer overflow

Debian DSA-1154-1 : squirrelmail - variable overwriting

Debian DSA-1155-2 : sendmail - programming error

Debian DSA-1156-1 : kdebase - programming error

Debian DSA-1157-1 : ruby1.8 - several vulnerabilities

Debian DSA-1158-1 : streamripper - buffer overflow

Debian DSA-1159-2 : mozilla-thunderbird - several vulnerabilities

Debian DSA-116-1 : cfs - buffer overflow

Debian DSA-1160-2 : mozilla - several vulnerabilities

Debian DSA-1161-2 : mozilla-firefox - several vulnerabilities

Debian DSA-1162-1 : libmusicbrainz-2.0 - buffer overflows

Debian DSA-1163-1 : gtetrinet - programming error

Debian DSA-1164-1 : sendmail - programming error

Debian DSA-1165-1 : capi4hylafax - missing input sanitising

Debian DSA-1166-2 : cheesetracker - buffer overflow

Debian DSA-1167-1 : apache - missing input sanitising

Debian DSA-1168-1 : imagemagick - several vulnerabilities

Debian DSA-1169-1 : mysql-dfsg-4.1 - several vulnerabilities

Debian DSA-117-1 : cvs - improper variable initialization

Debian DSA-1170-1 : gcc-3.4 - missing sanity check

Debian DSA-1171-1 : ethereal - several vulnerabilities

Debian DSA-1172-1 : bind9 - programming error

Debian DSA-1173-1 : openssl - cryptographic weakness

Debian DSA-1174-1 : openssl096 - cryptographic weakness

Debian DSA-1175-1 : isakmpd - programming error

Debian DSA-1176-1 : zope2.7 - programming error

Debian DSA-1177-1 : usermin - programming error

Debian DSA-1178-1 : freetype - integer overflow

Debian DSA-1179-1 : alsaplayer - programming error

Debian DSA-118-1 : xsane - insecure temporary files

Debian DSA-1180-1 : bomberclone - programming error

Debian DSA-1181-1 : gzip - several vulnerabilities

Debian DSA-1182-1 : gnutls11 - cryptographic weakness

Debian DSA-1183-1 : kernel-source-2.4.27 - several vulnerabilities

Debian DSA-1184-2 : kernel-source-2.6.8 - several vulnerabilities

Debian DSA-1185-2 : openssl - denial of service

Debian DSA-1186-1 : cscope - buffer overflows

Debian DSA-1187-1 : migrationtools - insecure temporary files

Debian DSA-1188-1 : mailman - format string

Debian DSA-1189-1 : openssh-krb5 - several vulnerabilities

Debian DSA-1190-1 : maxdb-7.5.00 - buffer overflow

Debian DSA-1191-1 : mozilla-thunderbird - several vulnerabilities

Debian DSA-1192-1 : mozilla - several vulnerabilities

Debian DSA-1193-1 : xfree86 - several vulnerabilities

Debian DSA-1194-1 : libwmf - integer overflow

Debian DSA-1195-1 : openssl096 - denial of service (multiple)

Debian DSA-1196-1 : clamav - several vulnerabilities

Debian DSA-1197-1 : python2.4 - buffer overflow

Debian DSA-1198-1 : python2.3 - buffer overflow

Debian DSA-1199-1 : webmin - multiple vulnerabilities

Debian DSA-120-1 : mod\_ssl - buffer overflow

Debian DSA-1200-1 : qt-x11-free - integer overflow

Debian DSA-1201-1 : ethereal - several vulnerabilities

Debian DSA-1202-1 : screen - programming error

Debian DSA-1203-1 : libpam-ldap - programming error

Debian DSA-1204-1 : ingo1 - missing input sanitising

Debian DSA-1205-2 : thttpd - insecure temporary files

Debian DSA-1206-1 : php4 - several vulnerabilities

Debian DSA-1207-2 : phpmyadmin - several vulnerabilities

Debian DSA-1208-1 : bugzilla - several vulnerabilities

Debian DSA-1209-2 : trac - cross-site request forgery

Debian DSA-121-1 : xtell - buffer overflow, symlink problem, '..' directory traversal

Debian DSA-1210-1 : mozilla-firefox - several vulnerabilities

Debian DSA-1211-1 : pdns - buffer overflow

Debian DSA-1212-1 : openssh - Denial of service

Debian DSA-1213-1 : imagemagick - several vulnerabilities

Debian DSA-1214-2 : gv - buffer overflow

Debian DSA-1215-1 : xine-lib - several vulnerabilities

Debian DSA-1216-1 : flexbackup - insecure temporary file

Debian DSA-1217-1 : linux-ftpd - programming error

Debian DSA-1218-1 : proftpd - programming error

Debian DSA-1219-1 : texinfo - buffer overflow

Debian DSA-122-1 : zlib - malloc error (double free)

Debian DSA-1220-1 : pstotext - insecure file name quoting

Debian DSA-1221-1 : libgsf - buffer overflow

Debian DSA-1222-2 : proftpd - several vulnerabilities

Debian DSA-1223-1 : tar - input validation error

Debian DSA-1224-1 : mozilla - several vulnerabilities

Debian DSA-1225-2 : mozilla-firefox - several vulnerabilities

Debian DSA-1226-1 : links - insufficient escaping

Debian DSA-1227-1 : mozilla-thunderbird - several vulnerabilities

Debian DSA-1228-1 : elinks - insufficient escaping

Debian DSA-1229-1 : asterisk - integer overflow

Debian DSA-123-1 : listar - remote exploit

Debian DSA-1230-1 : l2tpns - buffer overflow

Debian DSA-1231-1 : gnupg - several vulnerabilities

Debian DSA-1232-1 : clamav - missing sanity checks

Debian DSA-1233-1 : kernel-source-2.6.8 - several vulnerabilities

Debian DSA-1234-1 : ruby1.6 - denial of service

Debian DSA-1235-1 : ruby1.8 - denial of service

Debian DSA-1236-1 : enemies-of-carlotta - missing sanity checks

Debian DSA-1237-1 : kernel-source-2.4.27 - several vulnerabilities

Debian DSA-1238-1 : clamav - several vulnerabilities

Debian DSA-1239-1 : sql-ledger - several vulnerabilities

Debian DSA-124-1 : mtr - buffer overflow

Debian DSA-1240-1 : links2 - insufficient escaping

Debian DSA-1241-1 : squirrelmail - XSS

Debian DSA-1242-1 : elog - several vulnerabilities

Debian DSA-1243-1 : evince - buffer overflow

Debian DSA-1244-1 : xine-lib - buffer overflow

Debian DSA-1245-1 : proftpd - programming error

Debian DSA-1246-1 : openoffice.org - buffer overflow

Debian DSA-1247-1 : libapache-mod-auth-kerb - heap overflow

Debian DSA-1248-1 : libsoup - missing input sanitising

Debian DSA-1249-1 : xfree86 - several vulnerabilities

Debian DSA-125-1 : analog - XSS

Debian DSA-1250-1 : cacti - missing input sanitising

Debian DSA-1251-1 : netrick - insufficient escaping

Debian DSA-1252-1 : vlc - format string

Debian DSA-1253-1 : mozilla-firefox - several vulnerabilities

Debian DSA-1254-1 : bind9 - insufficient input sanitising

Debian DSA-1255-1 : libgtop2 - buffer overflow

Debian DSA-1256-1 : gtk+2.0 - programming error

Debian DSA-1257-1 : samba - several vulnerabilities

Debian DSA-1258-1 : mozilla-thunderbird - several vulnerabilities

Debian DSA-1259-1 : fetchmail - programming error

Debian DSA-126-1 : imp - XSS

Debian DSA-1260-1 : imagemagick - buffer overflow

Debian DSA-1261-1 : postgresql - several vulnerabilities

Debian DSA-1262-1 : gnomemeeting - format string

Debian DSA-1263-1 : clamav - several vulnerabilities

Debian DSA-1264-1 : php4 - several vulnerabilities

Debian DSA-1265-1 : mozilla - several vulnerabilities

Debian DSA-1266-1 : gnupg - several vulnerabilities

Debian DSA-1267-1 : webcalendar - missing input sanitising

Debian DSA-1268-1 : libwpd - integer overflow

Debian DSA-1269-1 : lookup-el - insecure temporary file

Debian DSA-127-1 : xpilot-server - remote buffer overflow

Debian DSA-1270-2 : openoffice.org - several vulnerabilities

Debian DSA-1271-1 : openafs - design error

Debian DSA-1272-1 : tcpdump - buffer overflow

Debian DSA-1273-1 : nas - several vulnerabilities

Debian DSA-1274-1 : file - buffer overflow

Debian DSA-1275-1 : zope2.7 - XSS

Debian DSA-1276-1 : krb5 - several vulnerabilities

Debian DSA-1277-1 : XMMS - several vulnerabilities

Debian DSA-1278-1 : man-db - buffer overflow

Debian DSA-1279-1 : webcalendar - missing input sanitising

Debian DSA-128-1 : sudo - buffer overflow

Debian DSA-1280-1 : aircrack-ng - buffer overflow

Debian DSA-1281-1 : clamav - several vulnerabilities

Debian DSA-1282-1 : php4 - several vulnerabilities

Debian DSA-1283-1 : php5 - several vulnerabilities

Debian DSA-1284-1 : qemu - several vulnerabilities

Debian DSA-1285-1 : wordpress - several vulnerabilities

Debian DSA-1286-1 : linux-2.6 - several vulnerabilities

Debian DSA-1287-1 : ldap-account-manager - multiple vulnerabilities

Debian DSA-1288-1 : pptpd - programming error

Debian DSA-1289-1 : linux-2.6 - several vulnerabilities

Debian DSA-129-1 : uucp - remote denial of service

Debian DSA-1290-1 : squirrelmail - missing input sanitising

Debian DSA-1291-1 : samba - several vulnerabilities

Debian DSA-1292-1 : qt4-x11 - missing input validation

Debian DSA-1293-1 : quagga - out of boundary read

Debian DSA-1294-1 : xfree86 - several vulnerabilities

Debian DSA-1295-1 : php5 - several vulnerabilities

Debian DSA-1296-1 : php4 - missing input sanitising

Debian DSA-1297-1 : gforge-plugin-scmcvs - missing input sanitising

Debian DSA-1298-1 : otrs2 - missing input sanitising

Debian DSA-1299-1 : ipsec-tools - missing input sanitising

Debian DSA-130-1 : ethereal - remotely triggered memory allocation error

Debian DSA-1300-1 : iceape - several vulnerabilities

Debian DSA-1301-1 : gimp - buffer overflow

Debian DSA-1302-1 : freetype - integer overflow

Debian DSA-1303-1 : lighttpd - denial of service

Debian DSA-1304-1 : kernel-source-2.6.8 - several vulnerabilities

Debian DSA-1305-1 : icedove - several vulnerabilities

Debian DSA-1306-1 : xulrunner - several vulnerabilities

Debian DSA-1307-1 : openoffice.org - heap overflow

Debian DSA-1308-1 : iceweasel - several vulnerabilities

Debian DSA-1309-1 : postgresql-8.1 - programming error

Debian DSA-131-1 : apache - remote DoS / exploit

Debian DSA-1310-1 : libexif - integer overflow

Debian DSA-1311-1 : postgresql-7.4 - programming error

Debian DSA-1312-1 : libapache-mod-jk - programming error

Debian DSA-1313-1 : mplayer - buffer overflow

Debian DSA-1314-1 : open-iscsi - several vulnerabilities

Debian DSA-1315-1 : libphp-phpmailer - missing input validation

Debian DSA-1316-1 : emacs21 - denial of service

Debian DSA-1317-1 : tinymux - buffer overflow

Debian DSA-1318-1 : ekg - several vulnerabilities

Debian DSA-1319-1 : maradns - memory leaks

Debian DSA-132-1 : apache-ssl - remote DoS / exploit

Debian DSA-1320-1 : clamav - several vulnerabilities

Debian DSA-1321-1 : evolution-data-server - programming error

Debian DSA-1322-1 : wireshark - several vulnerabilities

Debian DSA-1323-1 : krb5 - several vulnerabilities

Debian DSA-1324-1 : hiki - missing input sanitising

Debian DSA-1325-1 : evolution - several vulnerabilities

Debian DSA-1326-1 : fireflier-server - insecure temporary files

Debian DSA-1327-1 : gsambad - insecure temporary files

Debian DSA-1328-1 : unicon-imc2 - buffer overflow

Debian DSA-1329-1 : gfax - insecure temporary files

Debian DSA-133-1 : apache-perl - remote DoS / exploit

Debian DSA-1330-1 : php5 - several vulnerabilities

Debian DSA-1331-1 : php4 - several vulnerabilities

Debian DSA-1332-1 : vlc - several vulnerabilities

Debian DSA-1333-1 : libcurl3-gnutls - missing input validation

Debian DSA-1334-1 : freetype - integer overflow

Debian DSA-1335-1 : gimp - several vulnerabilities

Debian DSA-1336-1 : mozilla-firefox - several vulnerabilities

Debian DSA-1337-1 : xulrunner - several vulnerabilities

Debian DSA-1338-1 : iceweasel - several vulnerabilities

Debian DSA-1339-1 : iceape - several vulnerabilities

Debian DSA-134-4 : ssh - remote exploit

Debian DSA-1340-1 : clamav - NULL pointer dereference

Debian DSA-1341-2 : bind9 - design error

Debian DSA-1342-1 : xfs - race condition

Debian DSA-1343-1 : file - integer overflow

Debian DSA-1344-1 : iceweasel - several vulnerabilities

Debian DSA-1345-1 : xulrunner - several vulnerabilities

Debian DSA-1346-1 : iceape - several vulnerabilities

Debian DSA-1347-1 : xpdf - integer overflow

Debian DSA-1348-1 : poppler - integer overflow

Debian DSA-1349-1 : libextractor - integer overflow

Debian DSA-135-1 : libapache-mod-ssl - buffer overflow / DoS

Debian DSA-1350-1 : tetex-bin - integer overflow

Debian DSA-1351-1 : bochs - buffer overflow

Debian DSA-1352-1 : pdfkit.framework - integer overflow

Debian DSA-1353-1 : tcpdump - integer overflow

Debian DSA-1354-1 : gpdf - integer overflow

Debian DSA-1355-1 : kdegraphics - integer overflow

Debian DSA-1356-1 : linux-2.6 - several vulnerabilities

Debian DSA-1357-1 : koffice - integer overflow

Debian DSA-1358-1 : asterisk - several vulnerabilities

Debian DSA-1359-1 : dovecot - directory traversal

Debian DSA-136-1 : openssl - multiple remote exploits

Debian DSA-1360-1 : rsync - buffer overflow

Debian DSA-1361-1 : postfix-policyd - buffer overflow

Debian DSA-1362-2 : lighttpd - several vulnerabilities

Debian DSA-1363-1 : linux-2.6 - several vulnerabilities

Debian DSA-1364-2 : vim - several vulnerabilities

Debian DSA-1365-3 : id3lib3.8.3 - programming error

Debian DSA-1366-1 : clamav - several vulnerabilities

Debian DSA-1367-1 : krb5 - buffer overflow

Debian DSA-1368-1 : librpcsecgss - buffer overflow

Debian DSA-1369-1 : gforge - missing input sanitising

Debian DSA-137-1 : mm - insecure temporary files

Debian DSA-1370-1 : phpmyadmin - several vulnerabilities

Debian DSA-1371-1 : phpwiki - several vulnerabilities

Debian DSA-1372-1 : xorg-server - buffer overflow

Debian DSA-1373-2 : ktorrent - directory traversal

Debian DSA-1374-1 : jffnms - several vulnerabilities

Debian DSA-1375-1 : openoffice.org - buffer overflow

Debian DSA-1376-1 : kdebase - programming error

Debian DSA-1377-2 : fetchmail - NULL pointer dereference

Debian DSA-1378-2 : linux-2.6 - several vulnerabilities

Debian DSA-1379-1 : openssl - off-by-one error/buffer overflow

Debian DSA-138-1 : gallery - remote exploit

Debian DSA-1380-1 : elinks - programming error

Debian DSA-1381-2 : linux-2.6 - several vulnerabilities

Debian DSA-1382-1 : quagga - NULL pointer dereference

Debian DSA-1383-1 : gforge - XSS

Debian DSA-1384-1 : xen-utils - several vulnerabilities

Debian DSA-1385-1 : xfs - several vulnerabilities

Debian DSA-1386-1 : wesnoth - programming error

Debian DSA-1387-1 : librpcsecgss - buffer overflow

Debian DSA-1388-3 : dhcp - buffer overflow

Debian DSA-1389-2 : zoph - missing input sanitising

Debian DSA-139-1 : super - format string vulnerability

Debian DSA-1390-1 : t1lib - buffer overflow

Debian DSA-1391-1 : icedove - several vulnerabilities

Debian DSA-1392-1 : xulrunner - several vulnerabilities

Debian DSA-1393-1 : xfce4-terminal - insecure execution

Debian DSA-1394-1 : reprepro - authentication bypass

Debian DSA-1395-1 : xen-utils - insecure temporary files

Debian DSA-1396-1 : iceweasel - several vulnerabilities

Debian DSA-1397-1 : mono - integer overflow

Debian DSA-1398-1 : perdition - format string error

Debian DSA-1399-1 : pcre3 - several vulnerabilities

Debian DSA-140-2 : libpng - buffer overflow

Debian DSA-1400-1 : perl - heap overflow

Debian DSA-1401-1 : iceape - several vulnerabilities

Debian DSA-1402-1 : gforge - insecure temporary files

Debian DSA-1403-1 : phpmyadmin - missing input sanitising

Debian DSA-1404-1 : gallery2 - programming error

Debian DSA-1405-3 : zope-cmfplone - missing input sanitising

Debian DSA-1406-1 : horde3 - several vulnerabilities

Debian DSA-1407-1 : cupsys - buffer overflow

Debian DSA-1408-1 : kdegraphics - buffer overflow

Debian DSA-1409-3 : samba - several vulnerabilities

Debian DSA-141-1 : mpack - buffer overflow

Debian DSA-1410-1 : ruby1.8 - programming error

Debian DSA-1411-1 : libopenssl-ruby - programming error

Debian DSA-1412-1 : ruby1.9 - programming error

Debian DSA-1413-1 : mysql - multiple vulnerabilities

Debian DSA-1414-1 : wireshark - several vulnerabilities

Debian DSA-1415-1 : tk8.4 - buffer overflow

Debian DSA-1416-1 : tk8.3 - buffer overflow

Debian DSA-1417-1 : asterisk - missing input sanitising

Debian DSA-1418-1 : cacti - missing input sanitising

Debian DSA-1419-1 : openoffice.org - programming error

Debian DSA-142-1 : openafs - integer overflow

Debian DSA-1420-1 : zabbix - programming error

Debian DSA-1421-1 : wesnoth - directory traversal

Debian DSA-1422-1 : e2fsprogs - integer overflows

Debian DSA-1423-1 : sitebar - several vulnerabilities

Debian DSA-1424-1 : iceweasel - several vulnerabilities

Debian DSA-1425-1 : xulrunner - several vulnerabilities

Debian DSA-1426-1 : qt-x11-free - several vulnerabilities

Debian DSA-1427-1 : samba - buffer overflow

Debian DSA-1428-2 : linux-2.6 - several vulnerabilities

Debian DSA-1429-1 : htdig - XSS

Debian DSA-143-1 : krb5 - integer overflow

Debian DSA-1430-1 : libnss-ldap - denial of service

Debian DSA-1431-1 : ruby-gnome2 - format string

Debian DSA-1432-1 : link-grammar - buffer overflow

Debian DSA-1433-1 : centericq - buffer overflow

Debian DSA-1434-1 : mydns - buffer overflow

Debian DSA-1435-1 : clamav - several vulnerabilities

Debian DSA-1436-1 : linux-2.6 - several vulnerabilities

Debian DSA-1437-1 : cupsys - several vulnerabilities

Debian DSA-1438-1 : tar - several vulnerabilities

Debian DSA-1439-1 : typo3-src - missing input sanitising

Debian DSA-144-1 : wwwoffle - improper input handling

Debian DSA-1440-1 : inotify-tools - buffer overflow

Debian DSA-1441-1 : peercast - buffer overflow

Debian DSA-1442-1 : libsndfile - buffer overflow

Debian DSA-1443-1 : tcpreen - buffer overflows

Debian DSA-1444-2 : php5 - several vulnerabilities

Debian DSA-1445-1 : maradns - programming error

Debian DSA-1446-1 : wireshark - several vulnerabilities

Debian DSA-1447-1 : tomcat5.5 - several vulnerabilities

Debian DSA-1448-1 : eggdrop - buffer overflow

Debian DSA-1449-1 : loop-aes-utils - programming error

Debian DSA-145-1 : tinyproxy - doubly freed memory

Debian DSA-1450-1 : util-linux - programming error

Debian DSA-1451-1 : mysql-dfsg-5.0 - several vulnerabilities

Debian DSA-1452-1 : wzdftpd - denial of service

Debian DSA-1453-1 : tomcat5 - several vulnerabilities

Debian DSA-1454-1 : freetype - integer overflow

Debian DSA-1455-1 : libarchive - denial of service

Debian DSA-1456-1 : fail2ban - programming error

Debian DSA-1457-1 : dovecot - programming error

Debian DSA-1458-1 : openafs - programming error

Debian DSA-1459-1 : gforge - insufficient input validation

Debian DSA-146-2 : dietlibc - integer overflow

Debian DSA-1460-1 : postgresql-8.1 - several vulnerabilities

Debian DSA-1461-1 : libxml2 - missing input validation

Debian DSA-1462-1 : hplip - missing input sanitising

Debian DSA-1463-1 : postgresql-7.4 - several vulnerabilities

Debian DSA-1464-1 : syslog-ng - NULL pointer dereference

Debian DSA-1465-2 : apt-listchanges - programming error

Debian DSA-1466-1 : xorg-server - several vulnerabilities

Debian DSA-1467-1 : mantis - several vulnerabilities

Debian DSA-1468-1 : tomcat5.5 - several vulnerabilities

Debian DSA-1469-1 : flac - several vulnerabilities

Debian DSA-147-1 : mailman - XSS

Debian DSA-1470-1 : horde3 - missing input sanitising

Debian DSA-1471-1 : libvorbis - several vulnerabilities

Debian DSA-1472-1 : xine-lib - buffer overflow

Debian DSA-1473-1 : scponly - design flaw

Debian DSA-1474-1 : exiv2 - integer overflow

Debian DSA-1475-1 : gforge - missing input sanitising

Debian DSA-1476-1 : pulseaudio - programming error

Debian DSA-1477-1 : yarssr - missing input sanitising

Debian DSA-1478-1 : mysql-dfsg-5.0 - buffer overflows

Debian DSA-1479-1 : linux-2.6 - several vulnerabilities

Debian DSA-148-1 : hylafax - buffer overflows and format string vulnerabilities

Debian DSA-1480-1 : poppler - several vulnerabilities

Debian DSA-1481-1 : python-cherrypy - missing input sanitising

Debian DSA-1482-1 : squid - programming error

Debian DSA-1483-1 : net-snmp - design error

Debian DSA-1484-1 : xulrunner - several vulnerabilities

Debian DSA-1485-2 : icedove - several vulnerabilities

Debian DSA-1486-1 : gnatsweb - XSS

Debian DSA-1487-1 : libexif - several vulnerabilities

Debian DSA-1488-1 : phpbb2 - several vulnerabilities

Debian DSA-1489-1 : iceweasel - several vulnerabilities

Debian DSA-149-1 : glibc - integer overflow

Debian DSA-1490-1 : tk8.3 - buffer overflow

Debian DSA-1491-1 : tk8.4 - buffer overflow

Debian DSA-1492-1 : wml - insecure temporary files

Debian DSA-1493-2 : sdl-image1.2 - buffer overflows

Debian DSA-1494-2 : linux-2.6 - missing access checks

Debian DSA-1495-1 : nagios-plugins - buffer overflows

Debian DSA-1496-1 : mplayer - buffer overflows

Debian DSA-1497-1 : clamav - several vulnerabilities

Debian DSA-1498-1 : libimager-perl - buffer overflow

Debian DSA-1499-1 : pcre3 - buffer overflow

Debian DSA-150-1 : interchange - illegal file exposition

Debian DSA-1500-1 : splitvt - privilege escalation

Debian DSA-1501-1 : dspam - programming error

Debian DSA-1502-1 : wordpress - several vulnerabilities

Debian DSA-1503-1 : kernel-source-2.4.27 - several vulnerabilities

Debian DSA-1504-1 : kernel-source-2.6.8 - several vulnerabilities

Debian DSA-1505-1 : alsa-driver - kernel memory leak

Debian DSA-1506-1 : iceape - several vulnerabilities

Debian DSA-1507-1 : turba2 - programming error

Debian DSA-1508-1 : diatheke - insufficient input sanitising

Debian DSA-1509-1 : koffice - multiple vulnerabilities

Debian DSA-151-1 : xinetd - pipe exposure

Debian DSA-1510-1 : ghostscript - buffer overflow

Debian DSA-1511-1 : libicu - various

Debian DSA-1512-1 : evolution - format string attack

Debian DSA-1513-1 : lighttpd - information disclosure

Debian DSA-1514-1 : moin - several vulnerabilities

Debian DSA-1515-1 : libnet-dns-perl - several vulnerabilities

Debian DSA-1516-1 : dovecot - privilege escalation

Debian DSA-1517-1 : ldapscripts - programming error

Debian DSA-1518-1 : backup-manager - programming error

Debian DSA-1519-1 : horde3 - insufficient input sanitising

Debian DSA-152-1 : l2tpd - missing random seed

Debian DSA-1520-1 : smarty - insufficient input sanitising

Debian DSA-1521-1 : lighttpd - file disclosure

Debian DSA-1522-1 : unzip - programming error

Debian DSA-1523-1 : ikiwiki - XSS

Debian DSA-1524-1 : krb5 - several vulnerabilities

Debian DSA-1525-1 : asterisk - several vulnerabilities

Debian DSA-1526-1 : xwine - several vulnerabilities

Debian DSA-1527-1 : debian-goodies - insufficient input sanitising

Debian DSA-1528-1 : serendipity - insufficient input sanitising

Debian DSA-1529-1 : firebird -- multiple vulnerabilities

Debian DSA-153-1 : mantis - cross site code execution and privilege escalation

Debian DSA-1530-1 : cupsys - Several vulnerabilities

Debian DSA-1531-2 : policyd-weight - insecure temporary files

Debian DSA-1532-1 : xulrunner - several vulnerabilities

Debian DSA-1533-2 : exiftags - insufficient input sanitizing

Debian DSA-1534-1 : iceape - several vulnerabilities

Debian DSA-1535-1 : iceweasel - several vulnerabilities

Debian DSA-1536-1 : libxine - several vulnerabilities

Debian DSA-1537-1 : xpdf - several vulnerabilities

Debian DSA-1538-1 : alsaplayer - buffer overrun

Debian DSA-1539-1 : mapserver - several vulnerabilities

Debian DSA-154-1 : fam - privilege escalation

Debian DSA-1540-1 : lighttpd - denial of service

Debian DSA-1541-1 : openldap2.3 - several vulnerabilities

Debian DSA-1542-1 : libcairo - integer overflow

Debian DSA-1543-1 : vlc - several vulnerabilities

Debian DSA-1544-2 : pdns-recursor - design flaw

Debian DSA-1545-1 : rsync - integer overflow

Debian DSA-1546-1 : gnumeric - integer overflow

Debian DSA-1547-1 : openoffice.org - several vulnerabilities

Debian DSA-1548-1 : xpdf - several vulnerabilities

Debian DSA-1549-1 : clamav - buffer overflows

Debian DSA-155-1 : kdelibs - privacy escalation with Konqueror

Debian DSA-1550-1 : suphp - programming error

Debian DSA-1551-1 : python2.4 - several vulnerabilities

Debian DSA-1552-1 : mplayer - missing input sanitising

Debian DSA-1553-1 : ikiwiki - cross-site request forgery

Debian DSA-1554-2 : roundup - insufficient input sanitising

Debian DSA-1555-1 : iceweasel - programming error

Debian DSA-1556-2 : perl - heap buffer overflow

Debian DSA-1557-1 : phpmyadmin - insufficient input sanitising

Debian DSA-1558-1 : xulrunner - programming error

Debian DSA-1559-1 : phpgedview - insufficient input sanitising

Debian DSA-156-1 : epic4-script-light - arbitrary script execution

Debian DSA-1560-1 : kronolith2 - insufficient input sanitising

Debian DSA-1561-1 : ldm - programming error

Debian DSA-1562-1 : iceape - programming error

Debian DSA-1563-1 : asterisk - programming error

Debian DSA-1564-1 : wordpress - multiple vulnerabilities

Debian DSA-1565-1 : linux-2.6 - several vulnerabilities

Debian DSA-1566-1 : cpio - programming error

Debian DSA-1567-1 : blender - buffer overrun

Debian DSA-1568-1 : b2evolution - insufficient input sanitising

Debian DSA-1569-2 : cacti - insufficient input sanitising

Debian DSA-157-1 : irssi-text - denial of service

Debian DSA-1570-1 : kazehakase - various

Debian DSA-1571-1 : openssl - predictable random number generator

Debian DSA-1572-1 : php5 - several vulnerabilities

Debian DSA-1573-1 : rdesktop - several vulnerabilities

Debian DSA-1574-1 : icedove - several vulnerabilities

Debian DSA-1575-1 : linux-2.6 - denial of service

Debian DSA-1576-1 : openssh - predictable random number generator

Debian DSA-1577-1 : gforge - insecure temporary files

Debian DSA-1578-1 : php4 - several vulnerabilities

Debian DSA-1579-1 : netpbm-free - insufficient input sanitizing

Debian DSA-158-1 : gaim - arbitrary program execution

Debian DSA-1580-1 : phpgedview - programming error

Debian DSA-1581-1 : gnutls13 - several vulnerabilities

Debian DSA-1582-1 : peercast - buffer overflow

Debian DSA-1583-1 : gnome-peercast - buffer overflow

Debian DSA-1584-1 : libfishsound - buffer overflow

Debian DSA-1585-1 : speex - integer overflow

Debian DSA-1586-1 : xine-lib - multiple vulnerabilities

Debian DSA-1587-1 : mtr - buffer overflow

Debian DSA-1588-1 : linux-2.6 - denial of service

Debian DSA-1589-1 : libxslt - buffer overflow

Debian DSA-159-1 : python - insecure temporary files

Debian DSA-1590-1 : samba - buffer overflow

Debian DSA-1591-1 : libvorbis - several vulnerabilities

Debian DSA-1592-1 : linux-2.6 - heap overflow

Debian DSA-1593-1 : tomcat5.5 - missing input sanitising

Debian DSA-1594-1 : imlib2 - buffer overflows

Debian DSA-1595-1 : xorg-server - several vulnerabilities

Debian DSA-1596-1 : typo3 - several vulnerabilities

Debian DSA-1597-2 : mt-daapd - multiple vulnerabilities

Debian DSA-1598-1 : libtk-img - buffer overflow

Debian DSA-1599-1 : dbus - programming error

Debian DSA-160-1 : scrollkeeper - insecure temporary file creation

Debian DSA-1600-1 : sympa - dos

Debian DSA-1601-1 : wordpress - several vulnerabilities

Debian DSA-1602-1 : pcre3 - buffer overflow

Debian DSA-1603-1 : bind9 - DNS cache poisoning

Debian DSA-1606-1 : poppler - programming error

Debian DSA-1607-1 : iceweasel - several vulnerabilities

Debian DSA-1608-1 : mysql-dfsg-5.0 - authorization bypass

Debian DSA-1609-1 : lighttpd - various

Debian DSA-161-1 : mantis - privilege escalation

Debian DSA-1610-1 : gaim - integer overflow

Debian DSA-1611-1 : afuse - privilege escalation

Debian DSA-1612-1 : ruby1.8 - several vulnerabilities

Debian DSA-1613-1 : libgd2 - multiple vulnerabilities

Debian DSA-1614-1 : iceweasel - several vulnerabilities

Debian DSA-1615-1 : xulrunner - several vulnerabilities

Debian DSA-1616-2 : clamav - denial of service

Debian DSA-1617-1 : refpolicy - incompatible policy

Debian DSA-1618-1 : ruby1.9 - several vulnerabilities

Debian DSA-1619-1 : python-dns - DNS response spoofing

Debian DSA-162-1 : ethereal - buffer overflow

Debian DSA-1620-1 : python2.5 - several vulnerabilities

Debian DSA-1621-1 : icedove - several vulnerabilities

Debian DSA-1622-1 : newsx - buffer overflow

Debian DSA-1623-1 : dnsmasq - DNS cache poisoning

Debian DSA-1624-1 : libxslt - buffer overflows

Debian DSA-1625-1 : cupsys - buffer overflows

Debian DSA-1626-1 : httrack - buffer overflow

Debian DSA-1627-2 : opensc - programming error

Debian DSA-1628-1 : pdns - DNS response spoofing

Debian DSA-1629-2 : postfix - programming error

Debian DSA-163-1 : mhonarc - XSS

Debian DSA-1630-1 : linux-2.6 - denial of service/information leak

Debian DSA-1631-2 : libxml2 - denial of service

Debian DSA-1632-1 : tiff - buffer underflow

Debian DSA-1633-1 : slash - SQL Injection, XSS

Debian DSA-1634-1 : wordnet - stack and heap overflows

Debian DSA-1635-1 : freetype - multiple vulnerabilities

Debian DSA-1636-1 : linux-2.6.24 - denial of service/information leak

Debian DSA-1637-1 : git-core - buffer overflow

Debian DSA-1638-1 : openssh - denial of service

Debian DSA-1639-1 : twiki - command execution

Debian DSA-164-1 : cacti - arbitrary code execution

Debian DSA-1640-1 : python-django - several vulnerabilities

Debian DSA-1641-1 : phpmyadmin - several vulnerabilities

Debian DSA-1642-1 : horde3 - XSS

Debian DSA-1643-1 : feta - insecure temp file handling

Debian DSA-1644-1 : mplayer - integer overflow

Debian DSA-1645-1 : lighttpd - various

Debian DSA-1646-1 : squid - array bounds check

Debian DSA-1647-1 : php5 - several vulnerabilities

Debian DSA-1648-1 : mon - insecure temporary files

Debian DSA-1649-1 : iceweasel - several vulnerabilities

Debian DSA-165-1 : postgresql - buffer overflows

Debian DSA-1650-1 : openldap2.3 - denial of service

Debian DSA-1651-1 : ruby1.8 - several vulnerabilities

Debian DSA-1652-1 : ruby1.9 - several vulnerabilities

Debian DSA-1653-1 : linux-2.6 - denial of service/privilege escalation

Debian DSA-1654-1 : libxml2 - buffer overflow

Debian DSA-1655-1 : linux-2.6.24 - denial of service/information leak/privilege escalation

Debian DSA-1656-1 : cupsys - several vulnerabilities

Debian DSA-1657-1 : qemu - insecure temporary files

Debian DSA-1658-1 : dbus - programming error

Debian DSA-1659-1 : libspf2 - buffer overflow

Debian DSA-166-1 : purity - buffer overflows

Debian DSA-1660-1 : clamav - NULL pointer dereference, resource exhaustion

Debian DSA-1661-1 : openoffice.org - several vulnerabilities

Debian DSA-1662-1 : mysql-dfsg-5.0 - authorization bypass

Debian DSA-1663-1 : net-snmp - several vulnerabilities

Debian DSA-1664-1 : ekg - missing input sanitising

Debian DSA-1665-1 : libcdaudio - heap overflow

Debian DSA-1666-1 : libxml2 - several vulnerabilities

Debian DSA-1667-1 : python2.4 - several vulnerabilities

Debian DSA-1668-1 : hf - programming error

Debian DSA-1669-1 : xulrunner - several vulnerabilities

Debian DSA-167-1 : kdelibs - XSS

Debian DSA-1670-1 : enscript - buffer overflows

Debian DSA-1671-1 : iceweasel - several vulnerabilities

Debian DSA-1672-1 : imlib2 - buffer overflow

Debian DSA-1673-1 : wireshark - several vulnerabilities

Debian DSA-1674-1 : jailer - insecure temp file generation

Debian DSA-1675-1 : phpmyadmin - insufficient input sanitising

Debian DSA-1676-1 : flamethrower - insecure temp file generation

Debian DSA-1677-1 : cupsys - integer overflow

Debian DSA-1678-1 : perl - design flaws

Debian DSA-1679-1 : awstats - XSS

Debian DSA-168-1 : php - bypassing safe\_mode, CRLF injection

Debian DSA-1680-1 : clamav - buffer overflow, stack consumption

Debian DSA-1681-1 : linux-2.6.24 - denial of service/privilege escalation

Debian DSA-1682-1 : squirrelmail - insufficient input sanitising

Debian DSA-1683-1 : streamripper - buffer overflow

Debian DSA-1684-1 : lcms - multiple vulnerabilities

Debian DSA-1685-1 : uw-imap - buffer overflows, NULL pointer dereference

Debian DSA-1686-1 : no-ip - buffer overflow

Debian DSA-1687-1 : linux-2.6 - denial of service/privilege escalation

Debian DSA-1688-1 : courier-authlib - SQL injection

Debian DSA-1689-1 : proftpd-dfsg - missing input validation

Debian DSA-169-1 : htcheck - XSS

Debian DSA-1690-1 : avahi - assert errors

Debian DSA-1691-1 : moodle - several vulnerabilities

Debian DSA-1692-1 : php-xajax - insufficient input sanitising

Debian DSA-1693-2 : phppgadmin - several vulnerabilities

Debian DSA-1694-1 : xterm - design flaw

Debian DSA-1695-1 : ruby1.8, ruby1.9 - memory leak

Debian DSA-1696-1 : icedove - several vulnerabilities

Debian DSA-1697-1 : iceape - several vulnerabilities

Debian DSA-1698-1 : gforge - insufficient input sanitising

Debian DSA-1699-1 : zaptel - array index error

Debian DSA-170-1 : tomcat4 - source code disclosure

Debian DSA-1700-1 : lasso - incorrect API usage

Debian DSA-1701-1 : openssl, openssl097 - interpretation conflict

Debian DSA-1702-1 : ntp - interpretation conflict

Debian DSA-1703-1 : bind9 - interpretation conflict

Debian DSA-1704-1 : xulrunner - several vulnerabilities

Debian DSA-1705-1 : netatalk - missing input sanitising

Debian DSA-1706-1 : amarok - integer overflows

Debian DSA-1707-1 : iceweasel - several vulnerabilities

Debian DSA-1708-1 : git-core - shell command injection

Debian DSA-1709-1 : shadow - race condition

Debian DSA-171-1 : fetchmail - buffer overflows

Debian DSA-1710-1 : ganglia-monitor-core - buffer overflow

Debian DSA-1711-1 : typo3-src - several vulnerabilities

Debian DSA-1712-1 : rt2400 - integer overflow

Debian DSA-1713-1 : rt2500 - integer overflow

Debian DSA-1714-1 : rt2570 - integer overflow

Debian DSA-1715-1 : moin - insufficient input sanitising

Debian DSA-1716-1 : vnc4 - integer overflow

Debian DSA-1717-1 : devil - buffer overflow

Debian DSA-1718-1 : boinc - incorrect API usage

Debian DSA-1719-1 : gnutls13 - design flaw

Debian DSA-172-1 : tkmail - insecure temporary files

Debian DSA-1720-1 : typo3-src - several vulnerabilities

Debian DSA-1721-1 : libpam-krb5 - several vulnerabilities

Debian DSA-1722-1 : libpam-heimdal - programming error

Debian DSA-1723-1 : phpmyadmin - insufficient input sanitising

Debian DSA-1724-1 : moodle - several vulnerabilities

Debian DSA-1725-1 : websvn - programming error

Debian DSA-1726-1 : python-crypto - buffer overflow

Debian DSA-1727-1 : proftpd-dfsg - SQL injection vulnerabilites

Debian DSA-1728-1 : dkim-milter - improper assertion

Debian DSA-1729-1 : gst-plugins-bad0.10 - several vulnerabilities

Debian DSA-173-1 : bugzilla - privilege escalation

Debian DSA-1730-1 : proftpd-dfsg - SQL injection vulnerabilites

Debian DSA-1731-1 : ndiswrapper - buffer overflow

Debian DSA-1732-1 : squid3 - denial of service

Debian DSA-1733-1 : vim - several vulnerabilities

Debian DSA-1734-1 : opensc - programming error

Debian DSA-1735-1 : znc - missing input sanitization

Debian DSA-1736-1 : mahara - insufficient input sanitising

Debian DSA-1737-1 : wesnoth - several vulnerabilities

Debian DSA-1738-1 : curl - arbitrary file access

Debian DSA-1739-1 : mldonkey - path traversal

Debian DSA-174-1 : heartbeat - buffer overflow

Debian DSA-1740-1 : yaws - denial of service

Debian DSA-1741-1 : psi - integer overflow

Debian DSA-1742-1 : libsndfile - integer overflow

Debian DSA-1743-1 : libtk-img - buffer overflows

Debian DSA-1744-1 : weechat - missing input sanitization

Debian DSA-1745-1 : lcms - several vulnerabilities

Debian DSA-1746-1 : ghostscript - several vulnerabilities

Debian DSA-1747-1 : glib2.0 - integer overflow

Debian DSA-1748-1 : libsoup - integer overflow

Debian DSA-1749-1 : linux-2.6 - denial of service/privilege escalation/sensitive memory leak

Debian DSA-175-1 : syslog-ng - buffer overflow

Debian DSA-1750-1 : libpng - several vulnerabilities

Debian DSA-1751-1 : xulrunner - several vulnerabilities

Debian DSA-1752-1 : webcit - format string vulnerability

Debian DSA-1753-1 : iceweasel -- end-of-life announcement for Iceweasel in oldstable

Debian DSA-1754-1 : roundup - insufficient access checks

Debian DSA-1755-1 : systemtap - race condition

Debian DSA-1756-1 : xulrunner - multiple vulnerabilities

Debian DSA-1757-1 : auth2db - SQL injection

Debian DSA-1758-1 : nss-ldapd - insecure config file creation

Debian DSA-1759-1 : strongswan - denial of service

Debian DSA-176-1 : gv - buffer overflow

Debian DSA-1760-1 : openswan - denial of service

Debian DSA-1761-1 : moodle - missing input sanitization

Debian DSA-1762-1 : icu - insufficient input sanitising

Debian DSA-1763-1 : openssl - programming error

Debian DSA-1764-1 : tunapie - several vulnerabilities

Debian DSA-1765-1 : horde3 - Multiple vulnerabilities

Debian DSA-1766-1 : krb5 - several vulnerabilities

Debian DSA-1767-1 : multipath-tools - insecure file permissions

Debian DSA-1768-1 : openafs - several vulnerabilities

Debian DSA-1769-1 : openjdk-6 - several vulnerabilities

Debian DSA-177-1 : pam -- serious security violation

Debian DSA-1770-1 : imp4 - Insufficient input sanitising

Debian DSA-1771-1 : clamav - several vulnerabilities

Debian DSA-1772-1 : udev - several vulnerabilities

Debian DSA-1773-1 : cups - integer overflow

Debian DSA-1774-1 : ejabberd - insufficient input sanitising

Debian DSA-1775-1 : php-json-ext - denial of service

Debian DSA-1776-1 : slurm-llnl - programming error

Debian DSA-1777-1 : git-core - file permission error

Debian DSA-1778-1 : mahara - insufficient input sanitization

Debian DSA-1779-1 : apt - several vulnerabilities

Debian DSA-178-1 : heimdal - remote command execution

Debian DSA-1780-1 : libdbd-pg-perl - several vulnerabilities

Debian DSA-1781-1 : ffmpeg-debian - several vulnerabilities

Debian DSA-1782-1 : mplayer - several vulnerabilities

Debian DSA-1783-1 : mysql-dfsg-5.0 - multiple vulnerabilities

Debian DSA-1784-1 : freetype - integer overflows

Debian DSA-1785-1 : wireshark - several vulnerabilities

Debian DSA-1786-1 : acpid - denial of service

Debian DSA-1787-1 : linux-2.6.24 - denial of service/privilege escalation/information leak

Debian DSA-1788-1 : quagga - improper assertion

Debian DSA-1789-1 : php5 - several vulnerabilities

Debian DSA-179-1 : gnome-gv - buffer overflow

Debian DSA-1790-1 : xpdf - multiple vulnerabilities

Debian DSA-1791-1 : moin - insufficient input sanitising

Debian DSA-1792-1 : drupal6 - multiple vulnerabilities

Debian DSA-1793-1 : kdegraphics - multiple vulnerabilities

Debian DSA-1794-1 : linux-2.6 - denial of service/privilege escalation/information leak

Debian DSA-1795-1 : ldns - buffer overflow

Debian DSA-1796-1 : libwmf - pointer use-after-free

Debian DSA-1797-1 : xulrunner - several vulnerabilities

Debian DSA-1798-1 : pango1.0 - integer overflow

Debian DSA-1799-1 : qemu - several vulnerabilities

Debian DSA-180-1 : nis - information leak

Debian DSA-1800-1 : linux-2.6 - denial of service/privilege escalation/sensitive memory leak

Debian DSA-1801-1 : ntp - buffer overflows

Debian DSA-1802-2 : squirrelmail - several vulnerabilities

Debian DSA-1803-1 : nsd, nsd3 - buffer overflow

Debian DSA-1804-1 : ipsec-tools - NULL pointer dereference, memory leaks

Debian DSA-1805-1 : pidgin - several vulnerabilities

Debian DSA-1806-1 : cscope - buffer overflows

Debian DSA-1807-1 : cyrus-sasl2, cyrus-sasl2-heimdal - buffer overflow

Debian DSA-1808-1 : drupal6 - insufficient input sanitising

Debian DSA-1809-1 : linux-2.6 - denial of service, privilege escalation

Debian DSA-181-1 : libapache-mod-ssl - XSS

Debian DSA-1810-1 : libapache-mod-jk - information disclosure

Debian DSA-1811-1 : cups, cupsys - null ptr dereference

Debian DSA-1812-1 : apr-util - denial of service

Debian DSA-1813-1 : evolution-data-server - Several vulnerabilities

Debian DSA-1814-1 : libsndfile - heap-based buffer overflow

Debian DSA-1815-1 : libtorrent-rasterbar - programming error

Debian DSA-1816-1 : apache2 - insufficient security check

Debian DSA-1817-1 : ctorrent - stack-based buffer overflow

Debian DSA-1818-1 : gforge - insufficient input sanitising

Debian DSA-1819-1 : vlc - several vulnerabilities

Debian DSA-182-1 : kdegraphics - buffer overflow

Debian DSA-1820-1 : xulrunner - several vulnerabilities

Debian DSA-1821-1 : amule - insufficient input sanitising

Debian DSA-1822-1 : mahara - insufficient input sanitization

Debian DSA-1823-1 : samba - several vulnerabilities

Debian DSA-1824-1 : phpmyadmin - several vulnerabilities

Debian DSA-1825-1 : nagios2, nagios3 - insufficient input validation

Debian DSA-1826-1 : eggdrop - several vulnerabilities

Debian DSA-1827-1 : ipplan - insufficient input sanitising

Debian DSA-1828-1 : ocsinventory-agent - insecure module search path

Debian DSA-1829-1 : sork-passwd-h3 - insufficient input sanitising

Debian DSA-183-1 : krb5 - buffer overflow

Debian DSA-1830-1 : icedove - several vulnerabilities

Debian DSA-1831-1 : djbdns - programming error

Debian DSA-1832-1 : camlimages - integer overflow

Debian DSA-1833-1 : dhcp3 - several vulnerabilities

Debian DSA-1834-1 : apache2 - denial of service

Debian DSA-1835-1 : tiff - several vulnerabilities

Debian DSA-1836-1 : fckeditor - missing input sanitising

Debian DSA-1837-1 : dbus - programming error

Debian DSA-1838-1 : pulseaudio - privilege escalation

Debian DSA-1839-1 : gst-plugins-good0.10 - integer overflow

Debian DSA-184-1 : krb4 - buffer overflow

Debian DSA-1840-1 : xulrunner - several vulnerabilities

Debian DSA-1841-1 : git-core - denial of service

Debian DSA-1842-1 : openexr - several vulnerabilities

Debian DSA-1843-1 : squid3 - several vulnerabilities

Debian DSA-1844-1 : linux-2.6.24 - denial of service/privilege escalation

Debian DSA-1845-1 : linux-2.6 - denial of service, privilege escalation

Debian DSA-1846-1 : kvm - denial of service

Debian DSA-1847-1 : bind9 - improper assert

Debian DSA-1848-1 : znc - directory traversal

Debian DSA-1849-1 : xml-security-c - design flaw

Debian DSA-185-1 : heimdal - buffer overflow

Debian DSA-1850-1 : libmodplug - several vulnerabilities

Debian DSA-1851-1 : gst-plugins-bad0.10 - integer overflow

Debian DSA-1852-1 : fetchmail - insufficient input validation

Debian DSA-1853-1 : memcached - heap-based buffer overflow

Debian DSA-1854-1 : apr, apr-util - heap buffer overflow

Debian DSA-1855-1 : subversion - heap overflow

Debian DSA-1856-1 : mantis - information leak

Debian DSA-1857-1 : camlimages - integer overflow

Debian DSA-1858-1 : imagemagick - multiple vulnerabilities

Debian DSA-1859-1 : libxml2 - several vulnerabilities

Debian DSA-186-1 : log2mail - buffer overflow

Debian DSA-1860-1 : ruby1.8, ruby1.9 - several vulnerabilities

Debian DSA-1861-1 : libxml - several vulnerabilities

Debian DSA-1862-1 : linux-2.6 - privilege escalation

Debian DSA-1863-1 : zope2.10/zope2.9 - several vulnerabilities

Debian DSA-1864-1 : linux-2.6.24 - privilege escalation

Debian DSA-1865-1 : linux-2.6 - denial of service/privilege escalation

Debian DSA-1866-1 : kdegraphics - several vulnerabilities

Debian DSA-1867-1 : kdelibs - several vulnerabilities

Debian DSA-1868-1 : kde4libs - several vulnerabilities

Debian DSA-1869-1 : curl - insufficient input validation

Debian DSA-187-1 : apache - several vulnerabilities

Debian DSA-1870-1 : pidgin - insufficient input validation

Debian DSA-1871-1 : wordpress - several vulnerabilities

Debian DSA-1872-1 : linux-2.6 - denial of service/privilege escalation/information leak

Debian DSA-1873-1 : xulrunner - programming error

Debian DSA-1874-1 : nss - several vulnerabilities

Debian DSA-1875-1 : ikiwiki - missing input sanitising

Debian DSA-1876-1 : dnsmasq - buffer overflow

Debian DSA-1877-1 : mysql-dfsg-5.0 - denial of service/execution of arbitrary code

Debian DSA-1878-1 : devscripts - missing input sanitation

Debian DSA-1879-1 : silc-client/silc-toolkit - several vulnerabilities

Debian DSA-188-1 : apache-ssl - several vulnerabilities

Debian DSA-1880-1 : openoffice.org - several vulnerabilities

Debian DSA-1881-1 : cyrus-imapd-2.2 - buffer overflow

Debian DSA-1882-1 : xapian-omega - missing input sanitization

Debian DSA-1883-1 : nagios2 - missing input sanitising

Debian DSA-1884-1 : nginx - buffer underflow

Debian DSA-1885-1 : xulrunner - several vulnerabilities

Debian DSA-1886-1 : iceweasel - several vulnerabilities

Debian DSA-1887-1 : rails - missing input sanitising

Debian DSA-1888-1 : openssl, openssl097 - cryptographic weakness

Debian DSA-1889-1 : icu - programming error

Debian DSA-189-1 : luxman - local root exploit

Debian DSA-1890-1 : wxwindows2.4 wxwidgets2.6 wxwidgets2.8 - integer overflow

Debian DSA-1891-1 : changetrack - shell command execution

Debian DSA-1892-1 : dovecot - buffer overflow

Debian DSA-1893-1 : cyrus-imapd-2.2 kolab-cyrus-imapd - buffer overflow

Debian DSA-1894-1 : newt - buffer overflow

Debian DSA-1895-1 : xmltooling - several vulnerabilities

Debian DSA-1896-1 : opensaml, shibboleth-sp - several vulnerabilities

Debian DSA-1897-1 : horde3 - insufficient input sanitization

Debian DSA-1898-1 : openswan - denial of service

Debian DSA-1899-1 : strongswan - several vulnerabilities

Debian DSA-190-1 : wmaker - buffer overflow

Debian DSA-1900-1 : postgresql-7.4, postgresql-8.1, postgresql-8.3, postgresql-8.4 - several vulnerabilities

Debian DSA-1901-1 : mediawiki1.7 - several vulnerabilities

Debian DSA-1902-1 : elinks - buffer overflow

Debian DSA-1903-1 : graphicsmagick - several vulnerabilities

Debian DSA-1904-1 : wget - insufficient input validation

Debian DSA-1905-1 : python-django - insufficient input validation

Debian DSA-1907-1 : kvm - several vulnerabilities

Debian DSA-1908-1 : samba - several vulnerabilities

Debian DSA-1909-1 : postgresql-ocaml - missing escape function

Debian DSA-191-1 : squirrelmail - XSS

Debian DSA-1910-1 : mysql-ocaml - missing escape function

Debian DSA-1911-1 : pygresql - missing escape function

Debian DSA-1912-1 : camlimages - integer overflow

Debian DSA-1913-1 : bugzilla - SQL injection vulnerability

Debian DSA-1914-1 : mapserver - several vulnerabilities

Debian DSA-1915-1 : linux-2.6 - privilege escalation/denial of service/sensitive memory leak

Debian DSA-1916-1 : kdelibs - insufficient input validation

Debian DSA-1917-1 : mimetex - several vulnerabilities

Debian DSA-1918-1 : phpmyadmin - several vulnerabilities

Debian DSA-1919-1 : smarty - several vulnerabilities

Debian DSA-192-1 : html2ps - arbitrary code execution

Debian DSA-1920-1 : nginx - denial of service

Debian DSA-1921-1 : expat - denial of service

Debian DSA-1922-1 : xulrunner - several vulnerabilities

Debian DSA-1923-1 : libhtml-parser-perl - denial of service

Debian DSA-1924-1 : mahara - several vulnerabilities

Debian DSA-1925-1 : proftpd-dfsg - insufficient input validation

Debian DSA-1926-1 : typo3-src - several vulnerabilities

Debian DSA-1927-1 : linux-2.6 - privilege escalation/denial of service/sensitive memory leak

Debian DSA-1928-1 : linux-2.6.24 - privilege escalation/denial of service/sensitive memory leak

Debian DSA-1929-1 : linux-2.6 - privilege escalation/denial of service/sensitive memory leak

Debian DSA-193-1 : kdenetwork - buffer overflow

Debian DSA-1930-1 : drupal6 - several vulnerabilities

Debian DSA-1931-1 : nspr - several vulnerabilities

Debian DSA-1932-1 : pidgin - programming error

Debian DSA-1933-1 : cups - missing input sanitising

Debian DSA-1934-1 : apache2 - multiple issues

Debian DSA-1935-1 : gnutls13 gnutls26 - several vulnerabilities

Debian DSA-1936-1 : libgd2 - several vulnerabilities

Debian DSA-1937-1 : gforge - insufficient input sanitising

Debian DSA-1938-1 : php-mail - programming error

Debian DSA-1939-1 : libvorbis - several vulnerabilities

Debian DSA-194-1 : masqmail - buffer overflows

Debian DSA-1940-1 : php5 - multiple issues

Debian DSA-1941-1 : poppler - several vulnerabilities

Debian DSA-1942-1 : wireshark - several vulnerabilities

Debian DSA-1943-1 : openldap openldap2.3 - insufficient input validation

Debian DSA-1944-1 : request-tracker3.4 request-tracker3.6 - session hijack

Debian DSA-1945-1 : gforge - symlink attack

Debian DSA-1946-1 : belpic - cryptographic weakness

Debian DSA-1947-1 : shibboleth-sp, shibboleth-sp2, opensaml2 - missing input sanitising

Debian DSA-1948-1 : ntp - denial of service

Debian DSA-1949-1 : php-net-ping - programming error

Debian DSA-195-1 : apache-perl - several vulnerabilities

Debian DSA-1950-1 : webkit - several vulnerabilities

Debian DSA-1951-1 : firefox-sage - insufficient input sanitising

Debian DSA-1952-1 : asterisk - several vulnerabilities, end-of-life announcement in oldstable

Debian DSA-1953-1 : expat - denial of service

Debian DSA-1954-1 : cacti - insufficient input sanitising

Debian DSA-1955-1 : network-manager/network-manager-applet - information disclosure

Debian DSA-1956-1 : xulrunner - several vulnerabilities

Debian DSA-1957-1 : aria2 - buffer overflow

Debian DSA-1958-1 : libtool - privilege escalation

Debian DSA-1959-1 : ganeti - missing input sanitation

Debian DSA-196-1 : bind - several vulnerabilities

Debian DSA-1960-1 : acpid - programming error

Debian DSA-1961-1 : bind9 - DNS cache poisoning

Debian DSA-1962-1 : kvm - several vulnerabilities

Debian DSA-1963-1 : unbound - cryptographic implementation error

Debian DSA-1964-1 : postgresql-7.4, postgresql-8.1, postgresql-8.3 - several vulnerabilities

Debian DSA-1965-1 : phpldapadmin - missing input sanitising

Debian DSA-1966-1 : horde3 - insufficient input sanitising

Debian DSA-1967-1 : transmission - directory traversal

Debian DSA-1968-1 : pdns-recursor - several vulnerabilities

Debian DSA-1969-1 : krb5 - integer underflow

Debian DSA-197-1 : courier - buffer overflow

Debian DSA-1970-1 : openssl - denial of service

Debian DSA-1971-1 : libthai - integer overflow

Debian DSA-1972-1 : audiofile - buffer overflow

Debian DSA-1973-1 : glibc, eglibc - information disclosure

Debian DSA-1974-1 : gzip - several vulnerabilities

Debian DSA-1976-1 : dokuwiki - several vulnerabilities

Debian DSA-1977-1 : python2.4 python2.5 - several vulnerabilities

Debian DSA-1978-1 : phpgroupware - several vulnerabilities

Debian DSA-1979-1 : lintian - multiple vulnerabilities

Debian DSA-198-1 : nullmailer - denial of service

Debian DSA-1980-1 : ircd-hybrid/ircd-ratbox - integer underflow/denial of service

Debian DSA-1981-1 : maildrop - privilege escalation

Debian DSA-1982-1 : hybserv - denial of service

Debian DSA-1983-1 : wireshark - several vulnerabilities

Debian DSA-1984-1 : libxerces2-java - denial of service

Debian DSA-1985-1 : sendmail - insufficient input validation

Debian DSA-1986-1 : moodle - several vulnerabilities

Debian DSA-1987-1 : lighttpd - denial of service

Debian DSA-1988-1 : qt4-x11 - several vulnerabilities

Debian DSA-1989-1 : fuse - denial of service

Debian DSA-199-1 : mhonarc - XSS

Debian DSA-1990-1 : trac-git - shell command injection

Debian DSA-1991-1 : squid/squid3 - denial of service

Debian DSA-1992-1 : chrony - several vulnerabilities

Debian DSA-1993-1 : otrs2 - sql injection

Debian DSA-1994-1 : ajaxterm - weak session IDs

Debian DSA-1995-1 : openoffice.org - several vulnerabilities

Debian DSA-1996-1 : linux-2.6 - privilege escalation/denial of service/sensitive memory leak

Debian DSA-1997-1 : mysql-dfsg-5.0 - several vulnerabilities

Debian DSA-1998-1 : kdelibs - buffer overflow

Debian DSA-1999-1 : xulrunner - several vulnerabilities

Debian DSA-200-1 : samba - remote exploit

Debian DSA-2000-1 : ffmpeg-debian - several vulnerabilities

Debian DSA-2001-1 : php5 - multiple vulnerabilities

Debian DSA-2002-1 : polipo - denial of service

Debian DSA-2003-1 : linux-2.6 - privilege escalation/denial of service

Debian DSA-2004-1 : samba - several vulnerabilities

Debian DSA-2005-1 : linux-2.6.24 - privilege escalation/denial of service/sensitive memory leak

Debian DSA-2006-1 : sudo - several vulnerabilities

Debian DSA-2007-1 : cups - format string vulnerability

Debian DSA-2008-1 : typo3-src - several vulnerabilities

Debian DSA-2009-1 : tdiary - insufficient input sanitising

Debian DSA-201-1 : freeswan - denial of service

Debian DSA-2010-1 : kvm - privilege escalation/denial of service

Debian DSA-2011-1 : dpkg - path traversal

Debian DSA-2012-1 : linux-2.6 - privilege escalation/denial of service

Debian DSA-2013-1 : egroupware - several vulnerabilities

Debian DSA-2014-1 : moin - several vulnerabilities

Debian DSA-2015-1 : drbd8 - privilege escalation

Debian DSA-2016-1 : drupal6 - several vulnerabilities

Debian DSA-2017-1 : pulseaudio - insecure temporary directory

Debian DSA-2018-1 : php5 - DoS (crash)

Debian DSA-2019-1 : pango1.0 - missing input sanitization

Debian DSA-202-1 : im - insecure temporary files

Debian DSA-2020-1 : ikiwiki - insufficient input sanitization

Debian DSA-2021-1 : spamass-milter - missing input sanitization

Debian DSA-2022-1 : mediawiki - several vulnerabilities

Debian DSA-2023-1 : curl - buffer overflow

Debian DSA-2024-1 : moin - insufficient input sanitising

Debian DSA-2025-1 : icedove - several vulnerabilities

Debian DSA-2026-1 : netpbm-free - stack-based buffer overflow

Debian DSA-2027-1 : xulrunner - several vulnerabilities

Debian DSA-2028-1 : xpdf - multiple vulnerabilities

Debian DSA-2029-1 : imlib2 - several vulnerabilities

Debian DSA-203-1 : smb2www - arbitrary command execution

Debian DSA-2030-1 : mahara - sql injection

Debian DSA-2031-1 : krb5 - use-after-free

Debian DSA-2032-1 : libpng - several vulnerabilities

Debian DSA-2033-1 : ejabberd - heap overflow

Debian DSA-2034-1 : phpmyadmin - several vulnerabilities

Debian DSA-2035-1 : apache2 - multiple issues

Debian DSA-2036-1 : jasper - programming error

Debian DSA-2037-1 : kdm (kdebase) - race condition

Debian DSA-2038-1 : pidgin - several vulnerabilities

Debian DSA-2039-1 : cacti - missing input sanitising

Debian DSA-204-1 : kdelibs - arbitrary program execution

Debian DSA-2040-1 : squidguard - buffer overflow

Debian DSA-2041-1 : mediawiki - Cross-Site Request Forgery

Debian DSA-2042-1 : iscsitarget - format string

Debian DSA-2043-1 : vlc - integer overflow

Debian DSA-2044-1 : mplayer - integer overflow

Debian DSA-2045-1 : libtheora - integer overflow

Debian DSA-2046-1 : phpgroupware - several vulnerabilities

Debian DSA-2047-1 : aria2 - insufficient input sanitising

Debian DSA-2048-1 : dvipng - buffer overflow

Debian DSA-2049-1 : barnowl - buffer overflow

Debian DSA-205-1 : gtetrinet - buffer overflow

Debian DSA-2050-1 : kdegraphics - several vulnerabilities

Debian DSA-2051-1 : postgresql-8.3 - several vulnerabilities

Debian DSA-2052-1 : krb5 - NULL pointer dereference

Debian DSA-2053-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2054-1 : bind9 - DNS cache poisoning

Debian DSA-2055-1 : openoffice.org - macro execution

Debian DSA-2056-1 : zonecheck - missing input sanitizing

Debian DSA-2057-1 : mysql-dfsg-5.0 - several vulnerabilities

Debian DSA-2058-1 : glibc, eglibc - multiple vulnerabilities

Debian DSA-2059-1 : pcsc-lite - buffer overflow

Debian DSA-206-1 : tcpdump - denial of service

Debian DSA-2060-1 : cacti - insufficient input sanitization

Debian DSA-2061-1 : samba - memory corruption

Debian DSA-2062-1 : sudo - missing input sanitization

Debian DSA-2063-1 : pmount - insecure temporary file

Debian DSA-2064-1 : xulrunner - several vulnerabilities

Debian DSA-2065-1 : kvirc - several vulnerabilities

Debian DSA-2066-1 : wireshark - several vulnerabilities

Debian DSA-2067-1 : mahara - several vulnerabilities

Debian DSA-2068-1 : python-cjson - buffer overflow

Debian DSA-2069-1 : znc - denial of service

Debian DSA-207-1 : tetex-bin - arbitrary command execution

Debian DSA-2070-1 : freetype - several vulnerabilities

Debian DSA-2071-1 : libmikmod - buffer overflows

Debian DSA-2072-1 : libpng - several vulnerabilities

Debian DSA-2073-1 : mlmmj - insufficient input sanitising

Debian DSA-2074-1 : ncompress - integer underflow

Debian DSA-2075-1 : xulrunner - several vulnerabilities

Debian DSA-2076-1 : gnupg2 - use-after-free

Debian DSA-2077-1 : openldap - several vulnerabilities

Debian DSA-2078-1 : kvirc - programming error

Debian DSA-2079-1 : mapserver - several vulnerabilities

Debian DSA-208-1 : perl - broken safe compartment

Debian DSA-2080-1 : ghostscript - several vulnerabilities

Debian DSA-2081-1 : libmikmod - buffer overflow

Debian DSA-2082-1 : gmime2.2 - buffer overflow

Debian DSA-2083-1 : moin - missing input sanitization

Debian DSA-2084-1 : tiff - integer overflows

Debian DSA-2085-1 : lftp - missing input validation

Debian DSA-2086-1 : avahi - several vulnerabilities

Debian DSA-2087-1 : cabextract - programming error

Debian DSA-2088-1 : wget - missing input sanitization

Debian DSA-2089-1 : php5 - several vulnerabilities

Debian DSA-209-1 : wget - directory traversal

Debian DSA-2090-1 : socat - incorrect user-input validation

Debian DSA-2091-1 : squirrelmail - No user-specific token implemented

Debian DSA-2092-1 : lxr-cvs - missing input sanitizing

Debian DSA-2093-1 : ghostscript - several vulnerabilities

Debian DSA-2094-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2095-1 : lvm2 - insecure communication protocol

Debian DSA-2096-1 : zope-ldapuserfolder - missing input validation

Debian DSA-2097-1 : phpmyadmin - insufficient input sanitising

Debian DSA-2098-1 : typo3-src - several vulnerabilities

Debian DSA-2099-1 : openoffice.org - buffer overflows

Debian DSA-210-1 : lynx - CRLF injection

Debian DSA-2100-1 : openssl - double free

Debian DSA-2101-1 : wireshark - several vulnerabilities

Debian DSA-2102-1 : barnowl - unchecked return value

Debian DSA-2103-1 : smbind - sql injection

Debian DSA-2104-1 : quagga - several vulnerabilities

Debian DSA-2105-1 : freetype - several vulnerabilities

Debian DSA-2106-1 : xulrunner - several vulnerabilities

Debian DSA-2107-1 : couchdb - untrusted search path

Debian DSA-2108-1 : cvsnt - programming error

Debian DSA-2109-1 : samba - buffer overflow

Debian DSA-211-1 : micq - denial of service

Debian DSA-2110-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2111-1 : squid3 - denial of service

Debian DSA-2112-1 : bzip2 - integer overflow

Debian DSA-2113-1 : drupal6 - several vulnerabilities

Debian DSA-2114-1 : git-core - buffer overflow

Debian DSA-2115-1 : moodle - several vulnerabilities

Debian DSA-2116-1 : freetype - integer overflow

Debian DSA-2117-1 : apr-util - denial of service

Debian DSA-2118-1 : subversion - logic flaw

Debian DSA-2119-1 : poppler - several vulnerabilities

Debian DSA-212-1 : mysql - multiple problems

Debian DSA-2120-1 : postgresql-8.3 - privilege escalation

Debian DSA-2121-1 : typo3-src - several vulnerabilities

Debian DSA-2122-1 : glibc - missing input sanitization

Debian DSA-2123-1 : nss - several vulnerabilities

Debian DSA-2124-1 : xulrunner - several vulnerabilities

Debian DSA-2125-1 : openssl - buffer overflow

Debian DSA-2126-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2127-1 : wireshark - denial of service

Debian DSA-2128-1 : libxml2 - invalid memory access

Debian DSA-2129-1 : krb5 - checksum verification weakness

Debian DSA-213-1 : libpng - buffer overflow

Debian DSA-2130-1 : bind9 - several vulnerabilities

Debian DSA-2131-1 : exim4 - arbitrary code execution

Debian DSA-2132-1 : xulrunner - several vulnerabilities

Debian DSA-2133-1 : collectd - denial of service

Debian DSA-2135-1 : xpdf - several vulnerabilities

Debian DSA-2136-1 : tor - buffer overflow

Debian DSA-2137-1 : libxml2 - several vulnerabilities

Debian DSA-2138-1 : wordpress - SQL injection

Debian DSA-2139-1 : phpmyadmin - several vulnerabilities

Debian DSA-214-1 : kdenetwork - buffer overflows

Debian DSA-2140-1 : libapache2-mod-fcgid - stack overflow

Debian DSA-2141-1 : openssl - SSL/TLS insecure renegotiation protocol design flaw

Debian DSA-2142-1 : dpkg - directory traversal

Debian DSA-2143-1 : mysql-dfsg-5.0 - several vulnerabilities

Debian DSA-2144-1 : wireshark - buffer overflow

Debian DSA-2145-1 : libsmi - buffer overflow

Debian DSA-2146-1 : mydms - directory traversal

Debian DSA-2147-1 : pimd - insecure temporary files

Debian DSA-2148-1 : tor - several vulnerabilities

Debian DSA-2149-1 : dbus - denial of service

Debian DSA-215-1 : cyrus-imapd - buffer overflow

Debian DSA-2150-1 : request-tracker3.6 - unsalted password hashing

Debian DSA-2151-1 : openoffice.org - several vulnerabilities

Debian DSA-2152-1 : hplip - buffer overflow

Debian DSA-2153-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2154-1 : exim4 - privilege escalation

Debian DSA-2155-1 : freetype - several vulnerabilities

Debian DSA-2156-1 : pcscd - buffer overflow

Debian DSA-2157-1 : postgresql-8.3, postgresql-8.4, postgresql-9.0 - buffer overflow

Debian DSA-2158-1 : cgiirc - XSS

Debian DSA-2159-1 : vlc - missing input sanitising

Debian DSA-216-1 : fetchmail - buffer overflow

Debian DSA-2160-1 : tomcat6 - several vulnerabilities

Debian DSA-2161-1 : openjdk-6 - denial of service

Debian DSA-2162-1 : openssl - invalid memory access

Debian DSA-2163-1 : python-django - multiple vulnerabilities

Debian DSA-2164-1 : shadow - insufficient input sanitization

Debian DSA-2165-1 : ffmpeg-debian - buffer overflow

Debian DSA-2166-1 : chromium-browser - several vulnerabilities

Debian DSA-2167-1 : phpmyadmin - SQL injection

Debian DSA-2168-1 : openafs - several vulnerabilities

Debian DSA-2169-1 : telepathy-gabble - insufficient input validation

Debian DSA-217-1 : typespeed - buffer overflow

Debian DSA-2170-1 : mailman - several vulnerabilities

Debian DSA-2171-1 : asterisk - buffer overflow

Debian DSA-2172-1 : moodle - several vulnerabilities

Debian DSA-2173-1 : pam-pgsql - buffer overflow

Debian DSA-2174-1 : avahi - denial of service

Debian DSA-2175-1 : samba - missing input sanitising

Debian DSA-2176-1 : cups - several vulnerabilities

Debian DSA-2177-1 : pywebdav - SQL injection

Debian DSA-2178-1 : pango1.0 - NULL pointer dereference

Debian DSA-2179-1 : dtc - SQL injection

Debian DSA-218-1 : bugzilla - XSS

Debian DSA-2180-1 : iceape - several vulnerabilities

Debian DSA-2181-1 : subversion - denial of service

Debian DSA-2182-1 : logwatch - shell command injection

Debian DSA-2183-1 : nbd - buffer overflow

Debian DSA-2184-1 : isc-dhcp - denial of service

Debian DSA-2185-1 : proftpd-dfsg - integer overflow

Debian DSA-2186-1 : iceweasel - several vulnerabilities

Debian DSA-2187-1 : icedove - several vulnerabilities

Debian DSA-2188-1 : webkit - several vulnerabilities

Debian DSA-2189-1 : chromium-browser - several vulnerabilities

Debian DSA-219-1 : dhcpcd - remote command execution

Debian DSA-2190-1 : wordpress - several vulnerabilities

Debian DSA-2191-1 : proftpd-dfsg - several vulnerabilities

Debian DSA-2192-1 : chromium-browser - several vulnerabilities

Debian DSA-2193-1 : libcgroup - several vulnerabilities

Debian DSA-2194-1 : libvirt - insufficient checks

Debian DSA-2195-1 : php5 - several vulnerabilities

Debian DSA-2196-1 : maradns - buffer overflow

Debian DSA-2197-1 : quagga - denial of service

Debian DSA-2198-1 : tex-common - insufficient input sanitization

Debian DSA-2199-1 : iceape - ssl certificate blacklist update

Debian DSA-220-1 : squirrelmail - XSS

Debian DSA-2200-1 : iceweasel - ssl certificate blacklist update

Debian DSA-2201-1 : wireshark - several vulnerabilities

Debian DSA-2202-1 : apache2 - failure to drop root privileges

Debian DSA-2203-1 : nss - ssl certificate blacklist update

Debian DSA-2204-1 : imp4 - insufficient input sanitising

Debian DSA-2205-1 : gdm3 - privilege escalation

Debian DSA-2206-1 : mahara - several vulnerabilities

Debian DSA-2207-1 : tomcat5.5 - several vulnerabilities

Debian DSA-2208-1 : bind9 - denial of service

Debian DSA-2209-1 : tgt - double free

Debian DSA-221-1 : mhonarc - XSS

Debian DSA-2210-1 : tiff - several vulnerabilities

Debian DSA-2211-1 : vlc - missing input sanitising

Debian DSA-2212-1 : tmux - privilege escalation

Debian DSA-2213-1 : x11-xserver-utils - missing input sanitization

Debian DSA-2214-1 : ikiwiki - missing input validation

Debian DSA-2215-1 : gitolite - directory traversal

Debian DSA-2216-1 : isc-dhcp - missing input sanitization

Debian DSA-2217-1 : dhcp3 - missing input sanitization

Debian DSA-2218-1 : vlc - heap-based buffer overflow

Debian DSA-2219-1 : xmlsec1 - arbitrary file overwrite

Debian DSA-222-1 : xpdf - integer overflow

Debian DSA-2220-1 : request-tracker3.6, request-tracker3.8 - several vulnerabilities

Debian DSA-2221-1 : libmojolicious-perl - directory traversal

Debian DSA-2222-1 : tinyproxy - incorrect ACL processing

Debian DSA-2223-1 : doctrine - SQL injection

Debian DSA-2224-1 : openjdk-6 - several vulnerabilities

Debian DSA-2225-1 : asterisk - several vulnerabilities

Debian DSA-2226-1 : libmodplug - buffer overflow

Debian DSA-2227-1 : iceape - several vulnerabilities

Debian DSA-2228-1 : iceweasel - several vulnerabilities

Debian DSA-2229-1 : spip - programming error

Debian DSA-223-1 : geneweb - information exposure

Debian DSA-2230-1 : qemu-kvm - several vulnerabilities

Debian DSA-2231-1 : otrs2 - XSS

Debian DSA-2232-1 : exim4 - format string vulnerability

Debian DSA-2233-1 : postfix - several vulnerabilities

Debian DSA-2234-1 : zodb - several vulnerabilities

Debian DSA-2235-1 : icedove - several vulnerabilities

Debian DSA-2236-1 : exim4 - command injection

Debian DSA-2237-1 : apr - denial of service

Debian DSA-2238-1 : vino - several vulnerabilities

Debian DSA-2239-1 : libmojolicious-perl - several vulnerabilities

Debian DSA-224-1 : canna - buffer overflow and more

Debian DSA-2240-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2241-1 : qemu-kvm - implementation error

Debian DSA-2242-1 : cyrus-imapd-2.2 - implementation error

Debian DSA-2243-1 : unbound - design flaw

Debian DSA-2244-1 : bind9 - incorrect boundary condition

Debian DSA-2245-1 : chromium-browser - several vulnerabilities

Debian DSA-2246-1 : mahara - several vulnerabilities

Debian DSA-2247-1 : rails - several vulnerabilities

Debian DSA-2248-1 : ejabberd - denial of service

Debian DSA-2249-1 : jabberd14 - denial of service

Debian DSA-225-1 : tomcat4 - source disclosure

Debian DSA-2250-1 : citadel - denial of service

Debian DSA-2251-1 : subversion - several vulnerabilities

Debian DSA-2252-1 : dovecot - programming error

Debian DSA-2253-1 : fontforge - buffer overflow

Debian DSA-2254-1 : oprofile - command injection

Debian DSA-2255-1 : libxml2 - buffer overflow

Debian DSA-2256-1 : tiff - buffer overflow

Debian DSA-2257-1 : vlc - heap-based buffer overflow

Debian DSA-2258-1 : kolab-cyrus-imapd - implementation error

Debian DSA-2259-1 : fex - authentication bypass

Debian DSA-226-1 : xpdf-i - integer overflow

Debian DSA-2260-1 : rails - several vulnerabilities

Debian DSA-2261-1 : redmine - several vulnerabilities

Debian DSA-2262-1 : moodle - several vulnerabilities

Debian DSA-2263-2 : movabletype-opensource - several vulnerabilities

Debian DSA-2264-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2265-1 : perl - lack of tainted flag propagation

Debian DSA-2266-1 : php5 - several vulnerabilities

Debian DSA-2267-1 : perl - restriction bypass

Debian DSA-2268-1 : iceweasel - several vulnerabilities

Debian DSA-2269-1 : iceape - several vulnerabilities

Debian DSA-227-1 : openldap2 - buffer overflows and other bugs

Debian DSA-2270-1 : qemu-kvm - programming error

Debian DSA-2271-1 : curl - improper delegation of client credentials

Debian DSA-2272-1 : bind9 - denial of service

Debian DSA-2273-1 : icedove - several vulnerabilities

Debian DSA-2274-1 : wireshark - several vulnerabilities

Debian DSA-2275-1 : openoffice.org - stack-based buffer overflow

Debian DSA-2276-1 : asterisk - multiple denial of service

Debian DSA-2277-1 : xml-security-c - stack-based buffer overflow

Debian DSA-2278-1 : horde3 - several vulnerabilities

Debian DSA-2279-1 : libapache2-mod-authnz-external - SQL injection

Debian DSA-228-1 : libmcrypt - buffer overflows and memory leak

Debian DSA-2280-1 : libvirt - several vulnerabilities

Debian DSA-2281-1 : opie - several vulnerabilities

Debian DSA-2282-1 : qemu-kvm - several vulnerabilities

Debian DSA-2283-1 : krb5-appl - programming error

Debian DSA-2284-1 : opensaml2 - implementation error

Debian DSA-2285-1 : mapserver - several vulnerabilities

Debian DSA-2286-1 : phpmyadmin - several vulnerabilities

Debian DSA-2287-1 : libpng - several vulnerabilities

Debian DSA-2288-1 : libsndfile - integer overflow

Debian DSA-2289-1 : typo3-src - several vulnerabilities

Debian DSA-229-1 : imp - SQL injection

Debian DSA-2290-1 : samba - XSS

Debian DSA-2291-1 : squirrelmail - various vulnerabilities

Debian DSA-2292-1 : isc-dhcp - denial of service

Debian DSA-2293-1 : libxfont - buffer overflow

Debian DSA-2294-1 : freetype - missing input sanitising

Debian DSA-2295-1 : iceape - several vulnerabilities

Debian DSA-2296-1 : iceweasel - several vulnerabilities

Debian DSA-2297-1 : icedove - several vulnerabilities

Debian DSA-2298-2 : apache2 - denial of service

Debian DSA-2299-1 : ca-certificates - compromised certificate authority

Debian DSA-230-1 : bugzilla - insecure permissions, spurious backup files

Debian DSA-2300-2 : nss - compromised certificate authority

Debian DSA-2301-2 : rails - several vulnerabilities

Debian DSA-2302-1 : bcfg2 - missing input sanitization

Debian DSA-2303-2 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2304-1 : squid3 - buffer overflow

Debian DSA-2305-1 : vsftpd - denial of service

Debian DSA-2306-1 : ffmpeg - several vulnerabilities

Debian DSA-2307-1 : chromium-browser - several vulnerabilities

Debian DSA-2308-1 : mantis - several vulnerabilities

Debian DSA-2309-1 : openssl - compromised certificate authority

Debian DSA-231-1 : dhcp3 - stack overflows

Debian DSA-2310-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2311-1 : openjdk-6 - several vulnerabilities

Debian DSA-2312-1 : iceape - several vulnerabilities

Debian DSA-2313-1 : iceweasel - several vulnerabilities

Debian DSA-2314-1 : puppet - multiple vulnerabilities

Debian DSA-2315-1 : openoffice.org - multiple vulnerabilities

Debian DSA-2316-1 : quagga - several vulnerabilities

Debian DSA-2317-1 : icedove - several vulnerabilities

Debian DSA-2318-1 : cyrus-imapd-2.2 - multiple vulnerabilities

Debian DSA-2319-1 : policykit-1 - race condition

Debian DSA-232-1 : cupsys - several vulnerabilities

Debian DSA-2320-1 : dokuwiki - regression fix

Debian DSA-2321-1 : moin - XSS

Debian DSA-2322-1 : bugzilla - several vulnerabilities

Debian DSA-2323-1 : radvd - several vulnerabilities

Debian DSA-2324-1 : wireshark - programming error

Debian DSA-2325-1 : kfreebsd-8 - privilege escalation/denial of service

Debian DSA-2326-1 : pam - several vulnerabilities

Debian DSA-2327-1 : libfcgi-perl - authentication bypass

Debian DSA-2328-1 : freetype - missing input sanitising

Debian DSA-2329-1 : torque - buffer overflow

Debian DSA-233-1 : cvs - doubly freed memory

Debian DSA-2330-1 : simplesamlphp - XML encryption weakness

Debian DSA-2331-1 : tor - several vulnerabilities

Debian DSA-2332-1 : python-django - several issues

Debian DSA-2333-1 : phpldapadmin - several vulnerabilities

Debian DSA-2334-1 : mahara - several vulnerabilities

Debian DSA-2335-1 : man2html - missing input sanitization

Debian DSA-2336-1 : ffmpeg - several vulnerabilities

Debian DSA-2337-1 : xen - several vulnerabilities

Debian DSA-2338-1 : moodle - several vulnerabilities

Debian DSA-2339-1 : nss - several vulnerabilities

Debian DSA-234-1 : kdeadmin - several vulnerabilities

Debian DSA-2340-1 : postgresql-8.3, postgresql-8.4, postgresql-9.0 - weak password hashing

Debian DSA-2341-1 : iceweasel - several vulnerabilities

Debian DSA-2342-1 : iceape - several vulnerabilities

Debian DSA-2343-1 : openssl - CA trust revocation

Debian DSA-2344-1 : python-django-piston - deserialization vulnerability

Debian DSA-2345-1 : icedove - several vulnerabilities

Debian DSA-2346-2 : proftpd-dfsg - several vulnerabilities

Debian DSA-2347-1 : bind9 - improper assert

Debian DSA-2348-1 : systemtap - several vulnerabilities

Debian DSA-2349-1 : spip - several vulnerabilities

Debian DSA-235-1 : kdegraphics - several vulnerabilities

Debian DSA-2350-1 : freetype - missing input sanitising

Debian DSA-2351-1 : wireshark - buffer overflow

Debian DSA-2352-1 : puppet - programming error

Debian DSA-2353-1 : ldns - buffer overflow

Debian DSA-2354-1 : cups - several vulnerabilities

Debian DSA-2355-1 : clearsilver - format string vulnerability

Debian DSA-2356-1 : openjdk-6 - several vulnerabilities (BEAST)

Debian DSA-2357-1 : evince - several vulnerabilities

Debian DSA-2358-1 : openjdk-6 - several vulnerabilities (BEAST)

Debian DSA-2359-1 : mojarra - EL injection

Debian DSA-236-1 : kdelibs - several vulnerabilities

Debian DSA-2361-1 : chasen - buffer overflow

Debian DSA-2362-1 : acpid - several vulnerabilities

Debian DSA-2363-1 : tor - buffer overflow

Debian DSA-2364-1 : xorg - incorrect permission check

Debian DSA-2365-1 : dtc - several vulnerabilities

Debian DSA-2366-1 : mediawiki - multiple vulnerabilities

Debian DSA-2367-1 : asterisk - several vulnerabilities

Debian DSA-2368-1 : lighttpd - multiple vulnerabilities (BEAST)

Debian DSA-2369-1 : libsoup2.4 - insufficient input sanitization

Debian DSA-237-1 : kdenetwork - several vulnerabilities

Debian DSA-2370-1 : unbound - several vulnerabilities

Debian DSA-2371-1 : jasper - buffer overflows

Debian DSA-2372-1 : heimdal - buffer overflow

Debian DSA-2373-1 : inetutils - buffer overflow

Debian DSA-2374-1 : openswan - implementation error

Debian DSA-2375-1 : krb5, krb5-appl - buffer overflow

Debian DSA-2376-2 : ipmitool - insecure PID file

Debian DSA-2377-1 : cyrus-imapd-2.2 - NULL pointer dereference

Debian DSA-2378-1 : ffmpeg - several vulnerabilities

Debian DSA-2379-1 : krb5 - several vulnerabilities

Debian DSA-238-1 : kdepim - several vulnerabilities

Debian DSA-2380-1 : foomatic-filters - shell command injection

Debian DSA-2381-1 : squid3 - invalid memory deallocation

Debian DSA-2382-1 : ecryptfs-utils - multiple vulnerabilities

Debian DSA-2383-1 : super - buffer overflow

Debian DSA-2384-2 : cacti - several vulnerabilities

Debian DSA-2385-1 : pdns - packet loop

Debian DSA-2386-1 : openttd - several vulnerabilities

Debian DSA-2387-1 : simplesamlphp - insufficient input sanitation

Debian DSA-2388-1 : t1lib - several vulnerabilities

Debian DSA-2389-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-239-1 : kdesdk - several vulnerabilities

Debian DSA-2390-1 : openssl - several vulnerabilities

Debian DSA-2391-1 : phpmyadmin - several vulnerabilities

Debian DSA-2392-1 : openssl - out-of-bounds read

Debian DSA-2393-1 : bip - buffer overflow

Debian DSA-2394-1 : libxml2 - several vulnerabilities

Debian DSA-2395-1 : wireshark - buffer underflow

Debian DSA-2396-1 : qemu-kvm - buffer underflow

Debian DSA-2397-1 : icu - buffer underflow

Debian DSA-2398-2 : curl - several vulnerabilities (BEAST)

Debian DSA-2399-2 : php5 - several vulnerabilities

Debian DSA-240-1 : kdegames - several vulnerabilities

Debian DSA-2400-1 : iceweasel - several vulnerabilities

Debian DSA-2401-1 : tomcat6 - several vulnerabilities

Debian DSA-2402-1 : iceape - several vulnerabilities

Debian DSA-2403-2 : php5 - code injection

Debian DSA-2404-1 : xen-qemu-dm-4.0 - buffer overflow

Debian DSA-2405-1 : apache2 - multiple issues

Debian DSA-2406-1 : icedove - several vulnerabilities

Debian DSA-2407-1 : cvs - heap overflow

Debian DSA-2408-1 : php5 - several vulnerabilities

Debian DSA-2409-1 : devscripts - several vulnerabilities

Debian DSA-241-1 : kdeutils - several vulnerabilities

Debian DSA-2410-1 : libpng - integer overflow

Debian DSA-2411-1 : mumble - information disclosure

Debian DSA-2412-1 : libvorbis - buffer overflow

Debian DSA-2413-1 : libarchive - buffer overflows

Debian DSA-2414-2 : fex - insufficient input sanitization

Debian DSA-2415-1 : libmodplug - several vulnerabilities

Debian DSA-2416-1 : notmuch - information disclosure

Debian DSA-2417-1 : libxml2 - computational denial of service

Debian DSA-2418-1 : postgresql-8.4 - several vulnerabilities

Debian DSA-2419-1 : puppet - several vulnerabilities

Debian DSA-242-1 : kdebase - several vulnerabilities

Debian DSA-2420-1 : openjdk-6 - several vulnerabilities

Debian DSA-2421-1 : moodle - several vulnerabilities

Debian DSA-2422-2 : file - missing bounds checks

Debian DSA-2423-1 : movabletype-opensource - several vulnerabilities

Debian DSA-2424-1 : libxml-atom-perl - XML external entity expansion

Debian DSA-2425-1 : plib - buffer overflow

Debian DSA-2426-1 : gimp - several vulnerabilities

Debian DSA-2427-1 : imagemagick - several vulnerabilities

Debian DSA-2428-1 : freetype - several vulnerabilities

Debian DSA-2429-1 : mysql-5.1 - several vulnerabilities

Debian DSA-243-1 : kdemultimedia - several vulnerabilities

Debian DSA-2430-1 : python-pam - double free

Debian DSA-2431-1 : libdbd-pg-perl - format string vulnerabilities

Debian DSA-2432-1 : libyaml-libyaml-perl - format string vulnerabilities

Debian DSA-2433-1 : iceweasel - several vulnerabilities

Debian DSA-2434-1 : nginx - sensitive information leak

Debian DSA-2435-1 : gnash - several vulnerabilities

Debian DSA-2436-1 : libapache2-mod-fcgid - inactive resource limits

Debian DSA-2437-1 : icedove - several vulnerabilities

Debian DSA-2438-1 : raptor - programming error

Debian DSA-2439-1 : libpng - buffer overflow

Debian DSA-244-1 : noffle - buffer overflows

Debian DSA-2440-1 : libtasn1-3 - missing bounds check

Debian DSA-2441-1 : gnutls26 - missing bounds check

Debian DSA-2442-2 : openarena - UDP traffic amplification

Debian DSA-2443-1 : linux-2.6 - privilege escalation/denial of service

Debian DSA-2444-1 : tryton-server - privilege escalation

Debian DSA-2445-1 : typo3-src - several vulnerabilities

Debian DSA-2446-1 : libpng - incorrect memory handling

Debian DSA-2447-1 : tiff - integer overflow

Debian DSA-2448-1 : inspircd - buffer overflow

Debian DSA-2449-1 : sqlalchemy - missing input sanitization

Debian DSA-245-1 : dhcp3 - ignored counter boundary

Debian DSA-2450-1 : samba - privilege escalation

Debian DSA-2451-1 : puppet - several vulnerabilities

Debian DSA-2452-1 : apache2 - insecure default configuration

Debian DSA-2453-1 : gajim - several vulnerabilities

Debian DSA-2454-2 : openssl - multiple vulnerabilities

Debian DSA-2455-1 : typo3-src - missing input sanitization

Debian DSA-2456-1 : dropbear - use after free

Debian DSA-2457-2 : iceweasel - several vulnerabilities

Debian DSA-2458-2 : iceape - several vulnerabilities

Debian DSA-2459-2 : quagga - several vulnerabilities

Debian DSA-246-1 : tomcat - information exposure, XSS

Debian DSA-2460-1 : asterisk - several vulnerabilities

Debian DSA-2461-1 : spip - several vulnerabilities

Debian DSA-2462-2 : imagemagick - several vulnerabilities

Debian DSA-2463-1 : samba - missing permission checks

Debian DSA-2464-2 : icedove - several vulnerabilities

Debian DSA-2465-1 : php5 - several vulnerabilities

Debian DSA-2466-1 : rails - XSS

Debian DSA-2467-1 : mahara - insecure defaults

Debian DSA-2468-1 : libjakarta-poi-java - unbounded memory allocation

Debian DSA-2469-1 : linux-2.6 - privilege escalation/denial of service

Debian DSA-247-1 : courier-ssl - missing input sanitizing

Debian DSA-2470-1 : wordpress - several vulnerabilities

Debian DSA-2471-1 : ffmpeg - several vulnerabilities

Debian DSA-2472-1 : gridengine - privilege escalation

Debian DSA-2473-1 : openoffice.org - buffer overflow

Debian DSA-2474-1 : ikiwiki - XSS

Debian DSA-2475-1 : openssl - integer underflow

Debian DSA-2476-1 : pidgin-otr - format string vulnerability

Debian DSA-2477-1 : sympa - authorization bypass

Debian DSA-2478-1 : sudo - parsing error

Debian DSA-2479-1 : libxml2 - off-by-one

Debian DSA-248-1 : hypermail - buffer overflows

Debian DSA-2480-4 : request-tracker3.8 - several vulnerabilities

Debian DSA-2481-1 : arpwatch - fails to drop supplementary groups

Debian DSA-2482-1 : libgdata - insufficient certificate validation

Debian DSA-2483-1 : strongswan - authentication bypass

Debian DSA-2484-1 : nut - denial of service

Debian DSA-2485-1 : imp4 - XSS

Debian DSA-2486-1 : bind9 - denial of service

Debian DSA-2487-1 : openoffice.org - buffer overflow

Debian DSA-2488-1 : iceweasel - several vulnerabilities

Debian DSA-2489-1 : iceape - several vulnerabilities

Debian DSA-249-1 : w3mmee - missing HTML quoting

Debian DSA-2490-1 : nss - denial of service

Debian DSA-2491-1 : postgresql-8.4 - several vulnerabilities

Debian DSA-2492-1 : php5 - buffer overflow

Debian DSA-2493-1 : asterisk - denial of service

Debian DSA-2494-1 : ffmpeg - several vulnerabilities

Debian DSA-2495-1 : openconnect - buffer overflow

Debian DSA-2496-1 : mysql-5.1 - several vulnerabilities

Debian DSA-2497-1 : quagga - denial of service

Debian DSA-2498-1 : dhcpcd - remote stack overflow

Debian DSA-2499-1 : icedove - several vulnerabilities

Debian DSA-250-1 : w3mmee-ssl - missing HTML quoting

Debian DSA-2500-1 : mantis - several vulnerabilities

Debian DSA-2501-1 : xen - several vulnerabilities

Debian DSA-2502-1 : python-crypto - programming error

Debian DSA-2503-1 : bcfg2 - shell command injection

Debian DSA-2504-1 : libspring-2.5-java - information disclosure

Debian DSA-2505-1 : zendframework - information disclosure

Debian DSA-2506-1 : libapache-mod-security - ModSecurity bypass

Debian DSA-2507-1 : openjdk-6 - several vulnerabilities

Debian DSA-2508-1 : kfreebsd-8 - privilege escalation

Debian DSA-2509-1 : pidgin - remote code execution

Debian DSA-251-1 : w3m - missing HTML quoting

Debian DSA-2510-1 : extplorer - Cross-site request forgery

Debian DSA-2511-1 : puppet - several vulnerabilities

Debian DSA-2512-1 : mono - missing input sanitising

Debian DSA-2513-1 : iceape - several vulnerabilities

Debian DSA-2514-1 : iceweasel - several vulnerabilities

Debian DSA-2515-1 : nsd3 - NULL pointer dereference

Debian DSA-2516-1 : isc-dhcp - several vulnerabilities

Debian DSA-2517-1 : bind9 - denial of service

Debian DSA-2518-1 : krb5 - denial of service and remote code execution

Debian DSA-2519-2 : isc-dhcp - several vulnerabilities

Debian DSA-252-1 : slocate - buffer overflow

Debian DSA-2520-1 : openoffice.org - Multiple heap-based buffer overflows

Debian DSA-2521-1 : libxml2 - integer overflows

Debian DSA-2522-1 : fckeditor - XSS

Debian DSA-2523-1 : globus-gridftp-server - programming error

Debian DSA-2524-1 : openttd - several vulnerabilities

Debian DSA-2525-1 : expat - several vulnerabilities

Debian DSA-2526-1 : libotr - heap-based buffer overflows

Debian DSA-2527-1 : php5 - several vulnerabilities

Debian DSA-2528-1 : icedove - several vulnerabilities

Debian DSA-2529-1 : python-django - several vulnerabilities

Debian DSA-253-1 : openssl - information leak

Debian DSA-2530-1 : rssh - shell command injection

Debian DSA-2531-1 : xen - Denial of Service

Debian DSA-2532-1 : libapache2-mod-rpaf - denial of service

Debian DSA-2533-1 : pcp - several vulnerabilities

Debian DSA-2534-1 : postgresql-8.4 - several vulnerabilities

Debian DSA-2535-1 : rtfm - XSS

Debian DSA-2536-1 : otrs2 - XSS

Debian DSA-2537-1 : typo3-src - several vulnerabilities

Debian DSA-2538-1 : moin - privilege escalation

Debian DSA-2539-1 : zabbix - SQL injection

Debian DSA-254-1 : traceroute-nanog - buffer overflow

Debian DSA-2540-1 : mahara - XSS

Debian DSA-2541-1 : beaker - information disclosure

Debian DSA-2542-1 : qemu-kvm - multiple vulnerabilities

Debian DSA-2543-1 : xen-qemu-dm-4.0 - multiple vulnerabilities

Debian DSA-2544-1 : xen - denial of service

Debian DSA-2545-1 : qemu - multiple vulnerabilities

Debian DSA-2546-1 : freeradius - stack-based buffer overflows

Debian DSA-2547-1 : bind9 - improper assert

Debian DSA-2548-1 : tor - several vulnerabilities

Debian DSA-2549-1 : devscripts - multiple vulnerabilities

Debian DSA-255-1 : tcpdump - infinite loop

Debian DSA-2550-2 : asterisk - several vulnerabilities

Debian DSA-2551-1 : isc-dhcp - denial of service

Debian DSA-2552-1 : tiff - several vulnerabilities

Debian DSA-2553-1 : iceweasel - several vulnerabilities

Debian DSA-2554-1 : iceape - several vulnerabilities

Debian DSA-2555-1 : libxslt - several vulnerabilities

Debian DSA-2556-1 : icedove - several vulnerabilities

Debian DSA-2557-1 : hostapd - buffer overflow

Debian DSA-2558-1 : bacula - information disclosure

Debian DSA-2559-1 : libexif - several vulnerabilities

Debian DSA-256-1 : mhc - insecure temporary file

Debian DSA-2560-1 : bind9 - denial of service

Debian DSA-2561-1 : tiff - buffer overflow

Debian DSA-2562-1 : cups-pk-helper - privilege escalation

Debian DSA-2563-1 : viewvc - several vulnerabilities

Debian DSA-2564-1 : tinyproxy - denial of service

Debian DSA-2565-1 : iceweasel - several vulnerabilities

Debian DSA-2566-1 : exim4 - heap-based buffer overflow

Debian DSA-2567-1 : request-tracker3.8 - several vulnerabilities

Debian DSA-2568-1 : rtfm - privilege escalation

Debian DSA-2569-1 : icedove - several vulnerabilities

Debian DSA-257-1 : sendmail - remote exploit

Debian DSA-2570-1 : openoffice.org - several vulnerabilities

Debian DSA-2571-1 : libproxy - buffer overflow

Debian DSA-2572-1 : iceape - several vulnerabilities

Debian DSA-2573-1 : radsecproxy - SSL certificate verification weakness

Debian DSA-2574-1 : typo3-src - several vulnerabilities

Debian DSA-2575-1 : tiff - heap-based buffer overflow

Debian DSA-2576-1 : trousers - denial of service

Debian DSA-2577-1 : libssh - several vulnerabilities

Debian DSA-2578-1 : rssh - insufficient filtering of rsync command line

Debian DSA-2579-1 : apache2 - Multiple issues

Debian DSA-258-1 : ethereal - format string vulnerability

Debian DSA-2580-1 : libxml2 - buffer overflow

Debian DSA-2581-1 : mysql-5.1 - several vulnerabilities

Debian DSA-2582-1 : xen - several vulnerabilities

Debian DSA-2583-1 : iceweasel - several vulnerabilities

Debian DSA-2584-1 : iceape - several vulnerabilities

Debian DSA-2585-1 : bogofilter - buffer overflow

Debian DSA-2586-1 : perl - several vulnerabilities

Debian DSA-2587-1 : libcgi-pm-perl - HTTP header injection

Debian DSA-2588-1 : icedove - several vulnerabilities

Debian DSA-2589-1 : tiff - buffer overflow

Debian DSA-259-1 : qpopper - mail user privilege escalation

Debian DSA-2590-1 : wireshark - several vulnerabilities

Debian DSA-2591-1 : mahara - several vulnerabilities

Debian DSA-2592-1 : elinks - programming error

Debian DSA-2593-1 : moin - several vulnerabilities

Debian DSA-2594-1 : virtualbox-ose - programming error

Debian DSA-2595-1 : ghostscript - integer overflow

Debian DSA-2596-1 : mediawiki-extensions - XSS

Debian DSA-2597-1 : rails - input validation error

Debian DSA-2598-1 : weechat - several vulnerabilities

Debian DSA-2599-1 : nss - mis-issued intermediates

Debian DSA-260-1 : file - buffer overflow

Debian DSA-2600-1 : cups - privilege escalation

Debian DSA-2601-1 : gnupg, gnupg2 - missing input sanitation

Debian DSA-2602-1 : zendframework - XML external entity inclusion

Debian DSA-2603-1 : emacs23 - programming error

Debian DSA-2604-1 : rails - insufficient input validation

Debian DSA-2605-2 : asterisk - several issues

Debian DSA-2606-1 : proftpd-dfsg - symlink race

Debian DSA-2607-1 : qemu-kvm - buffer overflow

Debian DSA-2608-1 : qemu - buffer overflow

Debian DSA-2609-1 : rails - SQL query manipulation

Debian DSA-261-1 : tcpdump - infinite loop

Debian DSA-2610-1 : ganglia - arbitrary script execution

Debian DSA-2611-1 : movabletype-opensource - several vulnerabilities

Debian DSA-2612-2 : ircd-ratbox - programming error

Debian DSA-2613-1 : rails - insufficient input validation

Debian DSA-2614-1 : libupnp - several vulnerabilities

Debian DSA-2615-1 : libupnp4 - several vulnerabilities

Debian DSA-2616-1 : nagios3 - buffer overflow in CGI scripts

Debian DSA-2617-1 : samba - several issues

Debian DSA-2618-1 : ircd-hybrid - denial of service

Debian DSA-2619-1 : xen-qemu-dm-4.0 - buffer overflow

Debian DSA-262-1 : samba - remote exploit

Debian DSA-2620-1 : rails - several vulnerabilities

Debian DSA-2621-1 : openssl - several vulnerabilities

Debian DSA-2622-1 : polarssl - several vulnerabilities

Debian DSA-2623-1 : openconnect - buffer overflow

Debian DSA-2624-1 : ffmpeg - several vulnerabilities

Debian DSA-2625-1 : wireshark - several vulnerabilities

Debian DSA-2626-1 : lighttpd - several issues

Debian DSA-2627-1 : nginx - information leak

Debian DSA-2628-1 : nss-pam-ldapd - buffer overflow

Debian DSA-2629-1 : openjpeg - several issues

Debian DSA-263-1 : netpbm-free - math overflow errors

Debian DSA-2630-1 : postgresql-8.4 - programming error

Debian DSA-2631-1 : squid3 - denial of service

Debian DSA-2632-1 : linux-2.6 - privilege escalation/denial of service

Debian DSA-2633-1 : fusionforge - privilege escalation

Debian DSA-2634-1 : python-django - several vulnerabilities

Debian DSA-2635-1 : cfingerd - buffer overflow

Debian DSA-2636-2 : xen - several vulnerabilities

Debian DSA-2637-1 : apache2 - several issues

Debian DSA-2638-1 : openafs - buffer overflow

Debian DSA-2639-1 : php5 - several vulnerabilities

Debian DSA-264-1 : lxr - missing filename sanitizing

Debian DSA-2640-1 : zoneminder - several issues

Debian DSA-2641-2 : perl - rehashing flaw

Debian DSA-2642-1 : sudo - several issues

Debian DSA-2643-1 : puppet - several vulnerabilities

Debian DSA-2644-1 : wireshark - several vulnerabilities

Debian DSA-2645-1 : inetutils - denial of service

Debian DSA-2646-1 : typo3-src - several vulnerabilities

Debian DSA-2647-1 : firebird2.1 - buffer overflow

Debian DSA-2648-1 : firebird2.5 - several vulnerabilities

Debian DSA-2649-1 : lighttpd - fixed socket name in world-writable directory

Debian DSA-265-1 : bonsai - several vulnerabilities

Debian DSA-2650-2 : libvirt - files and device nodes ownership change to kvm group

Debian DSA-2651-1 : smokeping - XSS vulnerability

Debian DSA-2652-1 : libxml2 - external entity expansion

Debian DSA-2653-1 : icinga - buffer overflow

Debian DSA-2654-1 : libxslt - denial of service

Debian DSA-2655-1 : rails - several vulnerabilities

Debian DSA-2656-1 : bind9 - denial of service

Debian DSA-2657-1 : postgresql-8.4 - guessable random numbers

Debian DSA-2659-1 : libapache-mod-security - XML external entity processing vulnerability

Debian DSA-266-1 : krb5 - several vulnerabilities

Debian DSA-2660-1 : curl - exposure of sensitive information

Debian DSA-2661-1 : xorg-server - information disclosure

Debian DSA-2662-1 : xen - several vulnerabilities

Debian DSA-2663-1 : tinc - stack based buffer overflow

Debian DSA-2664-1 : stunnel4 - buffer overflow

Debian DSA-2665-1 : strongswan - authentication bypass

Debian DSA-2666-1 : xen - several vulnerabilities

Debian DSA-2667-1 : mysql-5.5 - several vulnerabilities

Debian DSA-2668-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2669-1 : linux - privilege escalation/denial of service/information leak

Debian DSA-267-1 : lpr - buffer overflow

Debian DSA-2670-1 : request-tracker3.8 - several vulnerabilities

Debian DSA-2671-1 : request-tracker4 - several vulnerabilities

Debian DSA-2672-1 : kfreebsd-9 - interpretation conflict

Debian DSA-2673-1 : libdmx - several vulnerabilities

Debian DSA-2674-1 : libxv - several vulnerabilities

Debian DSA-2675-2 : libxvmc - several vulnerabilities

Debian DSA-2676-1 : libxfixes - several vulnerabilities

Debian DSA-2677-1 : libxrender - several vulnerabilities

Debian DSA-2678-1 : mesa - several vulnerabilities

Debian DSA-2679-1 : xserver-xorg-video-openchrome - several vulnerabilities

Debian DSA-268-1 : mutt - buffer overflow

Debian DSA-2680-1 : libxt - several vulnerabilities

Debian DSA-2681-1 : libxcursor - several vulnerabilities

Debian DSA-2682-1 : libxext - several vulnerabilities

Debian DSA-2683-1 : libxi - several vulnerabilities

Debian DSA-2684-1 : libxrandr - several vulnerabilities

Debian DSA-2685-1 : libxp - several vulnerabilities

Debian DSA-2686-1 : libxcb - several vulnerabilities

Debian DSA-2687-1 : libfs - several vulnerabilities

Debian DSA-2688-1 : libxres - several vulnerabilities

Debian DSA-2689-1 : libxtst - several vulnerabilities

Debian DSA-269-1 : heimdal - Cryptographic weakness

Debian DSA-2690-1 : libxxf86dga - several vulnerabilities

Debian DSA-2691-1 : libxinerama - several vulnerabilities

Debian DSA-2692-1 : libxxf86vm - several vulnerabilities

Debian DSA-2693-1 : libx11 - several vulnerabilities

Debian DSA-2694-1 : spip - privilege escalation

Debian DSA-2695-1 : chromium-browser - several issues

Debian DSA-2696-1 : otrs2 - privilege escalation

Debian DSA-2697-1 : gnutls26 - out-of-bounds array read

Debian DSA-2698-1 : tiff - buffer overflow

Debian DSA-2699-1 : iceweasel - several vulnerabilities

Debian DSA-270-1 : linux-kernel-mips - local privilege escalation

Debian DSA-2700-1 : wireshark - several vulnerabilities

Debian DSA-2701-1 : krb5 - denial of service

Debian DSA-2702-1 : telepathy-gabble - TLS verification bypass

Debian DSA-2703-1 : subversion - several vulnerabilities

Debian DSA-2704-1 : mesa - out of bounds access

Debian DSA-2705-1 : pymongo - denial of service

Debian DSA-2706-1 : chromium-browser - several vulnerabilities

Debian DSA-2707-1 : dbus - denial of service

Debian DSA-2708-1 : fail2ban - denial of service

Debian DSA-2709-1 : wireshark - several vulnerabilities

Debian DSA-271-1 : ecartis - unauthorized password change

Debian DSA-2710-1 : xml-security-c - several vulnerabilities

Debian DSA-2711-1 : haproxy - several vulnerabilities

Debian DSA-2712-1 : otrs2 - privilege escalation

Debian DSA-2713-1 : curl - heap overflow

Debian DSA-2714-1 : kfreebsd-9 - programming error

Debian DSA-2715-1 : puppet - code execution

Debian DSA-2716-1 : iceweasel - several vulnerabilities

Debian DSA-2717-1 : xml-security-c - heap overflow

Debian DSA-2718-1 : wordpress - several vulnerabilities

Debian DSA-2719-1 : poppler - several vulnerabilities

Debian DSA-272-1 : dietlibc - integer overflow

Debian DSA-2720-1 : icedove - several vulnerabilities

Debian DSA-2721-1 : nginx - buffer overflow

Debian DSA-2722-1 : openjdk-7 - several vulnerabilities

Debian DSA-2723-1 : php5 - heap corruption

Debian DSA-2724-1 : chromium-browser - several vulnerabilities

Debian DSA-2725-1 : tomcat6 - several vulnerabilities

Debian DSA-2726-1 : php-radius - buffer overflow

Debian DSA-2727-1 : openjdk-6 - several vulnerabilities

Debian DSA-2728-1 : bind9 - denial of service

Debian DSA-2729-1 : openafs - several vulnerabilities

Debian DSA-273-1 : krb4 - Cryptographic weakness

Debian DSA-2730-1 : gnupg - information leak

Debian DSA-2731-1 : libgcrypt11 - information leak

Debian DSA-2732-1 : chromium-browser - several vulnerabilities

Debian DSA-2733-1 : otrs2 - SQL injection

Debian DSA-2734-1 : wireshark - several vulnerabilities

Debian DSA-2735-1 : iceweasel - several vulnerabilities

Debian DSA-2736-1 : putty - several vulnerabilities

Debian DSA-2737-1 : swift - several vulnerabilities

Debian DSA-2738-1 : ruby1.9.1 - several vulnerabilities

Debian DSA-2739-1 : cacti - several vulnerabilities

Debian DSA-274-1 : mutt - buffer overflow

Debian DSA-2740-2 : python-django - XSS vulnerability

Debian DSA-2741-1 : chromium-browser - several vulnerabilities

Debian DSA-2742-1 : php5 - interpretation conflict

Debian DSA-2743-1 : kfreebsd-9 - privilege escalation/information leak

Debian DSA-2744-1 : tiff - several vulnerabilities

Debian DSA-2745-1 : linux - privilege escalation/denial of service/information leak

Debian DSA-2746-1 : icedove - several vulnerabilities

Debian DSA-2747-1 : cacti - several vulnerabilities

Debian DSA-2748-1 : exactimage - denial of service

Debian DSA-2749-1 : asterisk - several vulnerabilities

Debian DSA-275-1 : lpr-ppd - buffer overflow

Debian DSA-2750-1 : imagemagick - buffer overflow

Debian DSA-2751-1 : libmodplug - several vulnerabilities

Debian DSA-2752-1 : phpbb3 - permissions too wide

Debian DSA-2753-1 : mediawiki - information leak

Debian DSA-2754-1 : exactimage - denial of service

Debian DSA-2755-1 : python-django - directory traversal

Debian DSA-2756-1 : wireshark - several vulnerabilities

Debian DSA-2757-1 : wordpress - several vulnerabilities

Debian DSA-2758-1 : python-django - denial of service

Debian DSA-2759-1 : iceweasel - several vulnerabilities

Debian DSA-276-1 : linux-kernel-s390 - local privilege escalation

Debian DSA-2760-1 : chrony - several vulnerabilities

Debian DSA-2761-1 : puppet - several vulnerabilities

Debian DSA-2762-1 : icedove - several vulnerabilities

Debian DSA-2763-1 : pyopenssl - hostname check bypassing

Debian DSA-2764-1 : libvirt - programming error

Debian DSA-2765-1 : davfs2 - privilege escalation

Debian DSA-2766-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2767-1 : proftpd-dfsg - denial of service

Debian DSA-2768-1 : icedtea-web - heap-based buffer overflow

Debian DSA-2769-1 : kfreebsd-9 - privilege escalation/denial of service

Debian DSA-277-1 : apcupsd - buffer overflows, format string

Debian DSA-2770-1 : torque - authentication bypass

Debian DSA-2771-1 : nas - several vulnerabilities

Debian DSA-2772-1 : typo3-src - XSS

Debian DSA-2773-1 : gnupg - several vulnerabilities

Debian DSA-2774-1 : gnupg2 - several vulnerabilities

Debian DSA-2775-1 : ejabberd - insecure SSL usage

Debian DSA-2776-1 : drupal6 - several vulnerabilities

Debian DSA-2777-1 : systemd - several vulnerabilities

Debian DSA-2778-1 : libapache2-mod-fcgid - heap-based buffer overflow

Debian DSA-2779-1 : libxml2 - denial of service

Debian DSA-278-1 : sendmail - char-to-int conversion

Debian DSA-2780-1 : mysql-5.1 - several vulnerabilities

Debian DSA-2781-1 : python-crypto - PRNG not correctly reseeded in some situations

Debian DSA-2782-1 : polarssl - several vulnerabilities

Debian DSA-2783-1 : librack-ruby - several vulnerabilities

Debian DSA-2784-1 : xorg-server - use-after-free

Debian DSA-2785-1 : chromium-browser - several vulnerabilities

Debian DSA-2786-1 : icu - several vulnerabilities

Debian DSA-2787-1 : roundcube - design error

Debian DSA-2788-1 : iceweasel - several vulnerabilities

Debian DSA-2789-1 : strongswan - Denial of service and authorization bypass

Debian DSA-279-1 : metrics - insecure temporary file creation

Debian DSA-2790-1 : nss - uninitialized memory read

Debian DSA-2791-1 : tryton-client - missing input sanitization

Debian DSA-2792-1 : wireshark - several vulnerabilities

Debian DSA-2793-1 : libav - several vulnerabilities

Debian DSA-2794-1 : spip - several vulnerabilities

Debian DSA-2795-2 : lighttpd - several vulnerabilities

Debian DSA-2796-1 : torque - arbitrary code execution

Debian DSA-2797-1 : icedove - several vulnerabilities

Debian DSA-2798-1 : curl - unchecked ssl certificate host name

Debian DSA-2799-1 : chromium-browser - several vulnerabilities

Debian DSA-280-1 : samba - buffer overflow

Debian DSA-2800-1 : nss - buffer overflow

Debian DSA-2801-1 : libhttp-body-perl - design error

Debian DSA-2802-1 : nginx - restriction bypass

Debian DSA-2803-1 : quagga - several vulnerabilities

Debian DSA-2804-1 : drupal7 - several vulnerabilities

Debian DSA-2805-1 : sup-mail - command injection

Debian DSA-2806-1 : nbd - privilege escalation

Debian DSA-2807-1 : links2 - integer overflow

Debian DSA-2808-1 : openjpeg - several vulnerabilities

Debian DSA-2809-1 : ruby1.8 - several vulnerabilities

Debian DSA-281-1 : moxftp - buffer overflow

Debian DSA-2810-1 : ruby1.9.1 - heap overflow

Debian DSA-2811-1 : chromium-browser - several vulnerabilities

Debian DSA-2812-1 : samba - several vulnerabilities

Debian DSA-2813-1 : gimp - several vulnerabilities

Debian DSA-2814-1 : varnish - denial of service

Debian DSA-2815-1 : munin - denial of service

Debian DSA-2816-1 : php5 - several vulnerabilities

Debian DSA-2817-1 : libtar - Integer overflow

Debian DSA-2818-1 : mysql-5.5 - several vulnerabilities

Debian DSA-2819-1 : iceape End-of-Life Announcement

Debian DSA-282-1 : glibc - integer overflow

Debian DSA-2820-1 : nspr - integer overflow

Debian DSA-2821-1 : gnupg - side channel attack

Debian DSA-2822-1 : xorg-server - integer underflow

Debian DSA-2823-1 : pixman - integer underflow

Debian DSA-2824-1 : curl - unchecked tls/ssl certificate host name

Debian DSA-2825-1 : wireshark - several vulnerabilities

Debian DSA-2826-1 : denyhosts - remote denial of ssh service

Debian DSA-2827-1 : libcommons-fileupload-java - arbitrary file upload via deserialization

Debian DSA-2828-1 : drupal6 - several vulnerabilities

Debian DSA-2829-1 : hplip - several vulnerabilities

Debian DSA-283-1 : xfsdump - insecure file creation

Debian DSA-2830-1 : ruby-i18n - XSS

Debian DSA-2831-1 : puppet - insecure temporary files

Debian DSA-2832-1 : memcached - several vulnerabilities

Debian DSA-2833-1 : openssl - several vulnerabilities

Debian DSA-2834-1 : typo3-src - several vulnerabilities

Debian DSA-2835-1 : asterisk - buffer overflow

Debian DSA-2836-1 : devscripts - arbitrary code execution

Debian DSA-2837-1 : openssl - programming error

Debian DSA-2838-1 : libxfont - buffer overflow

Debian DSA-2839-1 : spice - denial of service

Debian DSA-284-1 : kdegraphics - insecure execution

Debian DSA-2840-1 : srtp - buffer overflow

Debian DSA-2841-1 : movabletype-opensource - XSS

Debian DSA-2842-1 : libspring-java - denial of service

Debian DSA-2843-1 : graphviz - buffer overflow

Debian DSA-2844-1 : djvulibre - arbitrary code execution

Debian DSA-2845-1 : mysql-5.1 - several vulnerabilities

Debian DSA-2846-1 : libvirt - several vulnerabilities

Debian DSA-2847-1 : drupal7 - several vulnerabilities

Debian DSA-2848-1 : mysql-5.5 - several vulnerabilities

Debian DSA-2849-1 : curl - information disclosure

Debian DSA-285-1 : lprng - insecure temporary file

Debian DSA-2850-1 : libyaml - heap-based buffer overflow

Debian DSA-2851-1 : drupal6 - impersonation

Debian DSA-2852-1 : libgadu - heap-based buffer overflow

Debian DSA-2853-1 : horde3 - remote code execution

Debian DSA-2854-1 : mumble - several vulnerabilities

Debian DSA-2855-1 : libav - several vulnerabilities

Debian DSA-2856-1 : libcommons-fileupload-java - denial of service

Debian DSA-2857-1 : libspring-java - several vulnerabilities

Debian DSA-2858-1 : iceweasel - several vulnerabilities

Debian DSA-2859-1 : pidgin - several vulnerabilities

Debian DSA-286-1 : gs-common - insecure temporary file

Debian DSA-2860-1 : parcimonie - information disclosure

Debian DSA-2861-1 : file - denial of service

Debian DSA-2862-1 : chromium-browser - several vulnerabilities

Debian DSA-2863-1 : libtar - directory traversal

Debian DSA-2864-1 : postgresql-8.4 - several vulnerabilities

Debian DSA-2865-1 : postgresql-9.1 - several vulnerabilities

Debian DSA-2866-1 : gnutls26 - certificate verification flaw

Debian DSA-2867-1 : otrs2 - several vulnerabilities

Debian DSA-2868-1 : php5 - denial of service

Debian DSA-2869-1 : gnutls26 - incorrect certificate verification

Debian DSA-287-1 : epic - buffer overflows

Debian DSA-2870-1 : libyaml-libyaml-perl - heap-based buffer overflow

Debian DSA-2871-1 : wireshark - several vulnerabilities

Debian DSA-2872-1 : udisks - several vulnerabilities

Debian DSA-2873-1 : file - several vulnerabilities

Debian DSA-2874-1 : mutt - security update

Debian DSA-2875-1 : cups-filters - security update

Debian DSA-2876-1 : cups - security update

Debian DSA-2877-1 : lighttpd - security update

Debian DSA-2878-1 : virtualbox - security update

Debian DSA-2879-1 : libssh - security update

Debian DSA-288-1 : openssl - several vulnerabilities

Debian DSA-2880-1 : python2.7 - security update

Debian DSA-2881-1 : iceweasel - security update

Debian DSA-2882-1 : extplorer - security update

Debian DSA-2883-1 : chromium-browser - security update

Debian DSA-2884-1 : libyaml - security update

Debian DSA-2885-1 : libyaml-libyaml-perl - security update

Debian DSA-2886-1 : libxalan2-java - security update

Debian DSA-2887-1 : ruby-actionmailer-3.2 - security update

Debian DSA-2888-1 : ruby-actionpack-3.2 - security update

Debian DSA-2889-1 : postfixadmin - security update

Debian DSA-289-1 : rinetd - incorrect memory resizing

Debian DSA-2890-1 : libspring-java - security update

Debian DSA-2891-1 : mediawiki, mediawiki-extensions Multiple Vulnerabilities

Debian DSA-2892-1 : a2ps - security update

Debian DSA-2893-1 : openswan - security update

Debian DSA-2894-1 : openssh - security update

Debian DSA-2895-1 : prosody - security update

Debian DSA-2896-1 : openssl - security update

Debian DSA-2897-1 : tomcat7 - security update

Debian DSA-2898-1 : imagemagick - security update

Debian DSA-2899-1 : openafs - security update

Debian DSA-290-1 : sendmail-wide - char-to-int conversion

Debian DSA-2900-1 : jbigkit - security update

Debian DSA-2901-1 : wordpress - security update

Debian DSA-2902-1 : curl - security update

Debian DSA-2903-1 : strongswan - security update

Debian DSA-2904-1 : virtualbox - security update

Debian DSA-2905-1 : chromium-browser - security update

Debian DSA-2906-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2908-1 : openssl - security update

Debian DSA-2909-1 : qemu - security update

Debian DSA-291-1 : ircii - buffer overflows

Debian DSA-2910-1 : qemu-kvm - security update

Debian DSA-2911-1 : icedove - security update

Debian DSA-2912-1 : openjdk-6 - security update

Debian DSA-2913-1 : drupal7 - security update

Debian DSA-2914-1 : drupal6 - security update

Debian DSA-2915-1 : dpkg - security update

Debian DSA-2916-1 : libmms - security update

Debian DSA-2917-1 : super - security update

Debian DSA-2918-1 : iceweasel - security update

Debian DSA-2919-1 : mysql-5.5 - security update

Debian DSA-292-3 : mime-support - insecure temporary file creation

Debian DSA-2920-1 : chromium-browser - security update

Debian DSA-2921-1 : xbuffy - security update

Debian DSA-2922-1 : strongswan - security update

Debian DSA-2923-1 : openjdk-7 - security update

Debian DSA-2924-1 : icedove - security update

Debian DSA-2925-1 : rxvt-unicode - security update

Debian DSA-2926-1 : linux - security update

Debian DSA-2927-1 : libxfont - security update

Debian DSA-2928-1 : linux-2.6 - privilege escalation/denial of service/information leak

Debian DSA-2929-1 : ruby-actionpack-3.2 - security update

Debian DSA-293-1 : kdelibs - insecure execution

Debian DSA-2930-1 : chromium-browser - security update

Debian DSA-2931-1 : openssl - security update

Debian DSA-2932-1 : qemu - security update

Debian DSA-2933-1 : qemu-kvm - security update

Debian DSA-2934-1 : python-django - security update

Debian DSA-2935-1 : libgadu - security update

Debian DSA-2936-1 : torque - security update

Debian DSA-2937-1 : mod-wsgi - security update

Debian DSA-2939-1 : chromium-browser - security update

Debian DSA-294-1 : gkrellm-newsticker - missing quoting, incomplete parser

Debian DSA-2940-1 : libstruts1.2-java - security update

Debian DSA-2941-1 : lxml - security update

Debian DSA-2942-1 : typo3-src - security update

Debian DSA-2943-1 : php5 - security update

Debian DSA-2944-1 : gnutls26 - security update

Debian DSA-2945-1 : chkrootkit - security update

Debian DSA-2946-1 : python-gnupg - security update

Debian DSA-2947-1 : libav - security update

Debian DSA-2948-1 : python-bottle - security update

Debian DSA-2949-1 : linux - security update

Debian DSA-295-1 : pptpd - buffer overflow

Debian DSA-2950-1 : openssl - security update

Debian DSA-2951-1 : mupdf - security update

Debian DSA-2952-1 : kfreebsd-9 - security update

Debian DSA-2953-1 : dpkg - security update

Debian DSA-2954-1 : dovecot - security update

Debian DSA-2955-1 : iceweasel - security update

Debian DSA-2956-1 : icinga - security update

Debian DSA-2957-1 : mediawiki - security update

Debian DSA-2958-1 : apt - security update

Debian DSA-2959-1 : chromium-browser - security update

Debian DSA-296-1 : kdebase - insecure execution

Debian DSA-2960-1 : icedove - security update

Debian DSA-2961-1 : php5 - security update

Debian DSA-2962-1 : nspr - security update

Debian DSA-2963-1 : lucene-solr - security update

Debian DSA-2964-1 : iodine - security update

Debian DSA-2965-1 : tiff - security update

Debian DSA-2966-1 : samba - security update

Debian DSA-2967-1 : gnupg - security update

Debian DSA-2968-1 : gnupg2 - security update

Debian DSA-2969-1 : libemail-address-perl - security update

Debian DSA-297-1 : snort - integer overflow, buffer overflow

Debian DSA-2970-1 : cacti - security update

Debian DSA-2971-1 : dbus - security update

Debian DSA-2972-1 : linux - security update

Debian DSA-2973-1 : vlc - security update

Debian DSA-2974-1 : php5 - security update

Debian DSA-2975-1 : phpmyadmin - security update

Debian DSA-2976-1 : eglibc - security update

Debian DSA-2977-1 : libav - security update

Debian DSA-2978-1 : libxml2 - security update

Debian DSA-2979-1 : fail2ban - security update

Debian DSA-298-1 : epic4 - buffer overflows

Debian DSA-2980-1 : openjdk-6 - security update

Debian DSA-2981-1 : polarssl - security update

Debian DSA-2982-1 : ruby-activerecord-3.2 - security update

Debian DSA-2983-1 : drupal7 - security update

Debian DSA-2984-1 : acpi-support - security update

Debian DSA-2985-1 : mysql-5.5 - security update

Debian DSA-2986-1 : iceweasel - security update

Debian DSA-2987-1 : openjdk-7 - security update

Debian DSA-2988-1 : transmission - security update

Debian DSA-2989-1 : apache2 - security update

Debian DSA-299-1 : leksbot - improper setuid-root execution

Debian DSA-2990-1 : cups - security update

Debian DSA-2991-1 : modsecurity-apache - security update

Debian DSA-2992-1 : linux - security update

Debian DSA-2993-1 : tor - security update

Debian DSA-2994-1 : nss - security update

Debian DSA-2995-1 : lzo2 - security update

Debian DSA-2996-1 : icedove - security update

Debian DSA-2997-1 : reportbug - security update

Debian DSA-2998-1 : openssl - security update

Debian DSA-2999-1 : drupal7 - security update

Debian DSA-300-1 : balsa - buffer overflow

Debian DSA-3000-1 : krb5 - security update

Debian DSA-3001-1 : wordpress - security update

Debian DSA-3002-1 : wireshark - security update

Debian DSA-3003-1 : libav - security update

Debian DSA-3004-1 : kde4libs - security update

Debian DSA-3005-1 : gpgme1.0 - security update

Debian DSA-3006-1 : xen - security update

Debian DSA-3007-1 : cacti - security update

Debian DSA-3008-1 : php5 - security update

Debian DSA-3009-1 : python-imaging - security update

Debian DSA-301-1 : libgtop - buffer overflow

Debian DSA-3010-1 : python-django - security update

Debian DSA-3011-1 : mediawiki - security update

Debian DSA-3012-1 : eglibc - security update

Debian DSA-3013-1 : s3ql - security update

Debian DSA-3014-1 : squid3 - security update

Debian DSA-3015-1 : lua5.1 - security update

Debian DSA-3016-1 : lua5.2 - security update

Debian DSA-3017-1 : php-cas - security update

Debian DSA-3018-1 : iceweasel - security update

Debian DSA-3019-1 : procmail - security update

Debian DSA-302-1 : fuzz - privilege escalation

Debian DSA-3020-1 : acpi-support - security update

Debian DSA-3021-1 : file - security update

Debian DSA-3022-1 : curl - security update

Debian DSA-3023-1 : bind9 - security update

Debian DSA-3024-1 : gnupg - security update

Debian DSA-3025-1 : apt - security update

Debian DSA-3026-1 : dbus - security update

Debian DSA-3027-1 : libav - security update

Debian DSA-3028-1 : icedove - security update

Debian DSA-3029-1 : nginx - security update

Debian DSA-303-1 : mysql - privilege escalation

Debian DSA-3030-1 : mantis - security update

Debian DSA-3031-1 : apt - security update

Debian DSA-3032-1 : bash - security update

Debian DSA-3033-1 : nss - security update

Debian DSA-3034-1 : iceweasel - security update

Debian DSA-3035-1 : bash - security update

Debian DSA-3036-1 : mediawiki - security update

Debian DSA-3037-1 : icedove - security update

Debian DSA-3038-1 : libvirt - security update

Debian DSA-3039-1 : chromium-browser - security update

Debian DSA-304-1 : lv - privilege escalation

Debian DSA-3040-1 : rsyslog - security update

Debian DSA-3041-1 : xen - security update

Debian DSA-3042-1 : exuberant-ctags - security update

Debian DSA-3043-1 : tryton-server - security update

Debian DSA-3044-1 : qemu-kvm - security update

Debian DSA-3045-1 : qemu - security update

Debian DSA-3046-1 : mediawiki - security update

Debian DSA-3047-1 : rsyslog - security update

Debian DSA-3048-1 : apt - security update

Debian DSA-3049-1 : wireshark - security update

Debian DSA-305-1 : sendmail - insecure temporary files

Debian DSA-3050-1 : iceweasel - security update

Debian DSA-3051-1 : drupal7 - security update

Debian DSA-3052-1 : wpa - security update

Debian DSA-3053-1 : openssl - security update (POODLE)

Debian DSA-3054-1 : mysql-5.5 - security update

Debian DSA-3055-1 : pidgin - security update

Debian DSA-3056-1 : libtasn1-3 - security update

Debian DSA-3057-1 : libxml2 - security update

Debian DSA-3058-1 : torque - security update

Debian DSA-3059-1 : dokuwiki - security update

Debian DSA-306-1 : ircii-pana - buffer overflows, integer overflow

Debian DSA-3060-1 : linux - security update

Debian DSA-3061-1 : icedove - security update

Debian DSA-3062-1 : wget - security update

Debian DSA-3063-1 : quassel - security update

Debian DSA-3064-1 : php5 - security update

Debian DSA-3065-1 : libxml-security-java - security update

Debian DSA-3066-1 : qemu - security update

Debian DSA-3067-1 : qemu-kvm - security update

Debian DSA-3068-1 : konversation - security update

Debian DSA-3069-1 : curl - security update

Debian DSA-307-1 : gps - multiple vulnerabilities

Debian DSA-3070-1 : kfreebsd-9 - security update

Debian DSA-3071-1 : nss - security update

Debian DSA-3072-1 : file - security update

Debian DSA-3073-1 : libgcrypt11 - security update

Debian DSA-3074-1 : php5 - security update

Debian DSA-3075-1 : drupal7 - security update

Debian DSA-3076-1 : wireshark - security update

Debian DSA-3077-1 : openjdk-6 - security update

Debian DSA-3078-1 : libksba - security update

Debian DSA-3079-1 : ppp - security update

Debian DSA-308-1 : gzip - insecure temporary files

Debian DSA-3080-1 : openjdk-7 - security update

Debian DSA-3081-1 : libvncserver - security update

Debian DSA-3082-1 : flac - security update

Debian DSA-3083-1 : mutt - security update

Debian DSA-3084-1 : openvpn - security update

Debian DSA-3085-1 : wordpress - security update

Debian DSA-3086-1 : tcpdump - security update

Debian DSA-3087-1 : qemu - security update

Debian DSA-3088-1 : qemu-kvm - security update

Debian DSA-3089-1 : jasper - security update

Debian DSA-309-1 : eterm - buffer overflow

Debian DSA-3090-1 : iceweasel - security update

Debian DSA-3091-1 : getmail4 - security update

Debian DSA-3092-1 : icedove - security update

Debian DSA-3093-1 : linux - security update

Debian DSA-3094-1 : bind9 - security update

Debian DSA-3095-1 : xorg-server - security update

Debian DSA-3096-1 : pdns-recursor - security update

Debian DSA-3097-1 : unbound - security update

Debian DSA-3098-1 : graphviz - security update

Debian DSA-3099-1 : dbus - security update

Debian DSA-310-1 : xaos - improper setuid-root execution

Debian DSA-3100-1 : mediawiki - security update

Debian DSA-3101-1 : c-icap - security update

Debian DSA-3102-1 : libyaml - security update

Debian DSA-3103-1 : libyaml-libyaml-perl - security update

Debian DSA-3104-1 : bsd-mailx - security update

Debian DSA-3105-1 : heirloom-mailx - security update

Debian DSA-3106-1 : jasper - security update

Debian DSA-3107-1 : subversion - security update

Debian DSA-3108-1 : ntp - security update

Debian DSA-3109-1 : firebird2.5 - security update

Debian DSA-311-1 : linux-kernel-2.4.18 - several vulnerabilities

Debian DSA-3110-1 : mediawiki - security update

Debian DSA-3111-1 : cpio - security update

Debian DSA-3112-1 : sox - security update

Debian DSA-3113-1 : unzip - security update

Debian DSA-3114-1 : mime-support - security update

Debian DSA-3115-1 : pyyaml - security update

Debian DSA-3116-1 : polarssl - security update

Debian DSA-3117-1 : php5 - security update

Debian DSA-3118-1 : strongswan - security update

Debian DSA-3119-1 : libevent - security update

Debian DSA-312-1 : kernel-patch-2.4.18-powerpc - several vulnerabilities

Debian DSA-3120-1 : mantis - security update

Debian DSA-3121-1 : file - security update

Debian DSA-3122-1 : curl - security update

Debian DSA-3123-1 : binutils - security update

Debian DSA-3124-1 : otrs2 - security update

Debian DSA-3125-1 : openssl - security update (FREAK)

Debian DSA-3126-1 : php5 - security update

Debian DSA-3127-1 : iceweasel - security update

Debian DSA-3128-1 : linux - security update

Debian DSA-3129-1 : rpm - security update

Debian DSA-313-1 : ethereal - buffer overflows, integer overflows

Debian DSA-3130-1 : lsyncd - security update

Debian DSA-3131-1 : xdg-utils - security update

Debian DSA-3132-1 : icedove - security update

Debian DSA-3133-1 : privoxy - security update

Debian DSA-3134-1 : sympa - security update

Debian DSA-3135-1 : mysql-5.5 - security update

Debian DSA-3136-1 : polarssl - security update

Debian DSA-3137-1 : websvn - security update

Debian DSA-3138-1 : jasper - security update

Debian DSA-3139-1 : squid - security update

Debian DSA-314-1 : atftp - buffer overflow

Debian DSA-3140-1 : xen - security update

Debian DSA-3141-1 : wireshark - security update

Debian DSA-3142-1 : eglibc - security update

Debian DSA-3143-1 : virtualbox - security update

Debian DSA-3144-1 : openjdk-7 - security update (POODLE)

Debian DSA-3145-1 : privoxy - security update

Debian DSA-3146-1 : requests - security update

Debian DSA-3147-1 : openjdk-6 - security update (POODLE)

Debian DSA-3149-1 : condor - security update

Debian DSA-315-1 : gnocatan - buffer overflows, denial of service

Debian DSA-3150-1 : vlc - security update

Debian DSA-3151-1 : python-django - security update

Debian DSA-3152-1 : unzip - security update

Debian DSA-3153-1 : krb5 - security update

Debian DSA-3154-1 : ntp - security update

Debian DSA-3155-1 : postgresql-9.1 - security update

Debian DSA-3156-1 : liblivemedia - security update

Debian DSA-3157-1 : ruby1.9.1 - security update

Debian DSA-3158-1 : unrtf - security update

Debian DSA-3159-1 : ruby1.8 - security update

Debian DSA-316-1 : nethack - buffer overflow, incorrect permissions

Debian DSA-3160-1 : xorg-server - security update

Debian DSA-3161-1 : dbus - security update

Debian DSA-3162-1 : bind9 - security update

Debian DSA-3163-1 : libreoffice - security update

Debian DSA-3164-1 : typo3-src - security update

Debian DSA-3165-1 : xdg-utils - security update

Debian DSA-3166-1 : e2fsprogs - security update

Debian DSA-3167-1 : sudo - security update

Debian DSA-3168-1 : ruby-redcloth - security update

Debian DSA-3169-1 : eglibc - security update

Debian DSA-317-1 : cupsys - denial of service

Debian DSA-3170-1 : linux - security update

Debian DSA-3171-1 : samba - security update

Debian DSA-3172-1 : cups - security update

Debian DSA-3173-1 : libgtk2-perl - security update

Debian DSA-3174-1 : iceweasel - security update

Debian DSA-3175-1 : kfreebsd-9 - security update

Debian DSA-3176-1 : request-tracker4 - security update

Debian DSA-3177-1 : mod-gnutls - security update

Debian DSA-3178-1 : unace - security update

Debian DSA-3179-1 : icedove - security update

Debian DSA-318-1 : lyskom-server - denial of service

Debian DSA-3180-1 : libarchive - security update

Debian DSA-3181-1 : xen - security update

Debian DSA-3182-1 : libssh2 - security update

Debian DSA-3183-1 : movabletype-opensource - security update

Debian DSA-3184-1 : gnupg - security update

Debian DSA-3185-1 : libgcrypt11 - security update

Debian DSA-3186-1 : nss - security update

Debian DSA-3187-1 : icu - security update

Debian DSA-3188-1 : freetype - security update

Debian DSA-3189-1 : libav - security update

Debian DSA-319-1 : webmin - session ID spoofing

Debian DSA-3190-1 : putty - security update

Debian DSA-3191-1 : gnutls26 - security update

Debian DSA-3192-1 : checkpw - security update

Debian DSA-3193-1 : tcpdump - security update

Debian DSA-3194-1 : libxfont - security update

Debian DSA-3195-1 : php5 - security update

Debian DSA-3196-1 : file - security update

Debian DSA-3197-1 : openssl - security update

Debian DSA-3198-1 : php5 - security update

Debian DSA-3199-1 : xerces-c - security update

Debian DSA-320-1 : mikmod - buffer overflow

Debian DSA-3200-1 : drupal7 - security update

Debian DSA-3201-1 : iceweasel - security update

Debian DSA-3202-1 : mono - security update

Debian DSA-3203-1 : tor - security update

Debian DSA-3204-1 : python-django - security update

Debian DSA-3205-1 : batik - security update

Debian DSA-3206-1 : dulwich - security update

Debian DSA-3207-1 : shibboleth-sp2 - security update

Debian DSA-3208-1 : freexl - security update

Debian DSA-3209-1 : openldap - security update

Debian DSA-321-1 : radiusd-cistron - buffer overflow

Debian DSA-3210-1 : wireshark - security update

Debian DSA-3211-1 : iceweasel - security update

Debian DSA-3212-1 : icedove - security update

Debian DSA-3213-1 : arj - security update

Debian DSA-3214-1 : mailman - security update

Debian DSA-3215-1 : libgd2 - security update

Debian DSA-3216-1 : tor - security update

Debian DSA-3217-1 : dpkg - security update

Debian DSA-3218-1 : wesnoth-1.10 - security update

Debian DSA-3219-1 : libdbd-firebird-perl - security update

Debian DSA-322-1 : typespeed - buffer overflow

Debian DSA-3220-1 : libtasn1-3 - security update

Debian DSA-3221-1 : das-watchdog - security update

Debian DSA-3222-1 : chrony - security update

Debian DSA-3223-1 : ntp - security update

Debian DSA-3224-1 : libx11 - security update

Debian DSA-3225-1 : gst-plugins-bad0.10 - security update

Debian DSA-3226-1 : inspircd - security update

Debian DSA-3227-1 : movabletype-opensource - security update

Debian DSA-3228-1 : ppp - security update

Debian DSA-3229-1 : mysql-5.5 - security update

Debian DSA-323-1 : noweb - insecure temporary files

Debian DSA-3230-1 : django-markupfield - security update

Debian DSA-3231-1 : subversion - security update

Debian DSA-3232-1 : curl - security update

Debian DSA-3233-1 : wpa - security update

Debian DSA-3234-1 : openjdk-6 - security update

Debian DSA-3235-1 : openjdk-7 - security update

Debian DSA-3236-1 : libreoffice - security update

Debian DSA-3237-1 : linux - security update

Debian DSA-3238-1 : chromium-browser - security update

Debian DSA-3239-1 : icecast2 - security update

Debian DSA-324-1 : ethereal - several vulnerabilities

Debian DSA-3240-1 : curl - security update

Debian DSA-3241-1 : elasticsearch - security update

Debian DSA-3242-1 : chromium-browser - security update

Debian DSA-3243-1 : libxml-libxml-perl - security update

Debian DSA-3244-1 : owncloud - security update

Debian DSA-3245-1 : ruby1.8 - security update

Debian DSA-3246-1 : ruby1.9.1 - security update

Debian DSA-3247-1 : ruby2.1 - security update

Debian DSA-3248-1 : libphp-snoopy - security update

Debian DSA-3249-1 : jqueryui - security update

Debian DSA-325-1 : eldav - insecure temporary file

Debian DSA-3250-1 : wordpress - security update

Debian DSA-3251-1 : dnsmasq - security update

Debian DSA-3252-1 : sqlite3 - security update

Debian DSA-3253-1 : pound - security update (POODLE)

Debian DSA-3254-1 : suricata - security update

Debian DSA-3255-1 : zeromq3 - security update

Debian DSA-3256-1 : libtasn1-6 - security update

Debian DSA-3257-1 : mercurial - security update

Debian DSA-3258-1 : quassel - security update

Debian DSA-3259-1 : qemu - security update (Venom)

Debian DSA-326-1 : orville-write - buffer overflows

Debian DSA-3260-1 : iceweasel - security update

Debian DSA-3261-1 : libmodule-signature-perl - security update

Debian DSA-3262-1 : xen - security update (Venom)

Debian DSA-3263-1 : proftpd-dfsg - security update

Debian DSA-3264-1 : icedove - security update

Debian DSA-3265-1 : zendframework - security update

Debian DSA-3266-1 : fuse - security update

Debian DSA-3267-1 : chromium-browser - security update

Debian DSA-3268-1 : ntfs-3g - security update

Debian DSA-3269-1 : postgresql-9.1 - security update

Debian DSA-327-1 : xbl - buffer overflows

Debian DSA-3270-1 : postgresql-9.4 - security update

Debian DSA-3271-1 : nbd - security update

Debian DSA-3272-1 : ipsec-tools - security update

Debian DSA-3273-1 : tiff - security update

Debian DSA-3274-1 : virtualbox - security update (Venom)

Debian DSA-3275-1 : fusionforge - security update

Debian DSA-3276-1 : symfony - security update

Debian DSA-3277-1 : wireshark - security update

Debian DSA-3278-1 : libapache-mod-jk - security update

Debian DSA-3279-1 : redis - security update

Debian DSA-328-1 : webfs - buffer overflow

Debian DSA-3280-1 : php5 - security update

Debian DSA-3282-1 : strongswan - security update

Debian DSA-3283-1 : cups - security update

Debian DSA-3284-1 : qemu - security update

Debian DSA-3285-1 : qemu-kvm - security update

Debian DSA-3286-1 : xen - security update

Debian DSA-3287-1 : openssl - security update (Logjam)

Debian DSA-3288-1 : libav - security update

Debian DSA-3289-1 : p7zip - security update

Debian DSA-329-1 : osh - buffer overflows

Debian DSA-3290-1 : linux - security update

Debian DSA-3291-1 : drupal7 - security update

Debian DSA-3292-1 : cinder - security update

Debian DSA-3293-1 : pyjwt - security update

Debian DSA-3294-1 : wireshark - security update

Debian DSA-3295-1 : cacti - security update

Debian DSA-3296-1 : libcrypto++ - security update

Debian DSA-3297-1 : unattended-upgrades - security update

Debian DSA-3298-1 : jackrabbit - security update

Debian DSA-3299-1 : stunnel4 - security update

Debian DSA-330-1 : tcptraceroute - failure to drop root privileges

Debian DSA-3300-1 : iceweasel - security update (Logjam)

Debian DSA-3301-1 : haproxy - security update

Debian DSA-3302-1 : libwmf - security update

Debian DSA-3303-1 : cups-filters - security update

Debian DSA-3304-1 : bind9 - security update

Debian DSA-3305-1 : python-django - security update

Debian DSA-3306-1 : pdns - security update

Debian DSA-3307-1 : pdns-recursor - security update

Debian DSA-3308-1 : mysql-5.5 - security update

Debian DSA-3309-1 : tidy - security update

Debian DSA-331-1 : imagemagick - insecure temporary file

Debian DSA-3310-1 : freexl - security update

Debian DSA-3311-1 : mariadb-10.0 - security update (BACKRONYM)

Debian DSA-3312-1 : cacti - security update

Debian DSA-3313-1 : linux - security update

Debian DSA-3315-1 : chromium-browser - security update

Debian DSA-3316-1 : openjdk-7 - security update (Bar Mitzvah) (Logjam)

Debian DSA-3317-1 : lxc - security update

Debian DSA-3318-1 : expat - security update

Debian DSA-3319-1 : bind9 - security update

Debian DSA-332-1 : linux-kernel-2.4.17 - several vulnerabilities

Debian DSA-3320-1 : openafs - security update

Debian DSA-3321-1 : xmltooling - security update

Debian DSA-3322-1 : ruby-rack - security update

Debian DSA-3323-1 : icu - security update

Debian DSA-3324-1 : icedove - security update (Logjam)

Debian DSA-3325-1 : apache2 - security update

Debian DSA-3326-1 : ghostscript - security update

Debian DSA-3327-1 : squid3 - security update

Debian DSA-3328-1 : wordpress - security update

Debian DSA-3329-1 : linux - security update

Debian DSA-333-1 : acm - integer overflow

Debian DSA-3330-1 : activemq - security update

Debian DSA-3331-1 : subversion - security update

Debian DSA-3332-1 : wordpress - security update

Debian DSA-3333-1 : iceweasel - security update

Debian DSA-3334-1 : gnutls28 - security update

Debian DSA-3335-1 : request-tracker4 - security update

Debian DSA-3336-1 : nss - security update

Debian DSA-3337-1 : gdk-pixbuf - security update

Debian DSA-3338-1 : python-django - security update

Debian DSA-3339-1 : openjdk-6 - security update (Bar Mitzvah) (Logjam)

Debian DSA-334-1 : xgalaga - buffer overflows

Debian DSA-3340-1 : zendframework - security update

Debian DSA-3341-1 : conntrack - security update

Debian DSA-3342-1 : vlc - security update

Debian DSA-3343-1 : twig - security update

Debian DSA-3344-1 : php5 - security update

Debian DSA-3345-1 : iceweasel - security update

Debian DSA-3346-1 : drupal7 - security update

Debian DSA-3347-1 : pdns - security update

Debian DSA-3348-1 : qemu - security update

Debian DSA-3349-1 : qemu-kvm - security update

Debian DSA-335-1 : mantis - incorrect permissions

Debian DSA-3350-1 : bind9 - security update

Debian DSA-3351-1 : chromium-browser - security update

Debian DSA-3352-1 : screen - security update

Debian DSA-3353-1 : openslp-dfsg - security update

Debian DSA-3354-1 : spice - security update

Debian DSA-3355-1 : libvdpau - security update

Debian DSA-3356-1 : openldap - security update

Debian DSA-3357-1 : vzctl - security update

Debian DSA-3358-1 : php5 - security update

Debian DSA-3359-1 : virtualbox - security update

Debian DSA-336-1 : linux-kernel-2.2.20 - several vulnerabilities

Debian DSA-3360-1 : icu - security update

Debian DSA-3361-1 : qemu - security update

Debian DSA-3362-1 : qemu-kvm - security update

Debian DSA-3363-1 : owncloud-client - security update

Debian DSA-3364-1 : linux - security update

Debian DSA-3365-1 : iceweasel - security update

Debian DSA-3366-1 : rpcbind - security update

Debian DSA-3367-1 : wireshark - security update

Debian DSA-3368-1 : cyrus-sasl2 - security update

Debian DSA-3369-1 : zendframework - security update

Debian DSA-337-1 : gtksee - buffer overflow

Debian DSA-3370-1 : freetype - security update

Debian DSA-3371-1 : spice - security update

Debian DSA-3372-1 : linux - security update

Debian DSA-3373-1 : owncloud - security update

Debian DSA-3374-1 : postgresql-9.4 - security update

Debian DSA-3375-1 : wordpress - security update

Debian DSA-3376-1 : chromium-browser - security update

Debian DSA-3377-1 : mysql-5.5 - security update

Debian DSA-3378-1 : gdk-pixbuf - security update

Debian DSA-3379-1 : miniupnpc - security update

Debian DSA-338-1 : proftpd - SQL injection

Debian DSA-3380-1 : php5 - security update

Debian DSA-3381-1 : openjdk-7 - security update

Debian DSA-3382-1 : phpmyadmin - security update

Debian DSA-3383-1 : wordpress - security update

Debian DSA-3384-1 : virtualbox - security update

Debian DSA-3385-1 : mariadb-10.0 - security update

Debian DSA-3386-1 : unzip - security update

Debian DSA-3387-1 : openafs - security update

Debian DSA-3388-1 : ntp - security update

Debian DSA-339-1 : semi - insecure temporary file

Debian DSA-3390-1 : xen - security update

Debian DSA-3391-1 : php-horde - security update

Debian DSA-3392-1 : freeimage - security update

Debian DSA-3393-1 : iceweasel - security update

Debian DSA-3394-1 : libreoffice - security update

Debian DSA-3395-1 : krb5 - security update

Debian DSA-3396-1 : linux - security update

Debian DSA-3397-1 : wpa - security update

Debian DSA-3398-1 : strongswan - security update

Debian DSA-3399-1 : libpng - security update

Debian DSA-340-1 : x-face-el - insecure temporary file

Debian DSA-3400-1 : lxc - security update

Debian DSA-3401-1 : openjdk-7 - security update

Debian DSA-3402-1 : symfony - security update

Debian DSA-3403-1 : libcommons-collections3-java - security update

Debian DSA-3404-1 : python-django - security update

Debian DSA-3405-1 : smokeping - security update

Debian DSA-3406-1 : nspr - security update

Debian DSA-3407-1 : dpkg - security update

Debian DSA-3408-1 : gnutls26 - security update

Debian DSA-3409-1 : putty - security update

Debian DSA-341-1 : liece - insecure temporary file

Debian DSA-3410-1 : icedove - security update

Debian DSA-3411-1 : cups-filters - security update

Debian DSA-3412-1 : redis - security update

Debian DSA-3413-1 : openssl - security update

Debian DSA-3414-1 : xen - security update

Debian DSA-3415-1 : chromium-browser - security update

Debian DSA-3416-1 : libphp-phpmailer - security update

Debian DSA-3417-1 : bouncycastle - security update

Debian DSA-3418-1 : chromium-browser - security update

Debian DSA-3419-1 : cups-filters - security update

Debian DSA-342-1 : mozart - unsafe mailcap configuration

Debian DSA-3420-1 : bind9 - security update

Debian DSA-3421-1 : grub2 - security update

Debian DSA-3422-1 : iceweasel - security update

Debian DSA-3423-1 : cacti - security update

Debian DSA-3424-1 : subversion - security update

Debian DSA-3425-1 : tryton-server - security update

Debian DSA-3426-1 : Linux Security Update

Debian DSA-3426-2 : ctdb - security update

Debian DSA-3427-1 : blueman - security update

Debian DSA-3428-1 : tomcat8 - security update

Debian DSA-3429-1 : foomatic-filters - security update

Debian DSA-343-1 : skk, ddskk - insecure temporary file

Debian DSA-3430-1 : libxml2 - security update

Debian DSA-3431-1 : ganeti - security update

Debian DSA-3432-1 : icedove - security update

Debian DSA-3433-1 : samba - security update

Debian DSA-3434-1 : linux - security update

Debian DSA-3435-1 : git - security update

Debian DSA-3436-1 : openssl - security update (SLOTH)

Debian DSA-3437-1 : gnutls26 - security update (SLOTH)

Debian DSA-3438-1 : xscreensaver - security update

Debian DSA-3439-1 : prosody - security update

Debian DSA-344-2 : unzip - directory traversal

Debian DSA-3440-1 : sudo - security update

Debian DSA-3441-1 : perl - security update

Debian DSA-3442-1 : isc-dhcp - security update

Debian DSA-3443-1 : libpng - security update

Debian DSA-3444-1 : wordpress - security update

Debian DSA-3445-1 : pygments - security update

Debian DSA-3446-1 : openssh - security update

Debian DSA-3447-1 : tomcat7 - security update

Debian DSA-3448-1 : linux - security update

Debian DSA-3449-1 : bind9 - security update

Debian DSA-345-1 : xbl - buffer overflow

Debian DSA-3450-1 : ecryptfs-utils - security update

Debian DSA-3451-1 : fuse - security update

Debian DSA-3452-1 : claws-mail - security update

Debian DSA-3453-1 : mariadb-10.0 - security update

Debian DSA-3454-1 : virtualbox - security update

Debian DSA-3455-1 : curl - security update

Debian DSA-3456-1 : chromium-browser - security update

Debian DSA-3457-1 : iceweasel - security update (SLOTH)

Debian DSA-3458-1 : openjdk-7 - security update (SLOTH)

Debian DSA-3459-1 : mysql-5.5 - security update

Debian DSA-346-1 : phpsysinfo - directory traversal

Debian DSA-3460-1 : privoxy - security update

Debian DSA-3461-1 : freetype - security update

Debian DSA-3462-1 : radicale - security update

Debian DSA-3463-1 : prosody - security update

Debian DSA-3464-1 : rails - security update

Debian DSA-3465-1 : openjdk-6 - security update (SLOTH)

Debian DSA-3466-1 : krb5 - security update

Debian DSA-3467-1 : tiff - security update

Debian DSA-3468-1 : polarssl - security update

Debian DSA-3469-1 : qemu - security update

Debian DSA-347-1 : teapop - SQL injection

Debian DSA-3470-1 : qemu-kvm - security update

Debian DSA-3471-1 : qemu - security update

Debian DSA-3472-1 : wordpress - security update

Debian DSA-3473-1 : nginx - security update

Debian DSA-3474-1 : libgcrypt20 - security update

Debian DSA-3475-1 : postgresql-9.1 - security update

Debian DSA-3476-1 : postgresql-9.4 - security update

Debian DSA-3477-1 : iceweasel - security update

Debian DSA-3478-1 : libgcrypt11 - security update

Debian DSA-3479-1 : graphite2 - security update

Debian DSA-348-1 : traceroute-nanog - integer overflow, buffer overflow

Debian DSA-3480-1 : eglibc - security update

Debian DSA-3481-1 : glibc - security update

Debian DSA-3482-1 : libreoffice - security update

Debian DSA-3483-1 : cpio - security update

Debian DSA-3484-1 : xdelta3 - security update

Debian DSA-3485-1 : didiwiki - security update

Debian DSA-3486-1 : chromium-browser - security update

Debian DSA-3487-1 : libssh2 - security update

Debian DSA-3488-1 : libssh - security update

Debian DSA-3489-1 : lighttpd - security update (POODLE)

Debian DSA-349-1 : nfs-utils - buffer overflow

Debian DSA-3490-1 : websvn - security update

Debian DSA-3491-1 : icedove - security update (SLOTH)

Debian DSA-3492-2 : gajim - security update

Debian DSA-3493-1 : xerces-c - security update

Debian DSA-3494-1 : cacti - security update

Debian DSA-3495-1 : xymon - security update

Debian DSA-3496-1 : php-horde-core - security update

Debian DSA-3497-1 : php-horde - security update

Debian DSA-3498-1 : drupal7 - security update

Debian DSA-3499-1 : pillow - security update

Debian DSA-350-1 : falconseye - buffer overflow

Debian DSA-3500-1 : openssl - security update

Debian DSA-3501-1 : perl - security update

Debian DSA-3502-1 : roundup - security update

Debian DSA-3503-1 : linux - security update

Debian DSA-3504-1 : bsh - security update

Debian DSA-3505-1 : wireshark - security update

Debian DSA-3506-1 : libav - security update

Debian DSA-3507-1 : chromium-browser - security update

Debian DSA-3508-1 : jasper - security update

Debian DSA-3509-1 : rails - security update

Debian DSA-351-1 : php4 - XSS

Debian DSA-3510-1 : iceweasel - security update

Debian DSA-3511-1 : bind9 - security update

Debian DSA-3512-1 : libotr - security update

Debian DSA-3513-1 : chromium-browser - security update

Debian DSA-3514-1 : samba - security update

Debian DSA-3515-1 : graphite2 - security update

Debian DSA-3516-1 : wireshark - security update

Debian DSA-3517-1 : exim4 - security update

Debian DSA-3518-1 : spip - security update

Debian DSA-3519-1 : xen - security update

Debian DSA-352-1 : fdclone - insecure temporary directory

Debian DSA-3520-1 : icedove - security update

Debian DSA-3521-1 : git - security update

Debian DSA-3522-1 : squid3 - security update

Debian DSA-3523-1 : iceweasel - security update

Debian DSA-3524-1 : activemq - security update

Debian DSA-3525-1 : pixman - security update

Debian DSA-3526-1 : libmatroska - security update

Debian DSA-3527-1 : inspircd - security update

Debian DSA-3528-1 : pidgin-otr - security update

Debian DSA-3529-1 : redmine - security update

Debian DSA-353-1 : sup - insecure temporary file

Debian DSA-3530-1 : tomcat6 - security update

Debian DSA-3531-1 : chromium-browser - security update

Debian DSA-3532-1 : quagga - security update

Debian DSA-3533-1 : openvswitch - security update

Debian DSA-3534-1 : dhcpcd - security update

Debian DSA-3535-1 : kamailio - security update

Debian DSA-3536-1 : libstruts1.2-java - security update

Debian DSA-3537-1 : imlib2 - security update

Debian DSA-3538-1 : libebml - security update

Debian DSA-3539-1 : srtp - security update

Debian DSA-354-1 : xconq - buffer overflows

Debian DSA-3540-1 : lhasa - security update

Debian DSA-3541-1 : roundcube - security update

Debian DSA-3542-1 : mercurial - security update

Debian DSA-3543-1 : oar - security update

Debian DSA-3544-1 : python-django - security update

Debian DSA-3545-1 : cgit - security update

Debian DSA-3546-1 : optipng - security update

Debian DSA-3547-1 : imagemagick - security update

Debian DSA-3548-1 : samba - security update (Badlock)

Debian DSA-3549-1 : chromium-browser - security update

Debian DSA-355-1 : gallery - XSS

Debian DSA-3550-1 : openssh - security update

Debian DSA-3551-1 : fuseiso - security update

Debian DSA-3552-1 : tomcat7 - security update

Debian DSA-3553-1 : varnish - security update

Debian DSA-3554-1 : xen - security update

Debian DSA-3555-1 : imlib2 - security update

Debian DSA-3556-1 : libgd2 - security update

Debian DSA-3557-1 : mysql-5.5 - security update

Debian DSA-3558-1 : openjdk-7 - security update

Debian DSA-3559-1 : iceweasel - security update

Debian DSA-356-1 : xtokkaetama - buffer overflows

Debian DSA-3560-1 : php5 - security update

Debian DSA-3561-1 : subversion - security update

Debian DSA-3562-1 : tardiff - security update

Debian DSA-3563-1 : poppler - security update

Debian DSA-3564-1 : chromium-browser - security update

Debian DSA-3565-1 : botan1.10 - security update

Debian DSA-3566-1 : openssl - security update

Debian DSA-3567-1 : libpam-sshauth - security update

Debian DSA-3568-1 : libtasn1-6 - security update

Debian DSA-3569-1 : openafs - security update

Debian DSA-357-1 : wu-ftpd - remote root exploit

Debian DSA-3570-1 : mercurial - security update

Debian DSA-3571-1 : ikiwiki - security update

Debian DSA-3572-1 : websvn - security update

Debian DSA-3573-1 : qemu - security update

Debian DSA-3574-1 : libarchive - security update

Debian DSA-3575-1 : libxstream-java - security update

Debian DSA-3576-1 : icedove - security update

Debian DSA-3577-1 : jansson - security update

Debian DSA-3578-1 : libidn - security update

Debian DSA-3579-1 : xerces-c - security update

Debian DSA-358-4 : linux-kernel-2.4.18 - several vulnerabilities

Debian DSA-3580-1 : imagemagick - security update (ImageTragick)

Debian DSA-3581-1 : libndp - security update

Debian DSA-3582-1 : expat - security update

Debian DSA-3583-1 : swift-plugin-s3 - security update

Debian DSA-3584-1 : librsvg - security update

Debian DSA-3585-1 : wireshark - security update

Debian DSA-3586-1 : atheme-services - security update

Debian DSA-3587-1 : libgd2 - security update

Debian DSA-3588-1 : symfony - security update

Debian DSA-3589-1 : gdk-pixbuf - security update

Debian DSA-359-1 : atari800 - buffer overflows

Debian DSA-3590-1 : chromium-browser - security update

Debian DSA-3591-1 : imagemagick - security update

Debian DSA-3592-1 : nginx - security update

Debian DSA-3593-1 : libxml2 - security update

Debian DSA-3594-1 : chromium-browser - security update

Debian DSA-3595-1 : mariadb-10.0 - security update

Debian DSA-3596-1 : spice - security update

Debian DSA-3597-1 : expat - security update

Debian DSA-3598-1 : vlc - security update

Debian DSA-3599-1 : p7zip - security update

Debian DSA-360-1 : xfstt - several vulnerabilities

Debian DSA-3600-1 : firefox-esr - security update

Debian DSA-3601-1 : icedove - security update

Debian DSA-3602-1 : php5 - security update

Debian DSA-3603-1 : libav - security update

Debian DSA-3604-1 : drupal7 - security update

Debian DSA-3605-1 : libxslt - security update

Debian DSA-3606-1 : libpdfbox-java - security update

Debian DSA-3607-1 : linux - security update

Debian DSA-3608-1 : libreoffice - security update

Debian DSA-3609-1 : tomcat8 - security update

Debian DSA-361-2 : kdelibs, kdelibs-crypto - several vulnerabilities

Debian DSA-3610-1 : xerces-c - security update

Debian DSA-3611-1 : libcommons-fileupload-java - security update

Debian DSA-3612-1 : gimp - security update

Debian DSA-3613-1 : libvirt - security update

Debian DSA-3614-1 : tomcat7 - security update

Debian DSA-3615-1 : wireshark - security update

Debian DSA-3616-1 : linux - security update

Debian DSA-3617-1 : horizon - security update

Debian DSA-3618-1 : php5 - security update

Debian DSA-3619-1 : libgd2 - security update

Debian DSA-362-1 : mindi - insecure temporary file

Debian DSA-3620-1 : pidgin - security update

Debian DSA-3621-1 : mysql-connector-java - security update

Debian DSA-3622-1 : python-django - security update

Debian DSA-3623-1 : apache2 - security update (httpoxy)

Debian DSA-3624-1 : mysql-5.5 - security update

Debian DSA-3625-1 : squid3 - security update

Debian DSA-3626-1 : openssh - security update

Debian DSA-3627-1 : phpmyadmin - security update

Debian DSA-3628-1 : perl - security update

Debian DSA-3629-1 : ntp - security update

Debian DSA-363-1 : postfix - denial of service, bounce-scanning

Debian DSA-3630-1 : libgd2 - security update

Debian DSA-3631-1 : php5 - security update (httpoxy)

Debian DSA-3632-1 : mariadb-10.0 - security update

Debian DSA-3633-1 : xen - security update (Bunker Buster)

Debian DSA-3634-1 : redis - security update

Debian DSA-3635-1 : libdbd-mysql-perl - security update

Debian DSA-3636-1 : collectd - security update

Debian DSA-3637-1 : chromium-browser - security update

Debian DSA-3638-1 : curl - security update

Debian DSA-3639-1 : wordpress - security update

Debian DSA-364-3 : man-db - buffer overflows, arbitrary command execution

Debian DSA-3640-1 : firefox-esr - security update

Debian DSA-3641-1 : openjdk-7 - security update

Debian DSA-3642-1 : lighttpd - security update

Debian DSA-3643-1 : kde4libs - security update

Debian DSA-3644-1 : fontconfig - security update

Debian DSA-3645-1 : chromium-browser - security update

Debian DSA-3646-1 : postgresql-9.4 - security update

Debian DSA-3647-1 : icedove - security update

Debian DSA-3648-1 : wireshark - security update

Debian DSA-3649-1 : gnupg - security update

Debian DSA-365-1 : phpgroupware - several vulnerabilities

Debian DSA-3650-1 : libgcrypt20 - security update

Debian DSA-3651-1 : rails - security update

Debian DSA-3652-1 : imagemagick - security update

Debian DSA-3653-1 : flex - security update

Debian DSA-3654-1 : quagga - security update

Debian DSA-3655-1 : mupdf - security update

Debian DSA-3656-1 : tryton-server - security update

Debian DSA-3657-1 : libarchive - security update

Debian DSA-3658-1 : libidn - security update

Debian DSA-3659-1 : linux - security update

Debian DSA-366-1 : eroaster - insecure temporary file

Debian DSA-3660-1 : chromium-browser - security update

Debian DSA-3661-1 : charybdis - security update

Debian DSA-3662-1 : inspircd - security update

Debian DSA-3663-1 : xen - security update

Debian DSA-3664-1 : pdns - security update

Debian DSA-3665-1 : openjpeg2 - security update

Debian DSA-3666-1 : mysql-5.5 - security update

Debian DSA-3667-1 : chromium-browser - security update

Debian DSA-3668-1 : mailman - security update

Debian DSA-3669-1 : tomcat7 - security update

Debian DSA-367-1 : xtokkaetama - buffer overflow

Debian DSA-3670-1 : tomcat8 - security update

Debian DSA-3671-1 : wireshark - security update

Debian DSA-3672-1 : irssi - security update

Debian DSA-3673-1 : openssl - security update

Debian DSA-3674-1 : firefox-esr - security update

Debian DSA-3675-1 : imagemagick - security update

Debian DSA-3676-1 : unadf - security update

Debian DSA-3677-1 : libarchive - security update

Debian DSA-3678-1 : python-django - security update

Debian DSA-3679-1 : jackrabbit - security update

Debian DSA-368-1 : xpcd - buffer overflow

Debian DSA-3680-1 : bind9 - security update

Debian DSA-3681-1 : wordpress - security update

Debian DSA-3682-1 : c-ares - security update

Debian DSA-3683-1 : chromium-browser - security update

Debian DSA-3684-1 : libdbd-mysql-perl - security update

Debian DSA-3685-1 : libav - security update

Debian DSA-3686-1 : icedove - security update

Debian DSA-3687-1 : nspr - security update

Debian DSA-3688-1 : nss - security update (Logjam) (SLOTH)

Debian DSA-3689-1 : php5 - security update

Debian DSA-369-1 : zblast - buffer overflow

Debian DSA-3690-1 : icedove - security update

Debian DSA-3691-1 : ghostscript - security update

Debian DSA-3692-1 : freeimage - security update

Debian DSA-3693-1 : libgd2 - security update

Debian DSA-3694-1 : tor - security update

Debian DSA-3695-1 : quagga - security update

Debian DSA-3696-1 : linux - security update (Dirty COW)

Debian DSA-3697-1 : kdepimlibs - security update

Debian DSA-3698-1 : php5 - security update

Debian DSA-370-1 : pam-pgsql - format string

Debian DSA-3700-1 : asterisk - security update

Debian DSA-3701-1 : nginx - security update

Debian DSA-3702-1 : tar - security update

Debian DSA-3703-1 : bind9 - security update

Debian DSA-3704-1 : memcached - security update

Debian DSA-3705-1 : curl - security update

Debian DSA-3706-1 : mysql-5.5 - security update

Debian DSA-3707-1 : openjdk-7 - security update

Debian DSA-3708-1 : mat - security update

Debian DSA-3709-1 : libxslt - security update

Debian DSA-371-1 : perl - XSS

Debian DSA-3710-1 : pillow - security update

Debian DSA-3711-1 : mariadb-10.0 - security update

Debian DSA-3712-1 : terminology - security update

Debian DSA-3713-1 : gst-plugins-bad0.10 - security update

Debian DSA-3715-1 : moin - security update

Debian DSA-3716-1 : firefox-esr - security update

Debian DSA-3717-1 : gst-plugins-bad1.0, gst-plugins-bad0.10 - security update

Debian DSA-3718-1 : drupal7 - security update

Debian DSA-3719-1 : wireshark - security update

Debian DSA-372-1 : netris - buffer overflow

Debian DSA-3720-1 : tomcat8 - security update

Debian DSA-3721-1 : tomcat7 - security update

Debian DSA-3722-1 : vim - security update

Debian DSA-3723-1 : gst-plugins-good1.0 - security update

Debian DSA-3724-1 : gst-plugins-good0.10 - security update

Debian DSA-3725-1 : icu - security update

Debian DSA-3726-1 : imagemagick - security update

Debian DSA-3727-1 : hdf5 - security update

Debian DSA-3728-1 : firefox-esr - security update

Debian DSA-3729-1 : xen - security update

Debian DSA-373-1 : autorespond - buffer overflow

Debian DSA-3730-1 : icedove - security update

Debian DSA-3731-1 : chromium-browser - security update

Debian DSA-3732-1 : php5 - security update

Debian DSA-3733-1 : apt - security update

Debian DSA-3734-1 : firefox-esr - security update

Debian DSA-3735-1 : game-music-emu - security update

Debian DSA-3736-1 : libupnp - security update

Debian DSA-3737-1 : php5 - security update

Debian DSA-3738-1 : tomcat7 - security update

Debian DSA-3739-1 : tomcat8 - security update

Debian DSA-374-1 : libpam-smb - buffer overflow

Debian DSA-3740-1 : samba - security update

Debian DSA-3741-1 : tor - security update

Debian DSA-3742-1 : flightgear - security update

Debian DSA-3743-1 : python-bottle - security update

Debian DSA-3744-1 : libxml2 - security update

Debian DSA-3745-1 : squid3 - security update

Debian DSA-3746-1 : graphicsmagick - security update (ImageTragick)

Debian DSA-3747-1 : exim4 - security update

Debian DSA-3748-1 : libcrypto++ - security update

Debian DSA-3749-1 : dcmtk - security update

Debian DSA-375-1 : node - buffer overflow, format string

Debian DSA-3750-1 : libphp-phpmailer - security update

Debian DSA-3751-1 : libgd2 - security update

Debian DSA-3752-1 : pcsc-lite - security update

Debian DSA-3753-1 : libvncserver - security update

Debian DSA-3754-1 : tomcat7 - security update

Debian DSA-3755-1 : tomcat8 - security update

Debian DSA-3756-1 : icoutils - security update

Debian DSA-3757-1 : icedove - security update

Debian DSA-3758-1 : bind9 - security update

Debian DSA-3759-1 : python-pysaml2 - security update

Debian DSA-376-2 : exim - buffer overflow

Debian DSA-3760-1 : ikiwiki - security update

Debian DSA-3761-1 : rabbitmq-server - security update

Debian DSA-3762-1 : tiff - security update

Debian DSA-3763-1 : pdns-recursor - security update

Debian DSA-3764-1 : pdns - security update

Debian DSA-3765-1 : icoutils - security update

Debian DSA-3766-1 : mapserver - security update

Debian DSA-3767-1 : mysql-5.5 - security update

Debian DSA-3768-1 : openjpeg2 - security update

Debian DSA-3769-1 : libphp-swiftmailer - security update

Debian DSA-377-1 : wu-ftpd - insecure program execution

Debian DSA-3770-1 : mariadb-10.0 - security update

Debian DSA-3771-1 : firefox-esr - security update

Debian DSA-3772-1 : libxpm - security update

Debian DSA-3773-1 : openssl - security update

Debian DSA-3774-1 : lcms2 - security update

Debian DSA-3775-1 : tcpdump - security update

Debian DSA-3776-1 : chromium-browser - security update

Debian DSA-3777-1 : libgd2 - security update

Debian DSA-3778-1 : ruby-archive-tar-minitar - security update

Debian DSA-3779-1 : wordpress - security update

Debian DSA-378-1 : mah-jong - buffer overflows, denial of service

Debian DSA-3780-1 : ntfs-3g - security update

Debian DSA-3781-1 : svgsalamander - security update

Debian DSA-3782-1 : openjdk-7 - security update

Debian DSA-3783-1 : php5 - security update

Debian DSA-3784-1 : viewvc - security update

Debian DSA-3785-1 : jasper - security update

Debian DSA-3786-1 : vim - security update

Debian DSA-3787-1 : tomcat7 - security update

Debian DSA-3788-1 : tomcat8 - security update

Debian DSA-3789-1 : libevent - security update

Debian DSA-379-1 : sane-backends - several vulnerabilities

Debian DSA-3790-1 : spice - security update

Debian DSA-3791-1 : linux - security update

Debian DSA-3792-1 : libreoffice - security update

Debian DSA-3793-1 : shadow - security update

Debian DSA-3794-1 : munin - security update

Debian DSA-3795-1 : bind9 - security update

Debian DSA-3796-1 : apache2 - security update

Debian DSA-3797-1 : mupdf - security update

Debian DSA-3798-1 : tnef - security update

Debian DSA-3799-1 : imagemagick - security update

Debian DSA-380-1 : xfree86 - buffer overflows, denial of service

Debian DSA-3800-1 : libquicktime - security update

Debian DSA-3801-1 : ruby-zip - security update

Debian DSA-3802-1 : zabbix - security update

Debian DSA-3803-1 : texlive-base - security update

Debian DSA-3804-1 : linux - security update

Debian DSA-3805-1 : firefox-esr - security update

Debian DSA-3806-1 : pidgin - security update

Debian DSA-3807-1 : icoutils - security update

Debian DSA-3808-1 : imagemagick - security update

Debian DSA-3809-1 : mariadb-10.0 - security update

Debian DSA-381-1 : mysql - buffer overflow

Debian DSA-3810-1 : chromium-browser - security update

Debian DSA-3811-1 : wireshark - security update

Debian DSA-3812-1 : ioquake3 - security update

Debian DSA-3813-1 : r-base - security update

Debian DSA-3814-1 : audiofile - security update

Debian DSA-3815-1 : wordpress - security update

Debian DSA-3816-1 : samba - security update

Debian DSA-3817-1 : jbig2dec - security update

Debian DSA-3818-1 : gst-plugins-bad1.0 - security update

Debian DSA-3819-1 : gst-plugins-base1.0 - security update

Debian DSA-382-3 : ssh - possible remote vulnerability

Debian DSA-3820-1 : gst-plugins-good1.0 - security update

Debian DSA-3821-1 : gst-plugins-ugly1.0 - security update

Debian DSA-3822-1 : gstreamer1.0 - security update

Debian DSA-3823-1 : eject - security update

Debian DSA-3824-1 : firebird2.5 - security update

Debian DSA-3825-1 : jhead - security update

Debian DSA-3826-1 : tryton-server - security update

Debian DSA-3827-1 : jasper - security update

Debian DSA-3828-1 : dovecot - security update

Debian DSA-3829-1 : bouncycastle - security update

Debian DSA-383-2 : ssh-krb5 - possible remote vulnerability

Debian DSA-3830-1 : icu - security update

Debian DSA-3831-1 : firefox-esr - security update

Debian DSA-3832-1 : icedove - security update

Debian DSA-3833-1 : libav - security update

Debian DSA-3834-1 : mysql-5.5 - security update (Riddle)

Debian DSA-3835-1 : python-django - security update

Debian DSA-3836-1 : weechat - security update

Debian DSA-3837-1 : libreoffice - security update

Debian DSA-3838-1 : ghostscript - security update

Debian DSA-3839-1 : freetype - security update

Debian DSA-384-1 : sendmail - buffer overflows

Debian DSA-3840-1 : mysql-connector-java - security update

Debian DSA-3841-1 : libxstream-java - security update

Debian DSA-3842-1 : tomcat7 - security update

Debian DSA-3843-1 : tomcat8 - security update

Debian DSA-3844-1 : tiff - security update

Debian DSA-3845-1 : libtirpc - security update

Debian DSA-3846-1 : libytnef - security update

Debian DSA-3847-1 : xen - security update

Debian DSA-3848-1 : git - security update

Debian DSA-3849-1 : kde4libs - security update

Debian DSA-385-1 : hztty - buffer overflows

Debian DSA-3850-1 : rtmpdump - security update

Debian DSA-3851-1 : postgresql-9.4 - security update

Debian DSA-3852-1 : squirrelmail - security update

Debian DSA-3853-1 : bitlbee - security update

Debian DSA-3854-1 : bind9 - security update

Debian DSA-3855-1 : jbig2dec - security update

Debian DSA-3856-1 : deluge - security update

Debian DSA-3857-1 : mysql-connector-java - security update

Debian DSA-3858-1 : openjdk-7 - security update

Debian DSA-3859-1 : dropbear - security update

Debian DSA-386-1 : libmailtools-perl - input validation bug

Debian DSA-3860-1 : samba - security update (SambaCry)

Debian DSA-3861-1 : libtasn1-6 - security update

Debian DSA-3862-1 : puppet - security update

Debian DSA-3863-1 : imagemagick - security update

Debian DSA-3864-1 : fop - security update

Debian DSA-3865-1 : mosquitto - security update

Debian DSA-3866-1 : strongswan - security update

Debian DSA-3867-1 : sudo - security update

Debian DSA-3868-1 : openldap - security update

Debian DSA-3869-1 : tnef - security update

Debian DSA-387-1 : gopher - buffer overflows

Debian DSA-3870-1 : wordpress - security update

Debian DSA-3871-1 : zookeeper - security update

Debian DSA-3872-1 : nss - security update

Debian DSA-3873-1 : perl - security update

Debian DSA-3874-1 : ettercap - security update

Debian DSA-3875-1 : libmwaw - security update

Debian DSA-3876-1 : otrs2 - security update

Debian DSA-3877-1 : tor - security update

Debian DSA-3878-1 : zziplib - security update

Debian DSA-3879-1 : libosip2 - security update

Debian DSA-388-1 : kdebase - several vulnerabilities

Debian DSA-3880-1 : libgcrypt20 - security update

Debian DSA-3881-1 : firefox-esr - security update

Debian DSA-3882-1 : request-tracker4 - security update

Debian DSA-3883-1 : rt-authen-externalauth - security update

Debian DSA-3884-1 : gnutls28 - security update

Debian DSA-3885-1 : irssi - security update

Debian DSA-3886-1 : linux - security update (Stack Clash)

Debian DSA-3887-1 : glibc - security update (Stack Clash)

Debian DSA-3888-1 : exim4 - security update (Stack Clash)

Debian DSA-3889-1 : libffi - security update (Stack Clash)

Debian DSA-389-1 : ipmasq - insecure packet filtering rules

Debian DSA-3890-1 : spip - security update

Debian DSA-3891-1 : tomcat8 - security update

Debian DSA-3892-1 : tomcat7 - security update

Debian DSA-3893-1 : jython - security update

Debian DSA-3894-1 : graphite2 - security update

Debian DSA-3895-1 : flatpak - security update

Debian DSA-3896-1 : apache2 - security update

Debian DSA-3897-1 : drupal7 - security update

Debian DSA-3898-1 : expat - security update

Debian DSA-3899-1 : vlc - security update

Debian DSA-390-1 : marbles - buffer overflow

Debian DSA-3900-1 : openvpn - security update

Debian DSA-3901-1 : libgcrypt20 - security update

Debian DSA-3902-1 : jabberd2 - security update

Debian DSA-3903-1 : tiff - security update

Debian DSA-3904-1 : bind9 - security update

Debian DSA-3905-1 : xorg-server - security update

Debian DSA-3906-1 : undertow - security update

Debian DSA-3907-1 : spice - security update

Debian DSA-3908-1 : nginx - security update

Debian DSA-3909-1 : samba - security update (Orpheus' Lyre)

Debian DSA-391-1 : freesweep - buffer overflow

Debian DSA-3910-1 : knot - security update

Debian DSA-3911-1 : evince - security update

Debian DSA-3912-1 : heimdal - security update (Orpheus' Lyre)

Debian DSA-3913-1 : apache2 - security update

Debian DSA-3914-1 : imagemagick - security update

Debian DSA-3915-1 : ruby-mixlib-archive - security update

Debian DSA-3916-1 : atril - security update

Debian DSA-3917-1 : catdoc - security update

Debian DSA-3918-1 : icedove - security update

Debian DSA-3919-1 : openjdk-8 - security update

Debian DSA-392-1 : webfs - buffer overflows, file and directory exposure

Debian DSA-3920-1 : qemu - security update

Debian DSA-3921-1 : enigmail - security update

Debian DSA-3922-1 : mysql-5.5 - security update

Debian DSA-3923-1 : freerdp - security update

Debian DSA-3924-1 : varnish - security update

Debian DSA-3925-1 : qemu - security update

Debian DSA-3926-1 : chromium-browser - security update

Debian DSA-3927-1 : linux - security update (Stack Clash)

Debian DSA-3928-1 : firefox-esr - security update

Debian DSA-3929-1 : libsoup2.4 - security update

Debian DSA-393-1 : openssl - denial of service

Debian DSA-3930-1 : freeradius - security update

Debian DSA-3931-1 : ruby-rack-cors - security update

Debian DSA-3932-1 : subversion - security update

Debian DSA-3933-1 : pjproject - security update

Debian DSA-3934-1 : git - security update

Debian DSA-3935-1 : postgresql-9.4 - security update

Debian DSA-3936-1 : postgresql-9.6 - security update

Debian DSA-3937-1 : zabbix - security update

Debian DSA-3938-1 : libgd2 - security update

Debian DSA-3939-1 : botan1.10 - security update

Debian DSA-394-1 : openssl095 - ASN.1 parsing vulnerability

Debian DSA-3940-1 : cvs - security update

Debian DSA-3941-1 : iortcw - security update

Debian DSA-3942-1 : supervisor - security update

Debian DSA-3943-1 : gajim - security update

Debian DSA-3944-1 : mariadb-10.0 - security update

Debian DSA-3945-1 : linux - security update (Stack Clash)

Debian DSA-3946-1 : libmspack - security update

Debian DSA-3947-1 : newsbeuter - security update

Debian DSA-3948-1 : ioquake3 - security update

Debian DSA-3949-1 : augeas - security update

Debian DSA-395-1 : tomcat4 - incorrect input handling

Debian DSA-3950-1 : libraw - security update

Debian DSA-3951-1 : smb4k - security update

Debian DSA-3952-1 : libxml2 - security update

Debian DSA-3953-1 : aodh - security update

Debian DSA-3954-1 : openjdk-7 - security update

Debian DSA-3955-1 : mariadb-10.1 - security update

Debian DSA-3956-1 : connman - security update

Debian DSA-3957-1 : ffmpeg - security update

Debian DSA-3958-1 : fontforge - security update

Debian DSA-3959-1 : libgcrypt20 - security update

Debian DSA-396-1 : thttpd - missing input sanitizing, wrong calculation

Debian DSA-3960-1 : gnupg - security update

Debian DSA-3961-1 : libgd2 - security update

Debian DSA-3962-1 : strongswan - security update

Debian DSA-3963-1 : mercurial - security update

Debian DSA-3964-1 : asterisk - security update

Debian DSA-3965-1 : file - security update

Debian DSA-3966-1 : ruby2.3 - security update

Debian DSA-3967-1 : mbedtls - security update

Debian DSA-3968-1 : icedove - security update

Debian DSA-3969-1 : xen - security update

Debian DSA-397-1 : postgresql - buffer overflow

Debian DSA-3970-1 : emacs24 - security update

Debian DSA-3971-1 : tcpdump - security update

Debian DSA-3972-1 : bluez - security update (BlueBorne)

Debian DSA-3973-1 : wordpress-shibboleth - security update

Debian DSA-3974-1 : tomcat8 - security update

Debian DSA-3975-1 : emacs25 - security update

Debian DSA-3976-1 : freexl - security update

Debian DSA-3977-1 : newsbeuter - security update

Debian DSA-3978-1 : gdk-pixbuf - security update

Debian DSA-3979-1 : pyjwt - security update

Debian DSA-398-1 : conquest - buffer overflow

Debian DSA-3980-1 : apache2 - security update (Optionsbleed)

Debian DSA-3981-1 : linux - security update (BlueBorne) (Stack Clash)

Debian DSA-3982-1 : perl - security update

Debian DSA-3983-1 : samba - security update

Debian DSA-3984-1 : git - security update

Debian DSA-3985-1 : chromium-browser - security update

Debian DSA-3986-1 : ghostscript - security update

Debian DSA-3987-1 : firefox-esr - security update

Debian DSA-3988-1 : libidn2-0 - security update

Debian DSA-3989-1 : dnsmasq - security update

Debian DSA-399-1 : epic4 - buffer overflow

Debian DSA-3990-1 : asterisk - security update

Debian DSA-3991-1 : qemu - security update

Debian DSA-3992-1 : curl - security update

Debian DSA-3993-1 : tor - security update

Debian DSA-3994-1 : nautilus - security update

Debian DSA-3995-1 : libxfont - security update

Debian DSA-3996-1 : ffmpeg - security update

Debian DSA-3997-1 : wordpress - security update

Debian DSA-3998-1 : nss - security update

Debian DSA-3999-1 : wpa - security update (KRACK)

Debian DSA-400-1 : omega-rpg - buffer overflow

Debian DSA-4000-1 : xorg-server - security update

Debian DSA-4001-1 : yadifa - security update

Debian DSA-4002-1 : mysql-5.5 - security update

Debian DSA-4003-1 : libvirt - security update

Debian DSA-4004-1 : jackson-databind - security update

Debian DSA-4005-1 : openjfx - security update

Debian DSA-4006-1 : mupdf - security update

Debian DSA-4007-1 : curl - security update

Debian DSA-4008-1 : wget - security update

Debian DSA-4009-1 : shadowsocks-libev - security update

Debian DSA-401-1 : hylafax - format strings

Debian DSA-4010-1 : git-annex - security update

Debian DSA-4011-1 : quagga - security update

Debian DSA-4012-1 : libav - security update

Debian DSA-4013-1 : openjpeg2 - security update

Debian DSA-4014-1 : thunderbird - security update

Debian DSA-4015-1 : openjdk-8 - security update

Debian DSA-4016-1 : irssi - security update

Debian DSA-4017-1 : openssl1.0 - security update

Debian DSA-4018-1 : openssl - security update

Debian DSA-4019-1 : imagemagick - security update

Debian DSA-402-1 : minimalist - unsanitised input

Debian DSA-4020-1 : chromium-browser - security update

Debian DSA-4021-1 : otrs2 - security update

Debian DSA-4022-1 : libreoffice - security update

Debian DSA-4023-1 : slurm-llnl - security update

Debian DSA-4024-1 : chromium-browser - security update

Debian DSA-4025-1 : libpam4j - security update

Debian DSA-4026-1 : bchunk - security update

Debian DSA-4027-1 : postgresql-9.4 - security update

Debian DSA-4028-1 : postgresql-9.6 - security update

Debian DSA-4029-1 : postgresql-common - security update

Debian DSA-403-1 : kernel-image-2.4.18-1-alpha, kernel-image-2.4.18-1-i386, kernel-source-2.4.18 - local root exploit

Debian DSA-4030-1 : roundcube - security update

Debian DSA-4031-1 : ruby2.3 - security update

Debian DSA-4032-1 : imagemagick - security update

Debian DSA-4033-1 : konversation - security update

Debian DSA-4034-1 : varnish - security update

Debian DSA-4035-1 : firefox-esr - security update

Debian DSA-4036-1 : mediawiki - security update

Debian DSA-4037-1 : jackson-databind - security update

Debian DSA-4038-1 : shibboleth-sp2 - security update

Debian DSA-4039-1 : opensaml2 - security update

Debian DSA-404-1 : rsync - heap overflow

Debian DSA-4040-1 : imagemagick - security update

Debian DSA-4041-1 : procmail - security update

Debian DSA-4042-1 : libxml-libxml-perl - security update

Debian DSA-4043-1 : samba - security update

Debian DSA-4044-1 : swauth - security update

Debian DSA-4045-1 : vlc - security update

Debian DSA-4046-1 : libspring-ldap-java - security update

Debian DSA-4047-1 : otrs2 - security update

Debian DSA-4048-1 : openjdk-7 - security update

Debian DSA-4049-1 : ffmpeg - security update

Debian DSA-405-1 : xsok - missing privilege release

Debian DSA-4050-1 : xen - security update

Debian DSA-4051-1 : curl - security update

Debian DSA-4052-1 : bzr - security update

Debian DSA-4053-1 : exim4 - security update

Debian DSA-4054-1 : tor - security update

Debian DSA-4055-1 : heimdal - security update

Debian DSA-4056-1 : nova - security update

Debian DSA-4057-1 : erlang - security update (ROBOT)

Debian DSA-4058-1 : optipng - security update

Debian DSA-4059-1 : libxcursor - security update

Debian DSA-406-1 : lftp - buffer overflow

Debian DSA-4060-1 : wireshark - security update

Debian DSA-4061-1 : thunderbird - security update

Debian DSA-4062-1 : firefox-esr - security update

Debian DSA-4063-1 : pdns-recursor - security update

Debian DSA-4064-1 : chromium-browser - security update

Debian DSA-4065-1 : openssl1.0 - security update

Debian DSA-4066-1 : otrs2 - security update

Debian DSA-4067-1 : openafs - security update

Debian DSA-4068-1 : rsync - security update

Debian DSA-4069-1 : otrs2 - security update

Debian DSA-407-1 : ethereal - buffer overflows

Debian DSA-4070-1 : enigmail - security update

Debian DSA-4071-1 : sensible-utils - security update

Debian DSA-4072-1 : bouncycastle - security update

Debian DSA-4073-1 : linux - security update

Debian DSA-4074-1 : imagemagick - security update

Debian DSA-4075-1 : thunderbird - security update

Debian DSA-4076-1 : asterisk - security update

Debian DSA-4077-1 : gimp - security update

Debian DSA-4078-1 : linux - security update (Meltdown)

Debian DSA-4079-1 : poppler - security update

Debian DSA-408-1 : screen - integer overflow

Debian DSA-4080-1 : php7.0 - security update

Debian DSA-4081-1 : php5 - security update

Debian DSA-4082-1 : linux - security update (Meltdown)

Debian DSA-4083-1 : poco - security update

Debian DSA-4084-1 : gifsicle - security update

Debian DSA-4085-1 : xmltooling - security update

Debian DSA-4086-1 : libxml2 - security update

Debian DSA-4087-1 : transmission - security update

Debian DSA-4088-1 : gdk-pixbuf - security update

Debian DSA-4089-1 : bind9 - security update

Debian DSA-409-1 : bind - denial of service

Debian DSA-4090-1 : wordpress - security update

Debian DSA-4091-1 : mysql-5.5 - security update

Debian DSA-4092-1 : awstats - security update

Debian DSA-4093-1 : openocd - security update

Debian DSA-4094-1 : smarty3 - security update

Debian DSA-4095-1 : gcab - security update

Debian DSA-4096-1 : firefox-esr - security update

Debian DSA-4097-1 : poppler - security update

Debian DSA-4098-1 : curl - security update

Debian DSA-4099-1 : ffmpeg - security update

Debian DSA-410-1 : libnids - buffer overflow

Debian DSA-4100-1 : tiff - security update

Debian DSA-4101-1 : wireshark - security update

Debian DSA-4102-1 : thunderbird - security update

Debian DSA-4103-1 : chromium-browser - security update

Debian DSA-4104-1 : p7zip - security update

Debian DSA-4105-1 : mpv - security update

Debian DSA-4106-1 : libtasn1-6 - security update

Debian DSA-4107-1 : django-anymail - security update

Debian DSA-4108-1 : mailman - security update

Debian DSA-4109-1 : ruby-omniauth - security update

Debian DSA-411-1 : mpg321 - format string vulnerability

Debian DSA-4110-1 : exim4 - security update

Debian DSA-4111-1 : libreoffice - security update

Debian DSA-4112-1 : xen - security update

Debian DSA-4113-1 : libvorbis - security update

Debian DSA-4114-1 : jackson-databind - security update

Debian DSA-4115-1 : quagga - security update

Debian DSA-4116-1 : plasma-workspace - security update

Debian DSA-4117-1 : gcc-4.9 - security update

Debian DSA-4118-1 : tomcat-native - security update

Debian DSA-4119-1 : libav - security update

Debian DSA-412-1 : nd - buffer overflows

Debian DSA-4120-1 : linux - security update (Meltdown) (Spectre)

Debian DSA-4121-1 : gcc-6 - security update

Debian DSA-4122-1 : squid3 - security update

Debian DSA-4123-1 : drupal7 - security update

Debian DSA-4124-1 : lucene-solr - security update

Debian DSA-4125-1 : wavpack - security update

Debian DSA-4126-1 : xmltooling - security update

Debian DSA-4127-1 : simplesamlphp - security update

Debian DSA-4128-1 : trafficserver - security update

Debian DSA-4129-1 : freexl - security update

Debian DSA-413-2 : linux-kernel-2.4.18 - missing boundary check

Debian DSA-4130-1 : dovecot - security update

Debian DSA-4131-1 : xen - security update

Debian DSA-4132-1 : libvpx - security update

Debian DSA-4133-1 : isc-dhcp - security update

Debian DSA-4134-1 : util-linux - security update

Debian DSA-4135-1 : samba - security update

Debian DSA-4136-1 : curl - security update

Debian DSA-4137-1 : libvirt - security update

Debian DSA-4138-1 : mbedtls - security update

Debian DSA-4139-1 : firefox-esr - security update

Debian DSA-414-1 : jabber - denial of service

Debian DSA-4140-1 : libvorbis - security update

Debian DSA-4141-1 : libvorbisidec - security update

Debian DSA-4142-1 : uwsgi - security update

Debian DSA-4143-1 : firefox-esr - security update

Debian DSA-4144-1 : openjdk-8 - security update

Debian DSA-4145-1 : gitlab - security update

Debian DSA-4146-1 : plexus-utils - security update

Debian DSA-4147-1 : polarssl - security update

Debian DSA-4148-1 : kamailio - security update

Debian DSA-4149-1 : plexus-utils2 - security update

Debian DSA-415-1 : zebra - denial of service

Debian DSA-4150-1 : icu - security update

Debian DSA-4151-1 : librelp - security update

Debian DSA-4152-1 : mupdf - security update

Debian DSA-4153-1 : firefox-esr - security update

Debian DSA-4154-1 : net-snmp - security update

Debian DSA-4155-1 : thunderbird - security update

Debian DSA-4156-1 : drupal7 - security update (Drupalgeddon 2)

Debian DSA-4157-1 : openssl - security update

Debian DSA-4158-1 : openssl1.0 - security update

Debian DSA-4159-1 : remctl - security update

Debian DSA-416-1 : fsp - buffer overflow, directory traversal

Debian DSA-4160-1 : libevt - security update

Debian DSA-4161-1 : python-django - security update

Debian DSA-4162-1 : irssi - security update

Debian DSA-4163-1 : beep - security update

Debian DSA-4164-1 : apache2 - security update

Debian DSA-4165-1 : ldap-account-manager - security update

Debian DSA-4166-1 : openjdk-7 - security update

Debian DSA-4167-1 : sharutils - security update

Debian DSA-4168-1 : squirrelmail - security update

Debian DSA-4169-1 : pcs - security update

Debian DSA-417-1 : linux-kernel-2.4.18-powerpc+alpha - missing boundary check

Debian DSA-4170-1 : pjproject - security update

Debian DSA-4171-1 : ruby-loofah - security update

Debian DSA-4172-1 : perl - security update

Debian DSA-4173-1 : r-cran-readxl - security update

Debian DSA-4174-1 : corosync - security update

Debian DSA-4175-1 : freeplane - security update

Debian DSA-4176-1 : mysql-5.5 - security update

Debian DSA-4177-1 : libsdl2-image - security update

Debian DSA-4178-1 : libreoffice - security update

Debian DSA-4179-1 : linux-tools - security update

Debian DSA-418-1 : vbox3 - privilege leak

Debian DSA-4180-1 : drupal7 - security update (Drupalgeddon 2)

Debian DSA-4181-1 : roundcube - security update

Debian DSA-4182-1 : chromium-browser - security update

Debian DSA-4183-1 : tor - security update

Debian DSA-4184-1 : sdl-image1.2 - security update

Debian DSA-4185-1 : openjdk-8 - security update

Debian DSA-4186-1 : gunicorn - security update

Debian DSA-4187-1 : linux - security update (Spectre)

Debian DSA-4188-1 : linux - security update (Spectre)

Debian DSA-4189-1 : quassel - security update

Debian DSA-419-1 : phpgroupware - missing filename sanitising, SQL injection

Debian DSA-4190-1 : jackson-databind - security update

Debian DSA-4191-1 : redmine - security update

Debian DSA-4192-1 : libmad - security update

Debian DSA-4193-1 : wordpress - security update

Debian DSA-4194-1 : lucene-solr - security update

Debian DSA-4195-1 : wget - security update

Debian DSA-4196-1 : linux - security update

Debian DSA-4197-1 : wavpack - security update

Debian DSA-4198-1 : prosody - security update

Debian DSA-4199-1 : firefox-esr - security update

Debian DSA-420-1 : jitterbug - improperly sanitised input

Debian DSA-4200-1 : kwallet-pam - security update

Debian DSA-4201-1 : xen - security update

Debian DSA-4202-1 : curl - security update

Debian DSA-4203-1 : vlc - security update

Debian DSA-4204-1 : imagemagick - security update

Debian DSA-4206-1 : gitlab - security update

Debian DSA-4207-1 : packagekit - security update

Debian DSA-4208-1 : procps - security update

Debian DSA-4209-1 : thunderbird - security update

Debian DSA-421-1 : mod-auth-shadow - password expiration

Debian DSA-4210-1 : xen - security update (Spectre)

Debian DSA-4211-1 : xdg-utils - security update

Debian DSA-4212-1 : git - security update

Debian DSA-4213-1 : qemu - security update (Spectre)

Debian DSA-4214-1 : zookeeper - security update

Debian DSA-4215-1 : batik - security update

Debian DSA-4216-1 : prosody - security update

Debian DSA-4217-1 : wireshark - security update

Debian DSA-4218-1 : memcached - security update

Debian DSA-4219-1 : jruby - security update

Debian DSA-422-1 : cvs - remote vulnerability

Debian DSA-4220-1 : firefox-esr - security update

Debian DSA-4221-1 : libvncserver - security update

Debian DSA-4222-1 : gnupg2 - security update

Debian DSA-4223-1 : gnupg1 - security update

Debian DSA-4224-1 : gnupg - security update

Debian DSA-4225-1 : openjdk-7 - security update

Debian DSA-4226-1 : perl - security update

Debian DSA-4227-1 : plexus-archiver - security update

Debian DSA-4228-1 : spip - security update

Debian DSA-4229-1 : strongswan - security update

Debian DSA-423-1 : linux-kernel-2.4.17-ia64 - several vulnerabilities

Debian DSA-4230-1 : redis - security update

Debian DSA-4231-1 : libgcrypt20 - security update

Debian DSA-4232-1 : xen - security update

Debian DSA-4233-1 : bouncycastle - security update

Debian DSA-4234-1 : lava-server - security update

Debian DSA-4235-1 : firefox-esr - security update

Debian DSA-4236-1 : xen - security update

Debian DSA-4237-1 : chromium-browser - security update

Debian DSA-4238-1 : exiv2 - security update

Debian DSA-4239-1 : gosa - security update

Debian DSA-424-1 : mc - buffer overflow

Debian DSA-4240-1 : php7.0 - security update

Debian DSA-4241-1 : libsoup2.4 - security update

Debian DSA-4242-1 : ruby-sprockets - security update

Debian DSA-4243-1 : cups - security update

Debian DSA-4244-1 : thunderbird - security update

Debian DSA-4245-1 : imagemagick - security update

Debian DSA-4246-1 : mailman - security update

Debian DSA-4247-1 : ruby-rack-protection - security update

Debian DSA-4248-1 : blender - security update

Debian DSA-4249-1 : ffmpeg - security update

Debian DSA-425-1 : tcpdump - multiple vulnerabilities

Debian DSA-4250-1 : wordpress - security update

Debian DSA-4251-1 : vlc - security update

Debian DSA-4252-1 : znc - security update

Debian DSA-4253-1 : network-manager-vpnc - security update

Debian DSA-4254-1 : slurm-llnl - security update

Debian DSA-4255-1 : ant - security update

Debian DSA-4256-1 : chromium-browser - security update

Debian DSA-4257-1 : fuse - security update

Debian DSA-4258-1 : ffmpeg - security update

Debian DSA-4259-1 : ruby2.3 - security update

Debian DSA-426-1 : netpbm-free - insecure temporary files

Debian DSA-4260-1 : libmspack - security update

Debian DSA-4261-1 : vim-syntastic - security update

Debian DSA-4262-1 : symfony - security update

Debian DSA-4263-1 : cgit - security update

Debian DSA-4264-1 : python-django - security update

Debian DSA-4265-1 : xml-security-c - security update

Debian DSA-4266-1 : linux - security update

Debian DSA-4267-1 : kamailio - security update

Debian DSA-4268-1 : openjdk-8 - security update

Debian DSA-4269-1 : postgresql-9.6 - security update

Debian DSA-427-1 : linux-kernel-2.4.17-mips+mipsel - missing boundary check

Debian DSA-4270-1 : gdm3 - security update

Debian DSA-4271-1 : samba - security update

Debian DSA-4272-1 : linux - security update

Debian DSA-4273-1 : intel-microcode - security update (Spectre)

Debian DSA-4274-1 : xen - security update (Foreshadow)

Debian DSA-4275-1 : keystone - security update

Debian DSA-4276-1 : php-horde-image - security update

Debian DSA-4277-1 : mutt - security update

Debian DSA-4278-1 : jetty9 - security update

Debian DSA-4279-1 : linux - security update (Foreshadow)

Debian DSA-428-1 : slocate - buffer overflow

Debian DSA-4280-1 : openssh - security update

Debian DSA-4281-1 : tomcat8 - security update

Debian DSA-4282-1 : trafficserver - security update

Debian DSA-4283-1 : ruby-json-jwt - security update

Debian DSA-4284-1 : lcms2 - security update

Debian DSA-4285-1 : sympa - security update

Debian DSA-4286-1 : curl - security update

Debian DSA-4287-1 : firefox-esr - security update

Debian DSA-4288-1 : ghostscript - security update

Debian DSA-4289-1 : chromium-browser - security update

Debian DSA-429-1 : gnupg - cryptographic weakness

Debian DSA-4290-1 : libextractor - security update

Debian DSA-4291-1 : mgetty - security update

Debian DSA-4292-1 : kamailio - security update

Debian DSA-4293-1 : discount - security update

Debian DSA-4294-1 : ghostscript - security update

Debian DSA-4295-1 : thunderbird - security update

Debian DSA-4296-1 : mbedtls - security update

Debian DSA-4297-1 : chromium-browser - security update

Debian DSA-4298-1 : hylafax - security update

Debian DSA-4299-1 : texlive-bin - security update

Debian DSA-430-1 : trr19 - missing privilege release

Debian DSA-4300-1 : libarchive-zip-perl - security update

Debian DSA-4301-1 : mediawiki - security update

Debian DSA-4302-1 : openafs - security update

Debian DSA-4303-1 : okular - security update

Debian DSA-4304-1 : firefox-esr - security update

Debian DSA-4305-1 : strongswan - security update

Debian DSA-4306-1 : python2.7 - security update

Debian DSA-4307-1 : python3.5 - security update

Debian DSA-4308-1 : linux - security update

Debian DSA-4309-1 : strongswan - security update

Debian DSA-431-1 : perl - information leak

Debian DSA-4310-1 : firefox-esr - security update

Debian DSA-4311-1 : git - security update

Debian DSA-4312-1 : tinc - security update

Debian DSA-4313-1 : linux - security update

Debian DSA-4314-1 : net-snmp - security update

Debian DSA-4315-1 : wireshark - security update

Debian DSA-4316-1 : imagemagick - security update

Debian DSA-4317-1 : otrs2 - security update

Debian DSA-4318-1 : moin - security update

Debian DSA-4319-1 : spice - security update

Debian DSA-432-1 : crawl - buffer overflow

Debian DSA-4320-1 : asterisk - security update

Debian DSA-4321-1 : graphicsmagick - security update

Debian DSA-4322-1 : libssh - security update

Debian DSA-4323-1 : drupal7 - security update

Debian DSA-4324-1 : firefox-esr - security update

Debian DSA-4325-1 : mosquitto - security update

Debian DSA-4326-1 : openjdk-8 - security update

Debian DSA-4327-1 : thunderbird - security update

Debian DSA-4328-1 : xorg-server - security update

Debian DSA-4329-1 : teeworlds - security update

Debian DSA-433-1 : kernel-patch-2.4.17-mips - integer overflow

Debian DSA-4330-1 : chromium-browser - security update

Debian DSA-4331-1 : curl - security update

Debian DSA-4332-1 : ruby2.3 - security update

Debian DSA-4333-1 : icecast2 - security update

Debian DSA-4334-1 : mupdf - security update

Debian DSA-4335-1 : nginx - security update

Debian DSA-4336-1 : ghostscript - security update

Debian DSA-4337-1 : thunderbird - security update

Debian DSA-4338-1 : qemu - security update

Debian DSA-4339-1 : ceph - security update

Debian DSA-434-1 : gaim - several vulnerabilities

Debian DSA-4340-1 : chromium-browser - security update

Debian DSA-4341-1 : mariadb-10.1 - security update

Debian DSA-4342-1 : chromium-browser - security update

Debian DSA-4343-1 : liblivemedia - security update

Debian DSA-4344-1 : roundcube - security update

Debian DSA-4345-1 : samba - security update

Debian DSA-4346-1 : ghostscript - security update

Debian DSA-4347-1 : perl - security update

Debian DSA-4348-1 : openssl - security update

Debian DSA-4349-1 : tiff - security update

Debian DSA-435-1 : mpg123 - heap overflow

Debian DSA-4350-1 : policykit-1 - security update

Debian DSA-4351-1 : libphp-phpmailer - security update

Debian DSA-4352-1 : chromium-browser - security update

Debian DSA-4353-1 : php7.0 - security update

Debian DSA-4354-1 : firefox-esr - security update

Debian DSA-4355-1 : openssl1.0 - security update

Debian DSA-4356-1 : netatalk - security update

Debian DSA-4357-1 : libapache-mod-jk - security update

Debian DSA-4358-1 : ruby-sanitize - security update

Debian DSA-4359-1 : wireshark - security update

Debian DSA-436-1 : mailman - several vulnerabilities

Debian DSA-4360-1 : libarchive - security update

Debian DSA-4361-1 : libextractor - security update

Debian DSA-4362-1 : thunderbird - security update

Debian DSA-4363-1 : python-django - security update

Debian DSA-4364-1 : ruby-loofah - security update

Debian DSA-4365-1 : tmpreaper - security update

Debian DSA-4366-1 : vlc - security update

Debian DSA-4367-1 : systemd - security update

Debian DSA-4368-1 : zeromq3 - security update

Debian DSA-4369-1 : xen - security update

Debian DSA-437-1 : cgiemail - open mail relay

Debian DSA-4370-1 : drupal7 - security update

Debian DSA-4371-1 : apt - security update

Debian DSA-4372-1 : ghostscript - security update

Debian DSA-4373-1 : coturn - security update

Debian DSA-4374-1 : qtbase-opensource-src - security update

Debian DSA-4375-1 : spice - security update

Debian DSA-4376-1 : firefox-esr - security update

Debian DSA-4377-1 : rssh - security update

Debian DSA-4378-1 : php-pear - security update

Debian DSA-4379-1 : golang-1.7 - security update

Debian DSA-438-1 : linux-kernel-2.4.18-alpha+i386+powerpc - missing function return value check

Debian DSA-4380-1 : golang-1.8 - security update

Debian DSA-4381-1 : libreoffice - security update

Debian DSA-4382-1 : rssh - security update

Debian DSA-4383-1 : libvncserver - security update

Debian DSA-4384-1 : libgd2 - security update

Debian DSA-4385-1 : dovecot - security update

Debian DSA-4386-1 : curl - security update

Debian DSA-4387-1 : openssh - security update

Debian DSA-4388-1 : mosquitto - security update

Debian DSA-4389-1 : libu2f-host - security update

Debian DSA-439-1 : linux-kernel-2.4.16-arm - several vulnerabilities

Debian DSA-4390-1 : flatpak - security update

Debian DSA-4391-1 : firefox-esr - security update

Debian DSA-4392-1 : thunderbird - security update

Debian DSA-4393-1 : systemd - security update

Debian DSA-4394-1 : rdesktop - security update

Debian DSA-4395-1 : chromium - security update

Debian DSA-4396-1 : ansible - security update

Debian DSA-4397-1 : ldb - security update

Debian DSA-4398-1 : php7.0 - security update

Debian DSA-4399-1 : ikiwiki - security update

Debian DSA-440-1 : linux-kernel-2.4.17-powerpc-apus - several vulnerabilities

Debian DSA-4400-1 : openssl1.0 - security update

Debian DSA-4401-1 : wordpress - security update

Debian DSA-4402-1 : mumble - security update

Debian DSA-4403-1 : php7.0 - security update

Debian DSA-4404-1 : chromium - security update

Debian DSA-4405-1 : openjpeg2 - security update

Debian DSA-4406-1 : waagent - security update

Debian DSA-4407-1 : xmltooling - security update

Debian DSA-4408-1 : liblivemedia - security update

Debian DSA-4409-1 : neutron - security update

Debian DSA-441-1 : linux-kernel-2.4.17-mips+mipsel - missing function return value check

Debian DSA-4410-1 : openjdk-8 - security update

Debian DSA-4411-1 : firefox-esr - security update

Debian DSA-4412-1 : drupal7 - security update

Debian DSA-4413-1 : ntfs-3g - security update

Debian DSA-4414-1 : libapache2-mod-auth-mellon - security update

Debian DSA-4415-1 : passenger - security update

Debian DSA-4416-1 : wireshark - security update

Debian DSA-4417-1 : firefox-esr - security update

Debian DSA-4418-1 : dovecot - security update

Debian DSA-4419-1 : twig - security update

Debian DSA-442-1 : linux-kernel-2.4.17-s390 - several vulnerabilities

Debian DSA-4420-1 : thunderbird - security update

Debian DSA-4421-1 : chromium - security update

Debian DSA-4422-1 : apache2 - security update

Debian DSA-4423-1 : putty - security update

Debian DSA-4424-1 : pdns - security update

Debian DSA-4425-1 : wget - security update

Debian DSA-4426-1 : tryton-server - security update

Debian DSA-4427-1 : samba - security update

Debian DSA-4428-1 : systemd - security update

Debian DSA-4429-1 : spip - security update

Debian DSA-443-1 : xfree86 - several vulnerabilities

Debian DSA-4430-1 : wpa - security update

Debian DSA-4431-1 : libssh2 - security update

Debian DSA-4432-1 : ghostscript - security update

Debian DSA-4433-1 : ruby2.3 - security update

Debian DSA-4434-1 : drupal7 - security update

Debian DSA-4435-1 : libpng1.6 - security update

Debian DSA-4436-1 : imagemagick - security update

Debian DSA-4437-1 : gst-plugins-base1.0 - security update

Debian DSA-4438-1 : atftp - security update

Debian DSA-4439-1 : postgresql-9.6 - security update

Debian DSA-444-1 : linux-kernel-2.4.17-ia64 - missing function return value check

Debian DSA-4440-1 : bind9 - security update

Debian DSA-4441-1 : symfony - security update

Debian DSA-4442-1 : ghostscript - security update

Debian DSA-4443-1 : samba - security update

Debian DSA-4444-1 : linux - security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Debian DSA-4445-1 : drupal7 - security update

Debian DSA-4446-1 : lemonldap-ng - security update

Debian DSA-4447-1 : intel-microcode - security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Debian DSA-4448-1 : firefox-esr - security update

Debian DSA-4449-1 : ffmpeg - security update

Debian DSA-445-1 : lbreakout2 - buffer overflow

Debian DSA-4450-1 : wpa - security update

Debian DSA-4451-1 : thunderbird - security update

Debian DSA-4452-1 : jackson-databind - security update

Debian DSA-4453-1 : openjdk-8 - security update

Debian DSA-4454-1 : qemu - security update

Debian DSA-4455-1 : heimdal - security update

Debian DSA-4456-1 : exim4 - security update

Debian DSA-4457-1 : evolution - security update

Debian DSA-4458-1 : cyrus-imapd - security update

Debian DSA-4459-1 : vlc - security update

Debian DSA-446-1 : synaesthesia - insecure file creation

Debian DSA-4460-1 : mediawiki - security update

Debian DSA-4461-1 : zookeeper - security update

Debian DSA-4462-1 : dbus - security update

Debian DSA-4463-1 : znc - security update

Debian DSA-4464-1 : thunderbird - security update

Debian DSA-4465-1 : linux - security update (SACK Panic) (SACK Slowness)

Debian DSA-4466-1 : firefox-esr - security update

Debian DSA-4467-1 : vim - security update

Debian DSA-4468-1 : php-horde-form - security update

Debian DSA-4469-1 : libvirt - security update

Debian DSA-447-1 : hsftp - format string

Debian DSA-4470-1 : pdns - security update

Debian DSA-4471-1 : thunderbird - security update

Debian DSA-4472-1 : expat - security update

Debian DSA-4473-1 : rdesktop - security update

Debian DSA-4474-1 : firefox-esr - security update

Debian DSA-4475-1 : openssl - security update

Debian DSA-4476-1 : python-django - security update

Debian DSA-4477-1 : zeromq3 - security update

Debian DSA-4478-1 : dosbox - security update

Debian DSA-4479-1 : firefox-esr - security update

Debian DSA-448-1 : pwlib - several vulnerabilities

Debian DSA-4480-1 : redis - security update

Debian DSA-4481-1 : ruby-mini-magick - security update

Debian DSA-4482-1 : thunderbird - security update

Debian DSA-4483-1 : libreoffice - security update

Debian DSA-4484-1 : linux - security update

Debian DSA-4485-1 : openjdk-8 - security update

Debian DSA-4486-1 : openjdk-11 - security update

Debian DSA-4487-1 : neovim - security update

Debian DSA-4488-1 : exim4 - security update

Debian DSA-4489-1 : patch - security update

Debian DSA-449-1 : metamail - buffer overflow, format string bugs

Debian DSA-4490-1 : subversion - security update

Debian DSA-4491-1 : proftpd-dfsg - security update

Debian DSA-4492-1 : postgresql-9.6 - security update

Debian DSA-4493-1 : postgresql-11 - security update

Debian DSA-4494-1 : kconfig - security update

Debian DSA-4495-1 : linux - security update

Debian DSA-4496-1 : pango1.0 - security update

Debian DSA-4497-1 : linux - security update

Debian DSA-4498-1 : python-django - security update

Debian DSA-4499-1 : ghostscript - security update

Debian DSA-450-1 : linux-kernel-2.4.19-mips - several vulnerabilities

Debian DSA-4500-1 : chromium - security update

Debian DSA-4501-1 : libreoffice - security update

Debian DSA-4502-1 : ffmpeg - security update

Debian DSA-4503-1 : golang-1.11 - security update (Ping Flood) (Reset Flood)

Debian DSA-4504-1 : vlc - security update

Debian DSA-4505-1 : nginx - security update (0-Length Headers Leak) (Data Dribble) (Resource Loop)

Debian DSA-4506-1 : qemu - security update

Debian DSA-4507-1 : squid - security update

Debian DSA-4508-1 : h2o - security update (Ping Flood) (Reset Flood) (Settings Flood)

Debian DSA-4509-1 : apache2 - security update (Internal Data Buffering)

Debian DSA-451-1 : xboing - buffer overflows

Debian DSA-4510-1 : dovecot - security update

Debian DSA-4511-1 : nghttp2 - security update (Data Dribble) (Resource Loop)

Debian DSA-4512-1 : qemu - security update

Debian DSA-4513-1 : samba - security update

Debian DSA-4514-1 : varnish - security update

Debian DSA-4515-1 : webkit2gtk - security update

Debian DSA-4516-1 : firefox-esr - security update

Debian DSA-4517-1 : exim4 - security update

Debian DSA-4518-1 : ghostscript - security update

Debian DSA-4519-1 : libreoffice - security update

Debian DSA-452-1 : libapache-mod-python - denial of service

Debian DSA-4520-1 : trafficserver - security update (Empty Frames Flood) (Ping Flood) (Reset Flood) (Settings Flood)

Debian DSA-4521-1 : docker.io - security update

Debian DSA-4522-1 : faad2 - security update

Debian DSA-4523-1 : thunderbird - security update

Debian DSA-4524-1 : dino-im - security update

Debian DSA-4525-1 : ibus - security update

Debian DSA-4526-1 : opendmarc - security update

Debian DSA-4527-1 : php7.3 - security update

Debian DSA-4528-1 : bird - security update

Debian DSA-4529-1 : php7.0 - security update

Debian DSA-453-1 : linux-kernel-2.2.20-i386+m68k+powerpc - failing function and TLB flush

Debian DSA-4530-1 : expat - security update

Debian DSA-4531-1 : linux - security update

Debian DSA-4532-1 : spip - security update

Debian DSA-4533-1 : lemonldap-ng - security update

Debian DSA-4534-1 : golang-1.11 - security update

Debian DSA-4535-1 : e2fsprogs - security update

Debian DSA-4536-1 : exim4 - security update

Debian DSA-4537-1 : file-roller - security update

Debian DSA-4538-1 : wpa - security update

Debian DSA-4539-1 : openssl - security update

Debian DSA-454-1 : linux-kernel-2.2.22-alpha - failing function and TLB flush

Debian DSA-4540-1 : openssl1.0 - security update

Debian DSA-4541-1 : libapreq2 - security update

Debian DSA-4542-1 : jackson-databind - security update

Debian DSA-4543-1 : sudo - security update

Debian DSA-4544-1 : unbound - security update

Debian DSA-4545-1 : mediawiki - security update

Debian DSA-4546-1 : openjdk-11 - security update

Debian DSA-4547-1 : tcpdump - security update

Debian DSA-4548-1 : openjdk-8 - security update

Debian DSA-4549-1 : firefox-esr - security update

Debian DSA-455-1 : libxml - buffer overflows

Debian DSA-4550-1 : file - security update

Debian DSA-4551-1 : golang-1.11 - security update

Debian DSA-4552-1 : php7.0 - security update

Debian DSA-4553-1 : php7.3 - security update

Debian DSA-4554-1 : ruby-loofah - security update

Debian DSA-4555-1 : pam-python - security update

Debian DSA-4556-1 : qtbase-opensource-src - security update

Debian DSA-4557-1 : libarchive - security update

Debian DSA-4558-1 : webkit2gtk - security update

Debian DSA-4559-1 : proftpd-dfsg - security update

Debian DSA-456-1 : linux-kernel-2.2.19-arm - failing function and TLB flush

Debian DSA-4560-1 : simplesamlphp - security update

Debian DSA-4561-1 : fribidi - security update

Debian DSA-4562-1 : chromium - security update

Debian DSA-4563-1 : webkit2gtk - security update

Debian DSA-4564-1 : linux - security update

Debian DSA-4565-1 : intel-microcode - security update

Debian DSA-4566-1 : qemu - security update

Debian DSA-4567-1 : dpdk - security update

Debian DSA-4568-1 : postgresql-common - security update

Debian DSA-4569-1 : ghostscript - security update

Debian DSA-457-1 : wu-ftpd - several vulnerabilities

Debian DSA-4570-1 : mosquitto - security update

Debian DSA-4571-1 : thunderbird - security update

Debian DSA-4572-1 : slurm-llnl - security update

Debian DSA-4573-1 : symfony - security update

Debian DSA-4574-1 : redmine - security update

Debian DSA-4575-1 : chromium - security update

Debian DSA-4576-1 : php-imagick - security update

Debian DSA-4577-1 : haproxy - security update

Debian DSA-4578-1 : libvpx - security update

Debian DSA-4579-1 : nss - security update

Debian DSA-458-3 : python2.2 - buffer overflow

Debian DSA-4580-1 : firefox-esr - security update

Debian DSA-4581-1 : git - security update

Debian DSA-4582-1 : davical - security update

Debian DSA-4583-1 : spip - security update

Debian DSA-4584-1 : spamassassin - security update

Debian DSA-4585-1 : thunderbird - security update

Debian DSA-4586-1 : ruby2.5 - security update

Debian DSA-4587-1 : ruby2.3 - security update

Debian DSA-4588-1 : python-ecdsa - security update

Debian DSA-4589-1 : debian-edu-config - security update

Debian DSA-459-1 : kdelibs - cookie path traversal

Debian DSA-4590-1 : cyrus-imapd - security update

Debian DSA-4591-1 : cyrus-sasl2 - security update

Debian DSA-4592-1 : mediawiki - security update

Debian DSA-4593-1 : freeimage - security update

Debian DSA-4594-1 : openssl1.0 - security update

Debian DSA-4595-1 : debian-lan-config - security update

Debian DSA-4596-1 : tomcat8 - security update

Debian DSA-4597-1 : netty - security update

Debian DSA-4598-1 : python-django - security update

Debian DSA-4599-1 : wordpress - security update

Debian DSA-460-1 : sysstat - insecure temporary file

Debian DSA-4600-1 : firefox-esr - security update

Debian DSA-4601-1 : ldm - security update

Debian DSA-4602-1 : xen - security update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Debian DSA-4603-1 : thunderbird - security update

Debian DSA-4604-1 : cacti - security update

Debian DSA-4605-1 : openjdk-11 - security update

Debian DSA-4606-1 : chromium - security update

Debian DSA-4607-1 : openconnect - security update

Debian DSA-4608-1 : tiff - security update

Debian DSA-4609-1 : python-apt - security update

Debian DSA-461-1 : calife - buffer overflow

Debian DSA-4610-1 : webkit2gtk - security update

Debian DSA-4611-1 : opensmtpd - security update

Debian DSA-4612-1 : prosody-modules - security update

Debian DSA-4613-1 : libidn2 - security update

Debian DSA-4614-1 : sudo - security update

Debian DSA-4615-1 : spamassassin - security update

Debian DSA-4616-1 : qemu - security update

Debian DSA-4617-1 : qtbase-opensource-src - security update

Debian DSA-4618-1 : libexif - security update

Debian DSA-4619-1 : libxmlrpc3-java - security update

Debian DSA-462-1 : xitalk - missing privilege release

Debian DSA-4620-1 : firefox-esr - security update

Debian DSA-4621-1 : openjdk-8 - security update

Debian DSA-4622-1 : postgresql-9.6 - security update

Debian DSA-4623-1 : postgresql-11 - security update

Debian DSA-4624-1 : evince - security update

Debian DSA-4625-1 : thunderbird - security update

Debian DSA-4626-1 : php7.3 - security update

Debian DSA-4627-1 : webkit2gtk - security update

Debian DSA-4628-1 : php7.0 - security update

Debian DSA-4629-1 : python-django - security update

Debian DSA-463-1 : samba - privilege escalation

Debian DSA-4630-1 : python-pysaml2 - security update

Debian DSA-4631-1 : pillow - security update

Debian DSA-4632-1 : ppp - security update

Debian DSA-4633-1 : curl - security update

Debian DSA-4634-1 : opensmtpd - security update

Debian DSA-4635-1 : proftpd-dfsg - security update

Debian DSA-4636-1 : python-bleach - security update

Debian DSA-4637-1 : network-manager-ssh - security update

Debian DSA-4638-1 : chromium - security update

Debian DSA-4639-1 : firefox-esr - security update

Debian DSA-464-1 : gdk-pixbuf - broken image handling

Debian DSA-4640-1 : graphicsmagick - security update

Debian DSA-4641-1 : webkit2gtk - security update

Debian DSA-4642-1 : thunderbird - security update

Debian DSA-4643-1 : python-bleach - security update

Debian DSA-4644-1 : tor - security update

Debian DSA-4645-1 : chromium - security update

Debian DSA-4646-1 : icu - security update

Debian DSA-4647-1 : bluez - security update

Debian DSA-4648-1 : libpam-krb5 - security update

Debian DSA-4649-1 : haproxy - security update

Debian DSA-465-1 : openssl - several vulnerabilities

Debian DSA-4650-1 : qbittorrent - security update

Debian DSA-4651-1 : mediawiki - security update

Debian DSA-4652-1 : gnutls28 - security update

Debian DSA-4653-1 : firefox-esr - security update

Debian DSA-4654-1 : chromium - security update

Debian DSA-4655-1 : firefox-esr - security update

Debian DSA-4656-1 : thunderbird - security update

Debian DSA-4657-1 : git - security update

Debian DSA-466-1 : linux-kernel-2.2.10-powerpc-apus - failing function and TLB flush

Debian DSA-467-1 : ecartis - several vulnerabilities

Debian DSA-468-1 : emil - several vulnerabilities

Debian DSA-469-1 : pam-pgsql - missing input sanitising

Debian DSA-470-1 : linux-kernel-2.4.17-hppa - several vulnerabilities

Debian DSA-471-1 : interchange - missing input sanitising

Debian DSA-472-1 : fte - several vulnerabilities

Debian DSA-473-1 : oftpd - denial of service

Debian DSA-474-1 : squid - ACL bypass

Debian DSA-475-1 : linux-kernel-2.4.18-hppa - several vulnerabilities

Debian DSA-476-1 : heimdal - cross-realm

Debian DSA-477-1 : xine-ui - insecure temporary file creation

Debian DSA-478-1 : tcpdump - denial of service

Debian DSA-479-1 : linux-kernel-2.4.18-alpha+i386+powerpc - several vulnerabilities

Debian DSA-480-1 : linux-kernel-2.4.17+2.4.18-hppa - several vulnerabilities

Debian DSA-481-1 : linux-kernel-2.4.17-ia64 - several vulnerabilities

Debian DSA-482-1 : linux-kernel-2.4.17-apus+s390 - several vulnerabilities

Debian DSA-483-1 : mysql - insecure temporary file creation

Debian DSA-484-1 : xonix - failure to drop privileges

Debian DSA-485-1 : ssmtp - format string

Debian DSA-486-1 : cvs - several vulnerabilities

Debian DSA-487-1 : neon - format string

Debian DSA-488-1 : logcheck - insecure temporary directory

Debian DSA-489-1 : linux-kernel-2.4.17-mips+mipsel - several vulnerabilities

Debian DSA-490-1 : zope - arbitrary code execution

Debian DSA-491-1 : linux-kernel-2.4.19-mips - several vulnerabilities

Debian DSA-492-1 : iproute - denial of service

Debian DSA-493-1 : xchat - buffer overflow

Debian DSA-494-1 : ident2 - buffer overflow

Debian DSA-495-1 : linux-kernel-2.4.16-arm - several vulnerabilities

Debian DSA-496-1 : eterm - missing input sanitising

Debian DSA-497-1 : mc - several vulnerabilities

Debian DSA-498-1 : libpng - out of bound access

Debian DSA-499-2 : rsync - directory traversal

Debian DSA-500-1 : flim - insecure temporary file

Debian DSA-501-1 : exim - buffer overflow

Debian DSA-502-1 : exim-tls - buffer overflow

Debian DSA-503-1 : mah-jong - missing argument check

Debian DSA-504-1 : heimdal - missing input sanitising

Debian DSA-505-1 : cvs - heap overflow

Debian DSA-506-1 : neon - buffer overflow

Debian DSA-507-1 : cadaver - buffer overflow

Debian DSA-508-1 : xpcd - buffer overflow

Debian DSA-509-1 : gatos - privilege escalation

Debian DSA-510-1 : jftpgw - format string

Debian DSA-511-1 : ethereal - buffer overflows

Debian DSA-512-1 : gallery - unauthenticated access

Debian DSA-513-1 : log2mail - format string

Debian DSA-514-1 : kernel-image-sparc-2.2 - failing function and TLB flush

Debian DSA-515-1 : lha - several vulnerabilities

Debian DSA-516-1 : postgresql - buffer overflow

Debian DSA-517-1 : cvs - buffer overflow

Debian DSA-518-1 : kdelibs - unsanitised input

Debian DSA-519-1 : cvs - several vulnerabilities

Debian DSA-520-1 : krb5 - buffer overflows

Debian DSA-521-1 : sup - format string vulnerability

Debian DSA-522-1 : super - format string vulnerability

Debian DSA-523-1 : www-sql - buffer overflow

Debian DSA-524-1 : rlpr - several vulnerabilities

Debian DSA-525-1 : apache - buffer overflow

Debian DSA-526-1 : webmin - several vulnerabilities

Debian DSA-527-1 : pavuk - buffer overflow

Debian DSA-528-1 : ethereal - denial of service

Debian DSA-529-1 : netkit-telnet-ssl - format string

Debian DSA-530-1 : l2tpd - buffer overflow

Debian DSA-531-1 : php4 - several vulnerabilities

Debian DSA-532-2 : libapache-mod-ssl - several vulnerabilities

Debian DSA-533-1 : courier - XSS

Debian DSA-534-1 : mailreader - directory traversal

Debian DSA-535-1 : squirrelmail - several vulnerabilities

Debian DSA-536-1 : libpng - several vulnerabilities

Debian DSA-537-1 : ruby - insecure file permissions

Debian DSA-538-1 : rsync - unsanitised input processing

Debian DSA-539-1 : kdelibs - temporary directory vulnerability

Debian DSA-540-1 : mysql - insecure file creation

Debian DSA-541-1 : icecast-server - missing escape

Debian DSA-542-1 : qt - unsanitised input

Debian DSA-543-1 : krb5 - several vulnerabilities

Debian DSA-544-1 : webmin - insecure temporary directory

Debian DSA-545-1 : cupsys - denial of service

Debian DSA-546-1 : gdk-pixbuf - several vulnerabilities

Debian DSA-547-1 : imagemagick - buffer overflows

Debian DSA-548-2 : imlib - unsanitised input

Debian DSA-549-1 : gtk+ - several vulnerabilities

Debian DSA-550-1 : wv - buffer overflow

Debian DSA-551-1 : lukemftpd - incorrect internal variable handling

Debian DSA-552-1 : imlib2 - unsanitised input

Debian DSA-553-1 : getmail - symlink vulnerability

Debian DSA-554-1 : sendmail - pre-set password

Debian DSA-555-1 : freenet6 - wrong file permissions

Debian DSA-556-2 : netkit-telnet - invalid free(3)

Debian DSA-557-1 : rp-pppoe - missing privilege dropping

Debian DSA-558-1 : libapache-mod-dav - NULL pointer dereference

Debian DSA-559-1 : net-acct - insecure temporary file

Debian DSA-560-1 : lesstif1-1 - integer and stack overflows

Debian DSA-561-1 : xfree86 - integer and stack overflows

Debian DSA-562-1 : mysql - several vulnerabilities

Debian DSA-563-3 : cyrus-sasl - unsanitised input

Debian DSA-564-1 : mpg123 - missing user input sanitising

Debian DSA-565-1 : sox - buffer overflow

Debian DSA-566-1 : cupsys - unsanitised input

Debian DSA-567-1 : tiff - heap overflows

Debian DSA-568-1 : cyrus-sasl-mit - unsanitised input

Debian DSA-569-1 : netkit-telnet-ssl - invalid free(3)

Debian DSA-570-1 : libpng - integer overflow

Debian DSA-571-1 : libpng3 - buffer overflows, integer overflow

Debian DSA-572-1 : ecartis - several vulnerabilities

Debian DSA-573-1 : cupsys - integer overflows

Debian DSA-574-1 : cabextract - missing directory sanitising

Debian DSA-575-1 : catdoc - insecure temporary file

Debian DSA-576-1 : squid - several vulnerabilities

Debian DSA-577-1 : postgresql - insecure temporary file

Debian DSA-578-1 : mpg123 - buffer overflow

Debian DSA-579-1 : abiword - buffer overflow

Debian DSA-580-1 : iptables - missing initialisation

Debian DSA-581-1 : xpdf - integer overflows

Debian DSA-582-1 : libxml - buffer overflow

Debian DSA-583-1 : lvm10 - insecure temporary directory

Debian DSA-584-1 : dhcp - format string vulnerability

Debian DSA-585-1 : shadow - programming error

Debian DSA-586-1 : ruby - infinite loop

Debian DSA-587-1 : freeamp - buffer overflow

Debian DSA-588-1 : gzip - insecure temporary files

Debian DSA-589-1 : libgd1 - integer overflows

Debian DSA-590-1 : gnats - format string vulnerability

Debian DSA-591-1 : libgd2 - integer overflows

Debian DSA-592-1 : ez-ipupdate - format string

Debian DSA-593-1 : imagemagick - buffer overflow

Debian DSA-594-1 : apache - buffer overflows

Debian DSA-595-1 : bnc - buffer overflow

Debian DSA-596-2 : sudo - missing input sanitising

Debian DSA-597-1 : cyrus-imapd - buffer overflow

Debian DSA-598-1 : yardradius - buffer overflow

Debian DSA-599-1 : tetex-bin - integer overflows

Debian DSA-600-1 : samba - arbitrary file access

Debian DSA-601-1 : libgd - integer overflow

Debian DSA-602-1 : libgd2 - integer overflow

Debian DSA-603-1 : openssl - insecure temporary file

Debian DSA-604-1 : hpsockd - missing input sanitising

Debian DSA-605-1 : viewcvs - settings not honored

Debian DSA-606-1 : nfs-utils - wrong signal handler

Debian DSA-607-1 : xfree86 - several vulnerabilities

Debian DSA-608-1 : zgv - integer overflows, unsanitised input

Debian DSA-609-1 : atari800 - buffer overflows

Debian DSA-610-1 : cscope - insecure temporary file

Debian DSA-611-1 : htget - buffer overflow

Debian DSA-612-1 : a2ps - unsanitised input

Debian DSA-613-1 : ethereal - infinite loop

Debian DSA-614-1 : xzgv - integer overflows

Debian DSA-615-1 : debmake - insecure temporary files

Debian DSA-616-1 : netkit-telnet-ssl - format string

Debian DSA-617-1 : tiff - insufficient input validation

Debian DSA-618-1 : imlib - buffer overflows, integer overflows

Debian DSA-619-1 : xpdf - buffer overflow

Debian DSA-620-1 : perl - insecure temporary files / directories

Debian DSA-621-1 : cupsys - buffer overflow

Debian DSA-622-1 : htmlheadline - insecure temporary files

Debian DSA-623-1 : nasm - buffer overflow

Debian DSA-624-1 : zip - buffer overflow

Debian DSA-625-1 : pcal - buffer overflows

Debian DSA-626-1 : tiff - unsanitised input

Debian DSA-627-1 : namazu2 - unsanitised input

Debian DSA-628-1 : imlib2 - integer overflows

Debian DSA-629-1 : krb5 - buffer overflow

Debian DSA-630-1 : lintian - insecure temporary directory

Debian DSA-631-1 : kdelibs - unsanitised input

Debian DSA-632-1 : linpopup - buffer overflow

Debian DSA-633-1 : bmv - insecure temporary file

Debian DSA-634-1 : hylafax - weak hostname and username validation

Debian DSA-635-1 : exim - buffer overflow

Debian DSA-636-1 : glibc - insecure temporary files

Debian DSA-637-1 : exim-tls - buffer overflow

Debian DSA-638-1 : gopher - several vulnerabilities

Debian DSA-639-1 : mc - several vulnerabilities

Debian DSA-640-1 : gatos - buffer overflow

Debian DSA-641-1 : playmidi - buffer overflow

Debian DSA-642-1 : gallery - several vulnerabilities

Debian DSA-643-1 : queue - buffer overflows

Debian DSA-644-1 : chbg - buffer overflow

Debian DSA-645-1 : cupsys - buffer overflow

Debian DSA-646-1 : imagemagick - buffer overflow

Debian DSA-647-1 : mysql - insecure temporary files

Debian DSA-648-1 : xpdf - buffer overflow

Debian DSA-649-1 : xtrlock - buffer overflow

Debian DSA-650-1 : sword - missing input sanitising

Debian DSA-651-1 : squid - buffer overflow, integer overflow

Debian DSA-652-1 : unarj - several vulnerabilities

Debian DSA-653-1 : ethereal - buffer overflow

Debian DSA-654-1 : enscript - several vulnerabilities

Debian DSA-655-1 : zhcon - missing privilege release

Debian DSA-656-1 : vdr - insecure file access

Debian DSA-657-1 : xine-lib - buffer overflow

Debian DSA-658-1 : libdbi-perl - insecure temporary file

Debian DSA-659-1 : libpam-radius-auth - information leak, integer underflow

Debian DSA-660-1 : kdebase - missing return value check

Debian DSA-661-2 : f2c - insecure temporary files

Debian DSA-662-2 : squirrelmail - several vulnerabilities

Debian DSA-663-1 : prozilla - buffer overflows

Debian DSA-664-1 : cpio - broken file permissions

Debian DSA-665-1 : ncpfs - missing privilege release

Debian DSA-666-1 : python2.2 - design flaw

Debian DSA-667-1 : squid - several vulnerabilities

Debian DSA-668-1 : postgresql - privilege escalation

Debian DSA-669-1 : php3 - several vulnerabilities

Debian DSA-670-1 : emacs20 - format string

Debian DSA-671-1 : xemacs21 - format string

Debian DSA-672-1 : xview - buffer overflows

Debian DSA-673-1 : evolution - integer overflow

Debian DSA-674-3 : mailman - XSS, directory traversal

Debian DSA-675-1 : hztty - privilege escalation

Debian DSA-676-1 : xpcd - buffer overflow

Debian DSA-677-1 : sympa - buffer overflow

Debian DSA-678-1 : netkit-rwho - missing input validation

Debian DSA-679-1 : toolchain-source - insecure temporary files

Debian DSA-680-1 : htdig - unsanitised input

Debian DSA-681-1 : synaesthesia - privilege escalation

Debian DSA-682-1 : awstats - missing input sanitizing

Debian DSA-683-1 : postgresql - buffer overflows

Debian DSA-684-1 : typespeed - format string

Debian DSA-685-1 : emacs21 - format string

Debian DSA-686-1 : gftp - missing input sanitising

Debian DSA-687-1 : bidwatcher - format string

Debian DSA-688-1 : squid - missing input sanitising

Debian DSA-689-1 : libapache-mod-python - missing input sanitizing

Debian DSA-690-1 : bsmtpd - missing input sanitising

Debian DSA-691-1 : abuse - several vulnerabilities

Debian DSA-692-1 : kdenetwork - design flaw

Debian DSA-693-1 : luxman - buffer overflow

Debian DSA-694-1 : xloadimage - missing input sanitising, integer overflow

Debian DSA-695-1 : xli - buffer overflow, input sanitising, integer overflow

Debian DSA-696-1 : perl - design flaw

Debian DSA-697-1 : netkit-telnet - buffer overflow

Debian DSA-698-1 : mc - buffer overflow

Debian DSA-699-1 : netkit-telnet-ssl - buffer overflow

Debian DSA-700-1 : mailreader - missing input sanitising

Debian DSA-701-2 : samba - integer overflows

Debian DSA-702-1 : imagemagick - several vulnerabilities

Debian DSA-703-1 : krb5 - buffer overflows

Debian DSA-704-1 : remstats - tempfile, missing input sanitising

Debian DSA-705-1 : wu-ftpd - missing input sanitising

Debian DSA-706-1 : axel - buffer overflow

Debian DSA-707-1 : mysql - several vulnerabilities

Debian DSA-708-1 : php3 - missing input sanitising

Debian DSA-709-1 : libexif - buffer overflow

Debian DSA-710-1 : gtkhtml - NULL pointer dereference

Debian DSA-711-1 : info2www - missing input sanitising

Debian DSA-712-1 : geneweb - insecure file operations

Debian DSA-713-1 : junkbuster - several vulnerabilities

Debian DSA-714-1 : kdelibs - several vulnerabilities

Debian DSA-715-1 : cvs - several vulnerabilities

Debian DSA-716-1 : gaim - denial of service

Debian DSA-717-1 : lsh-utils - buffer overflow, typo

Debian DSA-718-2 : ethereal - buffer overflow

Debian DSA-719-1 : prozilla - format string problems

Debian DSA-720-1 : smartlist - wrong input processing

Debian DSA-721-1 : squid - design flaw

Debian DSA-722-1 : smail - buffer overflow

Debian DSA-723-1 : xfree86 - buffer overflow

Debian DSA-724-1 : phpsysinfo - design flaw

Debian DSA-725-2 : ppxp - missing privilege release

Debian DSA-726-1 : oops - format string vulnerability

Debian DSA-727-1 : libconvert-uulib-perl - buffer overflow

Debian DSA-728-2 : qpopper - missing privilege release

Debian DSA-729-1 : php4 - missing input sanitising

Debian DSA-730-1 : bzip2 - race condition

Debian DSA-731-1 : krb4 - buffer overflows

Debian DSA-732-1 : mailutils - several vulnerabilities

Debian DSA-733-1 : crip - insecure temporary files

Debian DSA-734-1 : gaim - denial of service

Debian DSA-735-1 : sudo - pathname validation race

Debian DSA-736-1 : spamassassin - remote denial of service

Debian DSA-737-1 : clamav - remote denial of service

Debian DSA-738-1 : razor - remote denial of service

Debian DSA-739-1 : trac - missing input sanitising

Debian DSA-740-1 : zlib - remote denial of service

Debian DSA-741-1 : bzip2 - infinite loop

Debian DSA-742-1 : cvs - buffer overflow

Debian DSA-743-1 : ht - buffer overflows, integer overflows

Debian DSA-744-1 : fuse - programming error

Debian DSA-745-1 : drupal - input validation errors

Debian DSA-746-1 : phpgroupware - input validation error

Debian DSA-747-1 : egroupware - input validation error

Debian DSA-748-1 : ruby1.8 - bad default value

Debian DSA-749-1 : ettercap - format string error

Debian DSA-750-1 : dhcpcd - out-of-bound memory access

Debian DSA-751-1 : squid - IP spoofing

Debian DSA-752-1 : gzip - several vulnerabilities

Debian DSA-753-1 : gedit - format string

Debian DSA-754-1 : centericq - insecure temporary file

Debian DSA-755-1 : tiff - buffer overflow

Debian DSA-756-1 : squirrelmail - several vulnerabilities

Debian DSA-757-1 : krb5 - buffer overflow, double-free memory

Debian DSA-758-1 : heimdal - buffer overflow

Debian DSA-759-1 : phppgadmin - missing input sanitising

Debian DSA-760-1 : ekg - several vulnerabilities

Debian DSA-761-2 : heartbeat - insecure temporary files

Debian DSA-762-1 : affix - several vulnerabilities

Debian DSA-763-1 : zlib - remote DoS

Debian DSA-764-1 : cacti - several vulnerabilities

Debian DSA-765-1 : heimdal - buffer overflow

Debian DSA-766-1 : webcalendar - authorisation failure

Debian DSA-767-1 : ekg - integer overflows

Debian DSA-768-1 : phpbb2 - missing input validation

Debian DSA-769-1 : gaim - memory alignment bug

Debian DSA-770-1 : gopher - insecure tmpfile creating

Debian DSA-771-1 : pdns - several vulnerabilities

Debian DSA-772-1 : apt-cacher - missing input sanitising

Debian DSA-773-1 : amd64 - several vulnerabilities

Debian DSA-774-1 : fetchmail - buffer overflow

Debian DSA-775-1 : mozilla-firefox - frame injection spoofing

Debian DSA-776-1 : clamav - integer overflows, infinite loop

Debian DSA-777-1 : mozilla - frame injection spoofing

Debian DSA-778-1 : mantis - missing input sanitising

Debian DSA-779-2 : mozilla-firefox - several vulnerabilities

Debian DSA-780-1 : kdegraphics - wrong input sanitising

Debian DSA-781-1 : mozilla-thunderbird - several vulnerabilities

Debian DSA-782-1 : bluez-utils - missing input sanitising

Debian DSA-783-1 : mysql-dfsg-4.1 - insecure temporary file

Debian DSA-784-1 : courier - programming error

Debian DSA-785-1 : libpam-ldap - authentication bypass

Debian DSA-786-1 : simpleproxy - format string vulnerability

Debian DSA-787-1 : backup-manager - insecure permissions and tempfile

Debian DSA-788-1 : kismet - several vulnerabilities

Debian DSA-789-1 : php4 - several vulnerabilities

Debian DSA-790-1 : phpldapadmin - programming error

Debian DSA-791-1 : maildrop - missing privilege release

Debian DSA-792-1 : pstotext - missing input sanitising

Debian DSA-793-1 : courier - missing input sanitising

Debian DSA-794-1 : polygen - programming error

Debian DSA-795-2 : proftpd - potential code execution

Debian DSA-796-1 : affix - remote command execution

Debian DSA-797-2 : zsync - denial of service

Debian DSA-798-1 : phpgroupware - several vulnerabilities

Debian DSA-799-1 : webcalendar - remote code execution

Debian DSA-800-1 : pcre3 - integer overflow

Debian DSA-801-1 : ntp - programming error

Debian DSA-802-1 : cvs - insecure temporary files

Debian DSA-803-1 : apache - programming error

Debian DSA-804-1 : kdelibs - insecure permissions

Debian DSA-805-1 : apache2 - several vulnerabilities

Debian DSA-806-1 : gcvs - insecure temporary files

Debian DSA-807-1 : libapache-mod-ssl - acl restriction bypass

Debian DSA-808-1 : tdiary - design error

Debian DSA-809-2 : squid - several vulnerabilities

Debian DSA-810-1 : mozilla - several vulnerabilities

Debian DSA-811-2 : common-lisp-controller - design error

Debian DSA-812-1 : turqstat - buffer overflow

Debian DSA-813-1 : centericq - several vulnerabilities

Debian DSA-814-1 : lm-sensors - insecure temporary file

Debian DSA-815-1 : kdebase - programming error

Debian DSA-816-1 : xfree86 - integer overflow

Debian DSA-817-1 : python2.2 - integer overflow

Debian DSA-818-1 : kdeedu - insecure temporary files

Debian DSA-819-1 : python2.1 - integer overflow

Debian DSA-820-1 : courier - missing input sanitising

Debian DSA-821-1 : python2.3 - integer overflow

Debian DSA-822-1 : gtkdiskfree - insecure temporary file creation

Debian DSA-823-1 : util-linux - privilege escalation

Debian DSA-824-1 : clamav - infinite loop, buffer overflow

Debian DSA-825-1 : loop-aes-utils - privilege escalation

Debian DSA-826-1 : helix-player - multiple vulnerabilities

Debian DSA-827-1 : backupninja - insecure temporary file

Debian DSA-828-1 : squid - authentication handling

Debian DSA-829-1 : mysql - buffer overflow

Debian DSA-830-1 : ntlmaps - wrong permissions

Debian DSA-831-1 : mysql-dfsg - buffer overflow

Debian DSA-832-1 : gopher - buffer overflows

Debian DSA-833-2 : mysql-dfsg-4.1 - buffer overflow

Debian DSA-834-1 : prozilla - buffer overflow

Debian DSA-835-1 : cfengine - insecure temporary files

Debian DSA-836-1 : cfengine2 - insecure temporary files

Debian DSA-837-1 : mozilla-firefox - buffer overflow

Debian DSA-838-1 : mozilla-firefox - multiple vulnerabilities

Debian DSA-839-1 : apachetop - insecure temporary file

Debian DSA-840-1 : drupal - missing input sanitising

Debian DSA-841-1 : mailutils - format string vulnerability

Debian DSA-842-1 : egroupware - missing input sanitising

Debian DSA-843-1 : arc - insecure temporary file

Debian DSA-844-1 : mod-auth-shadow - programming error

Debian DSA-845-1 : mason - programming error

Debian DSA-846-1 : cpio - several vulnerabilities

Debian DSA-847-1 : dia - missing input sanitising

Debian DSA-848-1 : masqmail - several vulnerabilities

Debian DSA-849-1 : shorewall - programming error

Debian DSA-850-1 : tcpdump - infinite loop

Debian DSA-851-1 : openvpn - programming errors

Debian DSA-852-1 : up-imapproxy - format string vulnerabilities

Debian DSA-853-1 : ethereal - several vulnerabilities

Debian DSA-854-1 : tcpdump - infinite loop

Debian DSA-855-1 : weex - format string vulnerability

Debian DSA-856-1 : py2play - design error

Debian DSA-857-1 : graphviz - insecure temporary file

Debian DSA-858-1 : xloadimage - buffer overflows

Debian DSA-859-1 : xli - buffer overflows

Debian DSA-860-1 : ruby - programming error

Debian DSA-861-1 : uw-imap - buffer overflow

Debian DSA-862-1 : ruby1.6 - programming error

Debian DSA-863-1 : xine-lib - format string vulnerability

Debian DSA-864-1 : ruby1.8 - programming error

Debian DSA-865-1 : hylafax - insecure temporary files

Debian DSA-866-1 : mozilla - several vulnerabilities

Debian DSA-867-1 : module-assistant - insecure temporary file

Debian DSA-868-1 : mozilla-thunderbird - several vulnerabilities

Debian DSA-869-1 : eric - missing input sanitising

Debian DSA-870-1 : sudo - missing input sanitising

Debian DSA-871-2 : libgda2 - format string

Debian DSA-872-1 : koffice - buffer overflow

Debian DSA-873-1 : net-snmp - programming error

Debian DSA-874-1 : lynx - buffer overflow

Debian DSA-875-1 : openssl094 - cryptographic weakness

Debian DSA-876-1 : lynx-ssl - buffer overflow

Debian DSA-877-1 : gnump3d - XSS, directory traversal

Debian DSA-878-1 : netpbm-free - buffer overflow

Debian DSA-879-1 : gallery - programming error

Debian DSA-880-1 : phpmyadmin - several vulnerabilities

Debian DSA-881-1 : openssl096 - cryptographic weakness

Debian DSA-882-1 : openssl095 - cryptographic weakness

Debian DSA-883-1 : thttpd - insecure temporary file

Debian DSA-884-1 : horde3 - design error

Debian DSA-885-1 : openvpn - several vulnerabilities

Debian DSA-886-1 : chmlib - several vulnerabilities

Debian DSA-887-1 : clamav - several vulnerabilities

Debian DSA-888-1 : openssl - cryptographic weakness

Debian DSA-889-1 : enigmail - programming error

Debian DSA-890-1 : libungif4 - several vulnerabilities

Debian DSA-891-1 : gpsdrive - format string

Debian DSA-892-1 : awstats - missing input sanitising

Debian DSA-893-1 : acidlab - missing input sanitising

Debian DSA-894-1 : abiword - buffer overflows

Debian DSA-895-1 : uim - programming error

Debian DSA-896-1 : linux-ftpd-ssl - buffer overflow

Debian DSA-897-1 : phpsysinfo - programming errors

Debian DSA-898-1 : phpgroupware - programming errors

Debian DSA-899-1 : egroupware - programming errors

Debian DSA-900-3 : fetchmail - programming error

Debian DSA-901-1 : gnump3d - programming error

Debian DSA-902-1 : xmail - buffer overflow

Debian DSA-903-2 : unzip - race condition

Debian DSA-904-1 : netpbm-free - buffer overflows

Debian DSA-905-1 : mantis - several vulnerabilities

Debian DSA-906-1 : sylpheed - buffer overflows

Debian DSA-907-1 : ipmenu - insecure temporary file

Debian DSA-908-1 : sylpheed-claws - buffer overflows

Debian DSA-909-1 : horde3 - missing input sanitising

Debian DSA-910-1 : zope.2.7 - design error

Debian DSA-911-1 : gtk+2.0 - several vulnerabilities

Debian DSA-912-1 : centericq - denial of service

Debian DSA-913-1 : gdk-pixbuf - several vulnerabilities

Debian DSA-914-1 : horde2 - missing input sanitising

Debian DSA-915-1 : helix-player - buffer overflow

Debian DSA-916-1 : inkscape - buffer overflow

Debian DSA-917-1 : courier - programming error

Debian DSA-918-1 : osh - programming error

Debian DSA-919-2 : curl - buffer overflow

Debian DSA-920-1 : ethereal - buffer overflow

Debian DSA-921-1 : kernel-source-2.4.27 - several vulnerabilities

Debian DSA-922-1 : kernel-source-2.6.8 - several vulnerabilities

Debian DSA-923-1 : dropbear - buffer overflow

Debian DSA-924-1 : nbd - buffer overflow

Debian DSA-925-1 : phpbb2 - several vulnerabilities

Debian DSA-926-2 : ketm - buffer overflow

Debian DSA-927-2 : tkdiff - insecure temporary file

Debian DSA-928-1 : dhis-tools-dns - insecure temporary file

Debian DSA-929-1 : petris - buffer overflow

Debian DSA-930-2 : smstools - format string attack

Debian DSA-931-1 : xpdf - buffer overflows

Debian DSA-932-1 : kdegraphics - buffer overflows

Debian DSA-933-1 : hylafax - arbitrary command execution

Debian DSA-934-1 : pound - several vulnerabilities

Debian DSA-935-1 : libapache2-mod-auth-pgsql - format string vulnerability

Debian DSA-936-1 : libextractor - buffer overflows

Debian DSA-937-1 : tetex-bin - buffer overflows

Debian DSA-938-1 : koffice - buffer overflows

Debian DSA-939-1 : fetchmail - programming error

Debian DSA-940-1 : gpdf - buffer overflows

Debian DSA-941-1 : tuxpaint - insecure temporary file

Debian DSA-942-1 : albatross - design error

Debian DSA-943-1 : perl - integer overflow

Debian DSA-944-1 : mantis - several vulnerabilities

Debian DSA-945-1 : antiword - insecure temporary file

Debian DSA-946-2 : sudo - missing input sanitising

Debian DSA-947-2 : clamav - heap overflow

Debian DSA-948-1 : kdelibs - buffer overflow

Debian DSA-949-1 : crawl - insecure program execution

Debian DSA-950-1 : cupsys - buffer overflows

Debian DSA-951-2 : trac - missing input sanitising

Debian DSA-952-1 : libapache-auth-ldap - format string

Debian DSA-953-1 : flyspray - missing input sanitising

Debian DSA-954-1 : wine - design flaw

Debian DSA-955-1 : mailman - DoS

Debian DSA-956-1 : lsh-server - filedescriptor leak

Debian DSA-957-2 : imagemagick - missing shell meta sanitising

Debian DSA-958-1 : drupal - several vulnerabilities

Debian DSA-959-1 : unalz - buffer overflow

Debian DSA-960-3 : libmail-audit-perl - insecure temporary file creation

Debian DSA-961-1 : pdfkit.framework - buffer overflows

Debian DSA-962-1 : pdftohtml - buffer overflows

Debian DSA-963-1 : mydns - missing input sanitising

Debian DSA-964-1 : gnocatan - buffer overflow

Debian DSA-965-1 : ipsec-tools - null dereference

Debian DSA-966-1 : adzapper - denial of service

Debian DSA-967-1 : elog - several vulnerabilities

Debian DSA-968-1 : noweb - insecure temporary file

Debian DSA-969-1 : scponly - design error

Debian DSA-970-1 : kronolith - missing input sanitising

Debian DSA-971-1 : xpdf - buffer overflow

Debian DSA-972-1 : pdfkit.framework - buffer overflows

Debian DSA-973-1 : otrs - several vulnerabilities

Debian DSA-974-1 : gpdf - buffer overflows

Debian DSA-975-1 : nfs-user-server - buffer overflow

Debian DSA-976-1 : libast - buffer overflow

Debian DSA-977-1 : heimdal - several vulnerabilities

Debian DSA-978-1 : gnupg - programming error

Debian DSA-979-1 : pdfkit.framework - several vulnerabilities

Debian DSA-980-1 : tutos - several vulnerabilities

Debian DSA-981-1 : bmv - integer overflow

Debian DSA-982-1 : gpdf - several vulnerabilities

Debian DSA-983-1 : pdftohtml - several vulnerabilities

Debian DSA-984-1 : xpdf - several vulnerabilities

Debian DSA-985-1 : libtasn1-2 - buffer overflows

Debian DSA-986-1 : gnutls11 - buffer overflows

Debian DSA-987-1 : tar - buffer overflow

Debian DSA-988-1 : squirrelmail - several vulnerabilities

Debian DSA-989-1 : zoph - SQL injection

Debian DSA-990-1 : bluez-hcidump - programming error

Debian DSA-991-1 : zoo - buffer overflow

Debian DSA-992-1 : ffmpeg - buffer overflow

Debian DSA-993-2 : gnupg - programming error

Debian DSA-994-1 : freeciv - denial of service

Debian DSA-995-1 : metamail - buffer overflow

Debian DSA-996-1 : libcrypt-cbc-perl - programming error

Debian DSA-997-1 : bomberclone - buffer overflows

Debian DSA-998-1 : libextractor - several vulnerabilities

Debian DSA-999-1 : lurker - several vulnerabilities

IBM General Parallel File System 3.4 < 3.4.0.27 / 3.5 < 3.5.0.16 DoS (Debian)

# Databases

Apache CouchDB 1.x / 2.1.x <= 2.1.2 Privilege Escalation

Apache CouchDB < 0.11.0 Hash Verification Information Leak

Apache CouchDB < 0.11.2 Futon admin interface Cross-Site Request Forgery

Apache CouchDB < 1.0.2 Futon Admin Interface XSS

Apache CouchDB < 1.0.4 / 1.1.2 / 1.2.1 Multiple Vulnerabilities

Apache CouchDB Detection

Apache CouchDB Unauthenticated Administrative Access

Apache Derby 'BUILTIN' Authentication Insecure Password Hashing

Cisco Mobility Services Engine Detection

Cisco Security Manager MySQL Accessible Without Authentication (cisco-sa-20090121-csm)

DB2 9.5 < Fix Pack 9 Multiple Vulnerabilities

DBTools DBManager catalog.mdb Plaintext Local Credential Disclosure

Default Password (db2admin) for 'db2admin' Account on Windows

Elasticsearch Transport Protocol Unspecified Remote Code Execution

Firebird DataBase Server fbserver.exe p\_cnct\_count Value Remote Overflow

Firebird DB Remote Database Name Overflow

Firebird Default Credentials

Firebird on Gentoo Linux /etc/conf.d/firebird Invocation ISC\_PASSWORD Authentication Bypass

HSQLDB Server Default Credentials

IBM DB2 10.1 < Fix Pack 1 Multiple Vulnerabilities

IBM DB2 10.1 < Fix Pack 3 Multiple Vulnerabilities

IBM DB2 10.1 < Fix Pack 3a Multiple Vulnerabilities

IBM DB2 10.1 < Fix Pack 5 Multiple Vulnerabilities (Bar Mitzvah)

IBM DB2 10.5 < Fix Pack 1 Security Bypass

IBM DB2 10.5 < Fix Pack 3a Multiple Vulnerabilities

IBM DB2 10.5 < Fix Pack 4 Multiple Vulnerabilities

IBM DB2 10.5 < Fix Pack 5 Multiple DoS Vulnerabilities

IBM DB2 10.5 < Fix Pack 6 Multiple Vulnerabilities (Bar Mitzvah)

IBM DB2 10.5 < Fix Pack 7 Multiple Vulnerabilities (Linux) (Bar Mitzvah) (FREAK) (Logjam)

IBM DB2 10.5 < Fix Pack 8 Multiple Vulnerabilities

IBM DB2 10.5 <= Fix Pack 5 Multiple Vulnerabilities

IBM DB2 8 < Fix Pack 17 Multiple Vulnerabilities

IBM DB2 8.1 < Fix Pack 18 Multiple Vulnerabilities

IBM DB2 9.1 < Fix Pack 10 Multiple Vulnerabilities

IBM DB2 9.1 < Fix Pack 11 Multiple DoS

IBM DB2 9.1 < Fix Pack 12 Multiple Vulnerabilities

IBM DB2 9.1 < Fix Pack 6 Multiple Vulnerabilities

IBM DB2 9.1 < Fix Pack 7 Multiple Vulnerabilities

IBM DB2 9.1 < Fix Pack 8 Multiple Vulnerabilities

IBM DB2 9.1 < Fix Pack 9 Multiple Vulnerabilities

IBM DB2 9.1 TLS/SSL Multiple DoS Vulnerabilities

IBM DB2 9.5 < Fix Pack 10 Multiple Vulnerabilities

IBM DB2 9.5 < Fix Pack 2 Multiple Vulnerabilities

IBM DB2 9.5 < Fix Pack 5 Multiple Unspecified Vulnerabilities

IBM DB2 9.5 < Fix Pack 6a Multiple Vulnerabilities

IBM DB2 9.5 < Fix Pack 7 Multiple Vulnerabilities

IBM DB2 9.5 <= Fix Pack 9 or 10 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 10 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 11 Multiple Vulnerabilities (Bar Mitzvah) (FREAK) (TLS POODLE)

IBM DB2 9.7 < Fix Pack 2 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 3 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 4 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 5 Multiple Denial of Service Vulnerabilities

IBM DB2 9.7 < Fix Pack 6 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 7 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 9 Multiple Vulnerabilities

IBM DB2 9.7 < Fix Pack 9a Multiple Vulnerabilities

IBM DB2 9.7 < FP11 39672 / 10.1 < FP6 39678 / 10.5 < FP10 39688 / 11.1.4 < FP5 39693 / 11.5 < FP0 39711 Multiple Vulnerabilities (UNIX)

IBM DB2 9.7 < FP11 Special Build 35317 / 10.1 < FP5 Special Build 35316 / 10.5 < FP7 Special Build 35315 Multiple Vulnerabilities (UNIX)

IBM DB2 9.7 < FP11 Special Build 36621 / 10.1 < FP6 Special Build 36610 / 10.5 < FP8 Special Build 36605 / 11.1.2 < FP2 Multiple Vulnerabilities (UNIX)

IBM DB2 9.7 < FP11 Special Build 36826 / 10.1 < FP6 Special Build 36827 / 10.5 < FP8 Special Build 36828 / 11.1.2.2 < FP2 Special Build 36792 Multiple Vulnerabilities (UNIX)

IBM DB2 9.7 < FP11 Special Build 37314 / 10.1 < FP6 Special Build 37313 / 10.5 < FP10 Special Build 37311 / 11.1.3 < FP3 JDBC Driver Unsafe Deserialization Local Privilege Escalation (UNIX)

IBM DB2 9.7 < FP11 Special Build 38744 / 10.1 < FP6 Special Build 38745 / 10.5 < FP10 Special Build 38746 / 11.1 < M4FP5 Buffer Overflow Vulnerability (UNIX)

IBM DB2 9.8 < Fix Pack 5 Multiple Vulnerabilities

IBM DB2 9.8 <= Fix Pack 5 Multiple Vulnerabilities

IBM DB2 < 8 Fix Pack 7a Multiple Vulnerabilities

IBM DB2 < 8.1 Fix Pack 13 CONNECT Processing Unspecified DoS

IBM DB2 < 8.1 Fix Pack 14 Multiple Vulnerabilities

IBM DB2 < 8.1 Fix Pack 16 Multiple Vulnerabilities

IBM DB2 < 8.1 FixPak 12 EXCSAT Long MGRLVLLS Message Remote DoS

IBM DB2 < 9 Fix Pack 2 Multiple Vulnerabilities

IBM DB2 < 9 Fix Pack 3 / 8 Fix Pack 15 Multiple Vulnerabilities

IBM DB2 < 9 Fix Pack 4 Multiple Vulnerabilities

IBM DB2 < 9 Fix Pack 5 Multiple Vulnerabilities

IBM DB2 < 9.5 Fix Pack 1 Multiple Vulnerabilities

IBM DB2 < 9.5 Fix Pack 4 Multiple Vulnerabilities

IBM DB2 Administration Server Detection

IBM DB2 Connection Port Detection

IBM DB2 Detection

IBM DB2 Discovery Service Detection

IBM DB2 Discovery Service Malformed UDP Packet Remote DoS

IBM DB2 Interrupt Port Detection

IBM DB2 JDBC Applet Server Detection

IBM DB2 Login Possible

IBM DB2 Multiple CGI Single Byte Request Remote DoS

IBM DB2 Stored Procedure Infrastructure Privilege Escalation Vulnerability

IBM DB2 Unsupported Version Detection

IBM Informix Dynamic Server 11.50.x / 11.70.x < 11.70.xC7 RCE (credentialed check)

IBM Informix Dynamic Server 11.50.xCn < 11.50.xC9 / 11.70.xCn < 11.70.xC9 / 12.10.xCn < 12.10.xC8W2 Multiple Vulnerabilities (SWEET32)

IBM Informix Dynamic Server 12.10.FC1 < 12.10.FC9W1 IBM Unspecified Local Privilege Escalation

IBM Informix Dynamic Server Detection (credentialed check)

IBM Informix Dynamic Server Detection (Linux/UNIX)

IBM solidDB 6.5 < 6.5.0.8 Interim Fix 6 Redundant WHERE Clause Select Statement Parsing Remote DoS

IBM solidDB 6.5 < 6.5.0.8 Multiple Denial of Service Vulnerabilities

IBM solidDB < 6.30.0.37 Invalid Error Code DoS

IBM solidDB < 7.0 Fix Pack 1 / 6.5.0.8 Interim Fix 5 Denial of Service

IBM solidDB Detection (local check)

IBM solidDB Password Hash Length Authentication Bypass

IBM solidDB Stored Procedure Call Remote Denial of Service

MariaDB 10 < 10.0.9 Multiple DoS Vulnerabilities

MariaDB 10.0.0 < 10.0.13 Multiple Vulnerabilities

MariaDB 10.0.0 < 10.0.15 Multiple Vulnerabilities

MariaDB 10.0.0 < 10.0.36 Multiple Vulnerabilities

MariaDB 10.0.0 < 10.0.37 Multiple Vulnerabilities

MariaDB 10.0.0 < 10.0.38 Multiple Vulnerabilities

MariaDB 10.0.0 < 10.0.8 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.20 Multiple Vulnerabilities (BACKRONYM)

MariaDB 10.0.x < 10.0.21 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.22 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.23 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.24 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.25 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.27 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.28 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.29 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.31 / 10.1.x < 10.1.23 / 10.2.x < 10.2.7 Multiple Vulnerabilities

MariaDB 10.0.x < 10.0.33 / 10.1.x < 10.1.27 Multiple Vulnerabilities

MariaDB 10.1 < 10.1.31 Multiple Vulnerabilities

MariaDB 10.1.0 < 10.1.35 Multiple Vulnerabilities

MariaDB 10.1.0 < 10.1.38 Multiple Vulnerabilities

MariaDB 10.1.0 < 10.1.39 Multiple Vulnerabilities

MariaDB 10.1.0 < 10.1.41 Multiple Vulnerabilities

MariaDB 10.1.0 < 10.1.44 A Vulnerability

MariaDB 10.1.x < 10.1.10 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.11 sql/sql\_yacc.yy SELECT Statement Keyword Handling DoS

MariaDB 10.1.x < 10.1.12 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.13 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.14 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.16 Multiple DoS

MariaDB 10.1.x < 10.1.17 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.18 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.19 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.20 Multiple DoS

MariaDB 10.1.x < 10.1.42 Denial Of Service Vulnerability

MariaDB 10.1.x < 10.1.5 wait\_for\_workers\_idle() Function Worker Thread Handling DoS

MariaDB 10.1.x < 10.1.6 Multiple DoS Vulnerabilities

MariaDB 10.1.x < 10.1.7 Multiple Vulnerabilities

MariaDB 10.1.x < 10.1.9 Multiple Vulnerabilities

MariaDB 10.2.0 < 10.2.17 Multiple Vulnerabilities

MariaDB 10.2.0 < 10.2.19 Multiple Vulnerabilities

MariaDB 10.2.0 < 10.2.22 Multiple Vulnerabilities

MariaDB 10.2.0 < 10.2.24 Multiple Vulnerabilities

MariaDB 10.2.0 < 10.2.26 Multiple Vulnerabilities

MariaDB 10.2.0 < 10.2.31 A Vulnerability

MariaDB 10.2.x < 10.2.10 Multiple Vulnerabilities

MariaDB 10.2.x < 10.2.28 Multiple Denial of Service Vulnerabilities

MariaDB 10.2.x < 10.2.3 Multiple DoS

MariaDB 10.3.0 < 10.3.13 Multiple Vulnerabilities

MariaDB 10.3.0 < 10.3.15 Multiple Vulnerabilities

MariaDB 10.3.0 < 10.3.17 Multiple Vulnerabilities

MariaDB 10.3.0 < 10.3.22 A Vulnerability

MariaDB 10.3.0 < 10.3.9 Multiple Vulnerabilities

MariaDB 10.3.1 < 10.3.2 Multiple DoS Vulnerabilities

MariaDB 10.3.x < 10.3.1 Multiple DoS Vulnerabilities

MariaDB 10.3.x < 10.3.19 Multiple Denial of Service Vulnerabilities

MariaDB 10.4.0 < 10.4.12 A Vulnerability

MariaDB 10.4.0 < 10.4.5 Multiple Vulnerabilities

MariaDB 10.4.0 < 10.4.7 Multiple Vulnerabilities

MariaDB 10.4.x < 10.4.9 Multiple Denial of Service Vulnerabilities

MariaDB 5.1 < 5.1.66 Buffer Overflow

MariaDB 5.1 < 5.1.67 Multiple Vulnerabilities

MariaDB 5.1 < 5.1.69 NAME\_CONST Query DoS

MariaDB 5.2 < 5.2.13 Buffer Overflow

MariaDB 5.2 < 5.2.14 Multiple Vulnerabilities

MariaDB 5.2 < 5.2.15 NAME\_CONST Query DoS

MariaDB 5.3 < 5.3.11 Buffer Overflow

MariaDB 5.3 < 5.3.12 Multiple Vulnerabilities

MariaDB 5.3 < 5.3.13 Multiple DoS Vulnerabilities

MariaDB 5.5 < 5.5.28 Multiple Vulnerabilities

MariaDB 5.5 < 5.5.28a Buffer Overflow

MariaDB 5.5 < 5.5.29 Multiple Vulnerabilities

MariaDB 5.5 < 5.5.30 Multiple Vulnerabilities

MariaDB 5.5 < 5.5.32 Multiple Vulnerabilities

MariaDB 5.5 < 5.5.35 Multiple Vulnerabilities

MariaDB 5.5 < 5.5.36 Multiple DoS Vulnerabilities

MariaDB 5.5 < 5.5.37 Multiple Vulnerabilities

MariaDB 5.5 < 5.5.47 Multiple Vulnerabilities

MariaDB 5.5 < 5.5.48 Multiple Vulnerabilities

MariaDB 5.5.0 < 5.5.39 Multiple Vulnerabilities

MariaDB 5.5.0 < 5.5.42 Multiple Vulnerabilities

MariaDB 5.5.0 < 5.5.63 A Vulnerability

MariaDB 5.5.0 < 5.5.64 Multiple Vulnerabilities

MariaDB 5.5.0 < 5.5.65 Multiple Vulnerabilities

MariaDB 5.5.0 < 5.5.67 A Vulnerability

MariaDB 5.5.43 < 5.5.44 'ADD INDEX' Statement DoS

MariaDB 5.5.x < 5.5.45 Multiple Vulnerabilities

MariaDB 5.5.x < 5.5.49 Multiple Vulnerabilities

MariaDB 5.5.x < 5.5.50 utf8mb4 Column Search DoS

MariaDB 5.5.x < 5.5.51 Multiple Vulnerabilities

MariaDB 5.5.x < 5.5.52 Multiple Vulnerabilities

MariaDB 5.5.x < 5.5.54 Multiple Vulnerabilities

MariaDB 5.5.x < 5.5.55 / 10.0.x < 10.0.30 / 10.1.x < 10.1.22 / 10.2.x < 10.2.5 Multiple Vulnerabilities

MariaDB 5.5.x < 5.5.62 Multiple Vulnerabilities

MariaDB 5.5.x < 5.5.66 Denial of Service Vulnerability

MariaDB < 5.5.46 Multiple Vulnerabilities

MariaDB Binary Log SQL Injection

MariaDB Client/Server Installed (Linux)

MariaDB Server Installed (Windows)

Microsoft SQL Server < 7 Local Privilege Escalation

Microsoft SQL Server Authentication Function Remote Overflow

Microsoft SQL Server Default Credentials

Microsoft SQL Server Default Credentials (PCI wordlist)

Microsoft SQL Server Detection (credentialed check)

Microsoft SQL Server Login Possible

Microsoft SQL Server sa Account Default Blank Password

Microsoft SQL Server TCP/IP Listener Product Database Detection

Microsoft SQL Server UDP Query Remote Version Disclosure

Microsoft SQL Server Unsupported Version Detection

Microsoft SQL Server Unsupported Version Detection (remote check)

MobiLink Server < 10.0.1 build 3649 mlsrv10.exe Multiple Remote Overflows

MongoDB 2.4 / 2.6 Denial of Service Vulnerability

MongoDB 2.4.x < 2.4.13 / 2.6.x < 2.6.8 / 3.0.x < 3.0.0-rc9 mongod BSON DoS

MongoDB 2.6.x < 2.6.9, 3.0.x < 3.0.14, 3.2.x < 3.2.8 mongod

MongoDB 3.0.x < 3.0.7 / 3.1.x < 3.1.9 Authentication Bypass

MongoDB 3.4.x < 3.4.10 / 3.5.x < 3.6.0-rc0 mongod

MongoDB < 2.3.2 BSON Object Length Handling Memory Disclosure

MongoDB < 2.4.5 / 2.5.1 Multiple Vulnerabilities

MongoDB Service Without Authentication Detection

MongoDB Unauthenticated REST API Detection

MongoDB Web Interface Detection

MS02-061: Microsoft SQL Server Multiple Vulnerabilities (uncredentialed check)

MS99-059: Microsoft SQL Server Crafted TCP Packet Remote DoS (uncredentialed check)

MySQL 3.20.32 - 3.23.52 Weak Default Configuration

MySQL 3.x Password Disclosure

MySQL 4.1 < 4.1.24 MyISAM Create Table Privilege Check Bypass

MySQL 4.1 < 4.1.3 Multiple Vulnerabilities

MySQL 5.0 < 5.0.40 Multiple Vulnerabilities

MySQL 5.0 < 5.0.88 Multiple Vulnerabilities

MySQL 5.0 < 5.0.95 Multiple Vulnerabilities

MySQL 5.0.18 Information Leak

MySQL 5.0.95 MyISAM Table Symbolic Link Local Restriction Bypass

MySQL 5.1 < 5.1.18 Multiple Vulnerabilities

MySQL 5.1 < 5.1.26 Empty Bit-String Literal Token SQL Statement DoS

MySQL 5.1 < 5.1.32 XPath Expression DoS

MySQL 5.1 < 5.1.41 Multiple Vulnerabilities

MySQL 5.1 < 5.1.61 Multiple Vulnerabilities

MySQL 5.1 < 5.1.62 Multiple Vulnerabilities

MySQL 5.1 < 5.1.63 Multiple Vulnerabilities

MySQL 5.1 < 5.1.64 Multiple Vulnerabilities

MySQL 5.1 < 5.1.65 Multiple Vulnerabilities

MySQL 5.1 < 5.1.66 Multiple Vulnerabilities

MySQL 5.1 < 5.1.67 Multiple Vulnerabilities

MySQL 5.1 < 5.1.68 Multiple Vulnerabilities

MySQL 5.1 < 5.1.69 Multiple Vulnerabilities

MySQL 5.1 < 5.1.70 Multiple Vulnerabilities

MySQL 5.1 < 5.1.71 Server Optimizer Denial of Service

MySQL 5.1.x < 5.1.72 Multiple Vulnerabilities

MySQL 5.1.x < 5.1.73 Multiple Vulnerabilities

MySQL 5.1.x < 5.7.3 SSL/TLS Downgrade MitM (BACKRONYM)

MySQL 5.5 < 5.5.20 Multiple Vulnerabilities

MySQL 5.5 < 5.5.22 Multiple Vulnerabilities

MySQL 5.5 < 5.5.23 Multiple Unspecified Vulnerabilities

MySQL 5.5 < 5.5.24 Security Bypass Vulnerability

MySQL 5.5 < 5.5.26 Multiple Vulnerabilities

MySQL 5.5 < 5.5.27 Multiple Vulnerabilities

MySQL 5.5 < 5.5.28 Multiple Vulnerabilities

MySQL 5.5 < 5.5.29 Multiple Vulnerabilities

MySQL 5.5 < 5.5.30 yaSSL Buffer Overflow

MySQL 5.5 < 5.5.31 Multiple Vulnerabilities

MySQL 5.5 < 5.5.32 Multiple Vulnerabilities

MySQL 5.5 < 5.5.33 Multiple Vulnerabilities

MySQL 5.5 < 5.5.34 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.35 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.36 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.37 MySQL Multiple Vulnerabilities

MySQL 5.5.x < 5.5.38 MySQL Multiple Vulnerabilities

MySQL 5.5.x < 5.5.39 Multiple Vulnerabilities (October 2014 CPU)

MySQL 5.5.x < 5.5.40 / 5.6.x < 5.6.21 Multiple Vulnerabilities (October 2014 CPU)

MySQL 5.5.x < 5.5.41 / 5.6.x < 5.6.22 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.42 / 5.6.x < 5.6.23 Multiple DoS Vulnerabilities (April 2015 CPU)

MySQL 5.5.x < 5.5.43 / 5.6.x < 5.6.24 Multiple DoS Vulnerabilities (April 2015 CPU)

MySQL 5.5.x < 5.5.44 / 5.6.x < 5.6.25 Multiple Vulnerabilities (July 2015 CPU)

MySQL 5.5.x < 5.5.45 / 5.6.x < 5.6.26 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.46 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.47 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.48 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.49 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.50 Multiple Vulnerabilities (July 2016 CPU)

MySQL 5.5.x < 5.5.51 Multiple DoS

MySQL 5.5.x < 5.5.51 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.52 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.52 Multiple Vulnerabilities

MySQL 5.5.x < 5.5.53 Multiple Vulnerabilities (October 2016 CPU)

MySQL 5.5.x < 5.5.53 Multiple Vulnerabilities (October 2016 CPU)

MySQL 5.5.x < 5.5.54 Multiple Vulnerabilities (January 2017 CPU)

MySQL 5.5.x < 5.5.54 Multiple Vulnerabilities (January 2017 CPU)

MySQL 5.5.x < 5.5.55 Multiple Vulnerabilities (April 2017 CPU) (Riddle)

MySQL 5.5.x < 5.5.55 Multiple Vulnerabilities (April 2017 CPU) (Riddle)

MySQL 5.5.x < 5.5.57 Multiple Vulnerabilities (July 2017 CPU)

MySQL 5.5.x < 5.5.57 Multiple Vulnerabilities (July 2017 CPU)

MySQL 5.5.x < 5.5.58 Multiple Vulnerabilities (October 2017 CPU)

MySQL 5.5.x < 5.5.58 Multiple Vulnerabilities (RPM Check) (October 2017 CPU)

MySQL 5.5.x < 5.5.59 Multiple Vulnerabilities (January 2018 CPU)

MySQL 5.5.x < 5.5.59 Multiple Vulnerabilities (RPM Check) (January 2018 CPU)

MySQL 5.5.x < 5.5.60 Multiple Vulnerabilities (April 2018 CPU)

MySQL 5.5.x < 5.5.60 Multiple Vulnerabilities (RPM Check) (April 2018 CPU)

MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (July 2018 CPU)

MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (RPM Check) (July 2018 CPU)

MySQL 5.5.x < 5.5.62 Multiple Vulnerabilities (October 2018 CPU)

MySQL 5.6.x < 5.6.11 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.12 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.13 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.14 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.15 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.16 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.17 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.19 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.20 client.c mysql\_prune\_stmt\_list() Function DoS (April 2017 CPU)

MySQL 5.6.x < 5.6.20 Multiple Vulnerabilities (October 2014 CPU)

MySQL 5.6.x < 5.6.27 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.28 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.29 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.30 Multiple Vulnerabilities (DROWN)

MySQL 5.6.x < 5.6.31 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.32 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.32 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.33 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.33 Multiple Vulnerabilities

MySQL 5.6.x < 5.6.34 Multiple Vulnerabilities (October 2016 CPU) (SWEET32)

MySQL 5.6.x < 5.6.34 Multiple Vulnerabilities (October 2016 CPU) (SWEET32)

MySQL 5.6.x < 5.6.35 Multiple Vulnerabilities (January 2017 CPU)

MySQL 5.6.x < 5.6.35 Multiple Vulnerabilities (January 2017 CPU)

MySQL 5.6.x < 5.6.36 Multiple Vulnerabilities (April 2017 CPU) (July 2017 CPU) (Riddle)

MySQL 5.6.x < 5.6.36 Multiple Vulnerabilities (April 2017 CPU) (July 2017 CPU) (Riddle)

MySQL 5.6.x < 5.6.37 Multiple Vulnerabilities (July 2017 CPU) (October 2017 CPU)

MySQL 5.6.x < 5.6.37 Multiple Vulnerabilities (RPM Check) (July 2017 CPU) (October 2017 CPU)

MySQL 5.6.x < 5.6.38 Multiple Vulnerabilities (October 2017 CPU)

MySQL 5.6.x < 5.6.38 Multiple Vulnerabilities (RPM Check) (October 2017 CPU)

MySQL 5.6.x < 5.6.39 Multiple Vulnerabilities (January 2018 CPU)

MySQL 5.6.x < 5.6.39 Multiple Vulnerabilities (RPM Check) (January 2018 CPU)

MySQL 5.6.x < 5.6.40 Multiple Vulnerabilities (April 2018 CPU)

MySQL 5.6.x < 5.6.40 Multiple Vulnerabilities (RPM Check) (April 2018 CPU)

MySQL 5.6.x < 5.6.41 Multiple Vulnerabilities (July 2018 CPU)

MySQL 5.6.x < 5.6.41 Multiple Vulnerabilities (RPM Check) (April 2018 CPU)

MySQL 5.6.x < 5.6.42 Multiple Vulnerabilities (October 2018 CPU)

MySQL 5.6.x < 5.6.43 Multiple Vulnerabilities (Jan 2019 CPU)

MySQL 5.6.x < 5.6.44 Multiple Vulnerabilities (Apr 2019 CPU)

MySQL 5.6.x < 5.6.45 Multiple Vulnerabilities (Jul 2019 CPU)

MySQL 5.6.x < 5.6.46 Multiple Vulnerabilities (Oct 2019 CPU)

MySQL 5.6.x < 5.6.47 Multiple Vulnerabilities (Jan 2020 CPU)

MySQL 5.6.x < 5.6.48 Multiple Vulnerabilities (Apr 2020 CPU)

MySQL 5.7.x < 5.7.10 Multiple DoS

MySQL 5.7.x < 5.7.11 Multiple Vulnerabilities

MySQL 5.7.x < 5.7.12 Multiple Vulnerabilities (DROWN)

MySQL 5.7.x < 5.7.13 Multiple Vulnerabilities

MySQL 5.7.x < 5.7.14 Multiple Vulnerabilities

MySQL 5.7.x < 5.7.14 Multiple Vulnerabilities

MySQL 5.7.x < 5.7.15 Multiple Vulnerabilities

MySQL 5.7.x < 5.7.15 Multiple Vulnerabilities

MySQL 5.7.x < 5.7.16 Multiple Vulnerabilities (October 2016 CPU) (SWEET32)

MySQL 5.7.x < 5.7.16 Multiple Vulnerabilities (October 2016 CPU) (SWEET32)

MySQL 5.7.x < 5.7.17 Multiple Vulnerabilities (January 2017 CPU) (July 2017 CPU)

MySQL 5.7.x < 5.7.17 Multiple Vulnerabilities (January 2017 CPU) (July 2017 CPU)

MySQL 5.7.x < 5.7.18 Multiple Vulnerabilities (April 2017 CPU) (July 2017 CPU)

MySQL 5.7.x < 5.7.18 Multiple Vulnerabilities (April 2017 CPU) (July 2017 CPU)

MySQL 5.7.x < 5.7.19 Multiple Vulnerabilities (Jul 2017 CPU) (Oct 2017 CPU) (Jul 2019 CPU)

MySQL 5.7.x < 5.7.19 Multiple Vulnerabilities (RPM Check) (July 2017 CPU) (October 2017 CPU)

MySQL 5.7.x < 5.7.20 Multiple Vulnerabilities (October 2017 CPU)

MySQL 5.7.x < 5.7.20 Multiple Vulnerabilities (RPM Check) (Oct 2017 CPU)

MySQL 5.7.x < 5.7.21 Multiple Vulnerabilities (January 2018 CPU)

MySQL 5.7.x < 5.7.21 Multiple Vulnerabilities (RPM Check) (January 2018 CPU)

MySQL 5.7.x < 5.7.22 Multiple Vulnerabilities (April 2018 CPU)

MySQL 5.7.x < 5.7.22 Multiple Vulnerabilities (RPM Check) (April 2018 CPU)

MySQL 5.7.x < 5.7.23 Multiple Vulnerabilities (July 2018 CPU)

MySQL 5.7.x < 5.7.23 Multiple Vulnerabilities (RPM Check) (July 2018 CPU)

MySQL 5.7.x < 5.7.24 Multiple Vulnerabilities (Oct 2018 CPU) (Jul 2019 CPU)

MySQL 5.7.x < 5.7.25 Multiple Vulnerabilities (Jan 2019 CPU)

MySQL 5.7.x < 5.7.26 Multiple Vulnerabilities (Apr 2019 CPU) (Jul 2019 CPU)

MySQL 5.7.x < 5.7.27 Multiple Vulnerabilities (Jul 2019 CPU)

MySQL 5.7.x < 5.7.28 Multiple Vulnerabilities (Oct 2019 CPU)

MySQL 5.7.x < 5.7.29 Multiple Vulnerabilities (Jan 2020 CPU)

MySQL 5.7.x < 5.7.30 Multiple Vulnerabilities (Jan 2020 CPU)

MySQL 6.0 < 6.0.10 XPath Expression DoS

MySQL 6.0 < 6.0.6 Empty Bit-String Literal Token SQL Statement DoS

MySQL 8.0.x < 8.0.12 Multiple Vulnerabilities (Jul 2018 CPU) (Jul 2019 CPU)

MySQL 8.0.x < 8.0.12 Multiple Vulnerabilities (RPM Check) (July 2018 CPU)

MySQL 8.0.x < 8.0.13 Multiple Vulnerabilities (Oct 2018 CPU) (Jul 2019 CPU)

MySQL 8.0.x < 8.0.14 Multiple Vulnerabilities (Jan 2019 CPU)

MySQL 8.0.x < 8.0.16 Multiple Vulnerabilities (Apr 2019 CPU) (Jul 2019 CPU)

MySQL 8.0.x < 8.0.17 Multiple Vulnerabilities (July 2019 CPU)

MySQL 8.0.x < 8.0.18 Multiple Vulnerabilities (Oct 2019 CPU)

MySQL 8.0.x < 8.0.19 Multiple Vulnerabilities (Jan 2020 CPU)

MySQL 8.0.x < 8.0.20 Multiple Vulnerabilities (Apr 2020 CPU)

MySQL < 5.0.54 / 5.1.23 / 6.0.4 Denial of Service

MySQL < 3.22 Readable Logs

MySQL < 3.23.31 Buffer Overflow

MySQL < 3.23.33 Multiple Buffer Overflows

MySQL < 3.23.36 Multiple Vulnerabilities

MySQL < 3.23.50 / 4.0.2 Local Code Execution

MySQL < 3.23.50 / 4.0.24 / 4.1.6 / 5.0.3 Insecure Temporary File Creation

MySQL < 3.23.54 / 4.0.6 Multiple Vulnerabilities

MySQL < 3.23.55 mysql\_change\_user() Double-free Memory Pointer DoS

MySQL < 3.23.56 Writable Configuration Files

MySQL < 3.23.59 / 4.0.21 Multiple Vulnerabilities

MySQL < 4.0.14 libmysqlclient Buffer Overflow

MySQL < 4.0.20 File Overwrite

MySQL < 4.0.21 Multiple Vulnerabilities

MySQL < 4.0.21 mysql\_real\_connect() Function Remote Overflow

MySQL < 4.0.21 mysqlhotcopy Insecure Temporary File Creation

MySQL < 4.0.24 / 4.1.10a Multiple Vulnerabilities

MySQL < 4.0.25 / 4.1.13 / 5.0.7 Multiple Vulnerabilies

MySQL < 4.0.27 / 4.1.19 / 5.0.21 Multiple Vulnerabilities

MySQL < 4.1.12 / 5.0.4 Insecure Permissions

MySQL < 4.1.13 / 5.0.8 DOS Device Name Denial of Service Vulnerabilities

MySQL < 4.1.13 Denial of Service

MySQL < 4.1.13a / 5.0.10 Zlib Library Buffer Overflow

MySQL < 4.1.13a / 5.0.11 Zlib Library Buffer Overflow

MySQL < 4.1.18 / 5.0.19 / 5.1.6 Denial of Service

MySQL < 4.1.2 Insecure Temporary File Creation

MySQL < 4.1.20 / 5.0.22 / 5.1.11 SQL Injection

MySQL < 4.1.21 / 5.0 Denial of Service

MySQL < 4.1.21 / 5.0.24 Privilege Persistence

MySQL < 4.1.21 / 5.0.25 / 5.1.12 Access Control

MySQL < 4.1.23 / 5.0.42 Access Control Vulnerability

MySQL < 5.0.22 / 5.1.10 Authentication Bypass

MySQL < 5.0.23 / 5.1.12 Denial of Service

MySQL < 5.0.25 / 5.1.12 Privilege Escalation

MySQL < 5.0.32 / 5.1.14 Denial of Service

MySQL < 5.0.36 Denial of Service

MySQL < 5.0.51a / 5.1.23 / 6.0.4 Multiple Vulnerabilities

MySQL < 5.0.83 Denial of Service

MySQL < 5.0.88 / 5.1.42 / 5.5.0 / 6.0.14 MyISAM CREATE TABLE Privilege Check Bypass

MySQL < 5.0.89 / 5.1.42 / 5.4.2 / 5.5.1 / 6.0.14 Client XSS

MySQL < 5.0.90 / 5.1.43 / 5.5.0-m2 Multiple Buffer Overflows

MySQL < 5.0.92 Multiple Denial of Service

MySQL < 5.5.6 Multiple Denial of Service

MySQL < 6.0.9-alpha / 5.5.3 Access Control Weakness

MySQL Anonymous Login Handshake Remote Information Disclosure

MySQL Authentication Protocol Token Comparison Casting Failure Password Bypass

MySQL Binary Log SQL Injection

MySQL Cluster 7.2.x < 7.2.20 General Subcomponent DoS (January 2017 CPU)

MySQL Cluster 7.2.x < 7.2.26 Multiple DoS (January 2017 CPU)

MySQL Cluster 7.2.x < 7.2.27 NDBAPI Subcomponent Buffer Overflow (January 2017 CPU)

MySQL Cluster 7.2.x < 7.2.28 DD Subcomponent Arbitrary Data Manipulation (April 2017 CPU)

MySQL Cluster 7.2.x < 7.2.33 / 7.3.x < 7.3.21 / 7.4.x < 7.4.19 / 7.5.x < 7.5.10 Denial of Service Vulnerability

MySQL Cluster 7.3.x < 7.3.15 Multiple Vulnerabilities (January 2017 CPU)

MySQL Cluster 7.3.x < 7.3.17 DD Subcomponent Arbitrary Data Manipulation (April 2017 CPU)

MySQL Cluster 7.3.x < 7.3.6 CLSTCONF RCE (July 2017 CPU)

MySQL Cluster 7.3.x < 7.3.9 General Subcomponent DoS (January 2017 CPU)

MySQL Cluster 7.4.x < 7.4.13 Multiple Vulnerabilities (January 2017 CPU)

MySQL Cluster 7.4.x < 7.4.15 DD Subcomponent Arbitrary Data Manipulation (April 2017 CPU)

MySQL Cluster 7.4.x < 7.4.6 General Subcomponent DoS (January 2017 CPU)

MySQL Cluster 7.5.x < 7.5.6 DD Subcomponent Arbitrary Data Manipulation (April 2017 CPU)

MySQL Community Server 5.0 < 5.0.45 Multiple Vulnerabilities

MySQL Community Server 5.0 < 5.0.51 RENAME TABLE Symlink System Table Overwrite

MySQL Community Server 5.0 < 5.0.67 Multiple Vulnerabilities

MySQL Community Server 5.1 < 5.1.46 Multiple Vulnerabilities

MySQL Community Server 5.1 < 5.1.52 Multiple Vulnerabilities

MySQL Community Server < 5.1.23 / 6.0.4 Multiple Vulnerabilities

MySQL Community Server < 5.1.47 / 5.0.91 Multiple Vulnerabilities

MySQL Community Server < 5.1.48 Denial of Service

MySQL Community Server < 5.1.49 Multiple Vulnerabilities

MySQL Community Server < 5.1.51 Multiple Vulnerabilities

MySQL Crafted IF Clause Divide-by-zero NULL Dereference DoS

MySQL datadir/my.cnf Modification Privilege Escalation

MySQL debian.cnf Plaintext Credential Disclosure

MySQL Default Account Credentials

MySQL Enterprise Server 5.0 < 5.0.52 Multiple Vulnerabilities

MySQL Enterprise Server 5.0 < 5.0.60 MyISAM CREATE TABLE Privilege Check Bypass

MySQL Enterprise Server 5.0 < 5.0.66 Empty Bit-String Literal Token SQL Statement DoS

MySQL Enterprise Server 5.0 < 5.0.70 Privilege Bypass

MySQL Enterprise Server 5.6.x < 5.6.29 / 5.7.x < 5.7.11 OpenSSL Multiple Vulnerabilities

MySQL libmysqlclient Prepared Statements API Overflow

MySQL Protocol Remote User Enumeration

MySQL Server COM\_CHANGE\_USER Command Security Bypass

MySQL Server Detection

MySQL Server Installed (Linux)

MySQL Server Login Possible

MySQL Short Check String Authentication Bypass

MySQL Single Row Subselect Remote DoS

MySQL sql\_acl.cc get\_salt\_from\_password Function Password Handling Remote Overflow

MySQL Unpassworded Account Check

MySQL Unsupported Version Detection

MySQL User-Defined Functions Multiple Vulnerabilities

MySQL Weak Hash Algorithm

MySQL Zero-length Scrambled String Crafted Packet Authentication Bypass

Openlink Virtuoso Server Default Credentials

Oracle 10g DBMS\_SCHEDULER Privilege Escalation

Oracle 8i/9i Database Server UTL\_FILE Traversal Arbitrary File Manipulation

Oracle 9iAS \_pages Directory Compiled JSP Source Disclosure

Oracle 9iAS Default SOAP Configuration Unauthorized Application Deployment

Oracle 9iAS DMS / JPM Pages Anonymous Access

Oracle 9iAS globals.jsa Database Credential Remote Disclosure

Oracle 9iAS Java Process Manager /oprocmgr-status Anonymous Process Manipulation

Oracle 9iAS mod\_plsql DAD Admin Interface Access

Oracle 9iAS mod\_plsql Encoded Traversal Arbitrary File Access

Oracle 9iAS mod\_plsql Help Page Request Remote Overflow

Oracle 9iAS Nonexistent .jsp File Request Error Message Path Disclosure

Oracle 9iAS OWA\_UTIL Stored Procedures Information Disclosure

Oracle 9iAS PL/SQL Gateway Web Admin Interface Null Authentication

Oracle 9iAS soapdocs Directory Remote Information Disclosure

Oracle 9iAS XSQLServlet soapConfig.xml Authentication Credentials Disclosure

Oracle Application Server 9i Webcache < 9.0.4.0 Multiple Vulnerabilities

Oracle Application Server ndwfn4.so HTTP Request Remote Overflow

Oracle Application Server Portal 10g Authentication Bypass

Oracle Application Server Web Cache <= 9.0.4.0 Multiple Vulnerabilities

Oracle Application Server Web Cache HTTP Request Overflow

Oracle Application Server Web Cache Multiple Remote DoS

Oracle Application Server Webcache Requests OHS mod\_access Restriction Bypass

Oracle Application Server XSQL Stylesheet Arbitrary Java Code Execution

Oracle Application Server XSQLServlet XSQLConfig.xml Information Disclosure

Oracle Database 10g Multiple Remote Vulnerabilities

Oracle Database 9i Multiple Functions Local Overflow

Oracle Database 9i/10g Fine Grained Auditing (FGA) SELECT Statement Logging Weakness

Oracle Database Listener Program (tnslsnr) Service Blank Password

Oracle Database Multiple Remote Vulnerabilities (Mar 2005)

Oracle Database Multiple Vulnerabilities (April 2006 CPU)

Oracle Database Multiple Vulnerabilities (April 2007 CPU)

Oracle Database Multiple Vulnerabilities (April 2008 CPU)

Oracle Database Multiple Vulnerabilities (April 2009 CPU)

Oracle Database Multiple Vulnerabilities (April 2010 CPU)

Oracle Database Multiple Vulnerabilities (April 2011 CPU)

Oracle Database Multiple Vulnerabilities (April 2012 CPU)

Oracle Database Multiple Vulnerabilities (April 2013 CPU)

Oracle Database Multiple Vulnerabilities (April 2014 CPU)

Oracle Database Multiple Vulnerabilities (April 2015 CPU)

Oracle Database Multiple Vulnerabilities (April 2016 CPU)

Oracle Database Multiple Vulnerabilities (April 2017 CPU)

Oracle Database Multiple Vulnerabilities (January 2005 CPU)

Oracle Database Multiple Vulnerabilities (January 2006 CPU)

Oracle Database Multiple Vulnerabilities (January 2007 CPU)

Oracle Database Multiple Vulnerabilities (January 2008 CPU)

Oracle Database Multiple Vulnerabilities (January 2009 CPU)

Oracle Database Multiple Vulnerabilities (January 2010 CPU)

Oracle Database Multiple Vulnerabilities (January 2011 CPU)

Oracle Database Multiple Vulnerabilities (January 2012 CPU)

Oracle Database Multiple Vulnerabilities (January 2013 CPU)

Oracle Database Multiple Vulnerabilities (January 2014 CPU)

Oracle Database Multiple Vulnerabilities (January 2015 CPU)

Oracle Database Multiple Vulnerabilities (January 2016 CPU)

Oracle Database Multiple Vulnerabilities (January 2017 CPU)

Oracle Database Multiple Vulnerabilities (January 2018 CPU)

Oracle Database Multiple Vulnerabilities (July 2006 CPU)

Oracle Database Multiple Vulnerabilities (July 2007 CPU)

Oracle Database Multiple Vulnerabilities (July 2008 CPU)

Oracle Database Multiple Vulnerabilities (July 2009 CPU)

Oracle Database Multiple Vulnerabilities (July 2010 CPU)

Oracle Database Multiple Vulnerabilities (July 2011 CPU)

Oracle Database Multiple Vulnerabilities (July 2012 CPU)

Oracle Database Multiple Vulnerabilities (July 2013 CPU)

Oracle Database Multiple Vulnerabilities (July 2014 CPU)

Oracle Database Multiple Vulnerabilities (July 2015 CPU)

Oracle Database Multiple Vulnerabilities (July 2016 CPU) (FREAK)

Oracle Database Multiple Vulnerabilities (July 2017 CPU) (POODLE) (SWEET32)

Oracle Database Multiple Vulnerabilities (October 2005 CPU)

Oracle Database Multiple Vulnerabilities (October 2006 CPU)

Oracle Database Multiple Vulnerabilities (October 2007 CPU)

Oracle Database Multiple Vulnerabilities (October 2008 CPU)

Oracle Database Multiple Vulnerabilities (October 2009 CPU)

Oracle Database Multiple Vulnerabilities (October 2010 CPU)

Oracle Database Multiple Vulnerabilities (October 2011 CPU)

Oracle Database Multiple Vulnerabilities (October 2012 CPU)

Oracle Database Multiple Vulnerabilities (October 2013 CPU) (BEAST)

Oracle Database Multiple Vulnerabilities (October 2014 CPU)

Oracle Database Multiple Vulnerabilities (October 2015 CPU)

Oracle Database Multiple Vulnerabilities (October 2016 CPU)

Oracle Database Multiple Vulnerabilities (October 2017 CPU)

Oracle Database Patch Info (credentialed check)

Oracle Database Patch Info (Unix / Linux) (credentialed check) (deprecated)

Oracle Database Patch Info (Windows) (credentialed check)

Oracle Database Server CVE-2018-3110

Oracle Database Server Java VM Unspecified Remote Code Execution (April 2018 CPU)

Oracle Database Server Multiple Vulnerabilities (Apr 2019 CPU)

Oracle Database Server Multiple Vulnerabilities (Apr 2020 CPU)

Oracle Database Server Multiple Vulnerabilities (Jan 2019 CPU)

Oracle Database Server Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Database Server Multiple Vulnerabilities (Jul 2019 CPU)

Oracle Database Server Multiple Vulnerabilities (July 2018 CPU)

Oracle Database Server Multiple Vulnerabilities (Oct 2019 CPU)

Oracle Database Server Multiple Vulnerabilities (October 2018 CPU)

Oracle Database tnslsnr Service Remote Version Disclosure

Oracle Database Unsupported Version Detection

Oracle DB Login Possible

Oracle Default Accounts

Oracle Default SID

Oracle Enterprise Manager Web Console Detection

Oracle JSP Apache/Jserv Path Translation Arbitrary JSP File Execution

Oracle Listener Program Logging Privilege Escalation (1361722)

Oracle Multiple Products SOAP Message Crafted DTD Remote DoS

Oracle MySQL 5.5.x < 5.5.32 Optimizer DoS (January 2016 CPU)

Oracle MySQL 5.5.x < 5.5.43 Optimizer DoS (July 2015 CPU)

Oracle MySQL 5.5.x < 5.5.44 Multiple Vulnerabilities (July 2015 CPU) (October 2015 CPU)

Oracle MySQL 5.5.x < 5.5.45 Multiple Vulnerabilities (October 2015 CPU)

Oracle MySQL 5.5.x < 5.5.46 Multiple Vulnerabilities (October 2015 CPU) (January 2016 CPU) (July 2016 CPU)

Oracle MySQL 5.5.x < 5.5.47 Multiple Vulnerabilities (January 2016 CPU) (April 2016 CPU)

Oracle MySQL 5.5.x < 5.5.48 Multiple Vulnerabilities (April 2016 CPU)

Oracle MySQL 5.5.x < 5.5.49 Multiple Vulnerabilities (April 2016 CPU) (July 2016 CPU)

Oracle MySQL 5.5.x < 5.5.50 Multiple Vulnerabilities (July 2016 CPU)

Oracle MySQL 5.6.x < 5.6.12 Optimizer DoS (January 2016 CPU)

Oracle MySQL 5.6.x < 5.6.21 Types DoS (October 2015 CPU)

Oracle MySQL 5.6.x < 5.6.22 DML DoS (January 2016 CPU)

Oracle MySQL 5.6.x < 5.6.23 InnoDB DoS (July 2015 CPU)

Oracle MySQL 5.6.x < 5.6.24 Multiple Vulnerabilities (July 2015 CPU) (October 2015 CPU)

Oracle MySQL 5.6.x < 5.6.25 Multiple Vulnerabilities (July 2015 CPU) (October 2015 CPU)

Oracle MySQL 5.6.x < 5.6.26 Multiple Vulnerabilities (October 2015 CPU)

Oracle MySQL 5.6.x < 5.6.27 Multiple Vulnerabilities (October 2015 CPU) (January 2016 CPU) (July 2016 CPU)

Oracle MySQL 5.6.x < 5.6.28 Multiple Vulnerabilities (January 2016 CPU)

Oracle MySQL 5.6.x < 5.6.29 Multiple Vulnerabilities (April 2016 CPU)

Oracle MySQL 5.6.x < 5.6.30 Multiple Vulnerabilities (April 2016 CPU) (July 2016 CPU) (DROWN)

Oracle MySQL 5.6.x < 5.6.31 Multiple Vulnerabilities

Oracle MySQL 5.7.x < 5.7.10 Multiple Vulnerabilities (January 2016 CPU)

Oracle MySQL 5.7.x < 5.7.11 Multiple Vulnerabilities (April 2016 CPU) (July 2016 CPU)

Oracle MySQL 5.7.x < 5.7.12 Multiple Vulnerabilities (RPM Check) (April 2016 CPU) (July 2016 CPU) (October 2017 CPU) (DROWN)

Oracle MySQL 5.7.x < 5.7.13 Multiple Vulnerabilities

Oracle Net Services CREATE DATABASE LINK Query Overflow

Oracle NoSQL Database Enterprise Server-Side Request Forgery (October 2019 CPU)

Oracle NoSQL Database Installed (Linux)

Oracle PORTAL\_DEMO.ORG\_CHART SQL Injection

Oracle RDBMS Host Name and Patch Info

Oracle RDBMS Patchset Out of Date (credentialed check)

Oracle RDBMS Patchset Out of Date (remote check)

Oracle Reports Server test.jsp Multiple Parameter XSS

Oracle TNS Listener Remote Poisoning

Oracle TNS Listener VSNNUM Version Remote Information Disclosure

Oracle Web Cache Admin Module Multiple GET Request Method DoS

Oracle Webserver PL/SQL Stored Procedure GET Request DoS

Oracle XDB Default Accounts

Oracle XSQL query.xsql sql Parameter SQL Injection

OrientDB Detection

PostgreSQL 10.x < 10.9 / 11.x < 11.4 Stack Overflow Vulnerability (CVE-2019-10164)

PostgreSQL 11.x < 11.5 Memory disclosure in cross-type comparison for hashed subplan

PostgreSQL 7.4 < 7.4.27 / 8.0 < 8.0.23 / 8.1 < 8.1.19 / 8.2 < 8.2.15 / 8.3 < 8.3.9 / 8.4 < 8.4.2 Multiple Vulnerabilities

PostgreSQL 7.4 < 7.4.29 / 8.0 < 8.0.25 / 8.1 < 8.1.21 / 8.2 < 8.2.17 / 8.3 < 8.3.11 / 8.4 < 8.4.4 Multiple Vulnerabilities

PostgreSQL 7.4 < 7.4.30 / 8.0 < 8.0.26 / 8.1 < 8.1.22 / 8.2 < 8.2.18 / 8.3 < 8.3.12 / 8.4 < 8.4.5 / 9.0 < 9.0.1

PostgreSQL 8.2 < 8.2.20 / 8.3 < 8.3.14 / 8.4 < 8.4.7 / 9.0 < 9.0.3 Buffer Overflow Vulnerability

PostgreSQL 8.3 < 8.3.18 Multiple Vulnerabilities

PostgreSQL 8.3 < 8.3.19 / 8.4 < 8.4.12 / 9.0 < 9.0.8 / 9.1 < 9.1.4 Multiple Vulnerabilities

PostgreSQL 8.3 < 8.3.20 / 8.4 < 8.4.13 / 9.0 < 9.0.9 / 9.1 < 9.1.5 Multiple Vulnerabilities

PostgreSQL 8.3 < 8.3.23 / 8.4 < 8.4.16 / 9.0 < 9.0.12 / 9.1 < 9.1.8 / 9.2 < 9.2.3 Denial of Service

PostgreSQL 8.4 < 8.4.11 / 9.0 < 9.0.7 / 9.1 < 9.1.3 Multiple Vulnerabilities

PostgreSQL 8.4 < 8.4.17 / 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 Multiple Vulnerabilities

PostgreSQL 8.4 < 8.4.17 / 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 Predictable Random Number Generator

PostgreSQL 8.4 < 8.4.20 / 9.0 < 9.0.16 / 9.1 < 9.1.12 / 9.2 < 9.2.7 / 9.3 < 9.3.3 Multiple Vulnerabilities

PostgreSQL 9.0 < 9.0.13 / 9.1 < 9.1.9 / 9.2 < 9.2.4 File Deletion

PostgreSQL 9.0 < 9.0.19 / 9.1 < 9.1.15 / 9.2 < 9.2.10 / 9.3 < 9.3.6 / 9.4 < 9.4.1 Multiple Vulnerabilities

PostgreSQL 9.0 < 9.0.20 / 9.1 < 9.1.16 / 9.2 < 9.2.11 / 9.3 < 9.3.7 / 9.4 < 9.4.2 Multiple Vulnerabilities

PostgreSQL 9.0.x < 9.0.23 / 9.1.x < 9.1.19 / 9.2.x < 9.2.14 / 9.3.x < 9.3.10 / 9.4.x < 9.4.5 Multiple Vulnerabilities

PostgreSQL 9.1 < 9.1.9 / 9.2 < 9.2.4 Denial of Service

PostgreSQL 9.1.x < 9.1.20 / 9.2.x < 9.2.15 / 9.3.x < 9.3.11 / 9.4.x < 9.4.6 / 9.5.x < 9.5.1 Multiple Vulnerabilities

PostgreSQL 9.1.x < 9.1.23 / 9.2.x < 9.2.18 / 9.3.x < 9.3.14 / 9.4.x < 9.4.9 / 9.5.x < 9.5.4 Multiple Vulnerabilities

PostgreSQL 9.1.x < 9.1.24 / 9.2.x < 9.2.19 / 9.3.x < 9.3.15 / 9.4.x < 9.4.10 / 9.5.x < 9.5.5 / 9.6.x < 9.6.1 Aggregate Functions Use-after-free DoS

PostgreSQL 9.2.x < 9.2.20 / 9.3.x < 9.3.16 / 9.4.x < 9.4.11 / 9.5.x < 9.5.6 / 9.6.x < 9.6.2 Multiple Vulnerabilities

PostgreSQL 9.2.x < 9.2.21 / 9.3.x < 9.3.17 / 9.4.x < 9.4.12 / 9.5.x < 9.5.7 / 9.6.x < 9.6.3 Multiple Vulnerabilities

PostgreSQL 9.2.x < 9.2.22 / 9.3.x < 9.3.18 / 9.4.x < 9.4.13 / 9.5.x < 9.5.8 / 9.6.x < 9.6.4 Multiple Vulnerabilities

PostgreSQL 9.2.x < 9.2.24 / 9.3.x < 9.3.20 / 9.4.x < 9.4.15 / 9.5.x < 9.5.10 / 9.6.x < 9.6.6 / 10.x < 10.1 Multiple Vulnerabilities

PostgreSQL 9.3 < 9.3.23 / 9.4 < 9.4.18 / 9.5 < 9.5.13 / 9.6 < 9.6.9 / 10.3 Insecure ACL Remote Issue

PostgreSQL 9.3.x < 9.3.21 / 9.4.x < 9.4.16 / 9.5.x < 9.5.11 / 9.6.x < 9.6.7 / 10.x < 10.2 Multiple Vulnerabilities

PostgreSQL 9.3.x < 9.3.22 / 9.4.x < 9.4.17 / 9.5.x < 9.5.12 / 9.6.x < 9.6.8 / 10.x < 10.3 Privilege Escalation Vulnerability

PostgreSQL 9.3.x < 9.3.24 / 9.4.x < 9.4.19 / 9.5.x < 9.5.14 / 9.6.x < 9.6.10 / 10.x < 10.5 Multiple Vulnerabilities

PostgreSQL 9.3.x < 9.3.25 / 9.4.x < 9.4.20 / 9.5.x < 9.5.15 / 9.6.x < 9.6.11 / 10.x < 10.6 / 11.x < 11.1 SQL injection

PostgreSQL 9.4.x < 9.4.22 / 9.5.x < 9.5.17 / 9.6.x < 9.6.13 / 10.x < 10.8 / 11.x < 11.3 Multiple vulnerabilities

PostgreSQL 9.4.x < 9.4.24 / 9.5.x < 9.5.19 / 9.6.x < 9.6.15 / 10.x < 10.10 / 11.x < 11.5 Multiple Vulnerabilities

PostgreSQL 9.5.x < 9.5.2 Multiple Vulnerabilities

PostgreSQL 9.6.x < 9.6.17 / 10.x < 10.12 / 11.x < 11.7 / 12.x < 12.2 Missing Authorization

PostgreSQL < 7.2.3 Multiple Vulnerabilities

PostgreSQL < 7.2.7 / 7.3.9 / 7.4.7 / 8.0.1 Multiple Vulnerabilities

PostgreSQL < 8.0.3 Multiple Vulnerabilities

PostgreSQL Client/Server Installed (Linux)

PostgreSQL Default Unpassworded Account

PostgreSQL Empty Password Handling Remote Authentication Bypass

PostgreSQL LDAP Anonymous Bind Authentication Bypass

PostgreSQL make\_oidjoins\_check Arbitrary File Overwrite

PostgreSQL Server Installed (Windows)

PostgreSQL Server Login Possible

PostgreSQL to\_ascii() Function Remote Overflows

PostgreSQL Unauthenticated Version Detection

PostgreSQL Unsupported Version Detection

PostgreSQL Version Detection

Rocket U2 UniData < 7.3 unidata72 RPC Interface Call Parsing Arbitrary Command Execution

SAP DB / MaxDB Cons Program Arbitrary Command Execution

SAP MaxDB Multiple Vulnerabilities

solidDB Default Credentials

solidDB Detection

SQL Server Version Detection

Sybase Adaptive Server Enterprise < 12.5.4.0 Multiple Vulnerabilities

Sybase ASA Client Connection Broadcast Remote Information Disclosure

Sybase ASA Default Database Password

Sybase ASE Login Possible

Sybase SQL sa Account Blank Password

Teradata Database Detection

yaSSL 1.7.5 Buffer Overflow

# CISCO

A Vulnerability in IOS Firewall Feature Set - Cisco Systems

Access Point Web-browser Interface Vulnerability

Cable Modem Termination System Authentication Bypass - Cisco Systems

Cisco 10000 Series Denial of Service Vulnerability (cisco-sa-20110928-c10k)

Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability - Cisco Systems

Cisco 12000 Series Router ICMP Unreachable DoS

Cisco 12000 Series Routers Multiple Vulnerabilities (DoS, ACL Bypass)

Cisco 600 Series Router HTTP GET DoS (cisco-sa-20001204-cbos)

Cisco 6000/6500/7600 Crafted Layer 2 Frame Vulnerability - Cisco Systems

Cisco 6400 NRP2 Unauthenticated Telnet Access (CSCdt65960)

Cisco 675 Router Default Unpassworded Account

Cisco 7600 Series Route Switch Processor 720 with 10 Gigabit Ethernet Uplinks Denial of Service (cisco-sa-20140326-RSP72010GE)

Cisco 9900 Series IP Phone Crafted Header Unregister Vulnerability

Cisco ACE 4710 Appliance / ACE30 Module Multiple Vulnerabilities (Logjam)

Cisco ACE 4710 Device Manager GUI Remote Command Injection Vulnerability (cisco-sa-20160224-ace)

Cisco ACE30 and ACE4710 OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

Cisco Adaptive Security Appliance (ASA) Software Command Injection Vulnerability (cisco-sa-20200226-fxos-ucs-cli-cmdinj)

Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability (CSCvd82064)

Cisco Adaptive Security Appliance DOS (cisco-sa-20191002-asa-dos)

Cisco Adaptive Security Appliance ICMP Echo Request ACL Bypass (cisco-sa-20160711-asa)

Cisco Adaptive Security Appliance RCE (cisco-sa-20191112-asa-ftd-lua-rce)

Cisco Adaptive Security Appliance Smart Tunnel Vulnerabilities

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Low-Entropy Keys Vulnerability

Cisco Adaptive Security Appliance Software CLI Arbitrary File Read and Write Vulnerability (cisco-sa-20200226-fxos-cli-file)

Cisco Adaptive Security Appliance Software DHCPv6 Packet Handling DoS (cisco-sa-20160420-asa-dhcpv6)

Cisco Adaptive Security Appliance Software Direct Authentication Denial of Service Vulnerability

Cisco Adaptive Security Appliance Software DoS (cisco-sa-20181003-asa-syslog-dos)

Cisco Adaptive Security Appliance Software IKEv1 DoS (cisco-sa-20191002-asa-ftd-ikev1-dos)

Cisco Adaptive Security Appliance Software OSPF LSA Manipulation (cisco-sa-20170727-ospf)

Cisco Adaptive Security Appliance Software Secure Copy DoS (cisco-sa-20191002-asa-scp-dos)

Cisco Adaptive Security Appliance Software SIP Inspection DoS (cisco-sa-20191002-asa-ftd-sip-dos)

Cisco Adaptive Security Appliance Software SSL VPN Denial of Service Vulnerability

Cisco Adaptive Security Appliance Username Enumeration Information Disclosure Vulnerability (CSCvd47888)

Cisco Adaptive Security Appliance VPN SAML Authentication Bypass Vulnerability (cisco-sa-20190501-asaftd-saml-vpn)

Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability (CSCve19179)

Cisco Adaptive Security Appliance WebVPN XSS (cisco-sa-20191002-asa-xss)

Cisco Adaptive Security Appliance XML Parser DoS (cisco-sa-20160517-asa-xml)

Cisco Adaptive Security Appliances Multiple Vulnerabilities in OpenSSL

Cisco ADE-OS Identity Services Engine (ISE) Detection

Cisco ADE-OS Prime Collaboration Assurance Detection

Cisco ADE-OS Prime Collaboration Provisioning Detection

Cisco Aggregation Services Router 900 Route Switch Processor 3 OSPFv2 DoS (cisco-sa-20190327-rsp3-ospf)

Cisco Aggregation Services Router 9000 Series IPv6 Fragment Header DoS (cisco-sa-20180131-ipv6)

Cisco Aironet Telnet Invalid Username/Password DoS

Cisco ANI Configuration Overwrite DoS (CSCup62167)

Cisco APIC < 1.3(2f) Binary File Installation Handling Local Privilege Escalation

Cisco APIC Detection

Cisco APIC-EM 1.1 Unspecified XSS (credentialed check)

Cisco APIC-EM 1.x < 1.5 Unauthorized Access (credentialed check)

Cisco APIC-EM WebUI Detection

Cisco Application Control Engine (ACE) Version

Cisco Application Control Engine < A3(2.1) Multiple Unspecified Traversals (cisco-sa-20090225-anm)

Cisco Application Control Engine GNU glibc gethostbyname Function Buffer Overflow Vulnerability (cisco-sa-20150128-ghost) (GHOST)

Cisco Application Control Engine Login Administrator IP Address Overlap (cisco-sa-20120620-ace)

Cisco Application Extension Platform (AXP) Privilege Escalation (cisco-sa-20100609-axp)

Cisco Application Policy Infrastructure Controller Custom Binary Privilege Escalation Vulnerability

Cisco Application Policy Infrastructure Controller Linux Kernel IP Fragment Reassembly DoS

Cisco Application Policy Infrastructure Controller Out Of Band Management IP Tables Bypass (cisco-sa-iptable-bypass-GxW88XjL)

Cisco Application Policy Infrastructure Controller REST API Privilege Escalation Vulnerability

Cisco Application Policy Infrastructure Controller SSH Privilege Escalation Vulnerability

Cisco Application Policy Infrastructure Controller Web-Based Management Interface Cross-Site Scripting Vulnerability (cisco-sa-20190501-apic-xss)

Cisco ASA / IOS IKE Fragmentation Vulnerability

Cisco ASA 1000V H.323 Inspection DoS

Cisco ASA 5500 Series DoS (cisco-sa-20120620-asaipv6)

Cisco ASA 5500 Series Multiple DoS Vulnerabilities (cisco-sa-20100804-asa)

Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20110223-asa)

Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20111005-asa)

Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20120314-asa)

Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20121010-asa)

Cisco ASA 5500 Series SSH Timeout DoS

Cisco ASA AnyConnect Client Authentication Attempt Handling Information Disclosure (cisco-sa-20160115-asa)

Cisco ASA AnyConnect Client Authentication Attempt Handling Information Disclosure (cisco-sa-20160115-asa)

Cisco ASA Cavium SDK TLS Incorrect Padding Acceptance Plaintext Disclosure (CSCuu93339)

Cisco ASA Certificate Authority Enrollment Operation Packet Handling DoS (cisco-sa-20161019-asa-ca)

Cisco ASA Certificate Processing Denial of Service (CSCuh19462)

Cisco ASA Clientless SSL VPN Functionality CIFS RCE (cisco-sa-20170208-asa)

Cisco ASA Content Security and Control Security Services Module (CSC-SSM) DoS (cisco-sa-20160309-csc)

Cisco ASA Cut Through Proxy Authentication Vulnerability

Cisco ASA Denial of Service Vulnerability (cisco-sa-20181031-asaftd-sip-dos)

Cisco ASA DHCPv6 Relay DoS (cisco-sa-20151021-asa-dhcp1)

Cisco ASA DHCPv6 Relay DoS (CSCun45520)

Cisco ASA DHCPv6 Relay Function DHCP Packet Handling DoS (CSCur45455)

Cisco ASA DNS Packet Handling DoS (cisco-sa-20151021-asa-dns1)

Cisco ASA DNS Packet Handling DoS (cisco-sa-20151021-asa-dns2)

Cisco ASA FirePOWER Services Multiple Vulnerabilities in Wi-Fi Protected Access and Wi-Fi Protected Access II (KRACK)

Cisco ASA Firepower Version

Cisco ASA HTTP Server Information Disclosure (CSCun78551)

Cisco ASA IKEv1 ISAKMP Packet Handling DoS (cisco-sa-20151021-asa-ike)

Cisco ASA Inspection and Filter Overlap DoS (CSCui45606)

Cisco ASA libsrtp DoS (CSCux00686)

Cisco ASA Multiple Vulnerabilities (cisco-sa-20130410-asa)

Cisco ASA Multiple Vulnerabilities (cisco-sa-20180418-asa1 / cisco-sa-20180418-asa2 / cisco-sa-20180418-asa3 / cisco-sa-20180418-asaanyconnect / cisco-sa-20180418-asa\_inspect)

Cisco ASA Next-Generation Firewall Fragmented Traffic DoS (cisco-sa-20130626-ngfw)

Cisco ASA Next-Generation Firewall GNU Bash Environment Variable Handling Command Injection (cisco-sa-20140926-bash) (Shellshock)

Cisco ASA Next-Generation Firewall OpenSSL Alternative Chains Certificate Forgery (cisco-sa-20150710-openssl)

Cisco ASA Privilege Escalation Vulnerability (cisco-sa-20181219-asa-privesc)

Cisco ASA RADIUS radius\_rcv\_auth DoS (CSCun69561)

Cisco ASA Remote Code Execution and Denial of Service Vulnerability (cisco-sa-20180129-asa1)

Cisco ASA Remote Code Execution and Denial of Service Vulnerability (cisco-sa-20180129-asa1) (destructive check)

Cisco ASA SIP CPU Utilization DoS

Cisco ASA SIP Inspection DoS (CSCuf67469)

Cisco ASA SNMP Packet Handling RCE (CSCva92151) (EXTRABACON)

Cisco ASA Software CLI Command Injection (cisco-sa-20200226-fxos-ucs-cmdinj)

Cisco ASA Software CLI Invalid Command Invocation (cisco-sa-20160817-asa-cli) (EPICBANANA)

Cisco ASA Software Cryptographic TLS and SSL Driver Denial of Service Vulnerability (cisco-sa-20190710-asa-ftd-dos)

Cisco ASA Software DNS Response Message Handling DoS (cisco-sa-20170419-asa-dns)

Cisco ASA Software IKEv1 and IKEv2 UDP Packet Handling RCE (cisco-sa-20160210-asa-ike)

Cisco ASA Software IKEv1 XAUTH Parameter Handling Remote DoS (cisco-sa-20170419-asa-xauth)

Cisco ASA Software IPsec Packet Handling DoS (cisco-sa-20170419-asa-ipsec)

Cisco ASA Software Multiple Vulnerabilities (cisco-sa-20131009-asa)

Cisco ASA Software Multiple Vulnerabilities (cisco-sa-20140409-asa)

Cisco ASA Software Multiple Vulnerabilities (cisco-sa-20141008-asa)

Cisco ASA Software Multiple Vulnerabilities (cisco-sa-20150408-asa)

Cisco ASA Software SharePoint RAMFS Integrity and Lua Injection Vulnerabilities (CSCup54208 and CSCup54184)

Cisco ASA Software SSL / TLS Packet Handling DoS (cisco-sa-20170419-asa-tls)

Cisco ASA SSL VPN Functionality Version Information Disclosure (CSCuq65542)

Cisco ASA SSL VPN Information Disclosure (CSCuq65542)

Cisco ASA SSL VPN Memory Blocks Exhaustion DoS (CSCuq68888)

Cisco ASA SSL VPN Remote Information Disclosure (CSCuq65542)

Cisco ASA TLS CBC Information Disclosure (CSCus08101)

Cisco ASA VPN Denial of Service (CSCua91108)

Cisco ASA VPN Enabled Detection

Cisco ASA Web Interface Remote XML Command Injection (cisco-sa-20161116-asa)

Cisco ASA Web Services DoS (cisco-sa-20180606-asaftd)

Cisco ASA WebVPN CIFS Share Enumeration DoS (CSCuj83344)

Cisco ASA WebVPN Memory Leak DoS

Cisco ASA WebVPN XSS

Cisco ASR 5000 Series ipsecmgr Service DoS (cisco-sa-20161116-asr)

Cisco ASR 5000 Series StarOS SSH Subsystem Privilege Escalation (CSCux22492)

Cisco ASR 9000 Series Aggregation Services Routers Precision Time Protocol DoS (cisco-sa-20180815-asr-ptp-dos)

Cisco ASR StarOS Border Gateway Protocol Process DoS (cisco-sa-20170705-staros)

Cisco ASR StarOS CLI Command Injection Local Privilege Escalation (cisco-sa-20170705-asrcmd)

Cisco ASR StarOS Interface Forwarding Denial of Service Vulnerability (cisco-sa-20180418-staros)

Cisco ASR StarOS IPsec Manager Denial of Service Vulnerability (cisco-sa-20180418-starosasr)

Cisco ASR StarOS Multiple CLI Command Injection Vulnerabilities (cisco-sa-20180117-staros / cisco-sa-20180307-staros / cisco-sa-20180307-staros1)

Cisco ASR StarOS SSH Login Parameter Handling Privilege Escalation (cisco-sa-20170315-asr)

Cisco AsyncOS for Content Security Management Appliances Software Remote Code Execution (CSCug80118)

Cisco AsyncOS for Email Security Appliance Attachment MIME Header Handling Filter Bypass (cisco-sa-20170607-esa1)

Cisco AsyncOS for Email Security Appliances MIME Header Processing Filter Bypass (cisco-sa-20161116-esa1 / cisco-sa-20161116-esa2)

Cisco AsyncOS for Email Security Appliances Software Remote Code Execution (CSCug79377)

Cisco ATA-186 Password Circumvention / Recovery

Cisco Catalyst 3750-X Series Switch Default Credentials Vulnerability (CSCue92286)

Cisco Catalyst 4000 Series Switch Denial of Service Vulnerability (CSCug41049 / CSCue61890)

Cisco Catalyst 4000 Series Switches TCP Denial of Service Vulnerability (cisco-sa-20190925-cat4000-tcp-dos)

Cisco Catalyst 4500E Series Switch with Cisco Catalyst Supervisor Engine 7L-E Denial of Service Vulnerability (cisco-sa-20120926-ecc)

Cisco Catalyst 5000 Series Frame STP Port Broadcast DoS (CSCdt62732)

Cisco Catalyst 6000, 6500 and Cisco 7600 Series MPLS Packet Vulnerability

Cisco Catalyst 6000, 6500 Series and Cisco 7600 Series NAM (Network Analysis Module) Vulnerability

Cisco Catalyst 6500 and Cisco 7600 Series Devices Accessible via Loopback Address (cisco-sr-20070926-lb)

Cisco Catalyst Enable Access Authentication Bypass (CSCea42030)

Cisco Catalyst Hybrid Mode Malformed MPLS Packet Remote DoS (CSCsd37415, CSCef90002)

Cisco Catalyst SSH Large Packet CPU Consumption DoS (CSCdv85279, CSCdw59394)

Cisco Catalyst Supervisor Remote Reload DoS

Cisco Catalyst Switches Embedded HTTP Server Long HTTP Request DoS (CSCdy26428)

Cisco Catalyst Switches NMSP Port Information Disclosure Vulnerability (cisco-sa-20160413-nms)

Cisco Catalyst Telnetd Authentication Failure Saturation Memory Leak Remote DoS (CSCds66191)

Cisco Catalyst Web Interface Remote Command Execution

Cisco CatOS TCP-ACK Remote DoS (CSCec42751, CSCed45576, CSCed48590)

Cisco CatOS Telnet Option Handling Overflow (CSCdw19195)

Cisco cBR Series Converged Broadband Routers High CPU Usage DoS (cisco-sa-20180418-cbr8)

Cisco CHAP Authentication Vulnerabilities - Cisco Systems

Cisco CiscoWorks Internetwork Performance Monitor Remote Command Execution

Cisco Cloud Services Platform 2.x < 2.1.0 Multiple Vulnerabilities

Cisco Content Security Management Appliance (SMA) GUI Denial of Service Vulnerability

Cisco Content Security Management Appliance Denial of Service Vulnerability (CSCvo89182)

Cisco Content Security Management Appliance HTTP Header Injection Vulnerability

Cisco Content Security Management Appliance Privilege Escalation Vulnerability

Cisco Content Security Management Appliance TCP Flood DoS (CSCus79777)

Cisco Content Security Management Appliance Telnet Remote Code Execution (cisco-sa-20120126-ironport)

Cisco Content Security Management Appliance Version

Cisco Content Security Management Appliance Web Detection

Cisco Content Switching Module (CSM) Software Version

Cisco Content Switching Module Layer 7 Load Balancing DoS

Cisco CUCM / CUPS Detection

Cisco CUCM Voice Operating System-Based Products Unauthorized Access Vulnerability

Cisco Data Center Network Manager < 11.1(1) Authentication Bypass Vulnerability

Cisco Data Center Network Manager < 11.3(1) Multiple Vulnerabilities

Cisco Data Center Network Manager Arbitrary File Download Vulnerability

Cisco Data Center Network Manager Arbitrary File Upload and Remote Code Execution Vulnerability

Cisco Data Center Network Manager Information Disclosure Vulnerability

Cisco Device Default Password

Cisco Device Manager Command Execution Vulnerability (cisco-sa-20130424-fmdm)

Cisco Devices Multiple SSH Information Disclosure Vulnerabilities

Cisco EIGRP Multiple Vulnerabilities

Cisco Email Security Appliance (ESA) GUI Denial of Service Vulnerability

Cisco Email Security Appliance Content Filter Bypass Vulnerability (cisco-sa-20190417-esa-filter-bypass)

Cisco Email Security Appliance Content Filter Bypass Vulnerability (cisco-sa-20190703-esa-bypass)

Cisco Email Security Appliance Content Filter Bypass Vulnerability (cisco-sa-20190703-esa-filterpass)

Cisco Email Security Appliance Content Filter Bypass Vulnerability (CSCvq65126)

Cisco Email Security Appliance Content Filter Bypass Vulnerability (CSCvq66135)

Cisco Email Security Appliance Denial of Service Vulnerability

Cisco Email Security Appliance Denial of Service Vulnerability (CSCvo89192)

Cisco Email Security Appliance DoS (cisco-sa-20200219-esa-dos)

Cisco Email Security Appliance Filter Bypass Vulnerability

Cisco Email Security Appliance Filter Bypass Vulnerability

Cisco Email Security Appliance Filter Bypass Vulnerability (cisco-sa-20190501-esa-bypass)

Cisco Email Security Appliance Header Injection Vulnerability

Cisco Email Security Appliance Internal Testing Interface RCE

Cisco Email Security Appliance Malformed EML Attachment Bypass Vulnerability (cisco-sa-20170906-esa)

Cisco Email Security Appliance Multiple DoS Vulnerabilities (cisco-sa-20190109-esa-dos / cisco-sa-20190109-esa-url-dos)

Cisco Email Security Appliance Multiple Vulnerabilities

Cisco Email Security Appliance Privilege Escalation Vulnerability

Cisco Email Security Appliance Telnet Remote Code Execution (cisco-sa-20120126-ironport)

Cisco Email Security Appliance Uncontrolled Resource Exhaustion Vulnerability

Cisco Email Security Appliance URL Filtering Bypass (cisco-sa-20191120-esa-url-bypass)

Cisco Email Security Appliance Version

Cisco Email Security Appliance Web Detection

Cisco Email Security Appliance ZIP File Filter Bypass

Cisco Emergency Responder (CER) Appliance Detection (SSH)

Cisco Emergency Responder Denial of Service (cisco-sa-20171115-vos)

Cisco Emergency Responder Denial of Service (cisco-sa-20180606-diskdos)

Cisco Emergency Responder Open Redirect (cisco-sa-20181003-er-ucm-redirect)

Cisco Finesse Appliance Authentication Bypass Vulnerability (cisco-sa-20160202-fducce)

Cisco Finesse Appliance Cross-Site Scripting Vulnerability (Cisco-SA-20150501-CVE-2015-0714)

Cisco Finesse Appliance Detection (SSH)

Cisco Finesse Appliance Directory Read Information Disclosure Vulnerability (Cisco-SA-20130812-CVE-2013-3457)

Cisco Finesse Appliance HTTP Request Processing Server-Side Request Forgery Vulnerability (cisco-sa-20160504-finesse)

Cisco Finesse Appliance Multiple Cross-Site Scripting Vulnerabilities (Cisco-SA-20150818-CVE-2015-4310)

Cisco Finesse Appliance User Data Information Disclosure Vulnerability (Cisco-SA-20130812-CVE-2013-3455)

Cisco Finesse Appliance XML Processing Denial of Service Vulnerability (Cisco-SA-20150527-CVE-2015-0754)

Cisco Finesse Disk Utilization Denial of Service Vulnerability (cisco-sa-20180606-diskdos)

Cisco Finesse Information Disclosure (cisco-sa-20170503-finesse-ucce)

Cisco Finesse Information Disclosure (cisco-sa-20180718-finesse)

Cisco Finesse Reflected Cross-Site Scripting Vulnerability (cisco-sa-20170802-cf)

Cisco Finesse Server-Side Request Forgery (cisco-sa-20180718-finesse)

Cisco Finesse Unauthorized Access (cisco-sa-20171115-vos)

Cisco Firepower and FireSIGHT Multiple Vulnerabilities

Cisco Firepower Detection Engine Multiple Vulnerabilities

Cisco Firepower Detection Engine Pragmatic General Multicast Protocol Decoding DoS (cisco-sa-20170419-fpsnort)

Cisco Firepower Detection Engine SSL Multiple DoS (cisco-sa-20170405-cfpw) (cisco-sa-20170405-cfpw1)

Cisco Firepower Enumeration

Cisco Firepower Management Center 6.2.3.x < 6.2.3.10 / 6.3.0.x < 6.3.0.1 / 6.4.0 XSS (cisco-sa-20190206-fmc-xss)

Cisco Firepower Management Center 6.2.3.x < 6.2.3.12 / 6.3.0.x < 6.3.0.3 / 6.4.0 XSS (cisco-sa-20190417-cfmc-xss)

Cisco Firepower Management Center 6.2.3.x < 6.2.3.14 / 6.3.0.x < 6.3.0.4 / 6.4.0.x < 6.4.0.2 XSS (cisco-sa-20190703-fmc-xss)

Cisco Firepower Management Center < 6.2.2.2 Remote Code Execution Vulnerability

Cisco Firepower Management Center < 6.2.3 Directory Traversal Vulnerability

Cisco Firepower Management Center Command Injection (cisco-sa-20191002-fmc-com-inj)

Cisco Firepower Management Center Lightweight Directory Access Protocol Authentication Bypass (cisco-sa-20200122-fmc-auth)

Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities (cisco-sa-20191016-firepwr-xss)

Cisco Firepower Management Center Multiple SQLi (cisco-sa-20191002-fmc-sql-inj)

Cisco Firepower Management Center Multiple XSS

Cisco Firepower Management Center Multiple XSS

Cisco Firepower Management Center RCE (cisco-sa-20191002-fmc-rce)

Cisco Firepower Management Center Software File and Malware Policy Bypass Vulnerability (cisco-sa-20191002-fire-bypass)

Cisco Firepower Management Center Software Stored Cross-Site Scripting (XSS) Vulnerability (cisco-sa-20191016-fpwr-xss)

Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability (cisco-sa-20191016-firepwr-xss)

Cisco Firepower Management Center XSS Vulnerability

Cisco Firepower Packet Inspection Engine HTTP Stream DoS

Cisco Firepower System Detection

Cisco Firepower System Software Detection Engine RTF and RAR Malware and File Policy Bypass Vulnerabilities (cisco-sa-20191002-firepwr-bypass)

Cisco Firepower System Software SSL Logging DoS (cisco-sa-20170517-fpwr)

Cisco Firepower Threat Defense (FTD) Adaptive Security Appliance Denial of Service Vulnerability (cisco-sa-20181031-asaftd-sip-dos)

Cisco Firepower Threat Defense (FTD) Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability (cisco-sa-20180129-asa1)

Cisco Firepower Threat Defense (FTD) Secure Boot Hardware Tampering Vulnerability (cisco-sa-20190513-secureboot)

Cisco Firepower Threat Defense (FTD) Software CLI Arbitrary File Read and Write Vulnerability (cisco-sa-20200226-fxos-cli-file)

Cisco Firepower Threat Defense (FTD) Software Command Injection Vulnerability (cisco-sa-20200226-fxos-ucs-cli-cmdinj)

Cisco Firepower Threat Defense (FTD) Software IKEv1 DoS (cisco-sa-20191002-asa-ftd-ikev1-dos)

Cisco Firepower Threat Defense (FTD) VPN SAML Authentication Bypass Vulnerability (cisco-sa-20190501-asaftd-saml-vpn)

Cisco Firepower Threat Defense and Cisco ASA with FirePOWER Module Improper SSL Policy Packet Handling DoS (cisco-sa-20170503-ftd)

Cisco Firepower Threat Defense Device Manager Web UI Request Handling Arbitrary Log Entry Injection (cisco-sa-20170201-fpw2)

Cisco Firepower Threat Defense DOS (cisco-sa-20191002-asa-dos)

Cisco Firepower Threat Defense RCE (cisco-sa-20191112-asa-ftd-lua-rce)

Cisco Firepower Threat Defense Security Bypass Vulnerability

Cisco Firepower Threat Defense Software 6.x < 6.2.3.12 / 6.3.x < 6.3.0.3 Multiple Vulnerabilities

Cisco Firepower Threat Defense Software Command Injection Vulnerability (cisco-sa-20191002-ftd-cmdinj)

Cisco Firepower Threat Defense Software Detection Engine Policy Bypass Vulnerability

Cisco Firepower Threat Defense Software DoS (cisco-sa-20181003-asa-syslog-dos)

Cisco Firepower Threat Defense Software HTTP Filtering Bypass Vulnerability (cisco-sa-20190816-ftd-http)

Cisco Firepower Threat Defense Software Information Disclosure Vulnerability

Cisco Firepower Threat Defense Software Multiple DoS Vulnerabilities (cisco-sa-20181003-ftd-inspect-dos, cisco-sa-20181003-asa-dma-dos)

Cisco Firepower Threat Defense Software SIP Inspection DoS (cisco-sa-20191002-asa-ftd-sip-dos)

Cisco Firepower Threat Defense Software SSL/TLS Policy Bypass Vulnerability

Cisco Firepower Threat Defense Software WebVPN XSS (cisco-sa-20191002-asa-xss)

Cisco Firewall Services Module (FWSM) Version

Cisco Firewall Services Module Software Denial of Service (cisco-sa-20140219-fwsm)

Cisco Firewall Services Module Software Multiple Vulnerabilities (cisco-sa-20131009-fwsm)

Cisco FMC Software Pluggable Authentication Module DoS (cisco-sa-20191002-ftd-fpmc-dos)

Cisco FTD Multiple Vulnerabilities (cisco-sa-20180418-asa1 / cisco-sa-20180418-asa2 / cisco-sa-20180418-asa3 / cisco-sa-20180418-asaanyconnect / cisco-sa-20180418-asa\_inspect)

Cisco FTD Software CLI Command Injection (cisco-sa-20200226-fxos-ucs-cmdinj)

Cisco FTD Software Command Injection (cisco-sa-20191002-fxos-cmd-inject)

Cisco FTD Software Cryptographic TLS and SSL Driver Denial of Service Vulnerability (cisco-sa-20190710-asa-ftd-dos)

Cisco FTD Software Pluggable Authentication Module DoS (cisco-sa-20191002-ftd-fpmc-dos)

Cisco FTD Web Services DoS (cisco-sa-20180606-asaftd)

Cisco FXOS and NX-OS Lightweight Directory Access Protocol Denial of Service Vulnerabilities

Cisco FXOS Software Cisco Discovery Protocol Arbitrary Code Execution and DoS (cisco-sa-20200226-fxos-nxos-cdp)

Cisco FXOS Software Cisco Discovery Protocol Denial of Service Vulnerability (cisco-sa-20200205-fxnxos-iosxr-cdp-dos)

Cisco FXOS Software Cisco Fabric Services Denial of Service Vulnerability (cisco-sa-20180620-nx-os-fabric-services-dos)

Cisco FXOS Software CLI Arbitrary File Read and Write Vulnerability (cisco-sa-20200226-fxos-cli-file)

Cisco FXOS Software CLI Command Injection (cisco-sa-20200226-fxos-ucs-cmdinj)

Cisco FXOS Software CLI Command Injection Vulnerability (cisco-sa-20200226-fpwr-cmdinj)

Cisco FXOS Software Command Injection (cisco-sa-20190306-nxos-cmdinj-1611)

Cisco FXOS Software Command Injection (cisco-sa-20190515-nxos-cmdinj-1795)

Cisco FXOS Software Command Injection (cisco-sa-20191002-fxos-cmd-inject)

Cisco FXOS Software Command Injection Vulnerabilities (cisco-sa-20190515-fxos-nxos-cmdinj-1781-1782)

Cisco FXOS Software Command Injection Vulnerability (CVE-2019-1779)

Cisco FXOS Software Command Injection Vulnerability (CVE-2019-1780)

Cisco FXOS Software Link Layer Discovery Protocol DoS (cisco-sa-20181017-fxnx-os-dos)

Cisco FXOS Software Local Management CLI Command Injection Vulnerability (cisco-sa-20200226-fxos-ucs-cli-cmdinj)

Cisco FXOS Software Pluggable Authentication Module DoS (cisco-sa-20191002-ftd-fpmc-dos)

Cisco FXOS Software Secure Configuration Bypass (cisco-sa-20190515-nxos-conf-bypass)

Cisco FXOS Software Simple Network Management Protocol DoS (cisco-sa-20190515-nxos-snmp-dos)

Cisco Gigabit Switch Routers (GSR) Line Card Failure ACL Bypas (CSCdp35794)

Cisco Global Site Selector Appliances DNS Vulnerability (cisco-sa-20090107-gss)

Cisco GSS Version

Cisco Identify Services Engine (ISE) Admin Portal Unauthorized Access

Cisco Identity Services Engine Arbitrary Client Certificate Creation Vulnerability

Cisco Identity Services Engine Authentication Bypass Vulnerability

Cisco Identity Services Engine Authorization Bypass (cisco-sa-20200108-ise-auth-bypass)

Cisco Identity Services Engine Cross-Site Scripting Vulnerability

Cisco Identity Services Engine Cross-Site Scripting Vulnerability

Cisco Identity Services Engine Cross-Site Scripting Vulnerability

Cisco Identity Services Engine Cross-Site Scripting Vulnerability

Cisco Identity Services Engine Cross-Site Scripting Vulnerability

Cisco Identity Services Engine Cross-Site Scripting Vulnerability

Cisco Identity Services Engine Cross-Site Scripting Vulnerability (cisco-sa-20190206-ise-xss)

Cisco Identity Services Engine Cross-Site Scripting Vulnerability (cisco-sa-20190417-ise-xss)

Cisco Identity Services Engine DoS

Cisco Identity Services Engine Logging Cross-Site Scripting Vulnerability (cisco-sa-20190123-isel-xss)

Cisco Identity Services Engine Multiple Cross-Site Scripting Vulnerabilities (cisco-sa-20190109-ise-multi-xss)

Cisco Identity Services Engine Multiple Stored Cross-Site Scripting Vulnerabilities (cisco-sa-20191016-ise-stored-xss)

Cisco Identity Services Engine Privilege Escalation Vulnerability

Cisco Identity Services Engine Privilege Escalation Vulnerability (cisco-sa-20190123-ise-privilege)

Cisco Identity Services Engine SSL Renegotiation Denial of Service Vulnerability

Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability

Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability (cisco-sa-20191016-ise-store-xss)

Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability (cisco-sa-ise-xss-DxJsRWRx)

Cisco Identity Services Engine Struts2 Namespace Vulnerability

Cisco Identity Services Engine WebUI Detection

Cisco IDS Device Manager Detection

Cisco Industrial Ethernet Switches Device Manager CSRF (cisco-sa-20180418-iess)

Cisco Integrated Management Controller Cross-Site Scripting Vulnerability

Cisco Integrated Management Controller Detection

Cisco Integrated Management Controller Privilege Escalation Vulnerability

Cisco Integrated Management Controller Remote Code Execution Vulnerability

Cisco Integrated Management Controller User Session Hijacking Vulnerability

Cisco Intrusion Prevention System Jumbo Frame Denial of Service (cisco-sa-20080618-ips)

Cisco Intrusion Prevention System MainApp SSL/TLS DoS (cisco-sa-20150311-ips)

Cisco IOS 6000/6500/7600 Series Layer 2 Frame DoS (CSCdy15598, CSCeb56052)

Cisco IOS AAA Login DoS (cisco-sa-20160928-aaados)

Cisco IOS AAA RADIUS Long Username Authentication Bypass (CSCee45312)

Cisco IOS Aironet Access Point DoS

Cisco IOS and IOS XE Software Cluster Management Protocol Denial of Service Vulnerability

Cisco IOS and IOS XE Software IP Service Level Agreement Denial of Service Vulnerability

Cisco IOS and IOS XE Software Smart Call Home Certificate Validation Vulnerability

Cisco IOS ANI IPv6 Packets DoS (cisco-sa-20170320-aniipv6)

Cisco IOS ANI Registrar DoS (cisco-sa-20170320-ani)

Cisco IOS ARP Table Overwrite DoS (CSCdu81936)

Cisco IOS ARP Table Overwrite Vulnerability - Cisco Systems

Cisco IOS Autonomic Control Plane Channel Information Disclosure (cisco-sa-20170726-aniacp)

Cisco IOS Autonomic Networking Infrastructure DoS (cisco-sa-20170726-anidos)

Cisco IOS Autonomic Networking Infrastructure Multiple Vulnerabilities (cisco-sa-20150325-ani)

Cisco IOS BGP Attribute Corruption Vulnerability - Cisco Systems

Cisco IOS CDP Neighbor Announcement DoS

Cisco IOS Cisco Express Forwarding (CEF) Previous Packet Information Disclosure (CSCdu20643)

Cisco IOS Clientless SSL VPN DoS

Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)

Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp) (destructive check)

Cisco IOS Command EXEC Unspecified Vulnerability

Cisco IOS Common Network Service Remote Version Disclosure

Cisco IOS cTCP Denial of Service Vulnerability - Cisco Systems

Cisco IOS CUBE RTCP Request Processing DoS

Cisco IOS Data-link Switching (DLSw) Capabilities Exchange Remote DoS (CSCsf28840)

Cisco IOS Denial of Service Vulnerability (cisco-sa-20190925-sip-dos)

Cisco IOS DFS Access List Leakage - Cisco Systems

Cisco IOS DHCP Blocked Interface Denial-of-Service - Cisco Systems

Cisco IOS DHCP Client DoS (cisco-sa-20170322-dhcpc)

Cisco IOS DHCP Multiple Vulnerabilities

Cisco IOS DHCP Multiple Vulnerabilities

Cisco IOS DHCP Remember Functionality DoS (CSCuh46822)

Cisco IOS DHCPv6 Relay Message Handling DoS (cisco-sa-20160323-dhcpv6)

Cisco IOS EnergyWise DoS (cisco-sa-20170419-energywise)

Cisco IOS established Keyword ACL Bypass (CSCdi34061)

Cisco IOS Extensible Authentication Protocol Vulnerability (cisco-sr-20071019-eap)

Cisco IOS Firewall Authentication Proxy for FTP and Telnet Sessions Buffer Overflow

Cisco IOS Firewall CBAC ACL Bypass (CSCdv48261)

Cisco IOS Forwarding Information Base DoS (cisco-sa-20180328-FIB-dos)

Cisco IOS Generic Input/Output SNMP DoS

Cisco IOS GRE Decapsulation Vulnerability

Cisco IOS H.323 Message Validation DoS (cisco-sa-20160928-h323)

Cisco IOS H.323 Protocol Implementation Flaws

Cisco IOS Hot Standby Routing Protocol Crafted UDP Packets Denial of Service

Cisco IOS Hot Standby Routing Protocol IP Collision Denial of Service

Cisco IOS HTTP Client Information Disclosure Vulnerability (cisco-sa-20190925-http-client)

Cisco IOS HTTP Configuration Unauthorized Administrative Access

Cisco IOS HTTP Server ?/ String Local DoS

Cisco IOS HTTP Server Query Vulnerability - Cisco Systems

Cisco IOS HTTP Server Vulnerability - Cisco Systems

Cisco IOS HTTP Service GET Request Remote DoS

Cisco IOS ICMP Redirect Denial of Service

Cisco IOS ICMP Redirect Message Spoofing Remote DoS (CSCdx92043)

Cisco IOS IKE Module DoS

Cisco IOS IKE XAUTH ISAKMP IPSec SA Establish Authentication Bypass (CSCeg00277)

Cisco IOS IKEv1 Fragmentation DoS (cisco-sa-20160928-ios-ikev1)

Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN)

Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)

Cisco IOS IKEv2 DoS (cisco-sa-20150325-ikev2)

Cisco IOS IKEv2 Fragmentation DoS (cisco-sa-20160323-ios-ikev2)

Cisco IOS Interface Blocked by IPv4 Packets - Cisco Systems

Cisco IOS Internet Key Exchange Vulnerability (cisco-sa-20120328-ike)

Cisco IOS Intrusion Prevention System (IPS) Multiple Vulnerabilities (CSCsa53334, CSCsg15598)

Cisco IOS IP Detail Record DoS (cisco-sa-20160928-ipdr)

Cisco IOS IP Header Sanity Check DoS (CSCuj23992)

Cisco IOS IPS Denial of Service Vulnerability - Cisco Systems

Cisco IOS IPSec IKE Traffic Remote DoS (CSCed94829)

Cisco IOS IPSec Packet DoS (CSCui79745)

Cisco IOS IPv6 Packet ACL Restriction Bypass

Cisco IOS IPv6 Packet Processing Arbitrary Code Execution (CSCef68324)

Cisco IOS IPv6 Packet Processing Remote DoS (CSCed40933)

Cisco IOS IPv6 Snooping DoS (cisco-sa-20150923-fhs)

Cisco IOS ISDN Interface Denial of Service Vulnerability

Cisco IOS ISM Module for ISR G2 Authentication Header DoS

Cisco IOS L2TP Parsing DoS (cisco-sa-20170322-l2tp)

Cisco IOS Line Printer Daemon (LPD) Stack Overflow

Cisco IOS LISP ITR DoS (CSCun73782)

Cisco IOS LLDP Packet Handling Remote DoS (cisco-sa-20160616-ios)

Cisco IOS LLDP Request Processing DoS

Cisco IOS Locally Defined User Enumeration

Cisco IOS Malformed BGP Packet Causes Reload - Cisco Systems

Cisco IOS Malformed BGP Packet Processing Remote DoS (CSCee67450)

Cisco IOS Malformed DHCP Packet DoS (CSCee50294)

Cisco IOS Malformed IPv4 Packet Remote DoS

Cisco IOS Malformed LISP Packet DoS (CSCuu64279)

Cisco IOS Malformed OSPF Packet Causes Reload - Cisco Systems

Cisco IOS Malformed PPTP Packet Remote DoS (CSCdt46181)

Cisco IOS MallocLite BGP Update DoS

Cisco IOS Misformed BGP Packet Causes Reload - Cisco Systems

Cisco IOS MMoH Information Leak

Cisco IOS MMP Stack Group Bidding Protocol (SGBP) Crafted UDP Packet Remote DoS (CSCsb11124)

Cisco IOS MPLS Forwarding Infrastructure Denial of Service Vulnerability - Cisco Systems

Cisco IOS MPLS VPN May Leak Information - Cisco Systems

Cisco IOS Multi Protocol Label Switching (MPLS) Packet Remote DoS (CSCeb56909)

Cisco IOS Multicast Routing Multiple DoS (cisco-sa-20160928-msdp)

Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak - Cisco Systems

Cisco IOS Multiple OpenSSL Vulnerabilities (CSCup22590)

Cisco IOS Multiple OpenSSL Vulnerabilities (CSCut46130)

Cisco IOS Multiple Vulnerabilities

Cisco IOS NAT Skinny Call Control Protocol Vulnerability

Cisco IOS Next Hop Resolution Protocol Vulnerability

Cisco IOS NTP Information Disclosure (CSCuj66318)

Cisco IOS NTP Packet Handling Remote DoS (cisco-sa-20160804-wedge)

Cisco IOS NTP Subsystem Unauthorized Access (cisco-sa-20160419-ios)

Cisco IOS OSM Line Card Header Corruption

Cisco IOS OSPF LSA Manipulation (cisco-sa-20170727-ospf)

Cisco IOS OSPF Neighbor Announcement Remote Overflow (CSCdp58462)

Cisco IOS OSPF Opaque LSA DoS (CSCui21030)

Cisco IOS OSPF Packet Handling DoS (CSCec16481)

Cisco IOS Port Scan Remote DoS (CSCds07326)

Cisco IOS Portscan Remote Denial of Service

Cisco IOS PPTP Vulnerability - Cisco Systems

Cisco IOS SCCP Control Protocol Malformed Message DoS (CSCee08584)

Cisco IOS Secure Copy Authorization Bypass Vulnerability

Cisco IOS Secure Shell Denial of Service Vulnerabilities - Cisco Systems

Cisco IOS Secure Shell Server TACACS+ Multiple DoS (CSCed65778, CSCed65285)

Cisco IOS Short Message Service Denial of Service Vulnerability

Cisco IOS SIP Memory Leak DoS (CSCuj23293)

Cisco IOS SIP Packet Handling Remote DoS (CSCsh58082)

Cisco IOS SM-1T3/E3 Service Module DoS (cisco-sa-20180926-sm1t3e3)

Cisco IOS Smart Install Memory Leak (cisco-sa-20160928-smi)

Cisco IOS Smart Install Packet Image List Parameter Handling DoS (cisco-sa-20160323-smi)

Cisco IOS Smart Install Protocol Misuse (cisco-sr-20170214-smi)

Cisco IOS SNMP Community string write privileges.

Cisco IOS SNMP DoS (CSCug65204)

Cisco IOS SNMP Packet Handling Remote Buffer Overflow Multiple RCE (cisco-sa-20170629-snmp)

Cisco IOS Software 802.1x Multiple-Authentication Port Authentication Bypass (cisco-sa-20180328-dot1x)

Cisco IOS Software Authentication Proxy Vulnerability - Cisco Systems

Cisco IOS Software Bidirectional Forwarding Detection DoS (cisco-sa-20180328-bfd)

Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities - Cisco Systems

Cisco IOS Software Border Gateway Protocol Message Processing DoS (cisco-sa-20160715-bgp)

Cisco IOS Software Catalyst 6500 Series 802.1x Authentication Bypass (cisco-sa-20190327-c6500)

Cisco IOS Software CIP Multiple Vulnerabilities (cisco-sa-20170927-cip)

Cisco IOS Software CIP Request DoS (cisco-sa-20160928-cip)

Cisco IOS Software Cluster Management Protocol DoS Vulnerability (cisco-sa-20180926-cmp)

Cisco IOS Software Command Security Bypass (cisco-sa-20120328-pai)

Cisco IOS Software Crafted Encryption Packet Denial of Service Vulnerability - Cisco Systems

Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability (cisco-sa-20100324-tcp)

Cisco IOS Software Data-Link Switching Vulnerability (cisco-sa-20110928-dlsw)

Cisco IOS Software DHCP Denial of Service Vulnerability (cisco-sa-20120926-dhcp)

Cisco IOS Software DHCP Denial of Service Vulnerability (cisco-sa-20130925-dhcp)

Cisco IOS Software DHCP Remote Code Execution Vulnerability

Cisco IOS Software DHCP Version 6 Server Denial of Service Vulnerability (cisco-sa-20120926-dhcpv6)

Cisco IOS Software DHCPv6 DoS (cisco-sa-20140924-dhcpv6)

Cisco IOS Software DNS Forwarder Denial of Service Vulnerability (cisco-sa-20160928-dns)

Cisco IOS Software EnergyWise DoS (cisco-sa-20140806-energywise

Cisco IOS Software Ethernet Connectivity Fault Management (CFM) DoS

Cisco IOS Software Firewall Application Inspection Control Vulnerability

Cisco IOS Software for Cisco 800 Series Industrial Integrated Services Routers Arbitrary Memory Write (cisco-sa-20180926-ir800-memwrite)

Cisco IOS Software H.323 Denial of Service Vulnerabilities (cisco-sa-20100324-h323)

Cisco IOS Software H.323 Denial of Service Vulnerabilities (cisco-sa-20100922-h323)

Cisco IOS Software H.323 Denial of Service Vulnerability - Cisco Systems

Cisco IOS Software Hot Standby Router Protocol Information Leak Vulnerability

Cisco IOS Software IKEv1 State Machine DoS (CSCuw08236)

Cisco IOS Software Information Disclosure Vulnerability (cisco-sa-20190327-info)

Cisco IOS Software Input Access List Leakage with NAT - Cisco Systems

Cisco IOS Software Integrated Services Module for VPN DoS (cisco-sa-20180328-dos)

Cisco IOS Software Integrated Services Routers Generation 2 denial of service (cisco-sa-20170927-rbip-dos)

Cisco IOS Software Internet Group Management Protocol Denial of Service Vulnerability (cisco-sa-20100922-igmp)

Cisco IOS Software Internet Key Exchange Denial of Service Vulnerability

Cisco IOS Software Internet Key Exchange Memory Leak (cisco-sa-20180328-ike)

Cisco IOS Software Internet Key Exchange Memory Leak Vulnerability (cisco-sa-20130925-ike)

Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability - Cisco Systems

Cisco IOS Software Internet Key Exchange Version 1 DoS (cisco-sa-20180328-ike-dos)

Cisco IOS Software Internet Key Exchange Version 2 (IKEv2) Denial of Service (cisco-sa-20140326-ikev2)

Cisco IOS Software Internet Key Exchange Vulnerability (cisco-sa-20130327-ike)

Cisco IOS Software Intrusion Prevention System Denial of Service Vulnerability (cisco-sa-20120926-ios-ips)

Cisco IOS Software IP Device Tracking DoS

Cisco IOS Software IP Service Level Agreement Denial of Service Vulnerability

Cisco IOS Software IP Service Level Agreement Vulnerability (cisco-sa-20110928-ipsla)

Cisco IOS Software IP Service Level Agreement Vulnerability (cisco-sa-20130327-ipsla)

Cisco IOS Software IP Version 6 over Multiprotocol Label Switching Vulnerabilities (cisco-sa-20110928-ipv6mpls)

Cisco IOS Software IPS and Zone-Based Firewall Vulnerabilities - Cisco Systems

Cisco IOS Software IPsec Vulnerability (cisco-sa-20100324-ipsec)

Cisco IOS Software IPv6 Denial of Service (cisco-sa-20140326-ipv6

Cisco IOS Software IPv6 Denial of Service Vulnerability (cisco-sa-20110928-ipv6)

Cisco IOS Software IPv6 Hop-by-Hop DoS Vulnerability (cisco-sa-20180926-ipv6hbh)

Cisco IOS Software IPv6 Virtual Fragmentation Reassembly Denial of Service Vulnerability (cisco-sa-20130925-ipv6vfr)

Cisco IOS Software Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability

Cisco IOS Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities (cisco-sa-20180328-lldp)

Cisco IOS Software Login Enhancements Login Block Multiple DoS Vulnerabilities (cisco-sa-20180328-slogin)

Cisco IOS Software Malformed Border Gateway Protocol Attribute Vulnerability (cisco-sa-20120926-bgp)

Cisco IOS Software mDNS Gateway DoS

Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities - Cisco Systems

Cisco IOS Software Multicast Network Time Protocol Denial of Service Vulnerability (cisco-sa-20130925-ntp)

Cisco IOS Software Multicast Source Discovery Protocol DoS (cisco-sa-20120328-msdp)

Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability - Cisco Systems

Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability - Cisco Systems

Cisco IOS Software Multiple Features IP Sockets Vulnerability

Cisco IOS Software Multiple IPv6 Metadata Flow Vulnerabilities (cisco-sa-20140924-metadata)

Cisco IOS Software Multiple mDNS Gateway DoS Vulnerabilities (cisco-sa-20140924-mdns)

Cisco IOS Software Multiple Network Address Translation (NAT) Denial of Service Vulnerabilities (cisco-sa-20140326-nat)

Cisco IOS Software Multiple SNMP Community String Vulnerabilities - Cisco Systems

Cisco IOS Software Multiple Vulnerabilities in ntpd (cisco-sa-20150408-ntpd)

Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability (cisco-sa-20100324-ldp)

Cisco IOS Software NAT denial of service (cisco-sa-20170927-nat)

Cisco IOS Software NAT Skinny Call Control Protocol Vulnerability (cisco-sa-20100324-sccp)

Cisco IOS Software NAT64 Denial of Service Vulnerability

Cisco IOS Software Network Address Translation (NAT) ALG Module DoS (cisco-sa-20140924-nat)

Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20100922-nat)

Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20110928-nat)

Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20120926-nat)

Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20130925-nat)

Cisco IOS Software Network Address Translation Vulnerability (cisco-sa-20120328-nat)

Cisco IOS Software Network Address Translation Vulnerability (cisco-sa-20130327-nat)

Cisco IOS Software Network Plug-and-Play Agent Certificate Validation Vulnerability

Cisco IOS Software Network Time Protocol Packet Vulnerability - Cisco Systems

Cisco IOS Software Network-Based Application Recognition Denial of Service Vulnerabilities

Cisco IOS Software Object-group Access Control List Bypass Vulnerability - Cisco Systems

Cisco IOS Software OSPFv3 DoS Vulnerability (cisco-sa-20180926-ospfv3-dos)

Cisco IOS Software Overly Long GET Request Causes Buffer Overflow in HTTP Server

Cisco IOS Software Plug-and-Play PKI API Certificate Validation Vulnerability

Cisco IOS Software Processing of SAA Packets - Cisco Systems

Cisco IOS Software PROFINET denial of service (cisco-sa-20170927-profinet)

Cisco IOS Software Protocol Translation Vulnerability (cisco-sa-20130327-pt)

Cisco IOS Software PTP DoS Vulnerability (cisco-sa-20180926-ptp)

Cisco IOS Software Quality of Service Remote Code Execution Vulnerability

Cisco IOS Software Queue Wedge Denial of Service Vulnerability (cisco-sa-20130925-wedge)

Cisco IOS Software Resource Reservation Protocol Denial of Service Vulnerability (cisco-sa-20130327-rsvp)

Cisco IOS Software Resource Reservation Protocol Interface Queue Wedge Vulnerability (cisco-sa-20130925-rsvp)

Cisco IOS Software Reverse SSH Denial of Service Vulnerability (cisco-sa-20120328-ssh)

Cisco IOS Software RSVP Denial of Service Vulnerability (cisco-sa-20120328-rsvp)

Cisco IOS Software RSVP DoS (cisco-sa-20140924-rsvp)

Cisco IOS Software Secure Copy Privilege Escalation Vulnerability - Cisco Systems

Cisco IOS Software Secure Shell Connection on VRF (cisco-sa-20190109-ios-ssh-vrf)

Cisco IOS Software Session Initiation Protocol Denial of Service (cisco-sa-20140326-sip)

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20100324-sip)

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20100922-sip)

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20110928-sip)

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090325-sip)

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090923-sip)

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20120926-sip)

Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20131106-sip)

Cisco IOS Software Simple Network Management Protocol GET MIB Object ID DoS (cisco-sa-20180328-snmp)

Cisco IOS Software SIP DoS (cisco-sa-20140924-sip)

Cisco IOS Software Smart Install Denial of Service Vulnerability (cisco-sa-20120328-smartinstall)

Cisco IOS Software Smart Install Denial of Service Vulnerability (cisco-sa-20130327-smartinstall)

Cisco IOS Software Smart Install DoS (cisco-sa-20180328-smi)

Cisco IOS Software Smart Install Remote Code Execution Vulnerability

Cisco IOS Software Smart Install Remote Code Execution Vulnerability (cisco-sa-20110928-smart-install)

Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability - Cisco Systems

Cisco IOS Software Software Plug and Play Agent Memory Leak(cisco-sa-20180926-pnp-memleak)

Cisco IOS Software SSL VPN Denial of Service (cisco-sa-20140326-ios-sslvpn)

Cisco IOS Software TCP CIP DoS

Cisco IOS Software TCP Denial of Service Vulnerability - Cisco Systems

Cisco IOS Software TCP Initial Sequence Number Randomization Improvements - Cisco Systems

Cisco IOS Software TCP Memory Leak DoS (cisco-sa-20150325-tcpleak)

Cisco IOS Software TELNET Option Handling Vulnerability - Cisco Systems

Cisco IOS Software TFTP DoS (cisco-sa-20150722-tftp)

Cisco IOS Software Traffic Optimization Features Multiple DoS

Cisco IOS Software Tunneled Traffic Queue Wedge Vulnerability (cisco-sa-20120926-c10k-tunnels)

Cisco IOS Software Tunnels Vulnerability - Cisco Systems

Cisco IOS Software VPLS denial of service (cisco-sa-20170927-vpls)

Cisco IOS Software VRF ICMP Queue Wedge DoS (cisco-sa-20150325-wedge)

Cisco IOS Software WebVPN and SSLVPN Vulnerabilities - Cisco Systems

Cisco IOS Software Wide Area Application Services Express DoS

Cisco IOS Software Zone-Based Firewall and Content Filtering Vulnerability (cisco-sa-20130925-cce)

Cisco IOS Software Zone-Based Firewall Vulnerabilities (cisco-sa-20120328-zbfw)

Cisco IOS Software Zone-Based Policy Firewall Session Initiation Protocol Inspection Denial of Service Vulnerability (cisco-sa-20130327-cce)

Cisco IOS Software Zone-Based Policy Firewall Vulnerability - Cisco Systems

Cisco IOS SSH Large Packet CPU Consumption DoS (CSCdw33027)

Cisco IOS SSHv2 RSA-Based User Authentication Bypass (CSCus73013)

Cisco IOS SSL VPN Vulnerability (cisco-sa-20100922-sslvpn)

Cisco IOS Syslog Crash - Cisco Systems

Cisco IOS System Timers Remote Overflow (CSCei61732)

Cisco IOS tacacs Keyword ACL Bypass (CSCdi36962)

Cisco IOS TCLSH AAA Command Authorization Bypass (CSCeh73049)

Cisco IOS TCP Listener Crafted Packets Remote DoS (CSCek37177)

Cisco IOS TCP Sequence Prediction Connection Hijacking (CSCds04747)

Cisco IOS Telnet Service DoS (CSCef46191)

Cisco IOS Tunnel Interfaces Security Bypass

Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers - Cisco Systems

Cisco IOS Version

Cisco IOS Virtual PPP Interfaces Security Bypass

Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability - Cisco Systems

Cisco IOS VPN Enabled Detection

Cisco IOS Web Authentication DoS

Cisco IOS Web UI Cross-Site Request Forgery (cisco-sa-20200108-ios-csrf)

Cisco IOS XE ANI IPv6 Packets DoS (cisco-sa-20170320-aniipv6)

Cisco IOS XE ANI Registrar DoS (cisco-sa-20170320-ani)

Cisco IOS XE AppNav Component RCE

Cisco IOS XE Autonomic Networking Infrastructure Multiple Vulnerabilities (cisco-sa-20150325-ani)

Cisco IOS XE Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)

Cisco IOS XE Common Flow Table DoS

Cisco IOS XE Crafted MPLS IP Fragmentation DoS (CSCul00709)

Cisco IOS XE Denial of Service Vulnerability (cisco-sa-20190925-sip-dos)

Cisco IOS XE DHCP AAA Clients DoS (CSCuh04949)

Cisco IOS XE DHCP Client DoS (cisco-sa-20170322-dhcpc)

Cisco IOS XE DHCPv6 Relay Message Handling DoS (cisco-sa-20160323-dhcpv6)

Cisco IOS XE DHCPv6 Server DoS

Cisco IOS XE EnergyWise DoS (cisco-sa-20170419-energywise)

Cisco IOS XE for Cisco ASR 920 Series Routers Zero Touch Provisioning DoS (cisco-sa-20170322-ztp)

Cisco IOS XE Fragmented Packet DoS

Cisco IOS XE GNU C Library (glibc) Buffer Overflow (CSCus69732) (GHOST)

Cisco IOS XE GNU GNU C Library (glibc) Buffer Overflow (CSCus69731) (GHOST)

Cisco IOS XE HTTP Parameters Command Injection (cisco-sa-20170322-xeci)

Cisco IOS XE IKEv1 Fragmentation DoS (cisco-sa-20160928-ikev1)

Cisco IOS XE IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN)

Cisco IOS XE IKEv2 DoS (cisco-sa-20150325-ikev2)

Cisco IOS XE IKEv2 Fragmentation DoS (cisco-sa-20160323-ios-ikev2)

Cisco IOS XE IP Header Sanity Check DoS (CSCuj23992)

Cisco IOS XE IPv6 DoS

Cisco IOS XE IPv6 Snooping DoS (cisco-sa-20150923-fhs)

Cisco IOS XE L2TP Parsing DoS (cisco-sa-20170322-l2tp)

Cisco IOS XE Layer 4 Redirect DoS

Cisco IOS XE libsrtp DoS (CSCux04317)

Cisco IOS XE Line Card Console Access Vulnerability (cisco-sa-20170927-cc)

Cisco IOS XE LISP ITR DoS (CSCun73782)

Cisco IOS XE mDNS Manipulation (CSCun64867)

Cisco IOS XE Multicast Routing Multiple DoS (cisco-sa-20160928-msdp)

Cisco IOS XE Multiple OpenSSL Vulnerabilities (CSCup22487)

Cisco IOS XE Multiple OpenSSL Vulnerabilities (CSCut46130 / CSCut46126)

Cisco IOS XE Network Address Translation and Multiprotocol Label Switching DoS (CSCut96933)

Cisco IOS XE NGWC Legacy Wireless Device Manager GUI CSRF Vulnerability (cisco-sa-20190821-iosxe-ngwc-csrf)

Cisco IOS XE NTP Information Disclosure (CSCuj66318)

Cisco IOS XE NTP Packet Handling Remote DoS (cisco-sa-20160804-wedge)

Cisco IOS XE NTP Subsystem Unauthorized Access (cisco-sa-20160419-ios)

Cisco IOS XE OSPF Opaque LSA DoS (CSCui21030)

Cisco IOS XE PPPoE Packet DoS (CSCuo55180)

Cisco IOS XE SIP Memory Leak DoS (CSCuj23293)

Cisco IOS XE Smart Install Packet Image List Parameter Handling DoS (cisco-sa-20160323-smi)

Cisco IOS XE Smart Install Protocol Misuse (cisco-sr-20170214-smi)

Cisco IOS XE SNMP DoS (CSCug65204)

Cisco IOS XE SNMP Packet Handling Remote Buffer Overflow Multiple RCE (cisco-sa-20170629-snmp)

Cisco IOS XE Software AAA Login DoS (cisco-sa-20160928-aaados)

Cisco IOS XE Software Arbitrary Code Execution Vulnerability

Cisco IOS XE Software Arbitrary File Upload Vulnerability

Cisco IOS XE Software Arbitrary File Write (cisco-sa-20180328-wfw)

Cisco IOS XE Software ASIC Register Write Vulnerability

Cisco IOS XE Software Authentication, Authorization, and Accounting Login Authentication RCE (cisco-sa-20180606-aaa)

Cisco IOS XE Software Autonomic Control Plane Channel Information Disclosure (cisco-sa-20170726-aniacp)

Cisco IOS XE Software Autonomic Networking Infrastructure Certificate Revocation (cisco-sa-20170726-anicrl)

Cisco IOS XE Software Autonomic Networking Infrastructure DoS (cisco-sa-20170726-anidos)

Cisco IOS XE Software Border Gateway Protocol Message Processing DoS (cisco-sa-20160715-bgp)

Cisco IOS XE Software Catalyst 4500 Cisco Discovery Protocol Denial of Service Vulnerability

Cisco IOS XE Software CDP Memory Leak DoS Vulnerability (cisco-sa-20180926-cdp-memleak)

Cisco IOS XE Software Change of Authorization DoS (cisco-sa-20190925-tsec)

Cisco IOS XE Software CLI Command Injection Multiple Vulnerabilities (cisco-sa-20180328-cmdinj)

Cisco IOS XE Software Cluster Management Protocol DoS Vulnerability (cisco-sa-20180926-cmp)

Cisco IOS XE Software Command Injection Vulnerabilities (cisco-sa-20180926-iosxe-cmdinj)

Cisco IOS XE Software Command Injection Vulnerability

Cisco IOS XE Software Command Injection Vulnerability

Cisco IOS XE Software Command Injection Vulnerability (cisco-sa-20190327-iosxe-cmdinj)

Cisco IOS XE Software Connectivity Fault Management (CFM) DoS

Cisco IOS XE Software Consent Token Bypass Vulnerability (cisco-sa-20190925-iosxe-ctbypass)

Cisco IOS XE Software DHCP Denial of Service Vulnerability (cisco-sa-20130925-dhcp)

Cisco IOS XE Software DHCPv6 DoS (cisco-sa-20140924-dhcpv6)

Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability (cisco-sa-20180207-ios)

Cisco IOS XE Software Digital Signature Verification Bypass (cisco-sa-20180926-digsig)

Cisco IOS XE Software Digital Signature Verification Bypass Vulnerability

Cisco IOS XE Software DNS Forwarder Denial of Service Vulnerability (cisco-sa-20160928-dns)

Cisco IOS XE Software Encrypted Traffic Analytics Denial of Service Vulnerability

Cisco IOS XE Software EnergyWise DoS (cisco-sa-20140806-energywise

Cisco IOS XE Software Errdisable Vulnerabilities (cisco-sa-20180926-errdisable)

Cisco IOS XE Software Ethernet Virtual Private Network Border Gateway Protocol Denial of Service Vulnerability

Cisco IOS XE Software Filesystem Exhaustion Denial of Service Vulnerability

Cisco IOS XE Software for 1000 Series Aggregation Services Routers Fragmented Packet DoS

Cisco IOS XE Software for 1000 Series Aggregation Services Routers H.323 DoS

Cisco IOS XE Software for Cisco 4000 Series Integrated Services Routers Privileged EXEC Mode Root Shell Access (cisco-sa-20180328-privesc3)

Cisco IOS XE Software for Cisco 5760 WLC, Cisco Catalyst 4500E Supervisor Engine 8-E, and Cisco NGWC 3850 GUI Privilege Escalation (cisco-sa-20170927-ngwc)

Cisco IOS XE Software for Cisco Catalyst Switches IPv4 Denial of Service Vulnerability

Cisco IOS XE Software Forwarding Information Base DoS (cisco-sa-20180328-FIB-dos)

Cisco IOS XE Software FTP Application Layer Gateway for NAT, NAT64, and ZBFW Denial of Service Vulnerability

Cisco IOS XE Software Gigabit Ethernet Management Interface Access Control List Bypass Vulnerability

Cisco IOS XE Software H.323 Message Validation DoS (cisco-sa-20160928-h323)

Cisco IOS XE Software Hot Standby Router Protocol Information Leak Vulnerability

Cisco IOS XE Software HTTP Client Information Disclosure Vulnerability (cisco-sa-20190925-http-client)

Cisco IOS XE Software HTTP DoS Vulnerability (cisco-sa-20180926-webdos)

Cisco IOS XE Software HTTP Server DoS (cisco-sa-20190925-httpserv-dos)

Cisco IOS XE Software IKEv1 State Machine DoS (CSCuw08236)

Cisco IOS XE Software Information Disclosure Vulnerability

Cisco IOS XE Software Information Disclosure Vulnerability (cisco-sa-20190327-info)

Cisco IOS XE Software Internet Group Management Protocol Memory Leak (cisco-sa-20180328-igmp)

Cisco IOS XE Software Internet Key Exchange Denial of Service Vulnerability

Cisco IOS XE Software Internet Key Exchange Memory Leak (cisco-sa-20180328-ike)

Cisco IOS XE Software Internet Key Exchange Memory Leak Vulnerability (cisco-sa-20130925-ike)

Cisco IOS XE Software Internet Key Exchange Version 2 (IKEv2) Denial of Service (cisco-sa-20140326-ikev2)

Cisco IOS XE Software IOx Guest Shell Namespace Protection Vulnerability (cisco-sa-20190925-iox-gs)

Cisco IOS XE Software IP Detail Record DoS (cisco-sa-20160928-ipdr)

Cisco IOS XE Software IP Device Tracking DoS

Cisco IOS XE Software IP Fragment Reassembly DoS (cisco-sa-20160928-frag)

Cisco IOS XE Software IPsec DoS Vulnerability (cisco-sa-20180926-ipsec)

Cisco IOS XE Software IPv6 Denial of Service (cisco-sa-20140326-ipv6

Cisco IOS XE Software IPv6 Hop-by-Hop DoS Vulnerability (cisco-sa-20180926-ipv6hbh)

Cisco IOS XE Software IPv6 Neighbor Discovery DoS (CSCup28217)

Cisco IOS XE Software ISDN Data Leak Vulnerability

Cisco IOS XE Software ISDN Interface Denial of Service Vulnerability

Cisco IOS XE Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities (cisco-sa-20180328-lldp)

Cisco IOS XE Software Linux Kernel IP Fragment DoS (cisco-sa-20180824-linux-ip-fragment)

Cisco IOS XE Software Locator/ID Separation Protocol Authentication Bypass Vulnerability

Cisco IOS XE Software MACsec MKA Using EAP-TLS Authentication Bypass (cisco-sa-20180926-macsec)

Cisco IOS XE Software mDNS Gateway DoS

Cisco IOS XE Software Multicast Network Time Protocol Denial of Service Vulnerability (cisco-sa-20130925-ntp)

Cisco IOS XE Software Multiple IPv6 Metadata Flow Vulnerabilities (cisco-sa-20140924-metadata)

Cisco IOS XE Software Multiple mDNS Gateway DoS Vulnerabilities (cisco-sa-20140924-mdns)

Cisco IOS XE Software Multiple Vulnerabilities in ntpd (cisco-sa-20150408-ntpd)

Cisco IOS XE Software NAT DoS (cisco-sa-20160928-esp-nat)

Cisco IOS XE Software NAT Session Initiation Protocol Application Layer Gateway DoS (cisco-sa-20190925-sip-alg)

Cisco IOS XE Software NAT SIP Application Layer Gateway DoS Vulnerability (cisco-sa-20180926-sip-alg)

Cisco IOS XE Software Network Plug-and-Play Agent Certificate Validation Vulnerability

Cisco IOS XE Software Network-Based Application Recognition Denial of Service Vulnerabilities

Cisco IOS XE Software OSPF LSA Manipulation (cisco-sa-20170727-ospf)

Cisco IOS XE Software OSPFv3 DoS Vulnerability (cisco-sa-20180926-ospfv3-dos)

Cisco IOS XE Software Overlay Transport Virtualization (OTV) DoS

Cisco IOS XE Software Path Traversal Vulnerability

Cisco IOS XE Software Performance Routing Version 3 Denial of Service Vulnerability

Cisco IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability

Cisco IOS XE Software Privilege Escalation Vulnerability

Cisco IOS XE Software Privilege Escalation Vulnerability

Cisco IOS XE Software Privileged EXEC Mode Root Shell Access (cisco-sa-20180926-privesc)

Cisco IOS XE Software Privileged EXEC Mode Root Shell Access Vulnerability

Cisco IOS XE Software Quality of Service Remote Code Execution Vulnerability

Cisco IOS XE Software Raw Socket Transport Denial of Service Vulnerability

Cisco IOS XE Software Resource Reservation Protocol Interface Queue Wedge Vulnerability (cisco-sa-20130925-rsvp)

Cisco IOS XE Software REST API Authorization Bypass (cisco-sa-20180328-rest)

Cisco IOS XE Software RSVP DoS (cisco-sa-20140924-rsvp)

Cisco IOS XE Software Secure Shell Connection on VRF (cisco-sa-20190109-ios-ssh-vrf)

Cisco IOS XE Software Session Initiation Protocol Denial of Service (cisco-sa-20140326-sip)

Cisco IOS XE Software Shell Access Authentication Bypass (cisco-sa-20180926-shell-access)

Cisco IOS XE Software Short Message Service Denial of Service Vulnerability

Cisco IOS XE Software Simple Network Management Protocol Double-Free DoS (cisco-sa-20180328-snmp-dos)

Cisco IOS XE Software SIP DoS (cisco-sa-20140924-sip)

Cisco IOS XE Software SM-1T3/E3 Service Module DoS (cisco-sa-20180926-sm1t3e3)

Cisco IOS XE Software Smart Install DoS (cisco-sa-20180328-smi)

Cisco IOS XE Software Smart Install Memory Leak (cisco-sa-20160928-smi)

Cisco IOS XE Software Smart Install Remote Code Execution Vulnerability

Cisco IOS XE Software Software Plug and Play Agent Memory Leak(cisco-sa-20180926-pnp-memleak)

Cisco IOS XE Software Static Credential Vulnerability

Cisco IOS XE Software Stored Banner XSS (cisco-sa-20190925-sbxss)

Cisco IOS XE Software Stored XSS (cisco-sa-20190925-xss)

Cisco IOS XE Software Switch Integrated Security Features IPv6 DoS (cisco-sa-20180328-sisf)

Cisco IOS XE Software TCP Denial of Service Vulnerability

Cisco IOS XE Software TCP Memory Leak DoS (cisco-sa-20150325-tcpleak)

Cisco IOS XE Software TFTP DoS

Cisco IOS XE Software TFTP DoS (cisco-sa-20150722-tftp)

Cisco IOS XE Software TrustSec Protected Access Credential Provisioning DoS (cisco-sa-20190925-ctspac-dos)

Cisco IOS XE Software Unified Threat Defense Denial of Service Vulnerability

Cisco IOS XE Software User EXEC Mode Root Shell Access Multiple Vulnerabilities (cisco-sa-20180328-privesc1)

Cisco IOS XE Software Web UI Command Injection Vulnerabilities

Cisco IOS XE Software Web UI Command Injection Vulnerability

Cisco IOS XE Software Web UI Cross-Site Request Forgery (cisco-sa-20200108-ios-csrf)

Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability

Cisco IOS XE Software Web UI Cross-Site Scripting Multiple Vulnerabilities (cisco-sa-20180328-webuixss)

Cisco IOS XE Software Web UI DoS Vulnerability (cisco-sa-20180926-webuidos)

Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Cisco IOS XE Software Web UI Remote Access Privilege Escalation (cisco-sa-20180328-xepriv)

Cisco IOS XE Software Web UI REST API Authentication Bypass Vulnerability

Cisco IOS XE Software with Cisco Umbrella Integration DoS (cisco-sa-20180328-opendns-dos)

Cisco IOS XE Software Zone-Based Firewall IP Fragmentation DoS (cisco-sa-20180328-fwip)

Cisco IOS XE Source MAC Address DoS (CSCux48405)

Cisco IOS XE SSHv2 RSA-Based User Authentication Bypass (CSCus73013)

Cisco IOS XE TL1 Request Handling RCE (cisco-sa-20161102-tl1)

Cisco IOS XE Version

Cisco IOS XE VSS / BDF Traffic DoS (CSCug41049 / CSCue61890)

Cisco IOS XE Web User Interface DoS (cisco-sa-20170322-webui)

Cisco IOS XE Wireless Controller Manager DoS (cisco-sa-20170927-ios-xe)

Cisco IOS XR 5.1.x < 5.1.3 / 5.2.x < 5.2.4 / 5.3.x < 5.3.2 Fragmented Packet DoS (cisco-sa-20160810-iosxr)

Cisco IOS XR 6.0.1.x and 6.0.2.x < 6.0.2.7 / 6.1.x < 6.1.1.17 Command Input Handling Privilege Escalation

Cisco IOS XR 64-Bit Software for Cisco ASR 9000 Series Aggregation Services Routers Network Isolation Vulnerability

Cisco IOS XR < 6.1.1 on ASR 9000 LPTS DoS

Cisco IOS XR DHCPv4 Message Saturation DoS

Cisco IOS XR DHCPv6 DoS

Cisco IOS XR DHCPv6 Multiple DoS Vulnerabilities

Cisco IOS XR GNU C Library (glibc) Buffer Overflow (GHOST)

Cisco IOS XR gRPC Software Denial of Service Vulnerability

Cisco IOS XR gRPC Software Denial of Service Vulnerability

Cisco IOS XR gRPC Software Denial of Service Vulnerability

Cisco IOS XR GSR 12000 Port Range BFD DoS (cisco-sa-20160311-gsr)

Cisco IOS XR ICMPv6 Redirect Denial of Service

Cisco IOS XR IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN)

Cisco IOS XR IPv6 Extension Header DoS (cisco-sa-20150220-ipv6)

Cisco IOS XR Malformed RSVP Packet DoS

Cisco IOS XR MPLS and Network Processor (NP) Chip DoS (Typhoon-based Line Cards)

Cisco IOS XR Multiple ntpd Vulnerabilities

Cisco IOS XR NCS 6000 Multiple ntpd Vulnerabilities

Cisco IOS XR NCS 6000 Packet Timer Leak DoS (cisco-sa-20160713-ncs6k)

Cisco IOS XR NetFlow and Network Processor (NP) Chip DoS (Typhoon-based Line Cards)

Cisco IOS XR OpenSSH Module SSH Login Channel Identifier DoS

Cisco IOS XR OpenSSL Security Bypass (CSCup22654)

Cisco IOS XR OSPF Link State Advertisement PCE DoS (cisco-sa-20160104-iosxr)

Cisco IOS XR OSPFv3 DoS (CSCuj82176)

Cisco IOS XR SCP and SFTP Modules DoS (cisco-sa-20160323-ncs)

Cisco IOS XR Software BGP EVPN DoS (cisco-sa-20200122-ios-xr-evpn)

Cisco IOS XR Software BGP EVPN Operational Routes DoS (cisco-sa-20200122-ios-xr-routes)

Cisco IOS XR Software BGP MPLS-Based EVPN Denial of Service Vulnerability (cisco-sa-20190515-iosxr-evpn-dos)

Cisco IOS XR Software Border Gateway Protocol Denial of Service Vulnerability

Cisco IOS XR Software Border Gateway Protocol Denial of Service Vulnerability (cisco-sa-20200122-ios-xr-bgp-dos)

Cisco IOS XR Software Border Gateway Protocol DoS (cisco-sa-20181003-iosxr-dos)

Cisco IOS XR Software Cisco Discovery Protocol Denial of Service Vulnerability (cisco-sa-20200205-fxnxos-iosxr-cdp-dos)

Cisco IOS XR Software Cisco Discovery Protocol Remote Code Execution Vulnerability (cisco-sa-20200205-iosxr-cdp-rce)

Cisco IOS XR Software Command-Line Interface Privilege Escalation (cisco-sa-20161005-iosxr)

Cisco IOS XR Software Crafted IPv6 Packet DoS (cisco-sa-20150611-iosxr)

Cisco IOS XR Software Event Management Service gRPC Handling DoS (cisco-sa-20170503-ios-xr)

Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers MPLS OAM Denial of Service Vulnerability

Cisco IOS XR Software for Cisco ASR 9000 VMAN CLI Privilege Escalation (cisco-sa-20190925-xr-asr9k-privesc)

Cisco IOS XR Software Intermediate System-to-Intermediate System Denial of Service Vulnerability

Cisco IOS XR Software Intermediate System-to-Intermediate System DoS (cisco-sa-20200122-ios-xr-dos)

Cisco IOS XR Software IPsec Packet Processor DoS (cisco-sa-iosxr-ipsec-dos-q8UPX6m)

Cisco IOS XR Software IPv6 Malformed Packet DoS (cisco-sa-20140611-ipv6)

Cisco IOS XR Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities (cisco-sa-20180328-lldp)

Cisco IOS XR Software Malformed Border Gateway Protocol Attribute Vulnerability (cisco-sa-20120926-bgp)

Cisco IOS XR Software Memory Exhaustion Vulnerability (cisco-sa-20131002-iosxr)

Cisco IOS XR Software Multiprotocol Label Switching Packet Vulnerability (cisco-sa-20100324-ldp)

Cisco IOS XR Software netconf DoS (cisco-sa-20180502-iosxr)

Cisco IOS XR Software NETCONF Over Secure Shell ACL Bypass (cisco-sa-20191120-iosxr-ssh-bypass)

Cisco IOS XR Software Privilege Escalation (cisco-sa-20170621-ios1)

Cisco IOS XR Software Protocol Independent Multicast Denial of Service Vulnerability

Cisco IOS XR Software Route Processor Denial of Service Vulnerability (cisco-sa-20120530-iosxr)

Cisco IOS XR Software Route Processor Denial of Service Vulnerability (cisco-sa-20131023-iosxr)

Cisco IOS XR Software Secure Shell Authentication Vulnerability (cisco-sa-20190605-iosxr-ssh)

Cisco IOS XR Software Static Punt Policer DoS (CSCun83985)

Cisco IOS XR Software UDP Broadcast Forwarding Denial of Service Vulnerability (cisco-sa-20180418-iosxr)

Cisco IOS XR Typhoon-based Line Cards and Network Processor (NP) Chip DoS

Cisco IOS XR Typhoon-based Line Cards and Network Processor (NP) Chip DoS

Cisco IOS XR Version

Cisco IOS XSS and XSRF Vulnerabilities

Cisco IOS Zone-Based Firewall Feature Security Bypass (CSCun94946)

Cisco IOS-XE Zone-Based Firewall Feature Security Bypass (CSCun96847)

Cisco IOx Application Environment DoS Vulnerability (cisco-sa-20190925-iox)

Cisco IOx for IOS Software Guest Operating System Unauthorized Access Vulnerability (cisco-sa-20190925-ios-gos-auth)

Cisco IPS Authentication Manager Denial of Service Vulnerability (CSCuf20148)

Cisco IPS MainApp SNMP DoS (CSCul49309)

Cisco IPS Version

Cisco IPSec VPNSM IKE Packet DoS (CSCed30113)

Cisco IronPort Appliances Sophos Anti-Virus Vulnerabilities (cisco-sa-20121108-sophos)

Cisco IronPort PostX < 6.2.9.1 Multiple Vulnerabilities

Cisco Ironport Security Appliance Authorized Key Vulnerability

Cisco Ironport Security Appliance Default Host Key Vulnerability

Cisco Jabber for Windows DLL Preloading Vulnerability (cisco-sa-20190703-jabber-dll)

Cisco Malformed SNMP Message Handling DoS (CSCdw67458)

Cisco MDS 9000 Series Multilayer Switches Denial of Service Vulnerability

Cisco MDS 9000 VRRP DoS (CSCte27874)

Cisco MDS 9700 Series Multilayer Directors and Nexus 7000/7700 Series Switches Software Patch Signature Verification Vulnerability

Cisco Multiple Devices Crafted IP Option Remote Code Execution (CSCeh52410)

Cisco Multiple Devices Unpassworded Account

Cisco Multiple Products Network Analysis Module (NAM) SNMP Spoofing Remote Code Execution

Cisco Network Admission Control (NAC) Version

Cisco Network Admission Control Guest Server System Software Authentication Bypass (cisco-sa-20110330-nac)

Cisco Network Admission Control Manager SQL Injection (cisco-sa-20130417-nac)

Cisco Network Admission Control Shared Information Disclosure (cisco-sa-20080416-nac)

Cisco Network Registrar 7.1 DHCPv6 DoS (CSCuo07437)

Cisco Network Registrar Web UI Detection

Cisco Nexus 1000V Series Switches Arbitrary Command Execution Vulnerability (CSCui21340)

Cisco Nexus 1000V Switch for VMware vSphere Secure Login Enhancements Denial of Service Vulnerability

Cisco Nexus 1000V VEM DoS (CSCtj17451)

Cisco Nexus 3000 / 9000 Series GNU C Library (glibc) getaddrinfo() RCE (cisco-sa-20160218-glibc)

Cisco Nexus 3000 and 3500 Insecure Default Telnet Credentials (cisco-sa-20160302-n3k)

Cisco Nexus 3000 Series and 9000 Series Switches in NX-OS Mode CLI Command Software Image Signature Verification Vulnerability

Cisco Nexus 4000 Series Switches IPv6 Denial of Service (CSCtd15904)

Cisco Nexus 5500 / 5600 / 6000 SNMP DoS (cisco-sa-20160302-n5ksnmp)

Cisco Nexus 5600 and 6000 Series Switches Fibre Channel over Ethernet Denial of Service Vulnerability

Cisco Nexus 9000 Series APIC Access Control Vulnerability (CSCut12998)

Cisco Nexus 9000 Series Fabric Switches ACI Mode Border Leaf Endpoint Learning (cisco-sa-20190828-nexus-aci-dos)

Cisco Nexus 9000 Series Fabric Switches ACI Mode Fabric Infrastructure VLAN Unauthorized Access Vulnerability

Cisco Nexus 9000 Series Fabric Switches ACI Mode Link Layer Discovery Protocol Buffer Overflow Vulnerability

Cisco Nexus 9000 Series Platform Manager Service DoS

Cisco Nexus TCP Packet TIME\_WAIT State Handling DoS (cisco-sa-20160302-netstack)

Cisco NTP ntpd readvar Variable Remote Overflow (CSCdt93866)

Cisco NX-OS Arbitrary File Read Vulnerability (CSCul05217 / CSCul23419)

Cisco NX-OS Border Gateway Protocol DoS (cisco-sa-20161005-bgp)

Cisco NX-OS Cisco Fabric Services Multiple Vulnerabilities.

Cisco NX-OS DHCP POAP Command Injection Vulnerability

Cisco NX-OS DHCPv4 Crafted Packet DoS (cisco-sa-20161005-dhcp1)

Cisco NX-OS DHCPv4 Crafted Packet DoS (cisco-sa-20161005-dhcp2)

Cisco NX-OS Failed Authentication Handling Remote DoS (cisco-sa-20170315-nss1)

Cisco NX-OS Fibre Channel over Ethernet DoS (cisco-sa-20170607-nxos)

Cisco NX-OS GNU Bash Environment Variable Command Injection Vulnerability (cisco-sa-20140926-bash) (Shellshock)

Cisco NX-OS GNU C Library (glibc) Buffer Overflow (GHOST)

Cisco NX-OS HSRP DoS (CSCup11309)

Cisco NX-OS IS-IS Packet Processing Denial of Service Vulnerability

Cisco NX-OS Malformed IP Packet DoS (cisco-sa-20120215-nxos)

Cisco NX-OS Malformed LISP Packet DoS (CSCuv11993)

Cisco NX-OS Multiple ntpd Vulnerabilities

Cisco NX-OS Multiple Vulnerabilities (cisco-sa-20140521-nxos)

Cisco NX-OS NXAPI Multiple Vulnerabilities.

Cisco NX-OS OpenSSL Multiple Vulnerabilities

Cisco NX-OS OpenSSL Multiple Vulnerabilities (cisco-sa-20150310-ssl) (FREAK)

Cisco NX-OS OTV GRE Packet Header Parameter Handling RCE (cisco-sa-20161005-otv)

Cisco NX-OS Precision Time Protocol (PTP) Denial of Service Vulnerability

Cisco NX-OS SNMP DoS.

Cisco NX-OS Software 802.1X Extensible Authentication Protocol over LAN Denial of Service Vulnerability

Cisco NX-OS Software Anycast Gateway Invalid ARP Vulnerability

Cisco NX-OS Software Arbitrary File Overwrite Vulnerability

Cisco NX-OS Software Authenticated Simple Network Management Protocol Denial of Service Vulnerability

Cisco NX-OS Software Authenticated Simple Network Management Protocol DoS (cisco-sa-20180620-nxossnmp)

Cisco NX-OS Software Bash Bypass Guest Shell (cisco-sa-20190515-nxos-bash-bypass)

Cisco NX-OS Software Bash Shell Privilege Escalation Vulnerability

Cisco NX-OS Software Bash Shell Role-Based Access Control Bypass Privilege Escalation Vulnerability

Cisco NX-OS Software BGP DoS (CSCtn13055)

Cisco NX-OS Software Border Gateway Protocol MD5 Authentication Bypass Vulnerability

Cisco NX-OS Software Buffer Overflow and Command Injection Vulnerabilities

Cisco NX-OS Software Cisco Discovery Protocol Arbitrary Code Execution and DoS (cisco-sa-20200226-fxos-nxos-cdp)

Cisco NX-OS Software Cisco Discovery Protocol Denial of Service Vulnerability (cisco-sa-20200205-fxnxos-iosxr-cdp-dos)

Cisco NX-OS Software Cisco Discovery Protocol Remote Code Execution Vulnerability (cisco-sa-20200205-nxos-cdp-rce)

Cisco NX-OS Software Cisco Fabric Services Denial of Service Vulnerability

Cisco NX-OS Software CLI Command Injection Vulnerability (cisco-sa-20190306-nxos-cmdinj-1608)

Cisco NX-OS Software CLI Command Injection Vulnerability (Cisco-Sa-20190306-Nxos-Cmdinj-1609)

Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1606)

Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1607)

Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1610)

Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1612)

Cisco NX-OS Software CLI Command Injection Vulnerability (CVE-2019-1613)

Cisco NX-OS Software Command Injection (cisco-sa-20190306-nxos-cmdinj-1611)

Cisco NX-OS Software Command Injection (cisco-sa-20190515-nxos-cmdinj-1735)

Cisco NX-OS Software Command Injection (cisco-sa-20190515-nxos-cmdinj-1770)

Cisco NX-OS Software Command Injection (cisco-sa-20190515-nxos-cmdinj-1776)

Cisco NX-OS Software Command Injection (cisco-sa-20190515-nxos-cmdinj-1783)

Cisco NX-OS Software Command Injection (cisco-sa-20190515-nxos-cmdinj-1790)

Cisco NX-OS Software Command Injection (cisco-sa-20190515-nxos-cmdinj-1795)

Cisco NX-OS Software Command Injection (CVE-2019-1784)

Cisco NX-OS Software Command Injection Vulnerabilities (cisco-sa-20190515-fxos-nxos-cmdinj-1781-1782)

Cisco NX-OS Software Command Injection Vulnerability (cisco-sa-20190925-nxos-vman-cmd-inj)

Cisco NX-OS Software Command Injection Vulnerability (CVE-2019-1778)

Cisco NX-OS Software Command Injection Vulnerability (CVE-2019-1779)

Cisco NX-OS Software Command Injection Vulnerability (CVE-2019-1780)

Cisco NX-OS Software Command Injection Vulnerability (CVE-2019-1791)

Cisco NX-OS Software Fabric Services over IP Denial of Service Vulnerability (CVE-2019-1962)

Cisco NX-OS Software IPv6 Denial of Service Vulnerability (cisco-sa-20190828-nxos-ipv6-dos)

Cisco NX-OS Software Line Card Command Injection (cisco-sa-20190515-nxos-linecardinj-1769)

Cisco NX-OS Software Link Layer Discovery Protocol Denial of Service Vulnerability

Cisco NX-OS Software Multiple Vulnerabilities (cisco-sa-20190515-nxos-cmdinj-1774-1775)

Cisco NX-OS Software Netstack DoS (cisco-sa-20190306-nxos-netstack)

Cisco NX-OS Software NX-API Arbitrary Code Execution Vulnerability

Cisco NX-OS Software NX-API Command Injection Vulnerability

Cisco NX-OS Software NX-API Denial of Service Vulnerability

Cisco NX-OS Software NX-API Denial of Service Vulnerability (CVE-2019-1968)

Cisco NX-OS Software NX-API Sandbox Cross-Site Scripting Vulnerability

Cisco NX-OS Software OSPF LSA Manipulation (cisco-sa-20170727-ospf)

Cisco NX-OS Software Privilege Escalation Vulnerability

Cisco NX-OS Software Privilege Escalation Vulnerability

Cisco NX-OS Software Privilege Escalation Vulnerability

Cisco NX-OS Software Python Parser Escape Vulnerability

Cisco NX-OS Software Python Parser Privilege Escalation Vulnerability

Cisco NX-OS Software Remote Management Memory Leak Denial of Service Vulnerability (CVE-2019-1965)

Cisco NX-OS Software Secure Configuration Bypass (cisco-sa-20190515-nxos-conf-bypass)

Cisco NX-OS Software Simple Network Management Protocol DoS (cisco-sa-20190515-nxos-snmp-dos)

Cisco NX-OS Software SNMP Access Control List Configuration Name Bypass Vulnerability (CVE-2019-1969)

Cisco NX-OS Software SSH Key Information Disclosure Vulnerability

Cisco NX-OS Software Unauthorized Directory Access Vulnerability

Cisco NX-OS Software Unauthorized Filesystem Access Vulnerability

Cisco NX-OS Software Virtual Service Image Signature Bypass Vulnerability

Cisco NX-OS SSH Connection Negotiation Remote Command Execution (cisco-sa-20161005-nxaaa)

Cisco NX-OS System Software Authentication, Authorization, and Accounting Denial of Service Vulnerability Vulnerability

Cisco NX-OS Telnet Packet Header Handling Remote DoS (cisco-sa-20170315-nss)

Cisco NX-OS Version

Cisco ONS 15400 Series Devices Multiple Vulnerabilities in OpenSSL

Cisco ONS 15454 Controller Card DoS (CSCug97315)

Cisco ONS 15454 Controller Card DoS (CSCug97348)

Cisco ONS 15454 Controller Card DoS (CSCug97416)

Cisco ONS 15454 Controller Card DoS (CSCun06870)

Cisco ONS Detection

Cisco ONS Multiple Remote Vulnerabilities (20040219-ONS)

Cisco ONS Multiple Remote Vulnerabilities (20040721-ons)

Cisco ONS Products Remote DoS

Cisco Open Network Environment Platform Unvalidated Pointer (CSCui51551)

Cisco Prime Collaboration Assurance 10.5.1.x < 10.5.1.58480 Multiple Vulnerabilities

Cisco Prime Collaboration Assurance 10.5.x / 10.6.x / 11.0.x / 11.1.x < 11.1.66527 Open Redirect (cisco-sa-20160503-pca)

Cisco Prime Collaboration Assurance Default 'cmuser' Credentials (cisco-sa-20151209-pca)

Cisco Prime Collaboration Assurance Multiple Vulnerabilities (cisco-sa-20100217-csa)

Cisco Prime Collaboration Provisioning 10.6.x / 11.0.x < 11.0.0.815 Web Framework SQLi (cisco-sa-20151008-pcp)

Cisco Prime Collaboration Provisioning 9.0.x / 11.0.x < 11.1 Local Privilege Escalation (cisco-sa-20160209-pcp)

Cisco Prime Collaboration Provisioning < 12.1 Multiple Vulnerabilities (cisco-sa-20170517-pcp1 - cisco-sa-20170517-pcp3)

Cisco Prime Collaboration Provisioning < 12.3 Authenticated SQL Injection Vulnerability (cisco-sa-20171101-cpcp)

Cisco Prime Collaboration Provisioning Cross-Site Scripting Vulnerability (cisco-sa-prime-collab-xss-RjRCe9n7)

Cisco Prime Collaboration Provisioning Hard-Coded Password Vulnerability (cisco-sa-20180307-cpcp

Cisco Prime Collaboration Provisioning Information Disclosure (cisco-sa-prim-collab-disclo-FAnX4DKB)

Cisco Prime Collaboration Provisioning ScriptMgr Servlet Authentication Bypass RCE

Cisco Prime Collaboration Provisioning Unauthorized Password Change Denial of Service Vulnerability (cisco-sa-20180801-pcp-dos

Cisco Prime Collaboration Provisioning Web Framework Access Controls Bypass Vulnerability (cisco-sa-20150916-pcp)

Cisco Prime Data Center Network Manager 10.1.x < 10.2.1 Multiple Vulnerabilities

Cisco Prime Data Center Network Manager 10.1.x < 10.2.1 Multiple Vulnerabilities (remote check)

Cisco Prime Data Center Network Manager 6.x XSS (credentialed check)

Cisco Prime Data Center Network Manager 6.x XSS (uncredentialed check)

Cisco Prime Data Center Network Manager < 11.0(1) Download Servlet Path Traversal Vulnerability

Cisco Prime Data Center Network Manager < 6.2(1) Multiple Vulnerabilities (credentialed check)

Cisco Prime Data Center Network Manager < 6.2(1) Multiple Vulnerabilities (uncredentialed check)

Cisco Prime Data Center Network Manager < 7.1(1) Directory Traversal Vulnerability

Cisco Prime Data Center Network Manager < 7.1(1) Directory Traversal Vulnerability

Cisco Prime Data Center Network Manager File Upload RCE (cisco-sa-20180502-prime-upload)

Cisco Prime Data Center Network Manager ntpd Multiple Vulnerabilities (uncredentialed check)

Cisco Prime Data Center Network Manager Static Credential Authentication Bypass (cisco-sa-20170607-dcnm2)

Cisco Prime Infrastructure Cross-Site Scripting Vulnerability (cisco-sa-20190123-cpi-xss)

Cisco Prime Infrastructure Detection

Cisco Prime Infrastructure Java Deserialization RCE (cisco-sa-20160406-remcode)

Cisco Prime Infrastructure Multiple Vulnerabilities (cisco-sa-20190515-pi-rce)

Cisco Prime Infrastructure TFTP Arbitrary File Upload and Command Execution Vulnerability (cisco-sa-20181003-pi-tftp)

Cisco Prime Infrastructure TFTP Arbitrary File Upload and Command Execution Vulnerability (cisco-sa-20181003-pi-tftp)

Cisco Prime LAN Management Solution ntpd Multiple Vulnerabilities

Cisco Prime LAN Management Solution Session Fixation Vulnerability

Cisco Prime Network Control System Default Credentials (cisco-sa-20130410-ncs)

Cisco Prime Network Control System Version

Cisco Prime Network Services Controller Unauthorized Local Command Execution (cisco-sa-20151217-pnsc)

Cisco Regular Expression Processing DoS

Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability

Cisco RV110W, RV130W, and RV215W Routers Management Interface Remote Command Execution Vulnerability (cisco-sa-20190227-rmi-cmd-ex)

Cisco RV110W, RV130W, and RV215W Routers Syslog HTTP Access Information Disclosure Vulnerability (cisco-sa-20190619-rv-fileaccess)

Cisco Secure Access Control (cisco-sa-20180502-acs1)

Cisco Secure Access Control Multiple Vulnerabilities (cisco-sa-20180307-acs1 / cisco-sa-20180307-acs2)

Cisco Secure Access Control Server (ACS) CSuserCGI.exe Multiple Remote Overflows

Cisco Secure Access Control Server Detection

Cisco Secure Access Control Server UCP service Detection

Cisco Secure Access Control System (ACS) Multiple Vulnerabilities

Cisco Secure Access Control System SQLi Vulnerability (cisco-sa-20150211-csacs)

Cisco Secure Access Control System TACACS+ Authentication Bypass (cisco-sa-20121107-acs)

Cisco Secure Access Control System Version

Cisco Secure ACS EAP Parsing Vulnerability (cisco-sr-20080903-csacs)

Cisco Secure ACS Portal Interface Session Hijacking

Cisco Secure ACS Portal XSS (CSCue65949)

Cisco Secure ACS RMI Arbitrary File Read (CSCud75169)

Cisco Secure ACS Unauthorized Password Change

Cisco Security Agent 5.2 DoS (cisco-sa-20100217-csa)

Cisco Security Manager Web Server Detection

Cisco SIP Crafted INVITE Message Handling DoS (CSCdz39284, CSCdz41124)

Cisco Small Business Router SNMP Detection

Cisco Small Business Routers RV016, RV042, RV042G, and RV082 Information Disclosure (cisco-sa-20191120-sbr-rv-infodis)

Cisco Small Business Routers RV016, RV042, RV042G, RV082, RV320, and RV325 Command Injection Vulnerability (cisco-sa-20191106-sbr-cominj)

Cisco Small Business RV132W and RV134W Remote Code Execution (cisco-sa-20180207-rv13x)

Cisco Small Business RV320 and RV325 Routers Multiple Vulnerabilities

Cisco Small Business RV320 and RV325 Routers Multiple Vulnerabilities (cisco-sa-20190123-rv-inject, cisco-sa-20190123-rv-info)

Cisco Software Maintenance Update Enumeration

Cisco SPA100 Series Multiple Vulnerabilities

Cisco SSH2 Server/Client Malformed Packet Remote DoS (CSCdz60229, CSCdy87221, CSCdu75477)

Cisco StarOS Denial of Service Vulnerability

Cisco StarOS for ASR 5000 Series Routers IPsec VPN Tunnel DoS (cisco-sa-20170621-asr)

Cisco TANDBERG MXP < 9.0 SNMP Packet Handling DoS

Cisco TelePresence CE 8.1.1 < 8.3.2 ICMP Packet Handling DoS (cisco-sa-20170503-ctp)

Cisco TelePresence Codecs DoS

Cisco TelePresence Collaboration Endpoint < 9.8.1 Audio Eavesdropping Vulnerability

Cisco TelePresence Collaboration Endpoint Software Arbitrary File Overwrite Vulnerabilities (cisco-sa-20191016-tele-ce-file-ovrwrt)

Cisco TelePresence Collaboration Endpoint Software Arbitrary File Write (cisco-sa-20191016-tele-ce-filewrite)

Cisco TelePresence Collaboration Endpoint Software Command Injection Vulnerability (cisco-sa-20191016-tele-ce-cmdinj)

Cisco TelePresence Conductor Bash Remote Code Execution (Shellshock)

Cisco TelePresence Conductor Detection

Cisco TelePresence Conductor GNU glibc gethostbyname Function Buffer Overflow Vulnerability (GHOST)

Cisco TelePresence Conductor Login Security Bypass Vulnerability

Cisco TelePresence Conductor REST API Server-Side Request Forgery Vulnerability

Cisco TelePresence Conductor SDP Media Description Vulnerability

Cisco TelePresence CVE-2013-3377 Malformed SIP Packet Handling Remote DoS

Cisco TelePresence CVE-2013-3378 Software Malformed SIP Packet Handling Remote DoS

Cisco TelePresence DSP Card Crafted RTP Packet H.264 Bit Stream Handling DoS

Cisco TelePresence Endpoint Command Shell Injection Vulnerability

Cisco TelePresence Endpoint SIP INVITE Packet Flood DoS (cisco-sa-20170607-tele)

Cisco TelePresence Endpoint Software Path Traversal (cisco-sa-telepresence-path-tr-wdrnYEZZ)

Cisco TelePresence Endpoint Software Privilege Escalation Vulnerability

Cisco TelePresence IP VCR Command Injection Vulnerability

Cisco TelePresence IP VCR Detection

Cisco TelePresence ISDN Gateway Command Injection Vulnerability

Cisco TelePresence ISDN Gateway D-Channel DoS

Cisco TelePresence ISDN Gateway Detection

Cisco TelePresence Management Address Unspecified Admin Access

Cisco TelePresence MCU Command Injection Vulnerability

Cisco TelePresence MCU Fragmented Packets Reassembly RCE

Cisco TelePresence MCU Series Devices Multiple Vulnerabilities in OpenSSL

Cisco TelePresence MCU Software Memory Exhaustion

Cisco TelePresence MSE 8050 Command Injection Vulnerability

Cisco TelePresence Multipoint Control Unit Detection

Cisco TelePresence Multipoint Switch Multiple Vulnerabilities (cisco-sa-20120711-ctms)

Cisco TelePresence MXP Series Software Multiple Vulnerabilities (cisco-sa-20140430-mxp)

Cisco TelePresence Server Command Injection Vulnerability

Cisco TelePresence Server Conference Control Protocol API URL Handling DoS (cisco-sa-20150916-tps)

Cisco TelePresence Server Crafted IPv6 Packet Handling DoS (cisco-sa-20160406-cts)

Cisco TelePresence Server HTTP Parsing Engine DoS (cisco-sa-20160406-cts1)

Cisco TelePresence Server Malformed STUN Packet Processing DoS (cisco-sa-20160406-cts2)

Cisco TelePresence Supervisor Detection

Cisco TelePresence Supervisor MSE 8050 Multiple Vulnerabilities in OpenSSL

Cisco TelePresence Supervisor MSE 8050 TCP Connection Request Saturation Remote DoS

Cisco TelePresence System Detection

Cisco TelePresence System Software Command Execution

Cisco TelePresence TC and TE Software Multiple Vulnerabilities (cisco-sa-20140430-tcte)

Cisco TelePresence TC and TE Software Multiple Vulnerabilities (cisco-sa-20150513-tc)

Cisco TelePresence TC Software Parameter Authentication Bypass (CSCuv00604)

Cisco TelePresence VCS / Expressway 12.5.x < 12.5.4 XSS

Cisco TelePresence VCS / Expressway 8.x < 8.8 Multiple Vulnerabilities (Bar Mitzvah)

Cisco TelePresence VCS / Expressway < 8.11 DoS

Cisco TelePresence VCS / Expressway < 8.8.2 Received Packet Parser DoS

Cisco TelePresence VCS / Expressway Series < 12.5 REST API Server-Side Request Forgery Vulnerability

Cisco TelePresence VCS / Expressway Series < 7.2.4 / 8.1.2 / 8.2.2 Login Security Bypass Vulnerability

Cisco TelePresence VCS / Expressway Series < 8.2 Multiple DoS Vulnerabilities

Cisco TelePresence VCS / Expressway Series < 8.2 SDP Media Description Vulnerability

Cisco TelePresence VCS 8.5.1 Unspecified XSRF (cisco-sa-20151120-tvcs)

Cisco TelePresence VCS Expressway 8.5.1 / 8.5.2 request-xconfdump Symbolic Link Local File Manipulation (cisco-sa-20141007-vcs)

Cisco TelePresence VCS Expressway 8.5.3 XML External Entity (XXE) Injection

Cisco TelePresence VCS Expressway Series 8.5.1 Information Disclosure

Cisco TelePresence VCS Expressway Series 8.5.2 Multiple Vulnerabilities

Cisco TelePresence Video Communication Server (VCS) Detection

Cisco TelePresence Video Communication Server and Cisco Expressway Series Server-Side Request Forgery Vulnerability

Cisco TelePresence Video Communication Server Bash Remote Code Execution (Shellshock)

Cisco TelePresence Video Communication Server Expressway Default SSL Certificate

Cisco TelePresence Video Communication Server GNU glibc gethostbyname Function Buffer Overflow Vulnerability (GHOST)

Cisco TelePresence Video Communication Server Heartbeat Information Disclosure (Heartbleed)

Cisco TelePresence Video Communication Server SIP DoS

Cisco TelePresence XML API HTTP Request Handling Authentication Bypass (cisco-sa-20160504-tpxml)

Cisco Telnet Denial of Service Vulnerability - Cisco Systems

Cisco TFTP Server Long Filename DoS (CSCdy03429)

Cisco uBR10012 Series Devices SNMP Vulnerability - Cisco Systems

Cisco UCS Central Software < 1.3(1c) HTTP Request Handling RCE

Cisco UCS Central Software < 2.0(1c) HTTP Request Handling RCE

Cisco UCS Director Authentication Bypass (cisco-sa-20190821-imcs-ucs-authby)

Cisco UCS Director Authentication Bypass (cisco-sa-20190821-imcs-ucs-cmdinj)

Cisco UCS Director Authentication Bypass (cisco-sa-20190821-ucsd-authbypass)

Cisco UCS Director Code Injection (CSCur02877) (Shellshock)

Cisco UCS Director Detection

Cisco UCS Director Loggoff DoS (cisco-sa-20190821-ucs-imc-dos)

Cisco UCS Director SCP User Default Credentials (cisco-sa-20190821-imcs-usercred)

Cisco UCS Integrated Management Controller < 2.3(1) DoS (cisco-sa-20140908-ucse)

Cisco UCS Manager Software CLI Command Injection (cisco-sa-20200226-fxos-ucs-cmdinj)

Cisco UCS Platform Emulator < 3.1(1ePE1) Multiple Vulnerabilities

Cisco UCS Platform Emulator Web UI Detection

Cisco UCS Software Cisco Discovery Protocol Arbitrary Code Execution and DoS (cisco-sa-20200226-fxos-nxos-cdp)

Cisco Unified Communication Manager Apache Struts RCE (CSCvm14042)

Cisco Unified Communication Manager HTTP Interface Information Disclosure Vulnerability (CSCvf20218)

Cisco Unified Communications Manager 'CTIManager' Remote Command Execution (CSCum95491)

Cisco Unified Communications Manager (CUCM) Detection

Cisco Unified Communications Manager Cross-Site Request Forgery (XSRF) Vulnerability (cisco-sa-20191002-cucm-csrf)

Cisco Unified Communications Manager Cross-Site Request Forgery Vulnerability (cisco-sa-20200122-cuc-info-disclosure)

Cisco Unified Communications Manager Cross-Site Request Forgery Vulnerability (cisco-sa-ucm-csrf-NbhZTxL)

Cisco Unified Communications Manager Cross-Site Scripting (XSS) Vulnerability

Cisco Unified Communications Manager Cross-Site Scripting (XSS) Vulnerability

Cisco Unified Communications Manager Cross-Site Scripting Vulnerability

Cisco Unified Communications Manager Cross-Site Scripting Vulnerability

Cisco Unified Communications Manager Denial of Service Vulnerability

Cisco Unified Communications Manager Denial-of-Service Vulnerability (DoS)

Cisco Unified Communications Manager Express Denial of Service Vulnerabilities (cisco-sa-20100324-cucme)

Cisco Unified Communications Manager Express Vulnerability - Cisco Systems

Cisco Unified Communications Manager IM & Presence Service Apache Struts RCE (CSCvm14049)

Cisco Unified Communications Manager IM and Presence GNU C Library (glibc) Buffer Overflow (CSCus69785) (GHOST)

Cisco Unified Communications Manager IM and Presence Server DoS (cisco-sa-20130821-cup)

Cisco Unified Communications Manager IM and Presence Service Enumeration Vulnerability (CSCur63497)

Cisco Unified Communications Manager IM and Presence XSS (cisco-sa-20191002-cuc-xss)

Cisco Unified Communications Manager Java Interface SQL Injection (CSCuo17337)

Cisco Unified Communications Manager Java Object Deserialization RCE (CSCux34835)

Cisco Unified Communications Manager Multiple Arbitrary File Manipulation Vulnerabilities (CSCuo17199 / CSCuo17302)

Cisco Unified Communications Manager Multiple DoS Vulnerabilities (cisco-sa-20130227-cucm)

Cisco Unified Communications Manager Multiple Reflected XSS

Cisco Unified Communications Manager Registration Messages DoS (CSCuf93466)

Cisco Unified Communications Manager Remote Buffer Overflow (CSCud54358)

Cisco Unified Communications Manager Remote Buffer Overflow (CSCus66650) (GHOST)

Cisco Unified Communications Manager Security Bypass Vulnerability (cisco-sa-20191002-ucm-secbypass)

Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability

Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20120926-cucm)

Cisco Unified Communications Manager SIP DoS (CSCub85597)

Cisco Unified Communications Manager SIP Memory Leak DoS (CSCuv39370)

Cisco Unified Communications Manager SIP UDP Throttling DoS (CSCuz72455)

Cisco Unified Communications Manager SQL Injection (CSCut33447 / CSCut33608)

Cisco Unified Communications Manager SQL Injection Vulnerability

Cisco Unified Communications Manager SQL Injection Vulnerability

Cisco Unified Communications Manager SQL Injection Vulnerability

Cisco Unified Communications Manager SQLi (cisco-sa-20191002-cuc-inject)

Cisco Unified Communications Manager SSLv3 Information Disclosure (cisco-sa-20141015-poodle) (POODLE)

Cisco Unified Communications Manager TLS SAN Field MitM (CSCuq86376)

Cisco Unified Communications Manager UDP Memory Leak DoS (CSCub85597)

Cisco Unified Communications Manager Unspecified SQL Injection (CSCup88089)

Cisco Unified Communications Manager XSS (cisco-sa-20170517-ucm)

Cisco Unified Communications Manager XSS (cisco-sa-20191002-cuc-xss)

Cisco Unified Computing System (UCS) Manager Version

Cisco Unified Computing System Cisco Management Controller Denial of Service Vulnerability (CSCtg20734)

Cisco Unified Computing System Fabric Interconnect Root Privilege Escalation (cisco-sa-20190828-ucs-privescalation)

Cisco Unified Computing System Integrated Management Controller XSRF (CSCuq45477)

Cisco Unified Computing System Manager CGI RCE (CSCur90888)

Cisco Unified Computing System Serial over LAN Static Private Key Vulnerability (CSCte90338)

Cisco Unified Computing System Smart Call Home Input Validation Vulnerability (CSCtl00186)

Cisco Unified Intelligence Center (CUIC) Appliance Detection (SSH)

Cisco Unified Intelligence Center (CUIC) Software Cross-Site Request Forgery Vulnerability

Cisco Unified Intelligence Center (CUIC) Software Cross-Site Scripting Vulnerability

Cisco Unified Intelligence Center (CUIC) Software Unauthenticated User Account Creation Vulnerability

Cisco Unified Intelligence Center Cross-Site Scripting Vulnerability

Cisco Unified Intelligence Center Cross-Site Scripting Vulnerability

Cisco Unified Intelligence Center Remote File Injection Vulnerability

Cisco Unified Intelligence Center Software Cross-Site Scripting Vulnerability

Cisco Unified IP Phones Multiple Vulnerabilities (cisco-sa-20110601-phone)

Cisco Unified IP Phones Privilege Escalation (cisco-sa-20130109-uipphone)

Cisco Unified MeetingPlace Multiple Session Weaknesses

Cisco Unified MeetingPlace Unspecified SQLi (CSCuu54037)

Cisco Unified MeetingPlace Web Conferencing Unauthorized Password Change Security Bypass

Cisco Unified MeetingPlace Web Page Source Code Remote Password Disclosure (CSCuu33050)

Cisco Unified MeetingPlace XML Processing Information Disclosure (CSCus97452)

Cisco Unified Presence Server DoS (cisco-sa-20120912-cupxcp)

Cisco Unified Presence Server DoS (cisco-sa-20130227-cups)

Cisco Unity Connection Administrator Password Bypass (cisco-sa-20120229-cuc)

Cisco Unity Connection Cross-Site Request Forgery Vulnerability

Cisco Unity Connection File Upload Denial of Service Vulnerability

Cisco Unity Connection libSRTP Denial of Service Vulnerability

Cisco Unity Connection libSRTP Denial of Service Vulnerability

Cisco Unity Connection Multiple Remote DoS (cisco-sa-20150401-cuc)

Cisco Unity Connection Reflected XSS Vulnerability (cisco-sa-20170906-cuc)

Cisco Unity Connection Remote Denial of Service (cisco-sa-20120229-cuc)

Cisco Unity Connection Version

Cisco Unity Connection Voice Operating System-Based Products Unauthorized Access Vulnerability

Cisco Unity Connection Web Framework Cross-Site Scripting Vulnerability

Cisco Unity Connection Web Framework Cross-Site Scripting Vulnerability

Cisco Unity Connection Web Framework XSS (cisco-sa-20191002-cuc-xss)

Cisco Unity Presence Voice Operating System-Based Products Unauthorized Access Vulnerability

Cisco Unsupported ACE Module Detection

Cisco VG248 Unpassworded Account

Cisco Video Surveillance Manager Appliance Default Password Vulnerability(cisco-sa-20180921-vsm)

Cisco Video Surveillance Manager Default Administrator Credentials

Cisco Video Surveillance Manager Multiple Vulnerabilities (cisco-sa-20130724-vsm)

Cisco Video Surveillance Manager Web Detection

Cisco Virtual Security Gateway OpenSSL Alternative Certificate Validation Bypass (cisco-sa-20150710-openssl)

Cisco Virtual Voice Browser (VVB) Appliance Detection (SSH)

Cisco VLAN Trunking Protocol Vulnerability (cisco-sr-20081105-vtp)

Cisco VoIP Phone Multiple Script Malformed Request DoS

Cisco VPN 3000 Concentrator Certificate Management Page HTML Source Certificate Password Disclosure (CSCdw50657)

Cisco VPN 3000 Concentrator HTML Interface Long URL DoS (CSCdu15622)

Cisco VPN 3000 Concentrator HTML Source Plaintext User Password Disclosure (CSCdv88230, CSCdw22408)

Cisco VPN 3000 Concentrator LAN-to-LAN IPSEC Tunnel Connection Termination DoS (CSCdx54675)

Cisco VPN 3000 Concentrator Malformed ISAKMP Packet Remote DoS (CSCdy38035)

Cisco VPN 3000 Concentrator Multiple Service Banner System Information Disclosure (CSCdu35577 HTTP Check)

Cisco VPN 3000 Concentrator Multiple Service Banner System Information Disclosure (CSCdu35577)

Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdt56514, CSCdv66718)

Cisco VPN 3000 Concentrator Multiple Vulnerabilities (CSCdx07754, CSCdx24622, CSCdx24632)

Cisco VPN 3000 Concentrator PPTP No Encryption Option Remote DoS (CSCdx39981)

Cisco VPN 3000 Concentrator PPTP/IPSEC Group Credential Authentication Bypass (CSCdv66718)

Cisco VPN 3000 Series Multiple Vulnerabilities (CSCdea77143, CSCdz15393, CSCdt84906)

Cisco VPN Concentrator Invalid Login DoS (CSCdu82823)

Cisco Web Cache Control Protocol Router Vulenrability

Cisco Web Security Appliance (WSA) GUI Denial of Service Vulnerability

Cisco Web Security Appliance Decryption Policy Bypass Vulnerability (cisco-sa-20190206-wsa-bypass)

Cisco Web Security Appliance FTP Authentication Bypass Vulnerability

Cisco Web Security Appliance HTTP Header Injection Vulnerability

Cisco Web Security Appliance HTTPS Certificate Denial of Service Vulnerability

Cisco Web Security Appliance HTTPS Packet Processing DoS (cisco-sa-20160302-wsa)

Cisco Web Security Appliance L4 Traffic Monitor Bypass

Cisco Web Security Appliance Malformed Request Denial of Service Vulnerability

Cisco Web Security Appliance Management Interface < 11.8.0-332 Cross-Site Scripting Vulnerability XSS

Cisco Web Security Appliance Multiple DoS Vulnerabilities

Cisco Web Security Appliance Multiple Vulnerabilities

Cisco Web Security Appliance Multiple Vulnerabilities

Cisco Web Security Appliance Multiple Vulnerabilities.

Cisco Web Security Appliance Privilege Escalation Vulnerability

Cisco Web Security Appliance Privilege Escalation Vulnerability.

Cisco Web Security Appliance Proxy Restrictions Bypass

Cisco Web Security Appliance Telnet Remote Code Execution (cisco-sa-20120126-ironport)

Cisco Web Security Appliance Unauthorized Device Reset Vulnerability

Cisco Web Security Appliance Version

Cisco Web Security Appliance Web Detection

Cisco Webex Network Recording Admin Page Privilege Escalation Vulnerability (cisco-sa-20191106-wbs-privilege)

Cisco Windows Jabber Client Multiple Vulnerabilities in OpenSSL (cisco-sa-20140605-openssl)

Cisco Wireless LAN Controller (WLC) Version

Cisco Wireless LAN Controller 802.11 WME Packet Header Handling DoS (cisco-sa-20170405-wlc)

Cisco Wireless LAN Controller 802.11i Management Frame DoS

Cisco Wireless LAN Controller CAPWAP Discovery Request Denial of Service Vulnerability

Cisco Wireless LAN Controller Client Disconnection DoS

Cisco Wireless LAN Controller HTTP Parsing Engine Denial of Service Vulnerability

Cisco Wireless LAN Controller IPv6 UDP Packet Handling DoS (cisco-sa-20170405-wlc2)

Cisco Wireless LAN Controller Locally Significant Certificate Denial of Service Vulnerability

Cisco Wireless LAN Controller Multiple DoS

Cisco Wireless LAN Controller Multiple Vulnerabilities

Cisco Wireless LAN Controller Multiple Vulnerabilities

Cisco Wireless LAN Controller Multiple Vulnerabilities

Cisco Wireless LAN Controller Multiple Vulnerabilities

Cisco Wireless LAN Controller Multiple Vulnerabilities

Cisco Wireless LAN Controller Path Traversal Vulnerability

Cisco Wireless LAN Controller Secure Shell (SSH) Denial of Service Vulnerability (cisco-sa-20191016-wlc-ssh-dos)

Cisco Wireless LAN Controller Secure Shell Unauthorized Access Vulnerability

Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities

Cisco Wireless LAN Controller Software IAPP Message Handling Denial of Service Vulnerabilities

Cisco Wireless LAN Controller Unauthorized Access Vulnerability

Cisco Wireless LAN Controller Web Authentication DoS (CSCum03269)

Cisco Wireless LAN Controllers 5500 Series (POODLE)

Cisco WLC Web-Based Management Interface XSS Vulnerability (CSCuf77810)

CiscoWorks Management Console Detection

Combined IOS Table for January 24, 2007 Security Advisories (deprecated)

Crafted ICMP Messages Can Cause Denial of Service - Cisco Systems

Crafted IP Option Vulnerability

Crafted IP Option Vulnerability (cisco-sa-20070124-crafted-ip-option)

Crafted Packet Causes Reload on Cisco Routers

Crafted TCP Packet Can Cause Denial of Service

CUCM IM and Presence Service GNU Bash Environment Variable Handling Command Injection (CSCur05454) (Shellshock)

Data Leak with Cisco Express Forwarding Enabled - Cisco Systems

DLSw Vulnerability - Cisco Systems

DOCSIS Read-Write Community String Enabled in Non-DOCSIS Platforms

Firewall Services Module Crafted ICMP Message (cisco-sa-20090819-fwsm)

HTTP DoS Vulnerability in Cisco Wireless LAN Controllers

HTTP GET Vulnerability in AP1x00

ICMP Unreachable Vulnerability in Cisco 12000 Series Internet Router - Cisco Systems

Information Leakage Using IPv6 Routing Header in Cisco IOS and Cisco IOS XR - Cisco Systems

Information Leakage Using IPv6 Routing Header in Cisco IOS XR (cisco-sa-20070808-IOS-IPv6-leak)

IOS Heap-based Overflow Vulnerability in System Timers - Cisco Systems

IOS HTTP Authorization Vulnerability - Cisco Systems

IOS HTTP Server Command Injection Vulnerability

IOS Reload after Scanning Vulnerability - Cisco Systems

IOS Stack Group Bidding Protocol Crafted Packet DoS - Cisco Systems

IPv6 Crafted Packet Vulnerability

IPv6 Routing Header Vulnerability

Linksys BEFSX41 System Log Viewer Log\_Page\_Num Variable Overflow DoS

Linksys Multiple Vulnerabilities (OF, DoS, more)

Linksys Router Debug Credentials (Gemtek / gemtekswd)

Linksys Router Default Password

Linksys Router Default Password (admin)

Linksys WRT54G Empty GET Request Remote DoS

Malformed SNMP Message-Handling Vulnerabilities - Cisco Systems

Management Center for Cisco Security Agents Detection

Management Center for Cisco Security Agents Remote Code Execution (cisco-sa-20110216-csa)

Multiple Cisco IOS Session Initiation Protocol Denial of Service Vulnerabilities

Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks

Multiple Crafted IPv6 Packets Cause Reload

Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS - Cisco Systems

Multiple IOS IPS Vulnerabilities

Multiple Multicast Vulnerabilities in Cisco IOS Software - Cisco Systems

Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite - Cisco Systems

Multiple SSH Vulnerabilities - Cisco Systems

Multiple Vulnerabilities Found by PROTOS IPSec Test Suite - Cisco Systems

Multiple Vulnerabilities in Access Control List Implementation for Cisco 12000 Series Internet Router - Cisco Systems

Multiple Vulnerabilities in Cisco Content Security Management Appliance (cisco-sa-20130626-sma)

Multiple Vulnerabilities in Cisco Email Security Appliance (cisco-sa-20130626-esa)

Multiple Vulnerabilities in Cisco Firewall Services Module Software (cisco-sa-20130410-fwsm)

Multiple Vulnerabilities in Cisco Intrusion Prevention System Software (cisco-sa-20130717-ips)

Multiple Vulnerabilities in Cisco Intrusion Prevention System Software (cisco-sa-20140219-ips)

Multiple Vulnerabilities in Cisco IOS While Processing SSL Packets - Cisco Systems

Multiple Vulnerabilities in Cisco IOS XE Software for 1000 Series Aggregation Services Routers (cisco-sa-20130410-asr1000)

Multiple Vulnerabilities in Cisco IOS XE Software for 1000 Series Aggregation Services Routers (cisco-sa-20131030-asr1000)

Multiple Vulnerabilities in Cisco NX-OS-Based Products (cisco-sa-20130424-nxosmulti)

Multiple Vulnerabilities in Cisco Secure Access Control System (cisco-sa-20140115-csacs)

Multiple Vulnerabilities in Cisco Security Agent (cisco-sa-20100217-csa)

Multiple Vulnerabilities in Cisco Unified Computing System (cisco-sa-20130424-ucsmulti)

Multiple Vulnerabilities in Cisco Web Security Appliance (cisco-sa-20130626-wsa)

Multiple Vulnerabilities in Cisco Wireless LAN Controllers (cisco-sa-20090727-wlc)

Multiple Vulnerabilities in Cisco Wireless LAN Controllers (cisco-sa-20130123-wlc)

Multiple Vulnerabilities in Cisco Wireless LAN Controllers (cisco-sa-20140305-wlc)

Multiple Vulnerabilities in the IOS FTP Server

NTP Vulnerability - Cisco Systems

OSPF LSA Manipulation Vulnerability in Cisco ASA (cisco-sa-20130801-lsaospf)

OSPF LSA Manipulation Vulnerability in Cisco IOS (cisco-sa-20130801-lsaospf)

OSPF LSA Manipulation Vulnerability in Cisco IOS XE (cisco-sa-20130801-lsaospf)

OSPF LSA Manipulation Vulnerability in Cisco NX-OS (cisco-sa-20130801-lsaospf)

RADIUS Authentication Bypass (cisco-sa-20050629-aaa)

Scanning for SSH Can Cause a Crash - Cisco Systems

SIP Packets Reload IOS Devices with support for SIP

SNMP Version 3 Authentication Bypass Vulnerabilities (cisco-sa-20080610-snmpv3)

SNMP Version 3 Authentication Vulnerabilities (cisco-sa-20080610-snmpv3)

SNMP Version 3 Authentication Vulnerabilities (cisco-sa-20080610-snmpv3)

SSH Malformed Packet Vulnerabilities - Cisco Systems

SSLv3 Padding Oracle On Downgraded Legacy Encryption in Cisco ASA Software (cisco-sa-20141015-poodle) (POODLE)

TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products - Cisco Systems

TCP Vulnerabilities in Multiple IOS-Based Cisco Products

Unified SIP Phone 3905 Unauthorized Access

Unsupported Cisco MXP Series Device

Unsupported Cisco Operating System

Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager - Cisco Systems

Vulnerabilities in Cisco IOS Secure Shell Server - Cisco Systems

Vulnerabilities in H.323 Message Processing - Cisco Systems

Vulnerabilities in SNMP Message Processing - Cisco Systems

Vulnerabilities in the Internet Key Exchange Xauth Implementation - Cisco Systems

Vulnerability in Cisco IOS Embedded Call Processing Solutions - Cisco Systems

Vulnerability in Cisco IOS While Processing SSL Packet - Cisco Systems

Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720

Vulnerability In Crypto Library - Cisco Systems

# CGI abuses : XSS

3CX Phone System login.php Multiple Parameter XSS

Adobe ColdFusion 'cfadminUserId' XSS (APSB10-11)

Adobe ColdFusion <= 8.0.1 \_logintowizard.cfm XSS

Adobe ColdFusion login.cfm Query String XSS (APSB11-04)

Adobe Connect < 9.5.7 event\_registration.html Multiple Parameter XSS (APSB16-35)

Adobe Flex 3 History Management historyFrame.html XSS

Adobe Flex SDK Cross-Site Scripting (APSB11-25)

Adobe RoboHelp FlashHelp Unspecified XSS (APSB11-09) (uncredentialed check)

Adobe/Apache Flex ASDoc Tool XSS

Advanced Guestbook User-Agent Header HTML Injection

AgoraCart agora.cgi cart\_id Parameter XSS

Apache Hadoop Jetty XSS

Apache Jackrabbit 'q' Parameter XSS

Apache Jakarta Lucene results.jsp XSS

Apache Jetspeed Portal URI Path Reflected XSS

Apache JServ Nonexistent JSP Request XSS

Apache mod\_ssl Host: Header XSS

Apache MyFaces Tomahawk JSF Application autoscroll Multiple XSS

Apache OFBiz Webslinger Component XSS

Apache Roller q Parameter XSS

Apache Struts 2 s:a / s:url Tag href Element XSS

Apache Struts 2 struts2-rest-showcase orders 'clientName' Parameter Persistent XSS

Apache Struts 2 struts2-showcase edit-person.action Persistent XSS

Apache Struts struts-cookbook processSimple.do message Parameter XSS

Apache Struts struts-examples upload-submit.do 'theText' Parameter XSS

Apache Tomcat / Geronimo Sample Script cal2.jsp time Parameter XSS

Apache Tomcat /servlet Mapping XSS

Apache Tomcat 4.1 XSS

Apache Tomcat DOS Device Name XSS

Apache Tomcat Implicit Objects XSS

Apache Tomcat JSP2 Examples XSS

Apache Tomcat Sample App cal2.jsp 'time' Parameter XSS (CVE-2006-7196)

Apache Tomcat SendMailServlet sendmail.jsp 'mailfrom' Parameter XSS

Apache Tomcat snoop.jsp URI XSS

Apache Traffic Server Host HTTP XSS

ArGoSoft Mail Server Pro Webmail viewheaders Multiple Field XSS

ArGoSoft Mail Server Unspecified XSS

ASP Portal User Profile XSS

ASP-DEv XM Forum post.asp IMG Tag XSS

ASUS Routers flag Parameter XSS

Atlassian Confluence 2.x >= 2.7 / 3.x < 3.4.6 Multiple XSS

Atlassian Confluence 2.x >= 2.7 / 3.x < 3.4.9 Multiple XSS

Atlassian Confluence < 6.3.4 usermacros Reflected XSS (CVE-2017-18084)

Atlassian Confluence < 6.4.2 issuesURL Parameter Reflected XSS (CVE-2017-18086)

Atlassian Confluence < 6.6.1 viewdefaultdecorator Reflected XSS (CVE-2017-18085)

Atlassian Confluence VelocityServlet Error Page XSS

Atlassian FishEye Code Metrics Report Plugin XSS

Atlassian JIRA 4.2.x < 4.4 / 4.3.x < 4.4 Multiple XSS

Atlassian JIRA 4.2.x < 5.1.1 Multiple XSS

Atlassian JIRA 500page.jsp Referer XSS

Atlassian JIRA 500page.jsp XSS

Atlassian JIRA 7.7.x < 7.13.1 XSS vulnerability (JRASERVER-69238)

Atlassian JIRA < 3.13.3 DWR 'c0-id' XSS

Atlassian JIRA < 7.13.3 / 8.x < 8.1 XSS vulnerability (JRASERVER-68855)

Atlassian JIRA < 7.4.2 XSS vulnerability (JRASERVER-66624)

Atlassian JIRA ConfigurePortalPages.jspa XSS

Atlassian JIRA global-translations.jsp XSS (JRASERVER-61888)

Atmail Webmail 4.x < 4.6.1 (4.61) 'Global.pm' XSS

Atmail Webmail 6.6.x < 6.6.3 / 7.x < 7.0.3 File Name Parameter XSS

Atmail WebMail < 6.2.0 (6.20) 'MailType' Parameter XSS

Atmail Webmail < 6.5.0 'DOM processor' XSS

Atmail WebMail <= 5.6.0 (5.60) Email Body Injection

Atmail WebMail <= 5.6.1 (5.61) webadmin/admin.php Multiple Parameter XSS

ATutor 1.5.1 Multiple Script XSS

Auction Deluxe auction.pl Multiple Parameter XSS

AutoIndex PHP Script index.php search Parameter XSS

AXIGEN Webmail < 7.1.0 HTML Body Script Insertion

Axon Virtual PBX /logon Multiple Parameter XSS

Aztek Forum Multiple Script XSS

Bandmin 1.4 index.cgi Multiple Parameter XSS

Barracuda Spam Firewall cgi-bin/ldap\_test.cgi email Parameter XSS

BASE < 1.4.4 base\_local\_rules.php dir Parameter XSS

BasiliX Message Content XSS

BasiliX Webmail Content-Type Header XSS

Basit CMS Multiple Script XSS

BEA Plumtree portal/server.pt name Parameter XSS

Better WP Security Plugin for WordPress Multiple XSS

BiTBOARD IMG BBCode Tag XSS

BlackBerry Enterprise Server MDS Connection Service XSS

BlackBerry Enterprise Service (BES) Management Console 12.x < 12.4.1 Multiple XSS

Blackboard Learning System <= 8.0 SP6 Unspecified XSS

BMForum Multiple Script XSS

BookReview 1.0 Multiple Script XSS

BreakCalendar < 1.3 XSS

Bugzilla Internal Error Response XSS

Bugzilla show\_bug.cgi id Parameter XSS

BuildBot WebStatus waterfall 'branch' Parameter XSS

Cacti < 0.8.7g Multiple XSS and HTML Injection Vulnerabilities

CC GuestBook cc\_guestbook.pl Multiple Parameter XSS

Ceilidh testcgi.exe query Parameter XSS

Cerb Multiple Vulnerabilities

cformsII Plugin for WordPress 'rs' Parameter XSS

CGI Generic HTML Injections (quick test)

CGI Generic Script Injection (quick test)

CGI Generic XSS (comprehensive test)

CGI Generic XSS (extended patterns)

CGI Generic XSS (HTTP Headers)

CGI Generic XSS (Parameters Names)

CGI Generic XSS (persistent)

CGI Generic XSS (persistent, 2nd pass)

CGI Generic XSS (persistent, 3rd Pass)

CGI Generic XSS (quick test)

CGIWrap Charset Specification Weakness Error Message XSS

Check\_MK < 1.4.0p6 webapi.py XSS

Check\_MK Internal Server Error XSS

Cherokee Web Server Error Page XSS

Cisco Prime LAN Management Solution Cross-Frame Scripting

Cisco Prime Network / Wireless Control System Health Monitor Reflected XSS

Cisco Secure Access Control Server (ACS) CSUserCGI.exe Help Facility XSS

CiscoWorks Server Common Services Login Page XSS

Citrix AGEE Logon Portal Unspecified XSS

Citrix MetaFrame XP login.asp NFuse\_Message Parameter XSS

Citrix NFuse Launch Scripts 'NFuse\_Application' Parameter XSS

CjOverkill trade.php Multiple Method XSS

CKEditor 4.5.11 < 4.9.2 Enhanced Image Plugin XSS

CKEditor Preview Plugin Unspecified XSS

CKEditor sample\_posteddata.php XSS

ClarkConnect proxy.php url Parameter XSS

Claroline add\_course.php Multiple Parameter XSS

CMSimple Guestbook Module index.php XSS

CMSimple index.php search Function XSS

ColdFusion MX Null Byte Tag XSS Protection Bypass

ColdFusion Web Server User-Agent HTTP Header Error Message XSS

Comersus Cart Account Username Field XSS

Comersus Cart comersus\_searchItem.asp curPage Parameter XSS

CommuniGate Pro WebMail < 5.2.15 XSS

CommuniGate Pro WebMail w/ MSIE STYLE Tag XSS

Coppermine Photo Gallery EXIF Data XSS

Coppermine Photo Gallery init.inc.php X-Forwarded-For XSS

CoSoSys Endpoint Protector < 4.4.0.1 Unspecified XSS

cPanel cpsrvd.pl user Parameter XSS

CPG Dragonfly Multiple XSS

Crystal Reports Server InfoView logonAction Parameter XSS

CubeCart < 3.0.4 Multiple Script XSS

CuteNews 1.4.5 Multiple Script XSS

CuteNews <= 1.3.6 Multiple XSS

CuteNews index.php mod Parameter XSS

CuteNews show\_archives.php archive Parameter XSS

CVSTrac < 1.1.5 Multiple XSS

Dada Mail Archived Message XSS

daloRADIUS login.php error Parameter XSS

DasBlog Activity / Event Viewer Multiple HTTP Header XSS

DCP-Portal Multiple Script XSS

Dell iDRAC6 / iDRAC7 Login Page 'ErrorMsg' Parameter XSS

Dell OpenManage Server Administrator index\_main.htm DOM-based XSS

Dell OpenManage Server Administrator omalogin.html DOM-based XSS

Django Administration Application Login Form XSS

DNN (DotNetNuke) 7.0.x < 7.0.6 Unspecified Modal Window XSS

DNN (DotNetNuke) < 3.0.12 Multiple XSS

DNN (DotNetNuke) < 5.2.0 SearchResults.aspx XSS

DNN (DotNetNuke) < 5.3.0 SearchResults.aspx XSS

DNN (DotNetNuke) < 7.2.2 Unspecified XSS

DNN (DotNetNuke) < 7.4.0 Unspecified Persistent XSS

DNN (DotNetNuke) < 7.4.2 Multiple Vulnerabilities

DNN (DotNetNuke) \_\_dnnVariable Parameter XSS

DNN (DotNetNuke) ErrorPage.aspx XSS

DNN (DotNetNuke) Language Flag Selector Culture XSS

Dolibarr 3.1.0 admin/company.php username Parameter XSS

Dolibarr Multiple Script URI XSS

dotCMS search-results.dot search\_query Parameter XSS

Drupal 7.x < 7.65 / 8.5.x < 8.5.14 / 8.6.x < 8.6.13 XSS (SA-CORE-2019-004)

Drupal Google Site Search Module API Data Handling XSS

e107 content\_preset.php URI XSS

e107 submitnews.php XSS

eGroupWare <= 1.0.00.003 Multiple Module XSS

Ektron CMS400.NET 'workarea/reterror.aspx' info Parameter XSS

Ektron CMS400.NET id Parameter XSS

Elgg index.php view Parameter XSS

EMC RSA Authentication Manager 7.x < 7.1 SP4 Patch 32 Unspecified XSS

EMC RSA Authentication Manager < 8.2 SP1 Patch 1 Token Profile Name Stored XSS (ESA-2017-068)

ESET Remote Administrator < 3.0.105 Additional Report Settings XSS

ExBB Netsted BBcode XSS

eZ Publish articleview.php XSS

ez Publish Multiple XSS

F5 BIG-IP Web Management Multiple XSS

FancyBox Plugin for WordPress 'mfbfw' Parameter Persistent XSS

Faq-O-Matic fom.cgi Multiple Parameter XSS

FastCGI Multiple Sample CGI XSS

FeedList Plugin for WordPress 'i' Parameter XSS

FireStats window-add-excluded-ip.php 'edit' parameter XSS

Fortinet FortiADC Model D < 4.2 Theme Login Page XSS

Fortinet FortiAnalyzer / FortiManager < 5.0.7 Multiple Unspecified XSS (FG-IR-14-033)

Fortinet FortiAnalyzer FortiOS 5.0.x < 5.0.11 / 5.2.x < 5.2.2 Dataset Reports XSS

Fortinet FortiAuthenticator 'operation' Parameter XSS

Fortinet FortiMail < 4.3.4 / 5.0.0 Multiple XSS

Fortinet FortiMail < 4.3.9 / 5.0.8 / 5.1.5 / 5.2.3 XSS

Fortinet FortiManager FortiOS 5.0.x >= 5.0.3 and < 5.0.11 Dataset Reports XSS

Fortinet FortiWeb 5.1.2 < 5.3.5 Autolearn Configuration Multiple XSS

Fortinet FortiWeb 5.x < 5.0.4 XSS

Fortinet FortiWeb 5.x < 5.1.0 XSS

Fortinet FortiWeb 5.x < 5.2.1 Multiple XSS Vulnerabilities

Fusebox index.cfm fuseaction Parameter XSS

FuseTalk categories.aspx FTVAR\_SORTORDER Parameter XSS

FuseTalk Forum img src Tag XSS

FuseTalk Multiple Script XSS

FuseTalk usersearchresults.cfm keyword Parameter XSS

Gallery 3.0.x < 3.0.8 Multiple XSS

Gallery Bank Plugin for WordPress < 2.0.20 XSS

Gallery EXIF Data XSS

Gallery login.php username Parameter XSS

Gallery search.php searchstring Parameter XSS

GForge <= 4.5 Multiple Script XSS

GForge account/verify.php confirm\_hash Parameter XSS

GForge help/tracker.php helpname Parameter XSS

Git gitweb Multiple Parameter XSS

Google Calendar Events Plugin for WordPress 'admin-ajax.php' XSS

Google Mini Search Appliance search Script ie Parameter XSS

Gossamer Threads Links < 3.0.4 Multiple Script XSS

Gossamer Threads Links user.cgi url Parameter XSS

Greymatter Comment Name Field Control Panel Log XSS

Guppy Multiple HTTP Header XSS

Gurock TestRail < 3.1.3 XSS

Horde < 3.0.1 Multiple Script XSS

Horde < 3.0.11 / 3.1.2 Multiple Script XSS

Horde Application Framework Help Window Multiple Parameter XSS

Horde Chora common-footer.inc Page Title XSS

Horde IMP HTML MIME Viewer Multiple XSS

Horde IMP IMP\_MIME\_Viewer\_html Class XSS

Horde IMP js/compose-dimp.js XSS

Horde IMP status.php3 script Parameter XSS

Horde IMP with MSIE MIME Viewer Email Message XSS

Horde Kronolith js/kronolith.js Multiple View XSS

Horde Mnemo common-footer.inc Parent Frame Page XSS

Horde Nag common-footer.inc Parent Frame Page Title XSS

Horde NLS.php Language Selection new\_lang Parameter XSS

Horde Parent Frame Page Title XSS

Horde Turba common-footer.inc Parent Frame Page Title XSS

Horde Turba Contact Manager common-footer.inc Parent Frame Page Title XSS

Horde util/icon\_browser.php subdir Parameter XSS

HP Autonomy Ultraseek 5 Unspecified XSS

HP LaserJet XSS Vulnerability

HP Managed Printing Administration < 2.7.0 XSS

HP OpenView Performance Insight sendEmail.jsp XSS

HP SiteScope XSS

HP System Management Homepage < 2.1.12 Unspecified XSS

HP System Management Homepage < 2.1.15.210 Unspecified XSS

HP System Management Homepage < 2.1.2 Unspecified XSS

ht://dig htsearch sort Parameter XSS

ht://Dig htsearch.cgi config Parameter XSS

ht://Dig htsearch.cgi words Parameter XSS

IBM Domino nsf File Argument XSS

IBM Lotus Notes/Domino Square Brackets Encoding Failure XSS

IBM Lotus Sametime Server stconf.nsf messageString Parameter XSS

IBM Multiple Products login.php Query String XSS

IBM Rational ClearQuest Multiple XSS Flaws

IBM Rational License Key Server Administration and Reporting Tool 8.1.4.x < 8.1.4.7 XSS

IBM Rational RequisitePro ReqWebHelp Multiple XSS

IBM Tivoli Directory Server Web Administration Tool Unspecified XSS

IBM WebSphere Application Server SOAP Connector Error Page XSS

IBM WebSphere Portal 'boot\_config.jsp' XSS (PI16041)

IBM WebSphere Portal 'FilterForm.jsp' XSS (PI15690)

IBM WebSphere Portal 7.0.0.x < 7.0.0.2 CF30 Unspecified XSS (PI80564)

IBM WebSphere Portal 8.0.0.1 CF11 Multiple XSS

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF22 Unspecified XSS (PI80564)

IBM WebSphere Portal 8.5.0.x < 8.5.0.0 CF15 Unspecified XSS (PI92039)

IBM WebSphere Portal 9.0.0.x < 9.0.0.0 CF15 Unspecified XSS (PI92039)

IBM WebSphere Portal Reflected XSS Vulnerability

IBM WebSphere Portal Tagging Reflected XSS (PM96047)

IBM WebSphere Portal Themes Unspecified XSS (PM90118)

IBM WebSphere Portal Unspecified JSP XSS (PI16040)

IBM WebSphere Portal Unspecified Reflected XSS

IBM WebSphere Portal Unspecified XSS (PI16127)

IBM WebSphere Portal Unspecified XSS (PI16174)

IBM WebSphere Portal Unspecified XSS (PI18845)

IBM WebSphere Portal Web Content Viewer Portlet XSS (PM84525)

IBM WebSphere Portal XSS (swg22008028)

IBM WebSphere Portal XSS Vulnerability

IBM WebSphere Portal XSS Vulnerability

IBM WebSphere Portal XSS Vulnerability (CVE-2018-1444)

IBM WebSphere Portal XSS Vulnerability (CVE-2018-1445)

IBM WebSphere Portal XSS Vulnerability (CVE-2018-1483)

IBM WebSphere Portal XSS Vulnerability (CVE-2018-1660)

IBM WebSphere Portal XSS Vulnerability (CVE-2018-1673)

IBM WebSphere Portal XSS Vulnerability (CVE-2018-1820)

IBM WebSphere Traversal Error Page XSS

Icecast list.cgi User-Agent XSS

IceWarp install/index.html lang Parameter XSS

IceWarp Mail Server admin/index.html message Parameter XSS

IceWarp Merak Mail Server < 9.0.0 BODY Element XSS

IceWarp Merak Mail Server < 9.4.0 IMG Tag XSS

IlohaMail Email Header XSS

IlohaMail read\_message.php Attachment Multiple Field XSS

IlohaMail user Parameter XSS

IMP common-footer.inc Parent Frame Page Title XSS

IMP Content-Type Header XSS

Incapsula Component for Joomla! 'token' Parameter Multiple XSS

InMail/InShop inmail.pl / inshop.pl XSS

Invision Power Board COLOR SML Tag XSS

Invision Power Board HTTP POST Request IFRAME Tag XSS

Invision Power Board index.php Multiple Parameter XSS

Invision Power Board index.php pop Parameter XSS

Invision Power Board Referer field XSS

JAWS Glossary Gadget Multiple XSS

jCart 1.1 my-item-name POST Parameter XSS

Jetty CookieDump.java Sample Application Persistent XSS

JForum jforum.page start Parameter XSS

Joomla! 'lang' Parameter XSS

Joomla! 2.5.x < 2.5.16 / 3.x < 3.1.6 Multiple XSS

Joomla! 2.5.x < 2.5.7 Multiple XSS

Joomla! 3.4.x < 3.4.4 Login Module XSS

Joomla! < 1.5.11 JA\_Purity Template Multiple XSS

Joomla! com\_content Component 'order' Parameter XSS

JQuery 1.6.x < 1.6.3 XSS

JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS

JQuery < 1.9.0 XSS

JQuery < 3.0.0 XSS

Juniper Junos EmbedThis AppWeb error Parameter XSS

Juniper ScreenOS < 5.4.0r10 / 6.0 < 6.0.0r6 / 6.1 < 6.1.0r2 Web Interface and Telnet Login Pages XSS (JSA10388)

Kayako eSupport index.php nav Parameter XSS

Kayako eSupport Troubleshooter Module index.php Multiple Parameter XSS

Keene Digital Media Server Multiple Script XSS

Kerio MailServer < 6.6.2 Multiple XSS (KSEC-2008-12-16-01)

Kerio MailServer < 6.6.2 Patch 3 / 6.7.0 Patch 1 XSS (KSEC-2009-06-08-01)

LedNews News Post XSS

Liferay Portal 6.2.0 CE GA1 Multiple XSS

Liferay Portal upload\_progress\_poller.jsp XSS

LiveZilla < 5.3.0.8 XSS

LogAnalyzer < 3.6.6 index.php / detail.php 'hostname' Parameter XSS

LogAnalyzer asktheoracle.php 'query' Parameter XSS

LogAnalyzer index.php 'filter' Parameter XSS

LogAnalyzer index.php 'highlight' Parameter XSS

LogAnalyzer userchange.php 'viewid' Parameter XSS

Lotus Domino Multiple Script Src / BaseTarget XSS

Lyris ListManager Multiple XSS

Lyris ListManager read/search/results words Parameter XSS

MailEnable ForgottenPassword.aspx Username Parameter XSS

Mailman < 2.1.14 Multiple XSS

MailMarshal Spam Quarantine Management (SQM) Multiple Component XSS

Mailreader network.cgi enriched/richtext MIME Message XSS

Mambo Site Server 4.0.10 XSS

Mambo Site Server itemid Parameter XSS

Mambo Site Server mos\_change\_template XSS

Mambo task Parameter XSS

ManageEngine ADAudit Plus 'reportList' Parameter XSS

ManageEngine ADManager Plus 'computerName' Parameter XSS

ManageEngine ADSelfService EmployeeSearch.cc Multiple XSS

ManageEngine ADSelfService Plus < 5.3 Build 5313 PasswordSelfServiceAPI XSS

ManageEngine AssetExplorer < 5.6.0 Build 5614 XML Asset Data XSS

ManageEngine AssetExplorer < 6.1.0 Build 6113 Multiple XSS

ManageEngine EventLog Analyzer 'j\_username' XSS

ManageEngine Firewall Analyzer Multiple XSS

ManageEngine OpManager Login.do Multiple Parameter XSS

ManageEngine OpStor availability730.do days Parameter XSS

ManageEngine ServiceDesk Plus 8.0.0 < Build 8015 Multiple XSS Vulnerabilities

ManageEngine SupportCenter Plus HomePage.do fromCustomer Parameter XSS

Mantis < 0.18.1 Multiple Unspecified XSS

MantisBT 1.2.x < 1.2.14 adm\_config\_report.php Multiple Parameter XSS

MantisBT nusoap/nusoap.php NuSOAP WSDL XSS

MantisBT search.php match\_type Parameter XSS

McAfee Email Gateway 7.6.x < 7.6.404 Blocked Email Alert XSS (SB10153)

McAfee ePolicy Orchestrator 5.1.x < 5.1.3 HF1110787 Computer Management Services XSS (SB10184)

McAfee ePolicy Orchestrator < 4.6.7 Multiple XSS

McAfee Vulnerability Manager cert\_cn Parameter XSS

McAfee Web Gateway < 7.1.0.5 / 7.1.5.2 XSS

McAfee WebShield UI Dashboard XSS (SB10026)

McAfee WebShield UI ProcessTextFile bodyStyle Parameter XSS (SB10020)

MDaemon WorldClient < 10.0.2 Email Handling XSS

MDaemon WorldClient < 12.0.3 Summary Page Email Subject XSS

MDaemon WorldClient < 12.5.7 Multiple XSS Vulnerabilities

MediaWiki 1.4.x < 1.4.6 / 1.5.x < 1.5.0 beta3 Page Move Template XSS

MediaWiki < 1.19.16 / 1.21.10 / 1.22.7 'Special:PasswordReset' XSS

MediaWiki < 1.19.19 / 1.22.11 / 1.23.4 SVG Upload and CSS XSS

MediaWiki < 1.19.20 / 1.22.12 / 1.23.5 'includes/OutputPage.php' XSS

MediaWiki < 1.21.9 / 1.22.6 'InfoAction.php' XSS

MediaWiki < 1.3.13 / 1.4.5 / 1.5.0 alpha2 Page Template Inclusions HTML Attributes XSS

MediaWiki API XSS

MediaWiki Backslash Escaped CSS Comments XSS

MediaWiki CSS Comments XSS

MediaWiki index.php 'uselang' Parameter XSS

MediaWiki profileinfo.php 'filter' Parameter XSS

Microsoft IIS 5.0 Form\_JScript.asp XSS

Microsoft IIS ASP Redirection Function XSS

Microsoft IIS IDC Extension XSS

Microsoft IIS shtml.dll XSS

Microsoft SharePoint Services Help.aspx 'cid0' Parameter XSS

miniBB bb\_func\_usernfo.php Website Name Field XSS

MODx < 2.0.3-pl modahsh Parameter XSS

MODx login.php 'username' Parameter XSS

MODx SearchHighlight plugin XSS

MoinMoin PageEditor.py template Parameter XSS

MoinMoin rsslink() Function page\_name Parameter XSS

MoniWiki < 1.0.9 wiki.php XSS

Mono ASP.NET action Attribute XSS

Moodle 'external.php' 'badge' Parameter XSS

Moodle 'PHPCOVERAGE\_HOME' Parameter XSS

Moodle 'post.php' 'reply' Parameter XSS

Moodle < 1.3.3 'help.php' 'file' Parameter XSS

Moodle MSA-11-0007 'coursetags\_more.php' XSS

Moodle Multiple XSS

Mort Bay Jetty Dump Servlet (webapps/test/jsp/dump.jsp) XSS

Mort Bay Jetty Multiple XSS

Movable Type mt-comments.cgi static Parameter XSS

Movable Type mt-wizard.cgi set\_static\_uri\_to Parameter XSS

MS Site Server < 3.0 formslogin.asp url Parameter XSS

MS10-072: Vulnerabilities in SafeHTML Could Allow Information Disclosure (2412048) (remote check)

MS11-061: Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250) (uncredentialed check)

MS15-087: Vulnerability in UDDI Services Could Allow Elevation of Privilege (3082459) (uncredentialed check)

Mura CMS link Parameter XSS

mvnForum activatemember Multiple Parameter XSS

mvnForum Search Parameter XSS

MyAbraCadaWeb header.php ma\_kw Parameter XSS

MyBB < 1.6.15 Video MyCode XSS

MyBB xmlhttp.php 'value' Parameter XSS

MySQL Eventum forgot\_password.php XSS

MySQL Eventum index.php email Parameter XSS

Nagios XI < 2009R1.3B Multiple Unspecified XSS

Nagios XI < 2009R1.3C grab\_request\_var() Multiple XSS

Nagios XI < 2011R1.9 login.php XSS

Nagios XI < 2011R3.0 Multiple XSS Vulnerabilities

NeoMail neomail.pl sort Parameter XSS

Neoteris IVE swsrv.cgi XSS

Nessus Web Server XSS

Nessus Web UI Scanned Content Stored XSS

NetScaler Web Management ws/generic\_api\_call.pl standalone Parameter XSS

Novell GroupWise 6.5.3 WebAccess Multiple XSS

Novell GroupWise < 7.03HP2 / 8.0HP1 WebAccess Multiple XSS

Novell GroupWise WebAccess Email IMG SRC XSS

Novell GroupWise WebAccess Login Page User.lang Parameter XSS

Novell GroupWise WebAccess User.interface XSS

Novell Identity Manager Roles Based Provisioning Module taskId XSS

Novell ZENworks Configuration Console Login.jsp language Parameter XSS

Ocean12 Guestbook XSS

Open WebMail Multiple Content Header XSS

Open WebMail openwebmail.pl logindomain Parameter XSS

Open WebMail sessionid Parameter XSS

OpenAdmin Tool for Informix informixserver Parameter XSS

OpenBB board.php FID Parameter XSS

OpenCA Client System Browser Form Input Field XSS

Openfire Admin Console login.jsp XSS

Oracle 9i Application Server HTTP Request Smuggling

Oracle 9iAS iSQLplus XSS

Oracle 9iAS mod\_plsql Multiple Procedures XSS

Oracle BPM Process Administrator tips.jsp context Parameter XSS

Oracle Containers for J2EE Component Unspecified XSS

Oracle Database Secure Enterprise Search search/query/search search\_p\_groups Parameter XSS

Oracle Fusion WebLogic Server Component WLS-Console Management Interface Unspecified XSS

Oracle Secure Backup Administration Server login.php XSS

Oracle WebCenter Content Help Component XSS

Oracle WebCenter Content idc/idcplg Multiple Parameter XSS

Orion Application Server Web Examples Multiple XSS

osCommerce 2.2ms1 Multiple Script XSS

osCommerce application\_top.php Multiple Parameter HTTP Response Splitting

osCommerce contact\_us.php enquiry Parameter XSS

OSSIM Framework session/login.php dest Parameter XSS

paBox pabox.php posticon Parameter XSS

paFileDB pafiledb.php id Parameter XSS

paNews comment.php showpost Parameter XSS

PeopleSoft PeopleTools JMS Listening Connector Activity Parameter XSS

pfSense 2.3.x < 2.3.5 / 2.4.x < 2.4.2 Multiple XSS Vulnerabilites (SA-17\_08 / SA-17\_09)

pfSense < 2.2 Multiple XSS Vulnerabilities (SA-15\_01)

Phorum 5.2.x < 5.2.17 'control.php' 'real\_name' XSS

Phorum < 5.0.15 Multiple XSS

Phorum register.php Username Field XSS

Phorum search.php subject Parameter XSS

PhotoPost PHP Pro EXIF Data XSS

PHP < 4.4.2 Multiple XSS Vulnerabilities

PHP Code Snippet Library index.php Multiple Parameter XSS

PHP-Fusion < 6.00.108 BBCode Nested URL Tag XSS

PHP-Fusion BBCode IMG Tag XSS

PHP-Fusion forum/viewthread.php highlight Parameter XSS

PHP-Fusion homepage address Parameter XSS

PHP-Nuke PhotoADay Module pad\_selected Parameter XSS

phpBB < 2.0.10 Multiple XSS

phpBB < 2.0.7 Multiple XSS

phpBB2 Plus <= 1.52 Multiple XSS

phpCMS parser.php file Parameter XSS

phpGraphy EXIF Data XSS

phpGroupWare index.php Calendar Date XSS

phpGroupWare Main Screen Message Body XSS

phpGroupWare Wiki Module XSS

phpLDAPadmin lib/QueryRender.php base Parameter XSS

phpMyAdmin 3.3.x / 3.4.x < 3.3.10.4 / 3.4.4 XSS (PMASA-2011-13

phpMyAdmin 3.4.x < 3.4.10.1 XSS (PMASA-2012-1)

phpMyAdmin 3.4.x < 3.4.11.1 / 3.5.x < 3.5.2.2 Multiple XSS (PMASA-2012-4)

phpMyAdmin 3.4.x < 3.4.5 XSS (PMASA-2011-14)

phpMyAdmin 3.4.x < 3.4.6 XSS (PMASA-2011-16)

phpMyAdmin 3.4.x < 3.4.8 XSS (PMASA-2011-18)

phpMyAdmin 3.4.x < 3.4.9 XSS (PMASA-2011-19 - PMASA-2011-20)

phpMyAdmin 3.5.x < 3.5.3 Multiple Vulnerabilities (PMASA-2012-6 - PMASA-2012-7)

phpMyAdmin 3.5.x < 3.5.8 tbl\_gis\_visualization.php Multiple XSS

phpMyAdmin 3.x >= 3.3.1 / 4.x < 4.1.7 import.php XSS (PMASA-2014-1)

phpMyAdmin 4.0.x < 4.0.10.2 / 4.1.x < 4.1.14.3 / 4.2.x < 4.2.7.1 Multiple XSS Vulnerabilities (PMASA-2014-8 - PMASA-2014-9)

phpMyAdmin 4.0.x < 4.0.10.4 / 4.1.x < 4.1.14.5 / 4.2.x < 4.2.9.1 'ENUM' Value XSS (PMASA-2014-11)

phpMyAdmin 4.0.x < 4.0.10.5 / 4.1.x < 4.1.14.6 / 4.2.x < 4.2.10.1 Multiple XSS (PMASA-2014-12)

phpMyAdmin 4.1.x < 4.1.14.1 / 4.2.x < 4.2.4 Navigation Hiding Items Multiple XSS (PMASA-2014-3)

phpMyAdmin 4.2.x < 4.2.4 Recent/Favorite Table Navigation Multiple XSS (PMASA-2014-2)

phpMyAdmin 4.x < 4.0.3 XSS (PMASA-2013-6)

phpMyAdmin < 2.6.0-pl3 Multiple XSS

phpMyAdmin < 2.6.1 pl2 Libraries and Themes Multiple XSS

phpMyAdmin < 2.6.4 Multiple XSS

phpMyAdmin < 4.8.3 Vulnerability (PMASA-2018-5)

phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

phpMyAdmin index.php convcharset Parameter XSS

phpMyAdmin Replication Setup js/replication.js Database Name XSS

phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

phpMyDirectory review.php subcat Parameter XSS

phpScheduleIt 1.0.0 RC1 Multiple XSS

PHPSysInfo < 2.5 Multiple Script XSS

Pinnacle Cart index.php pg Parameter XSS

Pinnacle ShowCenter SettingsBase.php Skin Parameter XSS

Piwik < 2.16.0 Unspecified XSS

Plesk Reloaded login\_up.php3 login\_name Parameter XSS

Pligg register.php reg\_username Parameter XSS

Pligg search.php search Parameter XSS

pLog register.php Multiple Parameter XSS

Plone spamProtect mailaddress Parameter XSS

pod.board 1.1 Multiple Script XSS

PostNuke < 0.7.2.3 Multiple Script XSS

PostNuke < 0.760 RC4 Multiple Script XSS

PostNuke News Module article.php sid Parameter XSS

PostNuke Reviews Module title Parameter XSS

Poweradmin index.php XSS

PowerPortal modules/private\_messages/index.php Multiple Parameter XSS

Pretty Link Plugin for WordPress 'pretty-bar.php' 'url' Parameter XSS

ProfitCode PayProCart usrdetails.php sgnuptype Parameter XSS

Project Woodstock 404 Error Page UTF-7 Encoded XSS

ProjectPier index.php Multiple Parameter XSS

PRTG Network Monitor login.htm errormsg Parameter XSS

PRTG Traffic Grapher login.htm url Parameter XSS

PsNews index.php Multiple Parameter XSS

Pubcookie Login Server index.cgi XSS

PunBB < 1.1.2 install.php XSS

PunBB IMG Tag Client Side Scripting XSS

PunBB profile.php Multiple Parameter XSS

PunBB profile.php XSS

PunBB URL Quote Tag XSS

Puppet Dashboard Multiple XSS Vulnerabilities

Puppet Enterprise Multiple XSS Vulnerabilities

PwsPHP profil.php id Parameter XSS

QNAP Photo Station < 5.7.0 Cross-Site Scripting Vulnerability

Resin resin-admin/digest.php XSS

Resin viewfile Servlet file Parameter XSS

Riverbed SteelApp (Stingray) Traffic Manager < 9.7 Multiple XSS

RM SafetyNet Plus snpfiltered.pl u Parameter XSS

RomPager HTTP Referer Header XSS

RSA ClearTrust ct\_logon.asp Multiple Parameter XSS

RSA Security RSA Authentication Agent For Web For IIS XSS

Sambar Server Administrative Interface Multiple XSS

Sambar Server Multiple Script XSS

SandSurfer < 1.7.1 XSS

SAP BusinessObjects viewError.jsp 'error' Parameter XSS

SAP DB / MaxDB WebDBM Multiple Parameter XSS

SAP Internet Transaction Server wgate Multiple Parameter XSS

Sawmill < 7.1.14 GET Request Query String XSS

Scrutinizer < 9.5.2 exporters.php XSS

Securimage example\_form.php XSS

SecurityCenter devform.php message Parameter XSS

Serendipity BBCode Plugin XSS

Serendipity compat.php searchTerm Parameter XSS

SGDynamo sgdynamo.exe HTNAME XSS

Sharebar Plugin for WordPress 'sharebar-admin.php' 'status' Parameter XSS

SHOUTcast Server Admin Log File XSS

SilverStripe Forums Module 'Search' Parameter XSS

Simple File Manager Directory / Filename XSS

SimpleSAMLphp logout.php link\_href Parameter XSS

Sitecore CMS 'default.aspx' XSS

Siteframe search.php searchfor Parameter XSS

Siteman forum.php page Parameter XSS

SiteMinder 5.5 Multiple Script XSS

Skull-Splitter Guestbook Multiple Field XSS

Slideshow Plugin for WordPress 'settings.php' Multiple Parameter XSS

SmarterMail Subject Field XSS

SmarterTools SmarterMail Attachment Upload XSS

Snitz Forums 2000 post.asp type Parameter XSS

SonicWALL SOHO Web Interface XSS

Sophos Web Appliance < 4.3.0 FTP Redirect Page Reflected XSS

Sophos Web Appliance < 4.3.2 FTP Redirect Page Reflected XSS

Sophos Web Protection Appliance end-user-/errdoc.php 'msg' Parameter XSS

sphpblog search.php q Parameter XSS

Splunk '/en-US/app/' Referer Header XSS

Splunk 4.x < 4.1.3 404 Response XSS

Splunk < 5.0.6 Unspecified XSS

Splunk < 5.0.8 Unspecified XSS

Splunk Enterprise 6.0.x < 6.0.15, 6.1.x < 6.1.14, 6.2.x < 6.2.14, 6.3.x < 6.3.12, 6.4.x < 6.4.9, 6.5.x < 6.5.5 or Splunk Light < 6.6.0 Persistent XSS

Splunk Enterprise 6.2.x < 6.2.6 / Splunk Light 6.2.x < 6.2.6 Splunk Web XSS

Splunk Enterprise 6.6.x < 6.6.3 / Splunk Light 6.6.x < 6.6.3 Multiple XSS

SquidClamav clwarn.cgi url Parameter XSS

SquirrelMail 1.2.9 / 1.2.10 read\_body.php Multiple Parameter XSS

SquirrelMail < 1.2.11 Multiple Script XSS

SquirrelMail contrib/decrypt\_headers.php XSS

SqWebMail redirect Parameter CRLF Injected XSS

Sun Java System Calendar Server login.wcap Fmt-out Parameter XSS

Sun Java System Identity Manager Multiple XSS

Sun Java System Web Server Search Module XSS

Sun Java Web Console helpwindow.jsp / masthead.jsp Multiple XSS

Sun Secure Global Desktop / Tarantella < 4.20.983 Multiple XSS

SunShop Shopping Cart index.php search Parameter XSS

SurgeMail <= 3.0c2 Multiple XSS

SurgeMail surgeweb XSS

Symantec Data Center Security Server 'SSO-Error.jsp' XSS (SYM15-001)

Symantec Data Center Security Server 'WCUnsupportedClass.jsp' XSS

Symantec Endpoint Protection Manager TestConnection.jsp 'Msg' Parameter XSS (SYM11-009 & SYM12-001)

Symantec Messaging Gateway 10.x < 10.5.2 Management Console XSS (SYM14-006)

Symantec SecurityExpressions Audit and Compliance Server Multiple XSS

Symantec Web Gateway timer.php XSS (SYM12-006)

Sympa New List Creation Description Field XSS

Symphony Password Retrieval Script XSS

Synology DiskStation Manager < 4.3-3776 Update 3 info.cgi Multiple Parameters XSS

TaskFreak! logout.php tznMessage Parameter XSS

TeeKai Tracking Online XSS

Tenable Nessus 6.8.x and 6.9.x < 6.9.1 Stored XSS (TNS-2016-17)

Tenable Nessus 6.x < 6.9 Multiple Vulnerabilities (TNS-2016-16) (SWEET32)

Tenable Nessus 6.x < 6.9.3 Multiple Stored XSS

Tenable Nessus < 6.5.5 Host Details Scan Results XSS

TestLink login.php req Parameter XSS

TikiWiki 'tiki-edit\_wiki\_section.php' type Parameter XSS

TikiWiki tiki-error.php XSS

TinyBrowser Multiple XSS

TIPS MailPost append Parameter XSS

TMaxSoft JEUS url.jsp URI XSS

Tomcat Sample App cal2.jsp 'time' Parameter XSS

Tomcat Sample App hello.jsp 'test' Parameter XSS

Traffic Analyzer Plugin for WordPress 'ta\_loaded.js.php' 'aoid' Parameter XSS

Twitter Feed for WordPress Plugin 'url' Parameter XSS

UBB.threads < 6.5.1 Multiple XSS

UBB.threads ubbthreads.php debug Parameter XSS

Ultimate PHP Board 1.9.6 GOLD Multiple Scripts XSS (1)

Ultimate PHP Board 1.9.6 GOLD Multiple Scripts XSS (2)

UseModWiki wiki.pl XSS

Usermin < 1.600 Multiple Vulnerabilities

vBulletin BB Tag XSS

vBulletin memberlist.php what Parameter XSS

vBulletin newreply.php WYSIWYG\_HTML Parameter XSS

vBulletin search.php query Parameter XSS

Verity Ultraseek Search Request XSS

vHost < 3.10r1 Unspecified XSS

ViewCVS viewcvs.cgi Multiple Parameter XSS

ViewVC Invalid Parameter Arbitrary HTML Injection

ViewVC viewvc.cgi search Parameter XSS

VLC Web Interface XML Services XSS

VMware ESX WebAccess Context Data XSS (VMSA-2010-0005)

VMware vCenter Server 5.0.x < 5.0u3g / 5.1.x < 5.1u3d / 5.5.x < 5.5u2d Reflected XSS (VMSA-2016-0009)

VMware vCenter Update Manager XSS

VMware vRealize Automation 6.x < 6.2.4 Unspecified Stored XSS (VMSA-2016-0003)

VMware vRealize Automation 7.0.x / 7.1.x / 7.2.x / 7.3.x < 7.3.1 DOM-based XSS Vulnerability (VMSA-2018-0009)

VMware vRealize Business Unspecified Stored XSS (VMSA-2016-0003)

VMware vRealize Log Insight 2.x / 3.x < 3.3.2 Multiple Vulnerabilities (VMSA-2016-0008)

W3 Total Cache Plugin For WordPress Cache Key XSS

WackoWiki TextSearch phrase Parameter XSS

WANem index-advanced.php XSS

Web Server Expect Header XSS

Web Server Generic XSS

Webalizer < 2.01-09 Multiple XSS

WebCam Watchdog sresult.exe XSS

WebcamXP Chat Name XSS

WebChat XSS

Webmin 1.370 / 1.390 webmin\_search.cgi Cross Site Scripting

Webmin < 1.350 pam\_login.cgi Cross Site Scripting

Webmin < 1.500 Cross Site Scripting

Webmin < 1.680 view.cgi Cross Site Scripting

Webmin < 1.690 Multiple XSS

Webmin < 1.760 xmlrpc.cgi Cross Site Scripting Vulnerability

Webmin < 1.830 Multiple Cross Site Scripting Vulnerabilities

Webmin < 1.850 Multiple Cross Site Scripting Vulnerabilities

Webmin < 1.860 Cross Site Scripting Vulnerability

Webmin < 1.870 Cross Site Scripting Vulnerability

Webmin <= 1.540 Cross Site Scripting

Webmin chooser.cgi Cross-Site Scripting (< 1.330)

WEBppliance ocw\_login\_username Parameter XSS

Websense Reporting Tools WsCgiLogin.exe username Parameter XSS

WebWasher < 4.4.1 Build 1613 Multiple XSS

Wing FTP Server < 3.5.1 XSS

Woltlab Burning Board pms.php folderid Parameter XSS

Wordfence Plugin for WordPress 'email' Parameter XSS

WordPress < 1.2.2 Multiple XSS

WordPress Multiple XSS

WordPress wp-includes/feed.php self\_link() Function Host Header RSS Feed XSS

WP Super Cache Plugin for WordPress wp-cache.php Cache List Content Handling XSS

Xerox DocuShare dsweb Servlet Multiple XSS

Xitami testssi.ssi HTTP Header XSS

XMB < 1.9.1 Multiple XSS

XOOPS <= 1.0 Dictionary Module Multiple Scripts XSS

XOOPS Glossary Module glossaire-aff.php lettre Parameter XSS

XOOPS misc.php Query String XSS

XOOPS viewtopic.php Multiple Parameter XSS

YaBB Shadow BBCode Tag XSS

YaBB YaBB.pl usersrecentposts Action username Parameter XSS

YaCy Peer-To-Peer Search Engine XSS

YUI charts.swf / swfstore.swf / uploader.swf XSS

Zenphoto 404 Error Page XSS

Zenphoto Verisign\_logon.php redirect Parameter XSS

Zeroboard < 4.1pl6 Multiple XSS

Zeus Admin vs\_diag.cgi XSS

Zimbra Collaboration Server aspell.php dictionary Parameter XSS

# CGI abuses

.bash\_history Files Disclosed via Web Server

.svn/entries Disclosed via Web Server

2BGal disp\_album.php id\_album Parameter SQL Injection

3Com Network Supervisor Traversal Arbitrary File Access

3Com Web Management Interface Default Credentials

4D WebSTAR Tomcat Plugin Remote Buffer Overflow

4Images <= 1.7.1 index.php template Parameter Traversal Local File Inclusion

@lex Guestbook livre\_include.php chem\_absolu Parameter Remote File Inclusion

A1Stats Multiple Script Traversal Arbitrary File Access

Aardvark Topsites CONFIG[path] Parameter Remote File Inclusion

Aborior Encore WebForum display.cgi file Parameter Command Execution

Acajoom Component for Joomla! 'mailingid' Parameter SQLi

Acajoom Component for Joomla! <= 3.2.6 Backdoor Detection

ACal embed/day.php path Parameter Remote File Inclusion

Accellion Secure File Transfer Appliance 'oauth\_token' Parameter Remote Command Execution

Accellion Secure File Transfer Appliance 'statecode' Cookie Remote File Disclosure

Accellion Secure File Transfer Appliance Detection

Achievo class.atkdateattribute.js.php config\_atkroot Parameter Remote File Inclusion

Active Auction Multiple Vulnerabilities (SQLi, XSS)

Active Directory Certificate Services Web Enrollment Anonymous Access

Active WebCam Webserver <= 5.5 Multiple Vulnerabilities (DoS, Path Disc)

ActiveMQ Double Slash Request Source Code Disclosure

ActivePerl findtar Sample Script Remote Command Execution

ActivePerl perlIS.dll Remote Buffer Overflow

ActualAnalyzer direct.php rf Parameter Remote File Inclusion

ActualAnalyzer Lite style Parameter Traversal Local File Inclusion

Adcycle build.cgi Remote Password Disclosure

Admbook content-data.php X-Forwarded-For Header Arbitrary PHP Code Injection

Adobe <= 9.7.5 Connect Authentication Bypass Vulnerability (APSB18-18, APSB18-22)

Adobe Breeze Directory Traversal Arbitrary File Access

Adobe Captivate Quiz Reporting Feature 'internalserverread.php' Remote File Disclosure (APSB17-19)

Adobe Captivate Quiz Reporting Feature 'internalServerReporting.php' File Upload RCE

Adobe ColdFusion 'locale' Parameter Directory Traversal

Adobe ColdFusion Admin Requires No Authentication

Adobe ColdFusion Authentication Bypass (APSB13-03)

Adobe ColdFusion Authentication Bypass (APSB13-13)

Adobe ColdFusion Authentication Bypass (APSB13-13) (intrusive check)

Adobe ColdFusion BlazeDS Java Object Deserialization RCE

Adobe ColdFusion Detection

Adobe ColdFusion FCKeditor 'CurrentFolder' File Upload

Adobe ColdFusion File Upload (APSB18-33) (CVE-2018-15961)

Adobe ColdFusion HTTP Response Splitting (APSB12-15)

Adobe ColdFusion Multiple Vulnerabilities (APSA13-03)

Adobe ColdFusion On Apache Double Encoded NULL Byte Request File Content Disclosure

Adobe ColdFusion Remote Development Services

Adobe ColdFusion Remote Development Services Enabled Without Authentication

Adobe ColdFusion Unsupported Version Detection

Adobe Connect < 9.6.2 Multiple Vulnerabilities (APSB17-22)

Adobe Connect < 9.7 Multiple Vulnerabilities (APSB17-35)

Adobe Connect < 9.7.5 Multiple Vulnerabilities (APSB18-06)

Adobe Connect <= 9.8.1 Session Token Exposure Vulnerability (ASPB19-05)

Adobe Connect Detection

Adobe Connect Enterprise Server Information Disclosure

Adobe Document Server Default Credentials

Adobe Document Server File URI Arbitrary Resource Manipulation

Adobe Document Server for Reader Extensions < 6.1 Multiple Vulnerabilities

Adobe Dreamweaver dwsync.xml Remote Information Disclosure

Adobe InDesign Server RunScript Arbitrary Command Execution

Adobe RoboHelp Server Security Bypass (APSA09-05 / intrusive check)

Adobe RoboHelp Server Security Bypass (APSA09-05)

ADOdb Lite adodb-perf-module.inc.php last\_module Parameter Arbitrary Code Execution

ADOdb server.php sql Parameter SQL Injection

ADOdb tmssql.php do Parameter Arbitrary PHP Function Execution

Advanced Custom Fields Plugin for WordPress 'acf\_abspath' Parameter Remote File Inclusion

Advanced Guestbook index.php entry Parameter SQL Injection

Advanced Guestbook index.php lang Cookie Parameter Path Disclosure

Advanced Poll admin/index.php Session Identifier Replay Authentication Bypass

Advanced Poll info.php Remote Information Disclosure

AEC Subscription Manager Component for Mambo / Joomla! 'usage' Parameter SQLi

airVision NVR path Parameter Traversal Arbitrary File Access

Ajax Pagination (twitter Style) Plugin for WordPress Local File Inclusion

AjaXplorer < 5.0.1 Multiple Command Execution Vulnerabilities

AjaXplorer < 5.0.3 Multiple Vulnerabilities

AjaXplorer checkInstall.php Arbitrary Command Injection

AjaXplorer Detection

AkoGallery Component for Mambo / Joomla! 'id' Parameter SQLi

ALCASAR 'index.php' Crafted HTTP Header RCE

ALCASAR Detection

Alcatel OmniSwitch Default Credentials (http)

Alchemy Eye/Network Monitor Traversal Arbitrary Command Execution

Alexandria-dev Multiple Script Upload Spoofing Arbitrary File Access

Alibaba get32.exe Arbitrary Command Execution

Alibaba tst.bat Arbitrary Command Execution

AlienForm2 alienform.cgi Traversal Arbitrary File Manipulation

AlienVault OSSIM 'av-centerd' get\_file() Information Disclosure

AlienVault OSSIM 'av-centerd' Remote Code Execution

AlienVault OSSIM 'av-centerd' set\_file() Remote Code Execution

AlienVault OSSIM Web Front End Detection

Alkalay.Net Multiple Scripts Arbitrary Command Execution

Allaire JRun Crafted Request Forced Directory Listing

Allaire JRun Encoded JSP Request Directory Listing

AllVideos Reloaded! Plugin for Joomla! 'divid' Parameter SQLi

alpha\_auth\_check() Function Remote Authentication Bypass

AlphaRegistration Component for Joomla! 'email' Parameter SQLi

Alt-N MDaemon Remote Administration 13.0.x < 13.0.8 RCE (MD041917) (EASYBEE)

Alt-N MDaemon Remote Administration Detection

Alt-N MDaemon WebAdmin Unsupported Version Detection

Alt-N WebAdmin Multiple Remote Vulnerabilities (XSS, Bypass Access)

Alt-N WebAdmin Multiple Vulnerabilities

AltaVista Intranet Search CGI query Traversal Arbitrary File Access

AMember Multiple Script config[root\_dir] Parameter Remote File Inclusion

AN HTTPd count.pl Traversal Arbitrary File Overwrite (deprecated)

AN-HTTPd Multiple Test CGIs Arbitrary Command Execution

Anaconda Foundation Directory apexec.pl template Parameter Traversal Arbitrary File Retrieval

Ananconda Partners Clipper anacondaclip.pl Traversal Arbitrary File Access

AngelineCMS loadkernel.php installPath Parameter Remote File Inclusion

Ansible AWX WebUI Detection

Ansible Tower 3.1.x < 3.1.8 / 3.2.x < 3.2.6 CSRF vulnerability

Ansible Tower 3.3.x < 3.3.6 / 3.4.x < 3.4.4 / 3.5.x < 3.5.1 CRLF Vulnerability

Ansible Tower 3.4.x < 3.4.6 / 3.5.x < 3.5.6 / 3.6.x < 3.6.4 Denial of Service Vulnerability

Ansible Tower 3.5.x < 3.5.4 / 3.6.x < 3.6.2 Multiple Vulnerabilities

Ansible Tower 3.6.x < 3.6.1 Information Disclosure

Ansible Tower 3.x < 3.3.3 Unauthorized Access vulnerability

Ansible Tower 3.x < 3.3.5 / 3.4.x < 3.4.3 Privilege Escalation Vulnerability

Ansible Tower Unsupported Version

Ansible Tower WebUI Detection

AntiBoard antiboard.php Multiple Parameter SQL Injection

AnyForm CGI Arbitrary Command Execution

Apache ActiveMQ 5.11.x < 5.11.4 / 5.12.x < 5.12.3 / 5.13.x < 5.13.1 Web Console Multiple XSS

Apache ActiveMQ 5.14.x - 5.15.2 OpenWire Information Disclosure

Apache ActiveMQ 5.x < 5.10.1 / 5.11.0 Multiple Vulnerabilities

Apache ActiveMQ 5.x < 5.13.0 Java Object Deserialization RCE

Apache ActiveMQ 5.x < 5.13.2 Multiple Vulnerabilities

Apache ActiveMQ 5.x < 5.14.0 ActiveMQ Fileserver web application remote code execution (Xbash)

Apache ActiveMQ 5.x < 5.14.2 Web-based Administration Console Unspecified XSS

Apache ActiveMQ 5.x < 5.14.5 ControlCommand DoS

Apache ActiveMQ 5.x < 5.15.5 Multiple Vulnerabilities

Apache ActiveMQ 5.x < 5.15.9 Corrupt MQTT Frame Denial of Service (DoS) (CVE-2019-0222)

Apache ActiveMQ Blob Message Directory Traversal

Apache ActiveMQ Client 5.x < 5.15.6 TLS Hostname Verification Weakness

Apache ActiveMQ Detection

Apache ActiveMQ Web Console Default Credentials

Apache ActiveMQ Web Console Missing X-Frame-Options Clickjacking

Apache ActiveMQ Web Console Test Pages Information Disclosure

Apache Archiva 1.2.x <= 1.2.2 / 1.3.x <= 1.3.6 Multiple Vulnerabilities

Apache Archiva < 1.3.5 Multiple Vulnerabilities

Apache Archiva Detection

Apache Axis2 'xsd' Parameter Directory Traversal

Apache Axis2 Default Credentials

Apache Axis2 Detection

Apache Hadoop HDFS DataNode Web Detection

Apache Hadoop HDFS NameNode Web Detection

Apache Hadoop MapReduce JobTracker Web Detection

Apache Hadoop MapReduce TaskTracker Web Interface

Apache Hadoop YARN ResourceManager Unauthenticated RCE (Remote) (Xbash)

Apache Hadoop YARN ResourceManager Web Interface

Apache Jetspeed User Manager Service SQLi

Apache mod\_jk Long URL Worker Map Stack Remote Overflow

Apache mod\_wsgi < 3.4 Remote Information Disclosure

Apache OFBiz Default Credentials

Apache OFBiz Detection

Apache OFBiz FlexibleStringExpander Remote Code Execution

Apache OFBiz Nested Expression Arbitrary UEL Function Execution

Apache on Windows mod\_alias URL Validation Canonicalization CGI Source Disclosure

Apache on Windows mod\_alias URL Validation Canonicalization CGI Source Information Disclosure

Apache PHP-CGI Remote Code Execution

Apache Shiro URI Path Security Directory Traversal Information Disclosure

Apache Solr 5.x < 5.5.5 / 6.x < 6.6.2 / 7.x < 7.1.0 Multiple Vulnerabilities

Apache Solr 5.x <= 5.5.5 or 6.x <= 6.6.5 Deserialization Vulnerability

Apache Solr 5.x <= 5.5.5 or 6.x <= 6.6.5 Deserialization Vulnerability (CVE-2019-0192)

Apache Solr 8.1.1 / 8.2.0 Remote Code Execution Vulnerability

Apache Solr 8.1.1, 8.2.0 Remote JMX RMI Deserialization Vulnerability

Apache Solr < 4.1.0 Multiple XML External Entity Injections

Apache Solr < 4.10.5 'plugin.js' XSS

Apache Solr < 4.3.1 XML External Entity Injection

Apache Solr < 4.6.0 'SolrResourceLoader' Directory Traversal

Apache Solr < 6.6.1 Kerberos Plugin Delegation Token Handling Remote Information Disclosure

Apache Solr < 8.4.0 Remote Code Execution

Apache Solr Config API Velocity Template RCE (Direct Check)

Apache Storm WebUI Detection

Apache Struts 2 'action:' Parameter Arbitrary Remote Command Execution

Apache Struts 2 'action:' Parameter Prefix Security Constraint Bypass

Apache Struts 2 'class' Parameter ClassLoader Manipulation

Apache Struts 2 'method:' Prefix Arbitrary Remote Command Execution

Apache Struts 2 / XWork Remote Code Execution (safe check)

Apache Struts 2 < 2.0.12 / 2.1.3 Dispatcher Directory Traversal

Apache Struts 2 Crafted Parameter Arbitrary OGNL Expression Remote Command Execution

Apache Struts 2 devMode Information Disclosure

Apache Struts 2 ExceptionDelegator Arbitrary Remote Command Execution

Apache Struts 2 Multiple Remote Code Execution and File Overwrite Vulnerabilities (safe check)

Apache Struts 2 OGNL Expression Handling Double Evaluation Error Remote Command Execution

Apache Struts 2 ParameterInterceptor Class OGNL Expression Parsing Remote Command Execution

Apache Struts 2 REST Plugin OGNL Expression Handling RCE

Apache Struts 2 REST Plugin XStream XML Request Deserialization RCE

Apache Struts 2 Tag Attribute Double OGNL Evaluation RCE

Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)

Apache Struts 2.3.x Struts 1 plugin RCE (remote)

Apache Struts Config Browser Plugin Detection

Apache Struts CVE-2018-11776 Results With No Namespace Remote Code Execution (S2-057) (remote)

Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Multiple Vulnerabilities

Apache Tomcat allowLinking UTF-8 Traversal Arbitrary File Access

Apache Tomcat Catalina org.apache.catalina.servlets.DefaultServlet Source Code Disclosure

Apache Tomcat Directory Listing and File Disclosure

Apache Tomcat Nonexistent File Error Message Path Disclosure

Apache Tomcat RequestDispatcher Directory Traversal Arbitrary File Access

Apache Tomcat Snoop Servlet Remote Information Disclosure

Apache Tomcat source.jsp Arbitrary Directory Listing

Apache Tomcat TroubleShooter Servlet Information Disclosure

Apache Win32 ScriptAlias php.exe Arbitrary File Access

Apple Mac OS X Wiki Server File Upload Security Bypass

Apple Mac OS X Wiki Server Weblog SACL Security Bypass

Apple QuickTime/Darwin Streaming Server Multiple Remote Vulnerabilities

Appointments Plugin for WordPress < 2.2.2 PHP Object Injection

AppServ appserv/main.php appserv\_root Parameter Remote File Inclusion

Aprox PHP Portal index.php Arbitrary File View

ArGoSoft Mail Server Multiple Remote Vulnerabilities (XSS, DoS, Traversal)

ArGoSoft Mail Server Multiple Traversals

ArGoSoft Mail Server Pro <= 1.8.7.6 Multiple Vulnerabilities (XSS, Traversal, Priv Esc)

ArtForms Component for Joomla! 'viewform' Parameter SQLi

Artica < 1.4.101900 mailattach Parameter Directory Traversal

Artica Default Credentials

Artica Detection

Artica mailattach Parameter Directory Traversal

Artifactory < 3.1.1.1 XStream Remote Code Execution

Artifactory Detect

Aruba VAN SDN default credentials

ASG-Sentry CGI Default Credentials

ASG-Sentry CGI Detection

ASG-Sentry File Check Utility /snmx-cgi/fcheck.exe Arbitrary File Overwrite

ashNews 0.83 Multiple Vulnerabilities

ASP PortalApp Multiple SQL Injection

ASP-Rider verify.asp username Parameter SQL Injection

ASP.NET DEBUG Method Enabled

ASPrunner 2.4 Multiple Vulnerabilities

AspUpload Test11.asp Arbitrary File Upload

aspWebAlbum album.asp SQL Injection

aspWebCalendar calendar.asp SQL Injection

Astaro Security Gateway Detection

AsteriDex callboth.php Multiple Parameter CRLF Injection Arbitrary Command Execution

Asterisk Recording Interface (ARI) Default Administrator Credentials

Asterisk Recording Interface (ARI) includes/main.conf Remote Credential Disclosure

Asterisk Recording Interface (ARI) misc/audio.php recording Parameter Traversal Arbitrary File Access

ASUSTOR Data Master (ADM) Detection

ASUSTOR Data Master < 3.1.3 Multiple Vulnerabilities

ASUSTOR Data Master < 3.1.6 Multiple Vulnerabilities

AT&T U-verse Arris Modems NVG589 / NVG599 / 5268AC Multiple Vulnerabilities (SharknATTo)

Athena Web Registration athenareg.php pass Parameter Command Execution

Atlassian Bamboo 2.2.x < 5.8.5 / 5.9.x < 5.9.7 Unspecified Resource Deserialization RCE

Atlassian Bamboo 5.x < 5.15.7 / 6.0.x < 6.0.1 Incorrect Permission Check RCE

Atlassian Bamboo 6.1.x < 6.1.6 / 6.2.x < 6.2.5 Incorrect Permission Check RCE

Atlassian Bamboo < 5.4.3 / 5.5.1 / 5.6.0 XWork Library ClassLoader Manipulation Remote Code Execution

Atlassian Bamboo < 6.0.0 OAuth plugin allows arbitrary HTTP requests to be proxied

Atlassian Bamboo Detection

Atlassian Bitbucket < 4.14.4 OAuth Plugin IconUriServlet Internal Network Resource Disclosure CSRF

Atlassian Bitbucket Data Center 5.13.x < 5.13.6 / 5.14.x < 5.14.4 / 5.15.x < 5.15.3 / 5.16.x < 5.16.3 / 6.0.x < 6.0.3 / 6.1.x < 6.1.2 Path Traversal Vulnerability (SA-2019-05-22)

Atlassian Bitbucket Detection

Atlassian Confluence 6.0.x < 6.0.7 Drafts diff REST Information Disclosure

Atlassian Confluence 6.1.x < 6.6.16 / 6.7.x < 6.13.7 / 6.14.x < 6.15.8 Local File Disclosure Vulnerability

Atlassian Confluence < 4.3.7 Multiple Vulnerabilities

Atlassian Confluence < 5.1.5 OGNL Expression Handling Double Evaluation Error Remote Code Execution

Atlassian Confluence < 5.5.2 XWork Library ClassLoader Manipulation Remote Code Execution

Atlassian Confluence < 6.1.3 OAuth Plugin IconUriServlet Internal Network Resource Disclosure CSRF

Atlassian Confluence < 6.13.1 Information Disclosure Vulnerability

Atlassian Confluence < 6.6.12 / 6.7.x < 6.12.3 / 6.13.x < 6.13.3 / 6.14.x < 6.14.2 Multiple Vulnerabilities

Atlassian Confluence < 6.6.12 / 6.7.x < 6.12.3 / 6.13.x < 6.13.3 / 6.14.x < 6.14.2 Template Injection

Atlassian Confluence < 6.6.13 / 6.7.x < 6.12.4 / 6.13.x < 6.13.4 / 6.14.x < 6.14.3 / 6.15.x < 6.15.2 Directory Traversal Vulnerability

Atlassian Confluence Wiki Detection

Atlassian Crowd 2.1.x < 3.0.5 / 3.1.x < 3.1.6 / 3.2.x < 3.2.8 / 3.3.x < 3.3.5 / 3.4.x < 3.4.4 RCE Vulnerability

Atlassian Crowd < 2.11.2 OAuth Plugin IconUriServlet Internal Network Resource Disclosure CSRF

Atlassian Crowd Detection

Atlassian Crowd XML External Entity Request Handling Arbitrary File Disclosure

Atlassian Crucible 2.5.8 / 2.6.8 / 2.7.12 XML Parsing Vulnerability

Atlassian Crucible 3.x < 3.0.4 / 3.1.7 / 3.2.5 / 3.3.4 / 3.4.4 Administrator Password Reset

Atlassian Crucible < 4.3.2 OAuth Plugin IconUriServlet Internal Network Resource Disclosure CSRF

Atlassian Crucible Detection

Atlassian Crucible for Windows < 4.4.6, 4.5.x < 4.5.3 Remote Code Execution Vulnerability

Atlassian FishEye 2.5.8 / 2.6.8 / 2.7.12 XML Parsing Vulnerability

Atlassian FishEye 3.x < 3.0.4 / 3.1.7 / 3.2.5 / 3.3.4 / 3.4.4 Administrator Password Reset

Atlassian FishEye < 4.3.2 OAuth Plugin IconUriServlet Internal Network Resource Disclosure CSRF

Atlassian FishEye Detection

Atlassian Fisheye for Windows < 4.4.6, 4.5.x < 4.5.3 Remote Code Execution Vulnerability

Atlassian JIRA 4.1.x < 4.1.2 Multiple Vulnerabilities

Atlassian JIRA 4.2.4 < 6.3.0 Multiple Vulnerabilities

Atlassian JIRA 4.2.x < 5.1 XSRF

Atlassian JIRA 4.3.x < 5.1.1 Multiple Open Redirect Vulnerabilities

Atlassian JIRA 6.2.1 < 7.4.4 Cross-Site Scripting (XSS) Vulnerability (JRASERVER-66719)

Atlassian Jira 7.13 < 8.5.5 Jira Project Key Information Disclosure (JRASERVER-70565)

Atlassian Jira 7.13.x < 7.13.3 / 8.0.x < 8.0.4 / 8.1.x < 8.1.1 Information Disclosure Vulnerability

Atlassian Jira 7.13.x < 7.13.3, 8.x < 8.1.1 Cross-Site Scripting Vulnerability

Atlassian Jira 7.13.x < 7.13.4, 8.0.x < 8.0.4, 8.1.x < 8.1.1 Multiple Vulnerabilities

Atlassian Jira 7.13.x < 7.13.4, 8.x < 8.2.2 CSRF vulnerability (JRASERVER-69858)

Atlassian JIRA 7.13.x < 7.13.6 / 8.x < 8.2.3 / 8.3.x < 8.3.2 Multiple Vulnerabilities

Atlassian Jira 7.13.x < 8.6.0 JMX monitoring flag CSRF Vulnerability (JRASERVER-70570)

Atlassian JIRA 7.6.5 / 7.7.x < 7.7.4 / 7.8.x < 7.8.4 / 7.9.x < 7.9.2 Multiple Vulnerabilities (SB18-141)

Atlassian JIRA 7.6.7 / 7.7.x < 7.7.5 / 7.8.x < 7.8.5 / 7.9.x < 7.9.3 / 7.10.x < 7.10.2 XSS

Atlassian Jira 7.6.x < 7.6.13, 7.7.0 < 7.13.3, 8.x < 8.1.1 Information Disclosure Vulnerability

Atlassian JIRA 7.x >= 7.6 / 8.x < 8.5.4 / 8.6.x < 8.6.2 Multiple CSRF

Atlassian JIRA 7.x.x < 7.13.1 / 8.0.0 Cross-Site Scripting (XSS) Vulnerability (SB18-141)

Atlassian Jira 8.2 < 8.5.4 Support Files Improper Authorization Vulnerability (JRASERVER-70564)

Atlassian Jira 8.2.x < 8.6.0 Improper Authorization on Project Titles Information Disclosure Vulnerability (JRASERVER\_70569)

Atlassian Jira 8.3.x < 8.5.2 DLL Hijacking Vulnerability (JRASERVER-70407)

Atlassian JIRA 8.5.x / 8.6.x 'Atlassian Application Links' Plugin CSRF

Atlassian Jira < 4.1.1 Multiple Vulnerabilities

Atlassian JIRA < 4.2 Multiple Vulnerabilities

Atlassian JIRA < 4.2.1 Multiple Vulnerabilities

Atlassian JIRA < 4.2.2 Open Redirect

Atlassian JIRA < 5.0.1 XML Parsing DoS

Atlassian JIRA < 5.0.7 Privilege Escalation

Atlassian JIRA < 5.1.5 SOAP API Arbitrary File Overwrite

Atlassian JIRA < 6.0.4 Arbitrary File Creation

Atlassian JIRA < 6.0.5 Multiple Vulnerabilities

Atlassian JIRA < 6.1.4 Privilege Escalation

Atlassian JIRA < 6.4.10 / 7.0.0-OD-02 MitM Plaintext Disclosure (Bar Mitzvah)

Atlassian Jira < 7.1.9 Role Name XSS (JRASERVER-61861)

Atlassian JIRA < 7.13.12 / 8.x < 8.4.3 / 8.5.x < 8.5.2 Authorization Bypass (JRASERVER-70405)

Atlassian JIRA < 7.13.12 / 8.x < 8.5.4 / 8.6.x < 8.6.1 'Atlassian Application Links' Plugin Privilege Escalation

Atlassian JIRA < 7.13.4 / 8.0.x < 8.1.0 Epic Name DoS (SB19-182)

Atlassian JIRA < 7.13.6 / 8.x < 8.4.0 XSS (JRASERVER-69795)

Atlassian JIRA < 7.13.9 / 8.x < 8.3.3 XSS (JRASERVER-69790)

Atlassian JIRA < 7.2.12 / 7.3.x < 7.6.1 Cross-Site Scripting

Atlassian Jira < 7.2.15 OAuth Plugin IconUriServlet Internal Network Resource Disclosure CSRF

Atlassian JIRA < 7.5.3 Cross-Site Scripting

Atlassian JIRA < 7.6.1 CSRF vulnerability (JRASERVER-66643)

Atlassian JIRA < 7.6.1 Multiple Vulnerabilities

Atlassian JIRA < 7.6.2 Cross-Site Request Forgery

Atlassian JIRA < 7.6.5 / 7.7.x < 7.7.3 / 7.8.x < 7.8.3 Limited Authentication Bypass

Atlassian JIRA < 7.6.7 / 7.7.x < 7.10.1 Cross-Site Scripting

Atlassian JIRA < 7.6.7 / 7.7.x < 7.11.0 Information Disclosure

Atlassian JIRA < 7.7.1 Cross-Site Scripting (XSS) Vulnerability (JRASERVER-67108)

Atlassian JIRA < 7.8.1 Cross-Site Scripting (XSS) Vulnerability (JRASERVER-67106)

Atlassian JIRA < 8.3.2 Multiple Vulnerabilities

Atlassian JIRA < 8.4.0 Multiple Vulnerabilities

Atlassian JIRA < 8.4.2 Information disclosure in Application links plugin

Atlassian JIRA < 8.6.1 Information Disclosure

Atlassian JIRA Authentication Bypass Vulnerability (JRASERVER-69239)

Atlassian JIRA Common Credentials

Atlassian JIRA ConfigureReport.jspa 'reportKey' Information Disclosure

Atlassian JIRA Cross-Site Scripting (XSS) Vulnerability (JRASERVER-68526)

Atlassian JIRA Cross-Site Scripting (XSS) Vulnerability (JRASERVER-68614)

Atlassian JIRA Detection

Atlassian JIRA Information Disclosure Vulnerability (JRASERVER-69797)

Atlassian JIRA Multiple Vulnerabilities (JRASERVER-69245) (JRASERVER-69246)

Atlassian JIRA Open Redirect Vulnerabilities

Atlassian JIRA Plugins Detection

Atlassian JIRA ProfileLinkUserFormat Information Disclosure Vulnerability

Atlassian JIRA Server & JIRA Data Center Template Injection Vulnerability

Atlassian Jira Server and Data Center Template Injection Vulnerability (JRASERVER-69933)

Atlassian JIRA Server Template Injection Vulnerability (CVE-2019-11581)

Atlassian JIRA Server-Side Request Forgery (SSRF) Vulnerability (JRASERVER-68527)

Atlassian JIRA Service Desk Path Traversal Vulnerability (2019-09-18)

Atlassian JIRA Unsupported Version Detection

Atlassian Jira Webroot Directory Traversal Vulnerability

Atlassian JIRA worklog Information Disclosure

Atlassian JIRA XSRF, Open Redirect, and Access Control Bypass Vulnerabilities

Atmail Email Server WebAdmin Control Panel dbconfig.ini Information Disclosure

Atmail Webmail / AtmailOpen Webmail Detection

Atmail Webmail 3.x < 3.6.4 (3.64) Multiple Vulnerabilities

Atmail Webmail 4.5.1 (4.51) / 5.x < 5.0.3 (5.03) util.pl Cross-Site Request Forgery

Atmail Webmail 6.x / 7.x < 7.2.0 Multiple Vulnerabilities

Atmail Webmail 6.x < 6.6.4 / 7.x < 7.1.2 Multiple Vulnerabilities

Atmail Webmail 7.x < 7.2.2 Multiple Vulnerabilities

Atmail Webmail < 5.4.2 (5.42) Multiple Information Disclosure Vulnerabilities

Atmail Webmail < 6.3.5 Multiple XSS Vulnerabilities

Atmail Webmail < 6.6.2 Exim Buffer Overflow

Atmail Webmail Unsupported Version Detection

Atomic Photo Album apa\_phpinclude.inc.php apa\_module\_basedir Parameter Remote File Inclusion

AtomicBoard Multiple Remote Vulnerabilities (Traversal, Path Disc)

ATutor < 1.5.1-pl1 Multiple Remote Vulnerabilities (XSS, RFI, Command Exe)

ATutor Password Reminder SQL Injection

Authentication Bypass (Forced Browse)

Autodesk VRED Python API Remote Code Execution

AutoLinks Pro 'al\_initialize.php alpath Parameter Remote File Inclusion

AutomatedShops webc.cgi Installation Detection

AutomatedShops WebC.cgi Multiple Overflows

Aventail ASAP Platform Management Console Detection

AVG Internet Security 2013.x < 2013.3495 / 2015.x < 2015.5557 Local Privilege Escalation

AVG Internet Security 2015.5736 Address Space Layout Disclosure

AVTech Multiple Vulnerabilities

AWOL helperfunction.php includedir Parameter Remote File Inclusion

AWStats 'awstats.pl' Path Disclosure

AWStats < 6.95 awredir.pl Arbitrary Site Redirect

AWStats awstats.pl configdir Parameter Arbitrary Command Execution

AWStats Detection

AWStats is Openly Accessible

AWStats migrate Parameter Arbitrary Command Execution

AWStats Multiple Remote Vulnerabilities (Cmd Exec, Traversal, ID)

AWStats rawlog.pm logfile Parameter Arbitrary Command Execution

AWStats Referrer Header Arbitrary Command Execution

AWStats Totals awstatstotals.php multisort() Function sort Parameter Arbitrary PHP Code Execution

Axis 2400 Network Camera Multiple Vulnerabilities

AXIS HTTP GET Heap Overflow

Axis Storpoint CD Admin Authentication Bypass

Backup Files Disclosure

BackWPup for WordPress Plugin Remote File Inclusion

Barco ClickShare Device Default Credentials

Barco ClickShare Device Detect

Barracuda Spam & Virus Firewall Console Management Detection

Barracuda Spam Firewall < 3.1.18 Multiple Vulnerabilities

Barracuda Spam Firewall < 3.5.12.007 Multiple Vulnerabilities

Barracuda Spam Firewall Default Credentials

Barracuda Web Filter <= 5.0.0.012 Remote Command Execution

Barracuda Web Filter Detection

BASE < 1.2.5 readRoleCookie() Auth Bypass

BASE Authentication Redirect Authentication Bypass

BASE base\_maintenance.php Authentication Bypass

BASE Multiple Script BASE\_path Parameter Remote File Inclusion

Basic Analysis and Security Engine Authentication Check

Basilic diff.php Command Injection

BasiliX Application Detection

BasiliX login.php3 username Variable Arbitrary Command Execution

Basilix Webmail .class / .inc Direct Request Remote Information Disclosure

Basilix Webmail Attachment Crafted POST Arbitrary File Access

Basilix Webmail basilix.php3 request\_id[DUMMY] Variable Traversal Arbitrary File Access

Basilix Webmail id Variable SQL Injection

Basilix Webmail tmp Directory Permission Weakness Attachment Disclosure

bBlog <= 0.7.4 Multiple Vulnerabilities (SQLi, XSS)

bBlog rss.php p Parameter SQL Injection

BBS E-Market Professional index.php filename Parameter Traversal Arbitrary File Access

BDPDT for DotNetNuke (.net nuke) uploadfilepopup.aspx File Upload Privilege Escalation

BEA WebLogic config.xml Operator/Admin Password Disclosure

BEA WebLogic FileServlet Source Code Disclosure

BEA WebLogic Hex Encoded Request JSP Source Disclosure

BEA WebLogic Null Byte Request JSP Source Disclosure

BEA WebLogic SSIServlet Invocation Source Code Disclosure

Beanwebb's Guestbook 1.0 Multiple Vulnerabilities

Behold! Software counter.exe Malformed HTTP Request Counter Log DoS

Belkin N750 Router 1.10.22 Command Injection

Belkin N750 Router Command Injection

BF Survey Pro Component for Joomla! 'table' Parameter SQLi

Big Brother bb-hist.sh History Module Directory Traversal

Big Brother bb-hostsvc.sh 'HOSTSVC' Parameter Traversal Arbitrary File Access

BigTree CMS Detection

BigTree CMS index.php SQL Injection

Bitdefender GravityZone < 5.1.11.432 Information Disclosure

Bitdefender GravityZone User Interface Detection

BitDefender Update Server HTTP Request Traversal Arbitrary File Access

Bitrix bitrix.mpbuilder Module < 1.0.12 bitrix.mpbuilder\_step2.php 'work[]' Path Traversal File Inclusion

Bitrix bitrix.xscan Module < 1.0.4 bitrix.xscan\_worker.php 'file' Parameter Path Traversal File Disclosure

Bitrix Product and Modules Detection

Bitweaver wiki/edit.php suck\_url Parameter Traversal Source Code Disclosure

Bitweaver wiki/rankings.php style Parameter Traversal Local File Inclusion

BizDB bizdb-search.cgi Arbitrary Command Execution

BizMail bizmail.cgi Arbitrary Mail Relay

BlackBoard Internet Newsboard System checkdb.inc.php libpath Parameter Remote File Inclusion

Blackboard Learn Detection

Blazix Trailing Character JSP Source Disclosure

BLNews objects.inc.php4 Server[path] Parameter Remote File Inclusion

Blog Torrent < 0.81 btdownload.php Multiple Vulnerabilities

Blog Torrent btdownload.php file Variable Traversal Arbitrary File Retrieval

BlogEngine.NET api/BlogImporter.asmx GetFile Function Unauthorized Access

Blue Coat ICAP Patience Page XSS

Blue Coat ProxyAV 3.5.1.1 - 3.5.1.6 Heartbeat Information Disclosure (Heartbleed)

Blue Coat ProxyAV 3.5.x < 3.5.4.1 Multiple DoS Vulnerabilities

Blue Coat ProxyAV < 3.2.6.1 Multiple Admin Function CSRF

Blue Coat ProxyAV Detection

BlueDragon 6.2.1 Multiple Remote Vulnerabilities (XSS, DoS)

BlueShoes lib/googlesearch/GoogleSearch.php APP[path][lib] Parameter Remote File Inclusion

boastMachine mail.php id Parameter SQL Injection

boastMachine users.inc.php File Extension Validation Arbitrary File Upload

Boozt index.cgi Banner Creation Name Field Overflow

Brightmail Control Center Default Password (symantec) for 'admin' Account

Brio Unix odscgi HTMLFile Parameter Traversal Arbitrary File Access

BroadBoard Multiple Script SQL Injection

BroadVision One-To-One Enterprise Nonexistent JSP Request Path Disclosure

Brother Printer Debut embedded httpd <= 1.20 DoS

Browsable Web Directories

Browser Rejector Plugin for WordPress 'wppath' Parameter Remote File Inclusion

bttlxeForum login.asp Multiple Field SQL Injection

BuddyPress Plugin for WordPress < 2.9.2 Information Disclosure

Buffalo LinkStation Detection

Buffalo LinkStation Direct Request Remote File Disclosure

BugPort Attached File Handling Unspecified Issue

Bugzilla 'reporter' field Information Disclosure

Bugzilla 'time-tracking' fields Information Disclosure

Bugzilla 2.0 < 4.0.12 / 4.2.8 / 4.4.3 / 4.5.3 Character Spoofing

Bugzilla 2.0 < 4.4.3 / 4.5.3 Login Form XSRF

Bugzilla 3.7/3.7.1 Information Disclosure

Bugzilla < 2.14.2 / 2.16rc2 / 2.17 Multiple Vulnerabilities (SQLi, XSS, ID, Cmd Exe)

Bugzilla < 2.16.3 / 2.17.4 Multiple Vulnerabilities (XSS, Symlink)

Bugzilla < 2.16.4 / 2.17.5 Multiple Vulnerabilities (SQLi, ID)

Bugzilla < 2.16.6 / 2.18rc1 Multiple Vulnerabilities (XSS, SQLi, Priv Esc, more)

Bugzilla < 2.16.7 / 2.18.0rc3 Multiple Information Disclosures

Bugzilla < 2.18.1 Multiple Information Disclosures

Bugzilla < 3.6.10 / 4.0.7 / 4.2.2 / 4.3.2 Multiple Information Disclosures

Bugzilla < 3.6.11 / 4.0.8 / 4.2.3 / 4.3.3 Multiple Vulnerabilities

Bugzilla < 3.6.12 / 4.0.9 / 4.2.4 / 4.4rc1 Multiple Vulnerabilities

Bugzilla < 3.6.13 / 4.0.10 / 4.2.5 / 4.4rc2 Multiple Vulnerabilities

Bugzilla < 4.0.11 / 4.2.7 / 4.4.1 Multiple Vulnerabilities

Bugzilla < 4.0.14 / 4.2.10 / 4.4.5 / 4.5.5 CSRF Vulnerability

Bugzilla < 4.0.15 / 4.2.11 / 4.4.6 / 4.5.6 Multiple Vulnerabilities

Bugzilla < 4.0.16 / 4.2.12 / 4.4.7 / 5.0rc1 Multiple Vulnerabilities

Bugzilla < 4.2.15 / 4.4.10 / 5.0.1 Unauthorized Account Creation Vulnerability

Bugzilla <= 2.18.1 / 2.19.3 Multiple Vulnerabilities (ID, more)

Bugzilla Directory Access Information Disclosure

Bugzilla Multiple Remote Command Execution

Bugzilla Response Splitting

Bugzilla Software Detection

Bugzilla Unsupported Version Detection

BuildBot WebStatus Detection

BulletScript MailList bsml.pl Information Disclosure

Bytes Interactive Web Shopper shopper.cgi Traversal Arbitrary File Access

c99shell Backdoor Detection

CA ERwin Web Portal 9.5 Multiple Directory Traversals

CA Host-Based Intrusion Prevention System Server Default Credentials

CA Unified Management Portal (UMP) Detection

Cacti < 0.8.6e Multiple Vulnerabilities

Cacti < 0.8.6f Authentication Bypass Vulnerability

Cacti < 0.8.6f Multiple Vulnerabilities

Cacti < 0.8.7f Multiple Input Validation Vulnerabilities

Cacti < 0.8.8b Command and SQL Injections

Cacti < 0.8.8c Multiple Vulnerabilities

Cacti < 0.8.8d Multiple Vulnerabilities

Cacti cmd.php Multiple Parameter SQL Injection Arbitrary Command Execution

Cacti copy\_cacti\_user.php template\_user Variable SQL Injection

Cacti Detection

Cacti index.php/sql.php Login Action login\_username Parameter SQL Injection

Cacti Local File Inclusion Vulnerability

CactuShop 5.x Multiple Remote Vulnerabilities (XSS, SQLi)

CafeLog B2 Multiple Script Remote File Inclusion

CakePHP vendors.php file Parameter Traversal Arbitrary File Access

Caldera '/costview3/xmlrpc\_server/xmlrpc.php' XMLRPC Request Remote Command Execution

Caldera 'cdir' Parameter Absolute Path Directory Traversal

Caldera Detection

Calendar Express Multiple Vulnerabilities (SQLi, XSS)

Calendarix Basic cal\_cat.php catview Parameter SQL Injection

Calendarix calendar.php Multiple Parameter SQL Injection

Calendarix Multiple Script id Parameter SQL Injection

Calendarix Multiple Vulnerabilities (SQLi, XSS)

Campsite Detection

Campsite TinyMCE plugin 'attachments.php' 'article\_id' Parameter SQL Injection

CandyPress Store admin/utilities\_ConfigHelp.asp helpfield Parameter SQL Injection

Canon PIXMA Printer Administration Authentication Bypass

Canon PIXMA Printer HTTP Detection

Canon PIXMA Printer WLAN Credential Disclosure

Carello E-Commerce Carello.dll Command Execution

Cart32 c32web.exe ImageName Traversal Arbitrary File Access

CDomain whois\_raw.cgi fqdn Parameter Arbitrary Command Execution

Centreon 'fileOreonConf' Parameter File Include Vulnerabilities

Centreon 'insertLog()' Function RCE

Centreon 2.3.3 < 2.4.0 menuXML.php 'menu' Parameter SQL Injection

Centreon 2.6.6 Multiple XSRF Vulnerabilities

Centreon 2.6.x < 2.6.2 File Upload RCE

Centreon 2.6.x < 2.6.5 Multiple Vulnerabilities

Centreon < 2.5.3 Multiple Vulnerabilities

Centreon < 2.5.4 Multiple Vulnerabilities

Centreon Default Administrator Password

Centreon Detection

Centreon GetXMLTrapsForVendor.php 'mnftr\_id' Parameter SQLi

Centreon GetXmlTree.php 'sid' Parameter SQLi

Centreon include/doc/get\_image.php 'img' Parameter Traversal Arbitrary File Access

Cerb Detection

Cerberus Helpdesk GUI Agent < 2.7.1 Multiple Remote Vulnerabilities (SQLi, XSS)

Cerberus Helpdesk rpc.php Arbitrary Ticket Information Disclosure

Cerberus Support Center Multiple Remote Vulnerabilities (SQLi, XSS)

cfWebStore Multiple Vulnerabilities (SQLi, XSS)

CGI Generic 2nd Order SQL Injection Detection (potential)

CGI Generic Command Execution

CGI Generic Command Execution (time-based)

CGI Generic Command Execution (time-based, intrusive)

CGI Generic Cookie Injection Scripting

CGI Generic Cross-Site Request Forgery Detection (potential)

CGI Generic Format String

CGI Generic Fragile Parameters Detection (potential)

CGI Generic Header Injection

CGI Generic Injectable Parameter

CGI Generic Local File Inclusion

CGI Generic Local File Inclusion (2nd pass)

CGI Generic On Site Request Forgery (OSRF)

CGI Generic Open Redirection

CGI Generic Padding Oracle

CGI Generic Path Traversal

CGI Generic Path Traversal (extended test)

CGI Generic Path Traversal (quick test)

CGI Generic Path Traversal (write test)

CGI Generic Remote File Inclusion

CGI Generic SQL Injection

CGI Generic SQL Injection (2nd pass)

CGI Generic SQL Injection (blind)

CGI Generic SQL Injection (blind, time based)

CGI Generic SQL Injection (HTTP Cookies)

CGI Generic SQL Injection (HTTP Headers)

CGI Generic SQL Injection (Parameters Names)

CGI Generic SQL Injection Detection (potential, 2nd order, 2nd pass)

CGI Generic SSI Injection

CGI Generic SSI Injection (HTTP headers)

CGI Generic Tests HTTP Errors

CGI Generic Tests Load Estimation (all tests)

CGI Generic Tests Load Estimation (full tests)

CGI Generic Tests Load Estimation (quick tests, HTML injection)

CGI Generic Tests Load Estimation (quick tests, text injection)

CGI Generic Tests Timeout

CGI Generic Unseen Parameters Discovery

CGI Generic XML Injection

CGI Generic XPath Injection (2nd pass)

CGI::Session File Driver CGISESSID Cookie Traversal Authentication Bypass

CGIForum cgiforum.pl thesection Parameter Traversal Arbitrary File Access

CGIProxy < 2.1.2 Multiple Unspecified Vulnerabilities

CGIProxy Detection

CGIScript.net csNews.cgi Advanced Settings Multiple Parameter Arbitrary File Retrieval

ChartDirector for .NET cacheId Parameter Arbitrary File Access

Check Point Endpoint Security Server Information Disclosure

Check\_MK 1.2.2 < 1.2.2p3 / 1.2.3 < 1.2.3i5 Multiple Vulnerabilities

Check\_MK 1.2.4 < 1.2.4p4 / 1.2.5 < 1.2.5i4 Multiple Vulnerabilities

Check\_MK Agent for Linux 1.2.3i < 1.2.5i3 Arbitrary File Disclosure

Check\_MK Server WebUI Detection

CherryPy staticFilter Traversal Arbitrary File Access

Chipmunk CMScore Multiple Script SQL Injection

Chipmunk Forum Multiple SQL Injections

Cisco Content Security Management Appliance Web UI Default Credentials

Cisco DCNM Authentication Bypass (CVE-2019-15977)

Cisco Email Security Appliance Web UI Default Credentials

Cisco Integrated Management Controller WebUI Detection

Cisco MSE <= 8.0.120.7 Multiple Vulnerabilities

Cisco PIX Firewall Manager (PFM) on Windows Arbitrary File Access

Cisco Prime Data Center Network Manager Web Detection

Cisco Prime LAN Management Solution Web Detection

Cisco Prime Network / Wireless Control System Health Monitor Detection

Cisco Prime Security Manager GNU Bash Environment Variable Handling Command Injection (cisco-sa-20140926-bash) (Shellshock)

Cisco Prime Security Manager Log Retention DoS (cisco-sa-20120912-asacx)

Cisco Prime Security Manager Network Time Protocol Daemon (ntpd) Multiple Vulnerabilities (cisco-sa-20141222-ntpd)

Cisco Prime Security Manager OpenSSL Alternative Chains Certificate Forgery (cisco-sa-20150710-openssl)

Cisco Prime Security Manager Web Detection

Cisco RV110W, RV130W, and RV215W Routers Syslog Disclosure (cisco-sa-20190619-rv-fileaccess)

Cisco Small Business RV320 and RV325 Routers Information Disclosure Vulnerability (cisco-sa-20190123-rv-info) (remote check)

Cisco TelePresence Conductor Default Credentials (Web UI)

Cisco TelePresence Conductor WebUI Detection

Cisco TelePresence Multipoint Switch < 1.7.0 Multiple Vulnerabilities (cisco-sa-20110223-telepresence-ctms)

Cisco TelePresence Multipoint Switch Web Detection

Cisco TelePresence Multipoint Switch XML-RPC DoS (cisco-sa-20110223-telepresence-ctms)

Cisco TelePresence Server Detection

Cisco TelePresence Video Communication Server (VCS) Web UI Detection

Cisco UCS Central Software Web UI Detection

Cisco UCS Director Default Credentials (Web UI)

Cisco UCS Director Web UI Detection

Cisco Unified Computing System Manager CGI RCE (CSCur90888) (remote check)

Cisco Unified MeetingPlace Detection

Cisco Unified Operations Manager 8.6 SQL Injection Vulnerability

Cisco Unified Operations Manager < 8.6 Multiple Vulnerabilities

Cisco Unified Operations Manager Detection

Cisco WAAS Mobile Server Web Administration Default Credentials

Cisco WAAS Mobile Server Web Administration Interface Detection

Cisco Webex Meetings Desktop App < 33.6.4 Command Injection Vulnerability

Cisco Wireless Control System SQL Injection (cisco-sa-20100811-wcs) (credentialed check)

CiscoWorks Common Services HTTP Response Splitting

Citrix Access Gateway 5.x < 5.0.4.223524 Unspecified Security Bypass

Citrix Access Gateway Administrative Web Interface Default Credentials

Citrix Access Gateway Administrative Web Interface Detection

Citrix Access Gateway User Web Interface Detection

Citrix ADC and Citrix NetScaler Gateway Arbitrary Code Execution (CTX267027)

Citrix ADC and Citrix NetScaler Gateway Arbitrary Code Execution (CTX267027) (Direct Check)

Citrix ADC and Citrix NetScaler Gateway buffer overflow vulnerability (CTX249976)

Citrix and NetScaler SD-WAN Center Unauthenticated Directory Traversal File Write

Citrix Application Delivery Management Agent Information Disclosure

Citrix CloudPlatform Default Credentials

Citrix CloudPlatform Unauthorized Access Vulnerability (CTX140989)

Citrix NetScaler Authentication Bypass Vulnerability (CTX227928)

Citrix NetScaler Authentication Bypass Vulnerability (CTX232199)

Citrix NetScaler Gateway Cross-Site Scripting Vulnerability (CTX232199)

Citrix NetScaler Gateway TLS Padding Oracle Vulnerability (CTX240139)

Citrix NetScaler Multiple Vulnerabilities (CTX140863)

Citrix NetScaler Multiple Vulnerabilities (CTX230238, CTX230612)

Citrix NetScaler Multiple Vulnerabilities (CTX232161)

Citrix NetScaler Unspecified Remote Code Execution (CTX200206)

Citrix NetScaler Unspecified Remote Unauthorized Access (CTX200254)

Citrix SD-WAN Appliance < 10.2.3 Unauthenticated Blind SQL Injection

Citrix SD-WAN Center and NetScaler SD-WAN Center addModifyZTDProxy Unauthenticated Remote Command Injection

Citrix SD-WAN Center Command Injection

Citrix SD-WAN Center trace\_route Unauthenticated Remote Command Injection

Citrix SD-WAN Center Unauthenticated Remote Command Injection

Citrix SD-WAN Cookie Command Injection

Citrix Workspace App and Receiver App for Windows Remote Code Execution Vulnerability (CTX251986)

Citrix XenDesktop Director Detection

Citrix XenServer vSwitch Controller < 2.0.0+build11349 Multiple Vulnerabilities

Citrix XenServer vSwitch Controller Detection

Citrix XenServer Web Self Service Detection

Citrix XenServer Workload Balancer Detection

CitrusDB Static id\_hash Admin Authentication Bypass

Claroline < 1.5.4 / 1.6.0 Multiple Vulnerabilities (RFI, SQLi, XSS, Traversal)

Claroline claro\_init\_local.inc.php extAuthSource[newUser] Parameter Remote File Inclusion

Claroline inc/lib/language.lib.php language Parameter Traversal Local File Inclusion

Claroline ldap.inc.php clarolineRepositorySys Parameter Remote File Inclusion

Claroline Multiple RemoteVulnerabilities (RFI, Traversal, XSS)

Claroline Multiple Script includePath Parameter Remote File Inclusion

Claroline Software Detection

ClearSpace Detection

Clever Copy connect.inc Direct Request Information Disclosure

Clever Copy Multiple Vulnerabilities (XSS, Path Disc, Inf Disc)

Cloudera Manager < 4.8.3 / 5.x < 5.0.1 Information Disclosure

Cloudera Manager Default Credentials

Cloudera Manager Detection

Cloudera Manager Unsupported Version Detection

Cloudsafe365 Plugin for WordPress 'file' Parameter Traversal Arbitrary File Access

CMS Made Simple admin/lang.php nls Parameter Remote File Inclusion

CMS Made Simple admin/login.php cms\_language Cookie Local File Inclusion

CMS Made Simple modules/TinyMCE/content\_css.php templateid Parameter SQL Injection

CMS Made Simple url Parameter Arbitrary File Access

Cobalt Qube WebMail readmsg.php mailbox Parameter Traversal Arbitrary File Access

Cobalt RaQ2 cgiwrap Multiple Vulnerabilities

Cobalt RaQ4 Administrative Interface backup.cgi Command Execution (EXTINCTSPINACH)

Cobalt RaQ4 Administrative Interface overflow.cgi Command Execution

Cobalt siteUserMod.cgi Arbitrary Password Modification

Cobbler Admin Interface Detection

Cobbler Linux Installation Server Detection

Cobbler xmlrpc API power\_system Method Remote Shell Command Execution

CodeGrrl Applications Remote File Inclusion Vulnerabilities

CodeMeter < 4.30.498.504 Virtual Directory Traversal Arbitrary File Access

CodeMeter < 5.20 Local Privilege Escalation Vulnerability

CodeMeter TCP Packet Parsing Unspecified Remote DoS

CodeMeter Virtual Directory Traversal Arbitrary File Access (remote check)

CodeMeter WebAdmin Detection

CodeThatShoppingCart Multiple Remote Vulnerabilities (SQLi, XSS, ID)

Cognos Powerplay WE Multiple Information Disclosure Vulnerabilities

Cold Fusion Administration Page Overflow DoS

ColdFusion / JRun on IIS Double Encoded NULL Byte Request File Content Disclosure

ColdFusion Debug Mode Information Disclosure

ColdFusion Extended Support Version Detection

ColdFusion Multiple Vulnerabilities (File Upload/Manipulation)

ColdFusion on IIS cfm/dbm Diagnostic Error Path Disclosure

Collector Component for Joomla! File Upload RCE

Comdev eCommerce 3.0 Multiple Vulnerabilities (RFI, Traversal)

Comersus BackOffice comersus\_backoffice\_menu.asp Multiple Parameter SQL Injection

Comersus Cart /comersus/database/comersus.mdb Direct Request Datbase Disclosure

Comersus Cart Multiple Input Validation Vulnerabilities (SQLi, XSS)

Comersus Cart Multiple Vulnerabilities (SQLi, XSS)

Comment Rating Plugin for WordPress 'id' Parameter SQL Injection

Commerce.CGI Shopping Cart commerce.cgi page Parameter Traversal Arbitrary File Access

CommonSpot < 7.0.2 / 8.0.3 / 9.0.0 Multiple Vulnerabilities

CommonSpot Detection

CommuniGate Pro Referer Field Session Token Disclosure

Community Link Pro login.cgi file Parameter Arbitrary Command Execution

Computer Associates ARCserve D2D Detection

Computer Associates ARCserve D2D homepageServlet Servlet Information Disclosure

Computer Associates XOsoft SOAP Request Username Enumeration (CA20100406)

Contact Form 7 Plugin for WordPress CAPTCHA Validation Bypass

Contenido contenido/classes/class.inuse.php Multiple Parameter Remote File Inclusion

CoolForum Multiple SQL Injections

CoolForum Multiple Vulnerabilities (SQLi, XSS)

CoolPHP 1.0 Multiple Vulnerabilities

CopperExport XP\_Publish.PHP SQL Injection Vulnerability

Coppermine imageObjectIM.class.php Command Execution Vulnerabilities

Coppermine Photo Gallery < 1.3.2 Multiple SQL Injections

Coppermine Photo Gallery album Password Cookie SQL Injection

Coppermine Photo Gallery bridge/coppermine.inc.php Bridge Wizard Session Cookie SQL Injection

Coppermine Photo Gallery Detection

Coppermine Photo Gallery displayimage.php SQL Injection

Coppermine Photo Gallery GLOBALS[USER[lang] Parameter Local File Inclusion

Coppermine Photo Gallery include/functions.inc.php \_data Cookie lang Parameter Traversal Local File Inclusion

Coppermine Photo Gallery index.php file Parameter Local File Inclusion

Coppermine Photo Gallery keysToSkip Parameter Overwrite

Coppermine Photo Gallery Multiple Extension File Upload Arbitrary PHP Code Execution

Coppermine Photo Gallery showdoc.php f Parameter Local File Inclusion

Coppermine Photo Gallery Voting Restriction Bypass

CoSoSys Endpoint Protector Detection

cPanel <= 9.1.0 Multiple Vulnerabilities

cPanel guestbook.cgi template Parameter Arbitrary Command Execution

CProxy 3.3.x - 3.4.4 Multiple Vulnerabilities

CrashPlan Server Default Administrative Credentials

Creative Contact Form Component for Joomla! File Upload RCE

Creative Contact Form Plugin for WordPress File Upload RCE

Credit Card Disclosure in HTML

Credit Card Disclosure over HTTP

Cross-Referencing Linux (lxr) CGI v Parameter Traversal Arbitrary File Access

csSearch csSearch.cgi setup Parameter Arbitrary Command Execution

CubeCart 'admin.php' Authentication Bypass Information Disclosure

CubeCart < 2.0.5 Multiple Vulnerabilities

CubeCart < 2.0.6 settings.inc.php Multiple Script XSS

CubeCart < 3.0.12 Multiple Vulnerabilities (SQLi, XSS)

CubeCart < 3.0.13 Multiple Remote Vulnerabilities (LFI, SQLi, XSS)

CubeCart <= 2.0.6 Multiple SQL Injections

CubeCart Admin Authentication Bypass

CubeCart Detection

CubeCart FCKeditor connector.php Arbitrary File Upload

CubeCart includes/content/viewProd.inc.php productId Parameter SQL Injection

CubeCart index.php cat\_id Parameter SQL Injection

Custom Pages for Joomla! 'cpage' Parameter Local File Include

CuteNews Debug Info Disclosure

CuteNews Detection

CuteNews flood.db.php Client-IP HTTP Header Arbitrary Code Injection

CuteNews inc/function.php archive Parameter Arbitrary File Access

CuteNews Multiple Script cutepath Parameter Arbitrary Command Execution

CuteNews Multiple Script Traversal Privilege Escalation

CuteNews search.php files\_arch Array Arbitrary File Access

Cuyahoga FCKEditor Misconfiguration Unrestricted File Upload

CVS (Web-Based) Directory Spider

CVS (Web-Based) Entries File Information Disclosure

CVSTrac cgi.c Multiple Overflows

CVSTrac chdir() chroot Jail Escape

CVSTrac CVSROOT/passwd Arbitrary Account Deletion

CVSTrac Database Plaintext Password Storage

CVSTrac Detection

CVSTrac filediff Arbitrary Remote Code Execution

CVSTrac history.c history\_update Function Overflow

CVSTrac Invalid Ticket DoS

CVSTrac Malformed URI Infinite Loop DoS

CVSTrac Text Output Formatter SQL Injection DoS

CVSTrac Ticket Title Arbitrary Command Execution

CVSTrac timeline.c timeline\_page Function Overflow

CVSweb 1.80 cvsweb.cgi Arbitrary Command Execution

CVSweb Detection

CyberArk Password Vault Web Access .NET Object Deserialization

CyberArk Password Vault Web Access .NET Object Deserialization (Direct Check)

CyberArk Password Vault Web Access Detection

Cyberoam Admin Console Detection

Cyberstrong eShop Multiple Script ProductCode Parameter SQL Injection

D-Link 704p Web Interface syslog.htm Malformed Query Remote DoS

D-Link DIR 850L Router Local File Inclusion

D-Link DIR Router Authenication Bypass

D-Link DIR Router Missing Authentication Check

D-Link DIR-300L/600L Remote Command Execution

D-Link DIR-645 getcfg.php Admin Password Disclosure

D-Link Router HNAP GetDeviceSettings Remote Command Execution

DatsoGallery Component for Joomla! sub\_votepic.php User-Agent HTTP Header SQLi

DB4Web Server db4web\_c Filename Request Traversal Arbitrary File Access

DB4Web Server Debug Mode TCP Port Scanning Proxy

DCForum dcboard.cgi Multiple Vulnerabilities

DCP-Portal lib.php root Parameter Remote File Inclusion

DCP-Portal Multiple Script Path Disclosure

DCP-Portal Multiple Scripts SQL Injection

DD-WRT Info.live.htm Information Disclosure

Default Password (changeme) for SHOUTcast Server Service Port

Dell iDRAC Buffer Overflow Vulnerability (CVE-2020-5344)

Dell iDRAC Improper Authorization (DSA-2019-137)

Dell iDRAC Products IPMI Arbitrary Command Injection Vulnerability

Dell iDRAC Products Multiple Vulnerabilities (December 2018)

Dell iDRAC Products Multiple Vulnerabilities (June 2018)

Dell iDRAC Products Multiple Vulnerabilities (Mar 2018)

Dell iDRAC6 / iDRAC7 / iDRAC8 Path Traversal Authentication Bypass

Dell iDRAC6 Multiple Vulnerabilities

Dell Integrated Remote Access Controller (iDRAC) Detection

Dell KACE K1000 < 5.5 Multiple SQL Injection Vulnerabilities

Dell KACE K1000 < 5.5.90547 / 5.4.76849 Arbitrary File Upload and Command Execution

Dell KACE K1000 Web Detection

Dell KACE K2000 < 3.3.52857 Multiple Vulnerabilities

Dell KACE K2000 Web Backdoor Account

Dell KACE K2000 Web Detection

Dell OpenManage Server Administrator 'HelpViewer' Redirect

Dell OpenManage Server Administrator 8.2 ViewFile Directory Traversal

Dell OpenManage Server Administrator Detection

Dell Remote Access Controller Default Password (calvin) for 'root' Account

DeluxeBB Multiple Scripts SQL Injection

DevoyBB Multiple Remote Vulnerabilities (SQLi, XSS)

DevTrack Web Service UserName Field SQL Injection

Digital Scribe login.php SQL Injection

Directory Manager edit\_image.php Arbitrary Command Execution

Directory Pro Traversal Arbitrary File Access

Directory Traversal

Discuz! <= 4.0.0 rc4 Arbitrary File Upload

Disk Savvy HTTP POST Request Handling Remote Stack Buffer Overflow

Disk Sorter HTTP POST Request Handling Remote Stack Buffer Overflow

DNN (DotNetNuke) 3.0.0 < 9.1.0 SWF File Handling XSS

DNN (DotNetNuke) 5.0.0 < 9.2.2 Multiple Vulnerabilities

DNN (DotNetNuke) 5.2.0 < 9.1.1 Multiple Vulnerabilities

DNN (DotNetNuke) 6.0.0 <= 9.3.2 Multiple Vulnerabilities

DNN (DotNetNuke) 6.2.x < 9.0.2 User Profile Information Disclosure

DNN (DotNetNuke) 7.0.0 < 9.3.1 Multiple Vulnerabilities

DNN (DotNetNuke) < 6.2.9 / 7.1.1 Multiple Vulnerabilities

DNN (DotNetNuke) < 7.4.1 Administration Authentication Bypass Vulnerability

DNN (DotNetNuke) < 8.0.1 Multiple Vulnerabilities

DNN (DotNetNuke) < 8.0.4 Multiple Vulnerabilities

DNN (DotNetNuke) Detection

DNN (DotNetNuke) DNNArticle Module categoryid Parameter SQL Injection

DNN (DotNetNuke) Upgrade Process ValidationKey Generation Weakness Privilege Escalation

Docebo GLOBALS Variable Overwrite Remote File Inclusion

Dokeos < 1.6.4 / 2.0.3 Multiple Scripts Remote File Inclusion

Dokeos claro\_init\_local.inc.php extAuthSource Parameter Array Remote File Inclusion

Dokeos main/inc/lib/events.lib.inc.php Referer HTTP Header SQL Injection

DokuWiki ajax.php cmd[del] Parameter Security Bypass

DokuWiki config\_cascade Parameter Remote File Inclusion

DokuWiki Detection

DokuWiki doku.php X-FORWARDED-FOR HTTP Header Arbitrary Code Injection

DokuWiki fetch.php Multiple Parameter imconvert Function Arbitrary Command Execution

DokuWiki Spell Checker Embedded Link Arbitrary PHP Code Execution

Dolibarr Detection

Dolibarr passwordforgotten.php theme Parameter Local File Inclusion

Dolphin Multiple Scripts Remote File Inclusion

dotCMS Multiple Script id Parameter Traversal Local File Inclusion

dotProject docs/ Directory Multiple Script Information Disclosure

dotProject Multiple Scripts Remote File Inclusion

Dragonfly CMS install.php newlang Parameter Local File Inclusion

Dream4 Koobi CMS index.php area Parameter SQL Injection

Drupal 5.x < 5.11 / 6.x < 6.5 Multiple Vulnerabilities (SA-2008-060)

Drupal 6.x < 6.27 / 7.x < 7.18 Multiple Vulnerabilities

Drupal 6.x < 6.28 / 7.x < 7.19 Multiple Vulnerabilities

Drupal 6.x < 6.29 Multiple Vulnerabilities

Drupal 6.x < 6.30 OpenID Module Account Hijacking

Drupal 6.x < 6.31 Forms API Information Disclosure

Drupal 6.x < 6.32 / 7.x < 7.29 Multiple Vulnerabilities

Drupal 6.x < 6.33 / 7.x < 7.31 XML-RPC DoS

Drupal 6.x < 6.34 / 7.x < 7.34 Multiple Vulnerabilities

Drupal 6.x < 6.35 / 7.x < 7.35 Multiple Vulnerabilities

Drupal 6.x < 6.36 OpenID Security Bypass

Drupal 6.x < 6.37 Multiple Vulnerabilities

Drupal 6.x < 6.38 Multiple Vulnerabilities

Drupal 7.0.x < 7.67 / 8.6.x < 8.6.16 / 8.7.x < 8.7.1 Drupal Vulnerability (SA-CORE-2019-007)

Drupal 7.0.x < 7.69 / 8.7.x < 8.7.11 / 8.8.x < 8.8.1 Multiple Vulnerabilities (drupal-2019-12-18)

Drupal 7.x < 7.16 Multiple Vulnerabilities

Drupal 7.x < 7.20 On-Demand Image Derivative Generation Handling Resource Exhaustion DoS

Drupal 7.x < 7.24 Multiple Vulnerabilities

Drupal 7.x < 7.26 Multiple Vulnerabilities

Drupal 7.x < 7.27 Forms API Information Disclosure

Drupal 7.x < 7.32 SQLi

Drupal 7.x < 7.38 Multiple Vulnerabilities

Drupal 7.x < 7.39 Multiple Vulnerabilities

Drupal 7.x < 7.41 Overlay Module Open Redirect

Drupal 7.x < 7.43 Multiple Vulnerabilities

Drupal 7.x < 7.44 / 8.x < 8.1.3 Multiple Vulnerabilities

Drupal 7.x < 7.52 / 8.x < 8.2.3 Multiple Vulnerabilities

Drupal 7.x < 7.56 / 8.x < 8.3.4 Multiple Vulnerabilities (SA-CORE-2017-003)

Drupal 7.x < 7.57 Multiple Vulnerabilities (SA-CORE-2018-001)

Drupal 7.x < 7.58 / 8.3.x < 8.3.9 / 8.4.x < 8.4.6 / 8.5.x < 8.5.1 Remote Code Execution Vulnerability (SA-CORE-2018-002)

Drupal 7.x < 7.59 / 8.4.x < 8.4.8 / 8.5.x < 8.5.3 Remote Code Execution Vulnerability (SA-CORE-2018-004)

Drupal 7.x < 7.60 / 8.5.x < 8.5.8 / 8.6.x < 8.6.2 Drupal Multiple Vulnerabilities (SA-CORE-2018-006)

Drupal 7.x < 7.62 / 8.5.x < 8.5.9 / 8.6.x < 8.6.6 Multiple Vulnerabilities (SA-CORE-2019-001, SA-CORE-2019-002)

Drupal 7.x < 7.66 / 8.5.x < 8.5.15 / 8.6.x < 8.6.15 Multiple Vulnerabilities (drupal-2019-04-17)

Drupal 8.5.x < 8.5.11 / 8.6.x < 8.6.10 Remote Code Execution (SA-CORE-2019-003)

Drupal 8.7.4 Access Bypass Vulnerability (SA-CORE-2019-008) (drupal-2019-07-17)

Drupal 8.7.x < 8.7.12 / 8.8.x < 8.8.4 Drupal Vulnerability (SA-CORE-2020-001) (drupal-2020-03-18)

Drupal 8.x < 8.1.10 Multiple Vulnerabilities

Drupal 8.x < 8.1.7 PHP HTTP\_PROXY Environment Variable Namespace Collision Vulnerability (httpoxy)

Drupal 8.x < 8.2.7 Multiple Vulnerabilities (SA-2017-001)

Drupal 8.x < 8.2.8 / 8.3.x < 8.3.1 Access Bypass Vulnerability (SA-CORE-2017-002)

Drupal 8.x < 8.3.7 Multiple Vulnerabilities (SA-CORE-2017-004)

Drupal 8.x < 8.4.5 Multiple Vulnerabilities (SA-CORE-2018-001)

Drupal 8.x < 8.5.6 Symfony Risky HTTP Header Restriction Bypass Vulnerability (SA-CORE-2018-005)

Drupal Coder Module Deserialization RCE

Drupal Comment Function Arbitrary Code Execution

Drupal Comment Module comment\_form\_add\_preview() Function Arbitrary Code Execution

Drupal Database Abstraction API SQLi

Drupal Multiple Module $\_SESSION Manipulation CAPTCHA Bypass

Drupal PHPUnit/Mailchimp Code Execution Vulnerability

Drupal Public Comment/Posting Arbitrary PHP Code Execution

Drupal Remote Code Execution Vulnerability (SA-CORE-2018-002) (exploit)

Drupal Remote Code Execution Vulnerability (SA-CORE-2019-003) (exploit)

Drupal RESTWS Module Page Callback RCE

Drupal SA-CONTRIB-2009-036: Services Module Key-Based Access Bypass

Drupal SA-CONTRIB-2009-080: Simplenews Statistics Open Redirect

Drupal Software Detection

Drupal Theme System Template Local File Inclusion

Drupal Unspecified Privilege Escalation

Drupal Unsupported Version Detection

Drupal XML-RPC for PHP Remote Code Injection

DUamazon Pro Multiple Scripts SQL Injection

DUclassmate Multiple Scripts SQL Injection

DUforum Multiple Scripts SQL Injection

Dune Web Server GET Request Remote Overflow

Dup Scout HTTP POST Request Handling Remote Stack Buffer Overflow

DUpaypal Pro Multiple Scripts SQL Injection

DUportal Pro Multiple Scripts SQL Injection (2)

DUPortal/DUPortal Pro Multiple Scripts SQL Injection (1)

DUware Multiple Products type.asp iType Parameter SQL Injection

DUware Products Multiple Remote Vulnerabilities (SQLi, XSS)

Dwarf HTTP Server < 1.3.3 Multiple Remote Vulnerabilities (XSS, Disc)

E-theni aff\_liste\_langue.php rep\_include Parameter Remote File Inclusion

e107 BBCode Arbitrary PHP Code Execution

e107 class2.php e107language\_e107cookie Cookie Traversal Local File Inclusion

e107 db.php User Database Disclosure

e107 Detection

e107 download.php extract() Function Variable Overwrite

e107 e107\_cookie Parameter SQL Injection

e107 email.php Arbitrary Mail Relay

e107 ePing Plugin doping.php Arbitrary Code Execution

e107 eTrace Plugin dotrace.php Arbitrary Code Execution

e107 ibrowser.php zend\_has\_del() Function Remote Code Execution

e107 Image Manager Unauthorized File Upload

e107 resetcore.php user Field SQL Injection

e107 search.php search\_info Parameter Traversal Arbitrary File Inclusion

e\_Board index2.cgi message Parameter Traversal Arbitrary File Access

eAccelerator encoder.php File Backup

Easy Address Book Web Server Query Remote Format String

Easy WP SMTP Plugin for WordPress 1.3.9 Unauthenticated Remote Code Execution

EasyDynamicPages Multiple Script edp\_relative\_path Parameter Remote File Inclusion

EasyPHPCalendar Multiple Script serverPath Parameter Remote File Inclusion

EasyWeb FileManager pathtext Traversal Arbitrary File/Directory Access

Eaton Network Shutdown Module < 3.20 Authentication Bypass / Command Execution

Eaton Network Shutdown Module Default Administrator Credentials

Eaton Network Shutdown Module Detection

Eaton Network Shutdown Module view\_list.php paneStatusListSortBy Parameter eval() Call Remote PHP Code Execution

Ecartis HTML Field Manipulation Arbitrary User Password Reset

eclime index.php ref Parameter SQL Injection

eclime login.php SQL Injection

Ecommerce Corp. Online Store Kit 3.0 Multiple Vulnerabilities

EDIMAX Wireless AP Default Password Check

eFiction < 2.0.2 Multiple Remote Vulnerabilities (SQLi, XSS, Disc)

eFront 'langname' Parameter Traversal Local File Inclusion

eFront < 3.6.15.4 Build 18023 Multiple Vulnerabilities

eFront Detection

eFront js/scripts.php 'load' Parameter Remote File Inclusion

eggBlog \_lib/user.php eb\_login Function Cookie Handling SQL Injection

eggBlog index.php eggblogpassword Parameter Cookie SQL Injection

eGroupWare Detection

EGroupWare Multiple Vulnerabilities (SQLi, ID)

eGroupWare spellchecker.php Arbitrary Shell Command Execution

Ektron CMS XslCompiledTransform Class Request Parsing Remote Code Execution

Ektron CMS400.NET Default Credentials

Ektron CMS400.NET Detection

Ektron CMS400.net TransformXslt Web Service Directory Traversal

Ektron CMS400.NET WorkArea/ContentRatingGraph.aspx res Parameter SQL Injection

Elasticsearch 'source' Parameter RCE

Elasticsearch Detection

Elasticsearch Detection (deprecated)

Elasticsearch ESA-2015-06

Elasticsearch ESA-2017-03

Elasticsearch ESA-2017-06

Elasticsearch ESA-2017-09

Elasticsearch ESA-2017-10

Elasticsearch ESA-2017-15

Elasticsearch ESA-2017-18

Elasticsearch ESA-2017-19

Elasticsearch ESA-2018-07

Elasticsearch ESA-2018-10

Elasticsearch ESA-2018-11

Elasticsearch ESA-2018-15

Elasticsearch ESA-2018-16

Elasticsearch ESA-2018-19

Elasticsearch ESA-2019-04

Elasticsearch Groovy Script RCE

Elasticsearch Unrestricted Access Information Disclosure

eLDAPo index.php Plaintext Password Disclosure

Elgg Detection

ELMAH (Error Logging Modules and Handlers) Remotely Accessible

ELOG < 2.6.1 Multiple Remote Vulnerabilities (Traversal, FS)

ELOG Remote Buffer Overflow Vulnerabilities

ELOG Web Logbook < 2.5.7 Multiple Remote Vulnerabilities (OF, Traversal)

ELOG Web LogBook global Denial of Service

eLouai's Force Download Script file Parameter File Disclosure

EMail Security Virtual Appliance Detection

EMail Security Virtual Appliance learn-msg.cgi Remote Code Execution

Embedded HP Web Server Detected

EMC Avamar ADS / AVE Server Detection

EMC Celerra Control Station Default Credentials

EMC Cloud Tiering Appliance User Interface Default Credentials

EMC Cloud Tiering Appliance XML External Entity (XXE) Arbitrary File Disclosure

EMC Data Protection Advisor < 6.4 Multiple Vulnerabilities

EMC Data Protection Advisor < 6.4.110 Database Hardcoded Password Vulnerability

EMC Data Protection Advisor < 6.4.130 Hardcoded Password Vulnerability

EMC Data Protection Advisor Web UI Detection

EMC Data Protection Advisor Web UI Directory Traversal

EMC RSA Archer 6.1.x, 6.2.x, 6.3.x < 6.3.0.7 and 6.4.x < 6.4.0.1 SQL Injection Vulnerability

EMC RSA Archer 6.x < 6.4.10500.1006 Authorization Bypass Vulnerability

EMC RSA Archer < 6.2.0.2 Multiple Vulnerabilities

EMC RSA Archer < 6.2.0.5 Multiple Vulnerabilities

EMC RSA Archer < 6.2.0.8 Multiple Vulnerabilities

EMC RSA Archer < 6.4.1.5 / 6.5.x < 6.5.0.2 Multiple Vulnerabilities

EMC RSA Archer WebUI Detection

EMC RSA Authentication Manager < 8.1 SP1 Patch 14 Multiple Vulnerabilities

EMC RSA Authentication Manager < 8.2 SP1 Patch 2 Self-Service Console Brute-force PIN Disclosure (ESA-2017-084)

EMC RSA Authentication Manager < 8.2 SP1 Patch 5 Reflected Cross-Site Scripting (ESA-2017-134)

EMC RSA Authentication Manager < 8.2 SP1 Patch 6 Stored Cross-Site Scripting (ESA-2017-152)

EMC RSA Authentication Manager < 8.2 SP1 Patch 7 Security Console Unspecified Blind SQL Injection (ESA-2018-002)

EMC RSA Authentication Manager < 8.3 Patch 1 Multiple Vulnerabilities (DSA-2018-086)

EMC RSA Authentication Manager < 8.3 Patch 3 Multiple Vulnerabilities (DSA-2018-152)

EMC RSA Authentication Manager < 8.4 P1 Insecure Credential Management (DSA-2019-038)

EMC RSA Authentication Manager < 8.4 P10 Multiple Vulnerabilites (DSA-2020-052)

EMC RSA Authentication Manager < 8.4 Patch 8 XSS (DSA-2019-168)

EMC RSA Authentication Manager < 8.4 Relative Path Traversal (DSA-2018-226)

EMC Solutions Enabler Virtual Appliance 8.x < 8.3.0 RCE

EMC Solutions Enabler Virtual Appliance < 8.4.0.15 Authentication Bypass Vulnerability

EMC Unisphere for VMAX Virtual Appliance 8.x < 8.3.0 RCE

EMC Unisphere for VMAX Virtual Appliance < 8.4.0.15 Authentication Bypass Vulnerability

EMC vApp Manager Default Credentials

EMC vApp Manager Detection

EMC VMAX VASA Provider Virtual Appliance < 8.4.0 File Upload RCE

EMC VMAX VASA Provider Virtual Appliance < 8.4.0.512 Authentication Bypass Vulnerability

EMC VMAX VASA Provider Virtual Appliance File Upload RCE

Emulive Server4 Authentication Bypass

Emumail WebMail Multiple Remote Vulnerabilities (XSS, Disc)

Episodex Guestbook Multiple Vulnerabilities (Auth Bypass, XSS)

Ericom AccessNow Server < 3.3.1.4095 Stack-Based Buffer Overflow

Ericom AccessNow Server Detection

eScan MWAdmin forgotpassword.php uname Parameter Arbitrary Command Execution

eScan MWAdmin Interface Detection

Etomite CMS index.php id Parameter SQL Injection

Eucalyptus Cloud Controller Console Detection

Eucalyptus Walrus Detection

Eucalyptus Walrus REST Interface Key Verification Authentication Bypass (ESA-03)

Eventing Component for Joomla! 'catid' Parameter SQLi

Excite for Web Server architext\_query.pl Shell Metacharacter Arbitrary Command Execution

Exhibit Engine list.php Multiple Parameter SQL Injection

Exhibit Engine styles.php toroot Parameter Remote File Inclusion

ExoPHPDesk faq.php id Parameter SQL Injection

Exponent CMS < 0.96.4 Multiple Remote Vulnerabilities (XSS, SQLi, Code Exe, Disc)

Exponent CMS index.php view Parameter Local File Inclusion

Exponent CMS Multiple Script pathos\_core\_version Parameter Path Disclosure

Expose for Joomla! File Upload RCE

ExtCalendar 'cat\_id' parameter SQL Injection

ExtCalendar Detection

Extent RBS Web Server Image Parameter Traversal Arbitrary File Access

ExtremeZ-IP File and Print Server Zidget/HTTP Server Traversal Arbitrary File Access

eXtropia Web Store web\_store.cgi Traversal Arbitrary File Access

EyeOS file Parameter Directory Traversal

eZ Publish settings/site.ini Configuration Disclosure

EZPhotoSales Multiple Configuration Files Remote Information Disclosure

EZPZ One Click Backup Plugin for WordPress 'cmd' Parameter Remote Command Execution

EZShopper Multiple Directory Traversal Vulnerabilities

EZsite Forum Discloses Passwords to Remote Users

ezUpload <= 2.2 Multiple Remote Vulnerabilities (SQLi, RFI, LFI)

F-Secure Internet Gatekeeper Default Administrator Credentials

F-Secure Internet Gatekeeper for Linux Log Disclosure (FSC-2011-1)

F-Secure Internet Gatekeeper Web Console Detection

F-Secure Policy Manager Path Disclosure

F5 BIG-IP Web Management Interface Version

F5 BIG/ip bigconf.cgi file Parameter Arbitrary File Access

F5 Networks ARX Data Manager Unsupported Version Detection

F5 Networks ARX Data Manager Web Interface Detection

F5 Networks BIG-IP : BIG-IP Virtual Server HTTP Explicit Proxy / SOCKS Profile RCE (SOL35520031) (uncredentialed check)

F5 Networks BIG-IP Web Interface Default Credential Check

F5 Networks BIG-IQ Configuration Utility Login Page Detection

F5 Networks BIG-IQ Configuration Utility Privilege Escalation

F5 Networks BIG-IQ REST API Authentication Bypass (SOL16861)

FAQManager 'faqmanager.cgi' 'toc' Parameter Arbitrary File Access

FCKeditor 'CurrentFolder' Arbitrary File Upload

FCKeditor for PHP-Nuke Arbitrary File Upload

FCKeditor on Apache connector.php Crafted File Extension Arbitrary File Upload

FCKeditor upload.php Type Parameter Arbitrary File Upload

FCKeditor.Java Connector Servlet 'CurrentFolder' Infinite Loop DoS

Fedora Directory Server Crafted IFRAME adm.conf Admin Server Password Disclosure

Feedsplitter <= 2006-01-21 Multiple Remote Vulnerabilities (XSS, Traversal, Disc)

FireEye Web MPS GUI Detection

Firefly Media Server Limited Directory Traversal Admin Credential Disclosure

FireStats < 1.6.2 Multiple Vulnerabilities

FireStats Detection

Flask < 0.12.3 Denial of Service Vulnerability

FlatNuke < 2.5.6 Multiple Remote Vulnerabilities

FlatNuke index.php id Parameter Traversal Arbitrary File Access

FlatNuke index.php url\_avatar Field Arbitrary PHP Code Execution

FlexCast Server Terminal Authentication Unspecified Remote Issue

FlexCMS Login Cookie SQL Injection

Flexera InstallShield Untrusted Search Path Vulnerability

Flickr Gallery Plugin for WordPress < 1.5.3 PHP Object Injection

Floating Social Media Links Plugin for WordPress 'wpp' Parameter Remote File Inclusion

Flyspeck lang Parameter Local File Inclusion

Flyspray install-0.9.7.php adodbpath Parameter Remote File Inclusion

FogBugz Interface Detection

Foreman Smart-Proxy TFTP Detection

Foreman Smart-Proxy TFTP Remote Command Injection

Fortify 360 Web Interface Detection

Fortinet FortiAnalyzer / FortiManager 5.4.x < 5.4.3 Open Redirect (FG-IR-17-014)

Fortinet FortiAnalyzer 5.0.x < 5.0.3 LDAP Authentication Bypass

Fortinet FortiAnalyzer 5.0.x < 5.0.8 Alert Email Plaintext Password Disclosure

Fortinet FortiAnalyzer < 4.3.7 / 5.0.5 Multiple XSRF

Fortinet FortiAuthenticator Appliance Web Interface Detection

Fortinet FortiAuthenticator Default Credentials

Fortinet FortiGate Web Console Management Detection

Fortinet FortiMail < 4.3.7 / 5.0.x < 5.0.2 Fragmented IPv6 Packet Handling DoS

Fortinet FortiMail < 5.0.9 / 5.1.6 / 5.2.4 HTTP Debug Information Disclosure

Fortinet FortiOS User Interface Default Credentials

Fortinet FortiOS Web Interface Cookie Parser RCE (EGREGIOUSBLUNDER)

Fortinet FortiWeb 4.x / 5.x < 5.0.3 Multiple Vulnerabilities

Fortinet FortiWeb < 5.2.0 Multiple XSRF Vulnerabilities

Fortinet FortiWeb < 5.3.5 Multiple Vulnerabilities

Forum51/Board51/News51 Users Disclosure

Forums Plugin for WordPress 'url' Parameter Arbitrary File Disclosure

Foscam 11.37.2.x < 11.37.2.49 Directory Traversal

Foscam Detection

Foswiki < 1.1.8 MAKETEXT Macro Arbitrary Code Injection

Foswiki Detection

Foxweb foxweb.exe / foxweb.dll Long URL Remote Overflow

Free Articles Directory index.php page Parameter Remote File Inclusion

FreeNAS 'exec\_raw.php' Arbitrary Command Execution

FreeNAS Web Detection

FreeNAS WebGUI Blank Password

FreePBX / PBXconfig Default Credentials

FreePBX /recordings/index.php 'ari\_auth' Cookie Authentication Bypass

FreePBX admin/cdr/call-comp.php 'dst' Parameter SQLi

FreePBX Backup Module page.backup.php 'dir' Parameter RCE

FreePBX Detection

FreePBX gen\_amp\_conf.php Information Disclosure

Freestyle Support Portal Component for Joomla! 'prodid' Parameter SQLi

Freestyle Testimonials Component for Joomla! Unspecified SQLi

FTGate <= 4.4.002 Multiple Remote Vulnerabilities (OF, FS, XSS)

FtpLocate flsearch.pl fsite Parameter Remote File Inclusion

FUDforum < 2.7.1 Avatar Upload Extension Validation Weakness Arbitrary Code Execution

Fuji Xerox Printing Systems (FXPS) Print Engine Crafted Request HTTP Authentication Bypass

FuseTalk Detection

FuseTalk index.cfm txForumID Parameter SQL Injection

Fusion News comments.php X-Forwarded-For HTTP Header Arbitrary Code Injection

fuzzylime (cms) comssrss.php files[] Parameter Traversal Local File Inclusion

Gallery 3.0.x < 3.0.7 Multiple Vulnerabilities

Gallery 3.0.x < 3.0.9 Multiple Vulnerabilities

Gallery < 2.0.3 IP Spoofing

Gallery < 3.0.5 Multiple Vulnerabilities

Gallery Detection

Gallery HTTP Global Variables File Inclusion

Gallery includedir Parameter Remote File Inclusion

Gallery index.php GALLERY\_BASEDIR Parameter Remote File Inclusion

Gallery init.php Authentication Bypass

Gallery Install Log Local Information Disclosure

Gallery main.php g2\_itemId Parameter Traversal Arbitrary File Access

Gallery Plugin for WordPress 'load' Parameter Remote File Inclusion

Gallery PostNuke Integration Access Validation Privilege Escalation

Gallery save\_photos.php Arbitrary Command Execution

Gallery stepOrder Parameter Local File Inclusion

Gallery Unspecified HTML Injection

Gallery Zipcart Module Arbitrary File Disclosure

GCalendar Component for Joomla! 'gcid' Parameter SQLi

gCards < 1.46 Multiple Vulnerabilities

GD Star Rating Plugin for WordPress 'export.php' Authentication Bypass Information Disclosure

Geeklog < 1.3.11sr4 / 1.4.0sr1 Multiple Remote Vulnerabilities (LFI, SQLi)

Geeklog <= 1.3.7sr1 Multiple Vulnerabilities (SQLi, XSS, Priv Esc)

Geeklog auth.inc.php loginname Parameter SQL Injection

Geeklog Detection

Geeklog lib-sessions.php Session Cookie Handling Authentication Bypass

Geeklog Multiple Script \_CONF[path] Parameter Remote File Inclusion

Geeklog SEC\_authenticate Function SQL Injection

Geeklog User Comment Retrieval SQL Injection

Geronimo Console Default Credentials

getID3 < 1.7.8-b1 Multiple Remote Vulnerabilities

GForge CVSWeb CGI cvsweb.php PATH\_INFO Parameter Arbitrary Command Execution

GForge Detection

GForge Multiple Script Traversal Arbitrary Directory Listing

GForge top/topusers.php offset Parameter SQL Injection

gigCalendar Component for Joomla! 'gigcal\_gigs\_id' Parameter SQLi

GIT gitweb git\_search Shell Metacharacter Arbitrary Command Execution

GIT gitweb git\_snapshot / git\_object Shell Metacharacter Arbitrary Command Execution

Git Repository Served by Web Server

GitHub Enterprise Management Console RCE

Glimpse HTTP aglimpse Arbitrary Command Execution

GMaps Component for Joomla! 'mapId' Parameter SQLi

GNU Bash Environment Variable Handling Code Injection (Shellshock)

GNU Bash Incomplete Fix Remote Code Injection (Shellshock)

GNU Mailman Multiple Unspecified Remote Vulnerabilities

GNUMP3d < 2.9.6 Multiple Remote Vulnerabilities (XSS, Traversal)

GoAhead Server CGI Remote Code Execution

GoAhead System.ini Leak

Google Analytics on An Internal Web Server Detection

Google Doc Embedder Plugin for WordPress 'File' Parameter Traversal Arbitrary File Disclosure

Google Search Appliance proxystylesheet Parameter Multiple Remote Vulnerabilities (XSS, Code Exec, ID)

Goollery < 0.04b Multiple Vulnerabilities

GOsa Multiple Script plugin Parameter Remote File Inclusion

GoScript go.cgi Arbitrary Command Execution

GoSmart Message Board Multiple Vulnerabilities (SQLi, XSS)

Grails resources plug-in WEB-INF / META-INF File Disclosure

GRAND Flash Album Gallery Plugin for WordPress 'f' Parameter Traversal Arbitrary Directory Enumeration

Grandstream Phone Web UI Information Disclosure

Gravity Board X <= 1.1 Multiple Vulnerabilities (SQLi, XSS, PD, Cmd Exe)

Graylog2 Default Credentials

Graylog2 LDAP Authentication Bypass Vulnerability

Graylog2 Web Interface Detection

Greenstone Detection

Greenstone Password File Disclosure

Gregarius ajax.php rsargs[] Parameter Array SQL Injection

Greymatter 1.3 Multiple Vulnerabilities

GroundWork Monitor Enterprise Default Credentials

GroundWork Monitor Enterprise Detection

GroundWork Monitor Enterprise Foundation Webapp Admin Arbitrary File Access

GroundWork Monitor Enterprise Foundation Webapp Admin Interface Authentication Bypass

GTcatalog index.php custom Parameter Remote File Inclusion

GTcatalog password.inc Direct Request Password Disclosure

Guestbook tr3.a Password Disclosure

GuppY < 4.5.6a Multiple Vulnerabilities

GuppY <= 4.5.9 Multiple Remote Vulnerabilities (Traversal, Code Exec)

GuppY inc/includes.inc selskin Parameter Traversal Local File Inclusion

Gurock TestRail Detection

GWExtranet gwextranet/scp.dll Multiple Parameter Traversal Local File Inclusion

Halon Security Router < 3.2r2 Multiple Vulnerabilities

Halon Security Router User Interface Default Credentials

HAMweather Template.php do\_parse\_code Function Arbitrary Code Execution

HappyMall Multiple Script Arbitrary Command Execution

HAProxy Statistics Page Detection

Hashicorp Consul Web UI and API access

HastyMail HTML Attachment Script Execution

Help Center Live class/auth.php check\_logout Function Admin Authentication Bypass

Help Center Live module.php file Parameter Local File Inclusion

Help Center Live Multiple Remote Vulnerabilities (Cmd Exec, XSS)

Help Center Live Multiple Vulnerabilities (SQLi, XSS, CSRF)

Help Center Live osTicket Module Multiple Unspecified SQL Injections

Hikvision IP Camera Remote Authentication Bypass

HIS AUktion auktion.cgi Traversal Arbitrary Command Execution

Home Free search.cgi Traversal Arbitrary File Access

HooToo HT-TM06 TripMate Elite Web Server 'protocol.csp' HTTP Cookie Header Handling RCE

Horde 3.3.12 open\_calendar.js Backdoor

Horde Admin Account Default Password

Horde Chora CVS Viewer diff Utility Arbitrary Command Execution

Horde Chora Software Detection

Horde go.php url Parameter Arbitrary File Access

Horde Help Viewer Arbitrary Code Execution

Horde Horde\_Image::factory driver Argument Local File Inclusion

Horde IMP mailbox.php3 Multiple Parameter SQL Injection

Horde Imp Webmail status.php3 message Parameter XSS

Horde Ingo Software Detection

Horde Kronolith Detection

Horde Mnemo Detection

Horde Nag Detection

Horde Software Detection

Horde test.php Direct Reqest Information Disclosure

Horde Turba Detection

Horde Turba status.php Path Disclosure

Hosting Controller < 6.1 Hotfix 2.1 Multiple Vulnerabilities

Hosting Controller < 6.1 Hotfix 2.2 Multiple Vulnerabilities

Hosting Controller <= 6.1 Hotfix 2.2 Multiple Vulnerabilities

Hosting Controller <= 6.1 Hotfix 2.3 Information Disclosure Vulnerabilities

Hosting Controller <= 6.1 Hotfix 3.1 Authenticated User Privilege Escalation

Hosting Controller addsubsite.asp Security Bypass

Hosting Controller HCDiskQuoteService.csv Direct Request Information Disclosure

Hosting Controller hosting/addreseller.asp reseller Parameter Authentication Bypass

Hosting Controller Multiple Script Arbitrary Directory Browsing

Hosting Controller Multiple Script ForumID Parameter SQL Injection

Hosting Controller Software Detection

HotNews Multiple Script Remote File Inclusion

HotOpentickets Privilege Escalation

HP ArcSight Logger HTTP Detection

HP AutoPass License Server Detection

HP AutoPass License Server Remote Code Execution (HPSBMU03045)

HP Client Automation Default Credentials

HP Client Automation Satellite Web Console Detection

HP Client Automation Web Console Detection

HP Data Protector DPNECentral Web Service Detection

HP Data Protector LogClientInstallation Method Userid Field SQL Execution

HP Database Archiving Software Detection

HP DDMI on Windows Unspecified Remote Agent Access

HP DDMI Web Interface Default Credentials

HP DesignJet Accounting.xls Information Disclosure Vulnerability

HP Diagnostics Server Default Credentials

HP Diagnostics Server Detection

HP iLO 2 <= 2.23 DoS

HP iLO 4 <= 2.52 RCE

HP Instant TopTools hpnst.exe CGI DoS

HP Integrated Lights-Out (iLO) Default Credentials

HP LaserJet Pro /dev/save\_restore.xml Administrative Password Disclosure

HP LaserJet Pro /IoMgmt/Adapters/wifi0/WPS/Pin WPS PIN Disclosure

HP LaserJet Web Server Unspecified Admin Component Traversal Arbitrary File Access

HP Managed Printing Administration < 2.6.4 Multiple Vulnerabilities

HP Managed Printing Administration Detection

HP Managed Printing Administration jobDelivery Script Directory Traversal (intrusive check)

HP Network Automation 10.0x < 10.00.023 / 10.1x < 10.11.06 / 10.2x < 10.21.05 / 10.3x < 10.30.03 / 10.4x < 10.40.01 / 10.5x < 10.50.01 Multiple Vulnerabilities

HP Network Automation 9.22.0x / 10.00.0x < 10.00.02 Multiple RCE

HP Network Automation 9.x, 10.x < 10.00.022 / 10.1x.x < 10.11.03 / 10.20.x < 10.21.01 Multiple Vulnerabilities

HP Network Automation Detection

HP Network Automation Multiple Remote Vulnerabilities (HPSBMU03264)

HP Network Automation Multiple Vulnerabilities (HPSBMU02693)

HP Network Automation RMI Registry Java Object Deserialization RCE

HP Network Automation RPCServlet Java Object Deserialization RCE

HP Network Node Manager Detection

HP Network Node Manager i (NNMi) Console Detection

HP Network Node Manager i < 10.20 Multiple Vulnerabilities

HP Onboard Administrator Detection

HP Onboard Administrator Multiple Vulnerabilities

HP OneView < 1.10 OpenSSL Multiple Vulnerabilities (HPSBGN03068)

HP OneView Detection

HP OneView Unspecified Remote Privilege Escalation (HPSBGN03034)

HP OpenView Client Configuration Manager Default Credentials

HP OpenView Network Node Manager Multiple CGI Remote Overflows

HP OpenView Network Node Manager Multiple Scripts hostname Parameter Remote Command Execution

HP OpenView Network Node Manager Multiple Scripts Remote Command Execution

HP OpenView Network Node Manager OpenView5.exe Action Parameter Traversal Arbitrary File Access

HP OpenView Network Node Manager ovlaunch.exe Information Disclosure (c01661610)

HP OpenView Network Node Manager Remote Execution of Arbitrary Code (HPSBMA02621 SSRT100352)

HP OpenView Network Node Manager webappmon.exe Command Injection (c01661610)

HP OpenView Performance Insight Server Backdoor Account

HP OpenView Performance Insight Server Detection

HP Operations Manager i Apache Flex BlazeDS External Entity Injection Vulnerability

HP Operations Orchestration 10.x < 10.22.001 XSRF

HP Operations Orchestration 10.x < 10.51 Java Object Deserialization RCE

HP Operations Orchestration 10.x < 10.70 wsExecutionBridgeService Servlet Java Object Deserialization RCE

HP Operations Orchestration 10.x < 10.80 Remote Code Execution

HP Operations Orchestration 10.x Authentication Bypass

HP Operations Orchestration 10.x Remote Information Disclosure

HP Operations Orchestration wsExecutionBridgeService Servlet Java Object Deserialization RCE

HP Power Manager < 4.2.10

HP Power Manager < 4.3.2

HP Power Manager Default Credentials

HP Power Manager Detection

HP Power Manager Unspecified Cross-Site Request Forgery

HP Service Manager 9.30.x / 9.31.x / 9.32.x / 9.33.x / 9.34.x / 9.35.x < 9.35.6007 / 9.40.x / 9.41.x < 9.41.6000 / 9.50.x / 9.51.x Remote SQL Injection

HP SiteScope 11.1x < 11.13 or 11.2x < 11.24 IP3 Remote Privilege Escalation

HP SiteScope Default Credentials

HP SiteScope Detection

HP SiteScope getFileInternal Arbitrary File Download

HP SiteScope Log Analysis Tool Remote Privilege Escalation (credentialed check)

HP SiteScope Log Analysis Tool Remote Privilege Escalation (uncredentialed check)

HP SiteScope Multiple Unspecified Remote Code Execution Vulnerabilities

HP SiteScope Multiple Vulnerabilities (HPESBGN03763)

HP SiteScope SOAP Call runOMAgentCommand SOAP Request Arbitrary Remote Code Execution

HP SiteScope SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

HP SiteScope Unspecified Authentication Bypass

HP Smart Update Manager 6.x < 6.4.1 Multiple Vulnerabilities

HP Smart Update Manager Detection

HP Smart Update Manager Remote Unauthorized Access.

HP Smart Update Manager Remote Unauthorized Access.

HP System Management Homepage (SMH) on Windows Namazu lang Parameter Traversal Arbitrary File Access

HP System Management Homepage < 3.0.1.73 Multiple Flaws

HP Systems Insight Control Detection

HP Systems Insight Dynamics Detection

HP Systems Insight Manager Detection

HP Systems Insight Manager logfile Parameter Arbitrary File Download

HP Systems Insight Manager Multiple Products Authentication Bypass

HP Systems Insight Manager Namazu lang Parameter Traversal Arbitrary File Access

HP UCMDB Server BeanUtils Java Deserialization RCE

HP UCMDB Server Java Deserialization RCE

HP Universal Configuration Management Database Data Flow Probe Gateway Cross-Site Tracing

HP Universal Configuration Management Database Data Flow Probe Gateway Detection

HP Universal Configuration Management Database Server Authentication Bypass

HP Universal Configuration Management Database Server Detection

HP Web JetAdmin <=7.0 Multiple Vulnerabilities (XSS, Code Exe, DoS, more)

HP Web Jetadmin Detection

HP Web JetAdmin setinfo.hts setinclude Parameter Traversal Arbitrary File Access

HP WebInspect REST API Unauthorized Access

HPE Moonshot Provisioning Manager < 1.22 Multiple Vulnerabilities

ht://Dig < 3.1.5 htsearch CGI Multiple Vulnerabilities

ht://Dig htsearch Multiple Vulnerabilities

htgrep hdr Parameter Arbitrary File access

HTTP Cookie 'secure' Property Transport Mismatch

HTTP Origin Response Header Usage

Huawei Multiple Device Authentication Bypass

Hunt CCTV DVR.cfg Direct Request Information Disclosure

Huru Helpdesk Component for Joomla! 'cid[0]' Parameter SQLi

HylaFAX faxsurvey Arbitrary Command Execution

Hyperic HQ Web GUI Default Credentials

Hyperic HQ Web GUI Detection

i-Gallery <= 3.3 Multiple Vulnerabilities

iBill ibillpm.pl Password Generation Weakness

IBM BigFix Remote Control < 9.1.3 Multiple Vulnerabilities (SWEET32)

IBM BigFix Remote Control < 9.1.4 Authentication Bypass

IBM BigFix Remote Control Detection

IBM Blade Center Advanced Management Console Detection

IBM DB2 Content Manager eClient < 8.4.1.1 Unspecified Security Vulnerability

IBM DB2 Content Manager eClient Detection

IBM Domino Web Administrator Multiple Vulnerabilities

IBM Endpoint Manager Enrollment and Apple iOS Management Extender Detection

IBM Endpoint Manager Mobile Device Management Component Unauthenticated Remote Code Execution (swg21691701)

IBM HTTP Server on AS/400 Trailing Slash Source Code Disclosure

IBM InfoSphere Data Replication Dashboard Default Credentials

IBM InfoSphere Data Replication Dashboard Detection

IBM InfoSphere Data Replication Dashboard Unpassworded User Enumeration

IBM InfoSphere Data Replication Dashboard User Enumeration

IBM InfoSphere IGC Multiple Vulnerabilities

IBM InfoSphere Information Governance Catalog Detection

IBM Jazz Team Server Detection

IBM Jazz Team Server Session Cookie Information Disclosure

IBM Lotus Domino Server time/date Fields Remote Overflow

IBM Net.Commerce orderdspc.d2w order\_rn Option SQL Injection

IBM Network Security Protection XGS Default Credentials

IBM Network Security Protection XGS Remote Code Execution (swg21690823) (credentialed attack)

IBM OpenAdmin Tool welcomeService.php Remote Code Execution

IBM Rational ClearQuest Multiple Script Information Disclosure

IBM Rational ClearQuest Web Client Detection

IBM Rational Focal Point Default Credentials

IBM Rational Focal Point Login Detection

IBM Rational Focal Point Login Servlet File Disclosure

IBM Rational Focal Point RequestAccessController Servlet File Disclosure

IBM Rational License Key Server Administration and Reporting Tool 8.1.4.x < 8.1.4.4 Multiple Vulnerabilities

IBM Rational License Key Server Administration and Reporting Tool Default Credentials

IBM Rational License Key Server Administration and Reporting Tool Detection

IBM Storwize Web Management Interface Detection

IBM Tivoli Directory Server Web Administration Tool Detection

IBM Tivoli Endpoint Manager Server < 8.2.1372 Multiple Vulnerabilities

IBM Tivoli Monitoring Service Console Detection

IBM WebSphere Application Server '%20' Request Source Disclosure

IBM WebSphere Application Server Malformed Host Header JSP Source Disclosure

IBM WebSphere Application Server navigateTree.do Multiple Vulnerabilities

IBM Websphere Commerce Database Update Information Disclosure

IBM WebSphere Commerce ResetPassword Servlet Caching Information Disclosure

IBM WebSphere Portal (swg22008586)

IBM WebSphere Portal 6.1.0.x < 6.1.0.6 CF27 Multiple Vulnerabilities

IBM WebSphere Portal 6.1.5.x < 6.1.5.3 CF27 Multiple Vulnerabilities

IBM WebSphere Portal 7.0.0.x < 7.0.0.2 CF28 Multiple Vulnerabilities

IBM WebSphere Portal 7.0.0.x < 7.0.0.2 CF29 Multiple Vulnerabilities

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF14 Multiple Vulnerabilities

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF15 / 8.5.0.0 < 8.5.0.0 CF05 Multiple XSRF / XSS (PI34987, PI33329, PI35228)

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF15 Multiple Vulnerabilities

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF17 Multiple Vulnerabilities

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF19 PI51395 and PI53426 Multiple Vulnerabilities

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF20 Multiple Vulnerabilities

IBM WebSphere Portal 8.0.0.x < 8.0.0.1 CF21 Multiple Vulnerabilities

IBM WebSphere Portal 8.0.0.x Unified Task List Portlet Multiple Vulnerabilities (PI18909)

IBM WebSphere Portal 8.5.0 < 8.5.0 CF01 Open Redirect

IBM WebSphere Portal 8.5.0 < 8.5.0 CF02 Multiple Vulnerabilities

IBM WebSphere Portal 8.5.0 < 8.5.0 CF03 Multiple Vulnerabilities

IBM WebSphere Portal 8.5.0 < 8.5.0 CF06 Multiple Vulnerabilities

IBM WebSphere Portal 8.5.0 CF08 - CF10 < 8.5.0 CF11 PA\_Theme\_Creator Application XSRF

IBM WebSphere Portal 8.5.0.0 < 8.5.0.0 CF10 Multiple Vulnerabilities

IBM WebSphere Portal 8.x < 8.0.0.1 CF12 Multiple Vulnerabilities

IBM WebSphere Portal 8.x < 8.0.0.1 CF13 Multiple Vulnerabilities

IBM WebSphere Portal AccessControl REST API Information Disclosure (PI51395)

IBM WebSphere Portal Active Content Filtering XSS (PI38732)

IBM WebSphere Portal Apache Commons FileUpload DoS

IBM WebSphere Portal Apache Struts ClassLoader Manipulation RCE

IBM WebSphere Portal CKEditor XSS (PI24992, PI26456)

IBM WebSphere Portal Cross-Site Redirection

IBM WebSphere Portal Dojo Module Arbitrary File Download

IBM WebSphere Portal Dojo Module URI Traversal Arbitrary File Access

IBM WebSphere Portal Entity Expansion DoS (PI24622)

IBM WebSphere Portal Error Codes Information Disclosure (PI21858)

IBM WebSphere Portal File Upload Temporary File Handling Remote DoS

IBM WebSphere Portal Improper Access Control Checks (PI07185)

IBM WebSphere Portal Information Disclosure

IBM WebSphere Portal Information Disclosure Vulnerability (CVE-2017-1423)

IBM WebSphere Portal Information Disclosure Vulnerability (PI27710)

IBM WebSphere Portal JCR Information Disclosure (PI36150)

IBM WebSphere Portal Multiple Vulnerabilities (PI37356, PI37661)

IBM WebSphere Portal Multiple Vulnerabilities (swg21976358)

IBM WebSphere Portal Open Redirect Vulnerability (CVE-2018-1736)

IBM WebSphere Portal Open Redirect Vulnerability (PI15689)

IBM WebSphere Portal Open Redirect Vulnerability (PI19877)

IBM WebSphere Portal Oracle Outside In Technology Component Remote DoS (PI10280)

IBM WebSphere Portal Outside In Technology Multiple Overflows (PI07290)

IBM WebSphere Portal Registration/Edit My Profile Portlet Unrestricted Remote File Upload (PI07013)

IBM WebSphere Portal Security Bypass Vulnerability (CVE-2018-1420)

IBM WebSphere Portal Security Bypass Vulnerability (CVE-2018-1672)

IBM WebSphere Portal Unauthorized User Directory Access

IBM WebSphere Portal Unspecified DoS (PI15692)

IBM WebSphere Portal Unspecified DoS (PI16462)

IBM WebSphere Portal Unspecified DoS (PI50952)

IBM WebSphere Portal Unspecified HTTP Response Splitting (PM85071)

IBM WebSphere Portal Unspecified Open Redirect (PI38632)

IBM WebSphere Portal Unspecified Reflected XSS (PI30620)

IBM WebSphere Portal Unspecified URL Manipulation Arbitrary File Access (PM99205)

IBM WebSphere Portal Unspecified Vulnerability (PI25993)

IBM WebSphere Portal Web Content Viewer Portlet Privilege Escalation (PI15723)

IBM WebSphere snoopservlet Path Disclosure

IBProArcade index.php Arcade Module gameid Parameter SQL Injection

icat carbo.dll icatcommand Parameter Traversal Arbitrary File Access

Icecast Encoded Traversal Arbitrary File Access

Icecast list\_directory Function Traversal File/Directory Enumeration

Icecast MP3 Client HTTP GET Request Remote Overflow

Icecast XSL Parser Multiple Vulnerabilities (OF, ID)

IceWarp /rpc/gw.html XML External Entity Arbitrary File Disclosure

IceWarp Merak WebMail Server < 9.4.2 Multiple Vulnerabilities

IceWarp Multiple Script Remote File Inclusion

IceWarp Web Mail Multiple Flaws (1)

IceWarp Web Mail Multiple Flaws (2)

IceWarp Web Mail Multiple Flaws (3)

IceWarp Web Mail Multiple Flaws (4)

IceWarp Webmail raw.php Information Disclosure

IceWarp webmail/basic/index.html \_c Parameter Directory Traversal

ICQ Web Front Service guestbook.cgi DoS

IdeaBox include.php ideaDir Parameter Remote File Inclusion

IdealBB < 1.5.4b Multiple Vulnerabilities (XSS, SQLi, Upload, Traversal)

IdealBB Multiple Vulnerabilities (XSS, SQLi, more)

IDoBlog Component for Joomla! 'userid' Parameter SQLi

Ignite Gallery Component for Joomla! 'gallery' Parameter SQLi

IIS 5.x Alternate Data Stream Authentication Bypass

iisPROTECT Admin Interface SiteAdmin.ASP GroupName Parameter SQL Injection

iisPROTECT Encoded URL Authentication Bypass

iisPROTECT Unpassworded Administrative Interface

Ikonboard FUNC.pm lang Cookie Arbitrary Command Execution

Ikonboard ikonboard.cgi Multiple Parameter SQL Injection

iLO 2 2.29 Remote Code Execution Vulnerability

iLO 2 < 2.27 / iLO 3 < 1.82 / iLO 4 < 2.10 Denial of Service Vulnerability

iLO 2 <= 2.23 Denial of Service Vulnerability

iLO 3 < 1.50 / iLO 4 < 1.13 Information Disclosure Vulnerability

iLO 3 < 1.57 / iLO 4 < 1.22 Unspecified Arbitrary Code Execution

iLO 3 < 1.65 / iLO 4 < 1.32 Multiple Vulnerabilities

iLO 3 < 1.65 / iLO 4 < 1.32 Multiple Vulnerabilities

iLO 3 < 1.85 / iLO 4 < 2.22 Denial of Service Vulnerability

iLO 3 < 1.88 / iLO 4 < 2.44 XSS Vulnerability

iLO 3 < 1.88 Information Disclosure Vulnerability

iLO 3 < 1.90 / iLO 4 < 2.61 / iLO 5 < 1.35 Remote Code Execution Vulnerability (HPESBHF03866)

iLO 4 < 2.53 Remote Code Execution Vulnerability

iLO 4 < 2.60 / iLO 5 < 1.30 Multiple Vulnerabilities

iLO 4 < 2.70 / iLO 5 < 1.40a Multiple Vulnerabilities

iLO 5 < 1.40 Cross Site Scripting (XSS) Vulnerability

IlohaMail < 0.8.14RC1 Unspecified Vulnerability

IlohaMail Attachment Arbitrary File Create/Overwrite

IlohaMail Configuration Scripts Remote Disclosure

IlohaMail Forged GET/POST Arbitrary Contacts Deletion

IlohaMail index.php init\_lang Parameter Arbitrary File Access

IlohaMail index.php session Parameter Arbitrary File Access

IlohaMail Multiple Configuration Files Remote Information Disclosure

IlohaMail Multiple External Programs Arbitrary Command Execution

IlohaMail Software Detection

IlohaMail Unspecified Database Password Disclosure Weakness

ImageFolio Default Password

imageVue < 16.2 admin/upload.php Unrestricted File Upload

IMP Software Detection

ImpressPages cm\_group Parameter Remote PHP Code Execution

ImpressPages Detection

Infinite Mobile Delivery Webmail Multiple Vulnerabilities (XSS, PD)

Infinity CGI Exploit Scanner Multiple Vulnerabilities

Infoblox IPAM Appliance Default Credentials

Informix SQL Web DataBlade Module Traversal Arbitrary File Access

Informix webdriver CGI Unauthenticated Database Access

Ingo Foldername Arbitrary Command Execution

Inktomi Search MS-DOS Device Name Request Path Disclosure

INL ulog-php port.php proto Parameter SQL Injection

Instaboard index.cfm Multiple Parameter SQL Injection

Interactive Story story.pl next Parameter Traversal Arbitrary File Access

Interchange < 5.0.2 / 5.2.1 Multiple Vulnerabilities (SQLi, Code Exe)

Interchange < 5.4.4 / 5.6.2 / 5.7.2 Search Request Information Disclosure

Interspire ArticleLive Multiple Remote Vulnerabilities (XSS, Auth Bypass)

Invision Community Blog Module eid Parameter SQL Injection

Invision Community Blog Multiple Vulnerabilities (SQLi, XSS)

Invision Gallery < 1.3.1 Multiple SQL Injections

Invision Gallery index.php st Parameter SQL Injection

Invision Power Board 2.x.x < 04-25-06 Multiple Vulnerabilities

Invision Power Board < 2.0.4 Multiple Vulnerabilities (SQLi, XSS)

Invision Power Board < 3.0.5 Multiple Vulnerabilities

Invision Power Board classes/class\_session.php CLIENT\_IP HTTP Header SQL Injection

Invision Power Board Dragoran Portal Module index.php site Parameter SQL Injection

Invision Power Board ibProArcade Module index.php cat Parameter SQL Injection

Invision Power Board index.php Members Action st Parameter SQL Injection

Invision Power Board ipchat.php root\_path Parameter Remote File Inclusion

Invision Power Board Multiple Vulnerabilities (Priv Esc, SQLi

Invision Power Board Software Detection

Invision Power Board sources/post.php qpid Parameter SQL Injection

Invision Power Board ssi.php f Parameter SQL Injection

Iomega smbwebclient.php Unauthenticated Filesystem Access

ION ion-p.exe page Parameter Traversal Arbitrary File Retrieval

ionCube loader-wizard.php Accessible

ionCube loader-wizard.php Remote Information Disclosure

IPCheck Server Monitor Traversal Arbitrary File Access

Ipswitch IMail Web Interface URI Referer Session Token Disclosure

Ipswitch WhatsUp Gold < 16.4 Multiple Vulnerabilities

Ipswitch WhatsUp Gold <= 8.04 Multiple Vulnerabilities

Ipswitch WhatsUp Gold \_maincfgret.cgi Remote Overflow

Ipswitch WhatsUp Gold Default Admin Account

Ipswitch WhatsUp Gold Detection

Ipswitch WhatsUp Professional Crafted Header Authentication Bypass

Ipswitch WhatsUp Professional Login.asp Multiple Field SQL Injection

Ipswitch WhatsUp Professional Multiple Vulnerabilities (XSS, Enum, ID)

Ipswitch WS\_FTP Server Manager /WSFTPSVR/FTPLogServer/LogViewer.asp Authentication Bypass

IRCXPro Default Admin Password

IRIX handler CGI Arbitrary Command Execution

IRIX pfdispaly Arbitrary File Access

IRIX webdist.cgi Arbitrary Command Execution

IRIX wrap CGI Traversal Arbitrary Directory Listing

IronMail IronWebMail IM\_FILE Identifier Encoded Traversal Arbitrary File Access

is\_human() Plugin for WordPress 'type' Parameter Command Injection

ISS ICEcap Default Password

ITA Forum Multiple Scripts SQL Injection

iWeb Hyperseek 2000 hsx.cgi show Parameter Traversal Arbitrary File Read

iWebNegar Multiple Scripts SQL Injection

iXmail index.php password Parameter SQL Injection

iXmail Multiple Script Arbitrary File Manipulation

J Walk Application Server Encoded Directory Traversal Arbitrary File Access

JamMail jammail.pl mail Parameter Arbitrary Command Execution

Java (.java / .class) Source Code Disclosure

Jaws BlogModel.php path Parameter Remote File Inclusion

JAWS index.php gadget Parameter Traversal Arbitrary File Access

Jaws language Parameter Multiple Local File Includes

JBoss %00 Request JSP Source Disclosure

JBoss Application Server (jbossas) JMX Console DeploymentFileRepository Traversal Arbitrary File Manipulation

JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure

JBoss JMX Console Unrestricted Access

JBoss Operations Network Server Detection

JBoss org.jboss.web.WebServer Class Multiple Vulnerabilities (Source Disc, ID)

JBoss Web Services Endpoint Enumeration

JBossWS Endpoint Uses Unsafe Encryption

JBrowser \_admin/ Direct Request Admin Authentication Bypass

JCE Admin Component for Joomla! 'plugin' Parameter Local File Include

Jenkins < (2.204.6 / 2.222.1) LTS / 2.228 Multiple Vulnerabilities

Jenkins < 1.498 / 1.480.2 and Jenkins Enterprise 1.447.x / 1.466.x < 1.447.6.1 / 1.466.12.1 Unspecified Master Cryptographic Key Information Disclosure

Jenkins < 1.502 / 1.480.3 and Jenkins Enterprise 1.447.x / 1.466.x / 1.480.x < 1.447.7.1 / 1.466.13.1 / 1.480.3.1 Multiple Vulnerabilities

Jenkins < 1.514 / 1.509.1 and Jenkins Enterprise 1.466.x / 1.480.x < 1.466.14.1 / 1.480.4.1 Multiple Vulnerabilities

Jenkins < 1.545 Subversion Plugin Information Disclosure

Jenkins < 1.551 / 1.532.2 and Jenkins Enterprise 1.509.x / 1.532.x < 1.509.5.1 / 1.532.2.2 Multiple Vulnerabilities

Jenkins < 1.565.3 / 1.586 Multiple Vulnerabilities

Jenkins < 1.583 / 1.565.3 and Jenkins Enterprise 1.532.x / 1.554.x / 1.565.x < 1.532.10.1 / 1.554.10.1 / 1.565.3.1 Multiple Vulnerabilities

Jenkins < 1.642.2 / 1.650 and Jenkins Enterprise < 1.609.16.1 / 1.625.16.1 / 1.642.2.1 Multiple Vulnerabilities

Jenkins < 2.107 / < 2.89.4 (LTS) Server-Side Request Forgery (SSRF) Vulnerability

Jenkins < 2.107.2 / 2.116 Multiple Vulnerabilities

Jenkins < 2.121 / < 2.107.3 (LTS) Multiple Vulnerabilities

Jenkins < 2.121.2 / 2.133 Multiple Vulnerabilities

Jenkins < 2.121.3 / 2.138 Multiple Vulnerabilities

Jenkins < 2.138.2 (LTS) / 2.146 Multiple Vulnerabilities

Jenkins < 2.138.4 LTS / 2.150.1 LTS / 2.154 Multiple Vulnerabilities

Jenkins < 2.150.2 LTS / 2.160 Multiple Vulnerabilities

Jenkins < 2.164.2 LTS / 2.172 Multiple Vulnerabilities

Jenkins < 2.176.2 LTS / 2.186 Multiple Vulnerabilities

Jenkins < 2.176.3 LTS / 2.192 Multiple Vulnerabilities

Jenkins < 2.176.4 LTS / 2.197 Multiple Vulnerabilities

Jenkins < 2.204.2 LTS / 2.219 Multiple Vulnerabilities

Jenkins < 2.44 / 2.32.x < 2.32.2, Jenkins Operations Center < 1.625.22.1 / 2.7.22.0.1 / 2.32.2.1, and Jenkins Enterprise < 1.651.22.1 / 2.7.22.0.1 / 2.32.2.1 Multiple Vulnerabilities

Jenkins < 2.46.2 / 2.57 and Jenkins Enterprise < 1.625.24.1 / 1.651.24.1 / 2.7.24.0.1 / 2.46.2.1 Multiple Vulnerabilities

Jenkins < 2.73.3 / 2.89 Multiple Vulnerabilities

Jenkins < 2.84 / < 2.73.2 (LTS) Multiple Vulnerabilities

Jenkins < 2.89.2 / 2.95 Multiple Vulnerabilities

Jenkins < 2.89.4 / 2.107 Multiple Vulnerabilities

Jenkins Accessible without Credentials

Jenkins Detection

Jenkins HP Application Automation Tools Plugin Password Encryption Security Weakness

Jenkins JDK / Ant Tools Job Configuration Stored XSS Vulnerability (SECURITY-624) (deprecated)

Jenkins Plugins Detection

Jenkins Security Advisory 2019-01-08 Multiple Vulnerabilities

Jetpack Plugin for WordPress Security Bypass

JFFNMS auth.php Multiple Parameter SQL Injection

JForum Detection

JGS-Portal for WoltLab Burning Board Multiple Vulnerabilities (SQLi, XSS)

Jinzora Multiple Script include\_path Parameter Remote File Inclusion

Jinzora Multiple Script include\_path Parameter Remote File Inclusion (2)

Jinzora name Parameter Local File Inclusion

JoomGallery for Joomla! < 3.3.4 SQL Injection

Joomla 1.7.x < 3.9.16 Multiple Vulnerabilities (5783-joomla-3-9-16)

Joomla 2.5.x < 3.9.14 Multiple Vulnerabilities (5781-joomla-3-9-14)

Joomla 3.0.x < 3.9.12 Joomla 3.9.12 Release (5776-joomla-3-9-12)

Joomla 3.0.x < 3.9.15 Multiple Vulnerabilities (5782-joomla-3-9-15)

Joomla 3.2.x < 3.9.13 Multiple Vulnerabilities (5780-joomla-3-9-13)

Joomla 3.6.x < 3.9.7 Multiple Vulnerabilites

Joomla 3.9.x < 3.9.9 Joomla 3.9.9 Release (5772-joomla-3-9-9-release)

Joomla! 'mosConfig\_absolute\_path' Parameter Remote File Include

Joomla! / Mambo Component 'view' Parameter Local File Include

Joomla! / Mambo Component Multiple Parameter Local File Include Vulnerabilities

Joomla! 1.0.0 < 3.7.4 Multiple Vulnerabilities

Joomla! 1.5.0 < 3.8.0 Multiple Vulnerabilities

Joomla! 1.5.0 < 3.8.2 Multiple Vulnerabilities

Joomla! 1.5.0 < 3.8.4 Multiple Vulnerabilities

Joomla! 1.5.0 < 3.9.5 Multiple Vulnerabilities

Joomla! 1.6.x < 3.9.11 Joomla 3.9.11 Release (5775-joomla-3-9-11)

Joomla! 1.7.3 < 3.7.3 Multiple Vulnerabilities

Joomla! 2.5.0 < 3.9.3 Multiple Vulnerabilities

Joomla! 2.5.x < 2.5.10 / 3.0.x < 3.0.4 Multiple Vulnerabilities

Joomla! 2.5.x < 2.5.14 / 3.x < 3.1.5 .php. File Upload RCE

Joomla! 2.5.x < 2.5.19 Multiple Vulnerabilities

Joomla! 2.5.x < 2.5.25 / 3.x < 3.2.5 / 3.3.x < 3.3.4 Multiple Vulnerabilities

Joomla! 2.5.x < 2.5.26 / 3.x < 3.2.6 / 3.3.x < 3.3.5 Multiple Vulnerabilities

Joomla! 2.5.x < 2.5.9 / 3.0.x < 3.0.3 Multiple Vulnerabilities

Joomla! 3.4.4 < 3.6.4 Multiple Vulnerabilities

Joomla! 3.5.0 < 3.8.6 User Notes List View SQL Injection

Joomla! 3.7.x < 3.7.1 fields.php getListQuery() Method SQLi

Joomla! 3.x < 3.2.3 Multiple Vulnerabilities

Joomla! 3.x < 3.4.2 Multiple Vulnerabilities

Joomla! 3.x < 3.4.5 Multiple Vulnerabilities

Joomla! 3.x < 3.9.4 Multiple Vulnerabilities

Joomla! < 1.0.11 administrator/index.php Input Weakness

Joomla! < 1.0.11 Unspecified Remote Code Execution

Joomla! < 1.0.8 Information Disclosure

Joomla! < 3.4.6 Multiple Vulnerabilities

Joomla! < 3.4.7 Multiple Vulnerabilities

Joomla! < 3.6.1 Multiple Vulnerabilities

Joomla! < 3.6.5 Multiple Vulnerabilities

Joomla! < 3.7.0 Multiple Vulnerabilities

Joomla! < 3.8.12 Multiple Vulnerabilities

Joomla! < 3.8.13 Multiple Vulnerabilities

Joomla! < 3.8.8 Multiple Vulnerabilities

Joomla! < 3.8.9 Local File Inclusion with PHP 5.3

Joomla! < 3.8.9 XSS vulnerability in language switcher module

Joomla! < 3.9.2 Multiple Stored XSS Vulnerabilities

Joomla! CMS com\_search Component 'searchword' Parameter RCE

Joomla! Detection

Joomla! Extension 'JCK Suite' - 'jckeditor' =< 6.4.4 Privilege Escalation

Joomla! Extension Detection

Joomla! JoomlaWorks AllVideos Plugin 'file' Parameter Directory Traversal

Joomla! prior to 3.9.3 Cross-Site Scripting (XSS) Vulnerability

Joomla! prior to 3.9.6 Cross-Site Scripting (XSS) Vulnerability

Joomla! reset.php Reset Token Validation Forgery

Joomla! Unsupported Version Detection

Joomla! User-Agent Object Injection RCE

jPortal print.inc.php id Parameter SQL Injection

JQuery < 3.4.0 Object Prototype Pollution Vulnerability

JQuery Detection

jQuery-File-Upload Arbitrary File Upload Vulnerability (Remote Check)

jRSS Widget Plugin for WordPress proxy.php 'url' Parameter Arbitrary File Access

JRun Multiple Sample Files Remote Information Disclosure

JRun viewsource.jsp Directory Traversal Arbitrary File Access

JRun Web Server (JWS) GET Request Traversal Arbitrary File Access

JS Jobs Component for Joomla! 'md' Parameter SQLi

jspwebshell Backdoor Detection

JSPWiki Edit.jsp editor Parameter Traversal Local File Inclusion

Jumi Component for Joomla! 'fileid' Parameter SQLi

Jumi Component for Joomla! <= 2.0.5 Backdoor Detection

Junos Space WebUI Default Credentials

Junos Space WebUI Detection

Justice Guestbook 1.3 Multiple Vulnerabilities

JVideo! Component for Joomla! 'user\_id' Parameter SQLi

K-COLLECT CSV\_DB / i\_DB csv\_db.cgi file Parameter Arbitrary Command Execution

Kaa IoT Administration Server Detection

Kaspersky Anti-Spam Control Center Web Config aslic\_status.cgi Directory Listing

Kayako LiveResponse Multiple Vulnerabilities

Kayako SupportSuite 3.x <= 3.70.02 Multiple Vulnerabilities

Kayako SupportSuite < 3.30.01 Multiple Vulnerabilities

Kayako SupportSuite Detection

Kayako SupportSuite syncml/index.php Direct Request Remote Information Disclosure

Kayako SupportSuite Ticket Subject XSS

Kebi Academy Home Page Administration file Parameter Traversal Arbitrary File Access

Kerio WebMail < 5.7.7 Multiple Vulnerabilities

Kerio WinRoute Firewall Web Server Remote Source Code Disclosure

Kibana Detection

Kibana ESA-2018-03

Kibana ESA-2018-05

Kibana ESA-2018-06

Kibana ESA-2018-08

Kibana ESA-2018-14

Kibana ESA-2018-17

Kibana ESA-2018-18

Kibana ESA-2019-01, ESA-2019-02, ESA-2019-03

Kietu index.php Remote File Inclusion

Kiwi Syslog Server Web Access Login Username Enumeration

Kodi Local File Inclusion Information Disclosure

Kodi Media Player Detection

KorWeblog < 1.6.2 Multiple Vulnerabilities

Kubernetes 1.x < 1.10.11 / 1.11.x < 1.11.5 / 1.12.x < 1.12.3 API Server Privilege Escalation

Kubernetes 1.x < 1.11.8 / 1.12.x < 1.12.6 / 1.13.x < 1.13.4 API server DOS

Kubernetes info API access

Kubernetes proxy request handling vulnerability (CVE-2018-1002105)

Kubernetes unprivileged API access

KW Whois CGI whois Parameter Arbitrary Command Execution

Land Down Under / Seditio polls.php id Parameter SQL Injection

Land Down Under <= 800 Multiple Vulnerabilities

Land Down Under <= 801 Multiple Vulnerabilities

Land Down Under HTTP Referer Header SQL Injection

Landing Pages Plugin for WordPress 'wp-admin/edit.php' 'post' Parameter SQL Injection

LDU Software/Version Detection

LeagueManager Plugin for WordPress 'wp-admin/admin.php' 'league\_id' Parameter SQL Injection

LedgerSMB / SQL-Ledger admin.pl Admin Authentication Bypass

LedgerSMB / SQL-Ledger file Parameter Multiple Vulnerabilities

LedgerSMB / SQL-Ledger login.pl script Parameter Arbitrary Perl Code Execution

Leif Wright ad.cgi file Parameter Arbitrary Command Execution

Leif Wright Web Blog blog.cgi ViewFile Request file Parameter Arbitrary Command Execution

Lenovo ThinkManagement Console Detection

Lenovo ThinkManagement Console RunAMTCommand Operation -PutUpdateFileCore Command Parsing Arbitrary File Upload

Les Visiteurs Multiple Remote File Inclusion

Lexmark Markvision Enterprise Default Credentials

Lexmark Markvision Enterprise Detection

Lexmark MarkVision Enterprise GfdFileUploadServerlet RCE Vulnerability

Liferay Portal 6.0.5 / 6.0.6 Arbitrary File Download

Liferay Portal 6.1.0 'addUser()' Security Bypass

Liferay Portal 6.1.0 / 6.1.10 Arbitrary File Deletion

Liferay Portal 6.1.0 Forward Target Handling Security Bypass

Liferay Portal 6.1.0 User Enumeration

Liferay Portal 6.1.x < 6.1 CE GA3 (6.1.2) Multiple Vulnerabilities

Liferay Portal < 6.0.6 Multiple Vulnerabilities

Liferay Portal Default Credentials

Liferay Portal Detection

LifeType for Drupal (pLog) index.php albumId Parameter SQL Injection

LifeType index.php articleId Parameter SQL Injection

LifeType index.php Date Parameter SQL Injection

LifeType rss.php profile Parameter Traversal Arbitrary File Access

Limbo CMS index.php Itemid Parameter Arbitrary Command Execution

Limbo CMS Multiple Vulnerabilities

Limbo CMS sql.php classes\_dir Parameter Remote File Inclusion

Limbo com\_fm Component sql.php classes\_dir Parameter Remote File Inclusion

Limbo Contact Component (com\_contact) contact.html.php contact\_attach Unrestricted File Upload

Limbo weblinks.html.php catid Parameter SQL Injection

LimeSurvey sUser Parameter SQL Injection

Lincoln D. Stein nph-publish.cgi pathname Parameter Traversal Arbitrary File Write

Linksys E1500/E2500 Authenticated Command Execution

Linksys Smart Wi-Fi Router CGI Scripts Information Disclosure

Linksys Smart Wi-Fi Router Default Credentials

Linksys WVC54GCA Wireless-G '/img/main.cgi' Information Disclosure

LinPHA <= 1.0 Multiple Vulnerabilities

LinPHA include/img\_view.class.php order parameter SQL Injection

ListManager < 8.9b Multiple Vulnerabilities

ListManager < 9.3b / 9.2c / 8.95d Multiple Vulnerabilities

ListManager Error Message Information Disclosure

Listserv < 14.3-2005a Multiple Vulnerabilities

Listserv < 14.5 Multiple Buffer Overflows

LiteSpeed Web Server MIME Type Injection Null Byte Script Source Code Disclosure

Live Chat Component for Joomla! 'last' Parameter Multiple SQLi

LiveZilla 'mobile/php/translation/index.php' 'g\_language' Parameter Local File Inclusion

LiveZilla < 5.1.1.0 Multiple Vulnerabilities

LiveZilla < 5.1.2.1 Multiple Vulnerabilities

LiveZilla Detection

Log Rover pword Parameter SQL Injection

LogAnalyzer Detection

Logstash ESA-2014-02

Logstash ESA-2015-04

Logstash ESA-2018-01

Logstash ESA-2019-05

Logstash JSON API Detection

Logstash JSON API Detection (deprecated)

Looking Glass Multiple Vulnerabilities

Loudblog < 0.42 template Parameter Traversal

Loudblog backend\_settings.php Multiple Parameter Remote File Inclusion

Loudblog index.php id Parameter SQL Injection

Loudblog loudblog/inc/parse\_old.php template Parameter Arbitrary Remote Code Execution

Lucent VitalNet VsSetCookie.exe Unauthorized Access

LyftenBloggie Component for Joomla! 'author' Parameter SQLi

Lyris ListManager Subscription Form Administrative Command Injection

Mac OS X Server Web Services Version Detection

Mac Photo Gallery for WordPress 'albid' Parameter Traversal Arbitrary File Access

Mac Photo Gallery Plugin for WordPress 'macphtajax.php' Access Restriction Bypass

Macallan Mail Solution Web Interface Authentication Bypass

Macromedia ColdFusion MX CFIDE/probe.cfm Direct Request Path Disclosure

Magento 2.2.x < 2.2.8 / 2.3.x < 2.3.1 Unauthenticated SQLi

Magento Detection

Magento Mage\_Adminhtml\_Block\_Report\_Search\_Grid Class 'popularity' Parameter SQLi

Magento XML-RPC XXE Arbitrary File Disclosure

Magnoware DataTrack System Detection

Magnoware DataTrack System Information Disclosure

Maia Mailguard login.php lang Parameter Local File Inclusion

Maian Scripts Cookie Manipulation Authentication Bypass

Mail-it Now! Upload2Server Predictable Filename Upload Arbitrary Code Execution

MailEnable HTTPMail Service Authorization Header Handling Remote DoS

MailEnable HTTPMail Service Authorization Header Remote Overflow

MailEnable HTTPMail Service Content-Length Header Overflow

MailEnable NetWebAdmin Unauthorized Access (ME-10019)

MailEnable Professional HTTPMail GET Request Remote Overflow

MailEnable Web Mail Client Multiple Vulnerabilities (XSS, CSRF)

MailEnable WebMail Detection

Mailgust Password Reminder email Field SQL Injection

Mailman Detection

Mailman private.py true\_path Function Traversal Arbitrary File Access

Mailman Utils.py Spoofed Log Entry Injection

MailMan Webmail mmstdod.cgi Arbitrary Command Execution

MailMarshal Spam Quarantine Interface Arbitrary Account Password Retrieval

MailMaxWeb Cookie Application Path Disclosure

MAILNEWS mailnews.cgi Arbitrary Command Execution

MailPoet Newsletters for WordPress Arbitrary File Upload

Mailreader 2.3.30 - 2.3.31 Multiple Vulnerabilities

MailScan WebAdministrator Cookie Authentication Bypass

MailWatch authenticate() Function SQL Injection

MailWatch for MailScanner mailscanner/docs.php doc Parameter Traversal Local File Inclusion

Majordomo 2 \_list\_file\_get() Function Traversal Arbitrary File Access

Majordomo Detection

Mambo / Joomla! Component / Module 'mosConfig\_absolute\_path' Multiple Parameter Remote File Include Vulnerabilities

Mambo / Joomla! Multiple Components 'mosConfig\_live\_site' Parameter Remote File Include

Mambo < 4.6.5 mos\_user\_template Local File Inclusion

Mambo Detection

Mambo Global Variables Unauthorized Access

Mambo mod\_mainmenu.php mosConfig\_absolute\_path Parameter Remote File Inclusion

Mambo MOStlyCE Mambot Arbitrary File Rename

Mambo Open Source / Joomla! GLOBALS Variable Remote File Include

Mambo Open Source < 4.5.2.3 Multiple Vulnerabilities

Mambo Open Source Multiple Vulnerabilities

Mambo Open Source Tar.php Remote File Inclusion

Mambo Open Source usercookie Parameter SQL Injection

Mambo phpBB Component download.php phpbb\_root\_path Parameter Remote File Inclusion

Mambo Site Server MD5 Hash Session ID Privilege Escalation

Mambo Site Server Multiple Vulnerabilities

man2web Multiple Scripts Arbitrary Command Execution

ManageEngine ADAudit Plus Default Credentials

ManageEngine ADAudit Plus Detection

ManageEngine ADManager Plus Default Credentials

ManageEngine ADManager Plus Detection

ManageEngine ADSelfService Plus Default Administrator Credentials

ManageEngine ADSelfService Plus Detection

ManageEngine ADSelfService Plus resetUnLock Authentication Bypass

ManageEngine Applications Manager Default Administrator Credentials

ManageEngine Applications Manager Detection

ManageEngine Applications Manager DowntimeSchedulerServlet 'TASKID' Blind SQLi

ManageEngine Applications Manager FailOverHelperServlet 'fileName' Parameter Arbitrary File Disclosure

ManageEngine Applications Manager Invalid URL Remote Information Disclosure

ManageEngine Applications Manager IT360UtilitiesServlet SQLi

ManageEngine Applications Manager Unsupported Version Detection

ManageEngine AssetExplorer Default Administrator Credentials

ManageEngine AssetExplorer Detection

ManageEngine AssetExplorer Multiple Vulnerabilities

ManageEngine Desktop Central 10 < Build 100282 Remote Privilege Escalation

ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution

ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check)

ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE

ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities

ManageEngine Desktop Central < 10 Build 10.0.515 Information Disclosure

ManageEngine Desktop Central < 9 build 90103 XSRF

ManageEngine Desktop Central < 9 Build 90135 Unauthenticated Admin Password Reset

ManageEngine Desktop Central AgentLogUploadServlet Arbitrary File Upload

ManageEngine Desktop Central AgentLogUploadServlet Arbitrary File Upload RCE (intrusive check)

ManageEngine Desktop Central Arbitrary File Upload and RCE (Safe Check)

ManageEngine Desktop Central Default Administrator Credentials

ManageEngine Desktop Central Detection

ManageEngine Desktop Central NativeAppServlet UDID JSON RCE

ManageEngine Desktop Central Remote Security Bypass

ManageEngine Desktop Central Remote Security Bypass (Intrusive Check)

ManageEngine Desktop Central statusUpdate Arbitrary File Upload RCE (intrusive check)

ManageEngine Desktop Central statusUpdate Arbitrary File Upload RCE (intrusive check)

ManageEngine Desktop Central Tools Execution Status Update RCE (intrusive check)

ManageEngine DeviceExpert Default Administrator Credentials

ManageEngine DeviceExpert Detection

ManageEngine DeviceExpert ScheduleResultViewer Remote Directory Traversal

ManageEngine DeviceExpert Unauthorized Information Disclosure

ManageEngine EventLog Analyzer

ManageEngine EventLog Analyzer 'agentHandler' Information Disclosure

ManageEngine EventLog Analyzer Default Credentials

ManageEngine EventLog Analyzer XSS Vulnerability

ManageEngine Firewall Analyzer < 12.0 Multiple Vulnerabilities

ManageEngine Firewall Analyzer Default Credentials

ManageEngine Firewall Analyzer Detection

ManageEngine NetFlow Analyzer Default Credentials

ManageEngine NetFlow Analyzer Detection

ManageEngine NetFlow Analyzer Multiple Path Traversal and File Access

ManageEngine OpManager 'probeName' SQL Injection Vulnerability

ManageEngine OpManager Default Credentials

ManageEngine OpManager Detection

ManageEngine OpManager Multiple Directory Traversal Vulnerabilities

ManageEngine OpStor Default Administrator Credentials

ManageEngine OpStor Detection

ManageEngine Password Manager Pro 6.5 < 7.1 Build 7105 Blind SQL Injection

ManageEngine Password Manager Pro < 7.0 Build 7003 SQL Injection

ManageEngine Password Manager Pro Default Credentials

ManageEngine Password Manager Pro Detection

ManageEngine Security Manager Plus 'f' Directory Traversal Arbitrary File Access

ManageEngine Security Manager Plus Default Administrator Credentials

ManageEngine Security Manager Plus Detection

ManageEngine ServiceDesk Plus 9.1.0 < Build 9103 Multiple Vulnerabilities

ManageEngine ServiceDesk Plus 9.2.0 < Build 9228 Multiple Vulnerabilities

ManageEngine ServiceDesk Plus Default Administrator Credentials

ManageEngine ServiceDesk Plus Detection

ManageEngine ServiceDesk Plus FileDownload.jsp FILENAME Parameter Traversal Arbitrary File Access

ManageEngine ServiceDesk Plus Multiple Vulnerabilities

ManageEngine ServiceDesk Plus User and Domain Enumeration

ManageEngine SupportCenter Plus < 7.9 Build 7905 Multiple Vulnerabilities

ManageEngine SupportCenter Plus < 7.9 Build 7917 attach Parameter Directory Traversal

ManageEngine SupportCenter Plus Default Administrator Credentials

ManageEngine SupportCenter Plus Detection

ManageEngine SupportCenter Plus FileDownload.jsp path Parameter Traversal Arbitrary File Access

Mantis < 0.17.5 Multiple Vulnerabilities

Mantis < 0.18.3 / 0.19.0a2 Multiple Vulnerabilities

Mantis < 0.19.1 Multiple Vulnerabilities

Mantis < 0.19.3 Multiple Vulnerabilities

Mantis < 1.0.0rc2 Multiple Vulnerabilities

Mantis manage\_user\_create.php CSRF New User Creation

MantisBT 'db\_type' Parameter Local File Inclusion

MantisBT 1.1.0 < 1.2.16 Multiple Vulnerabilities

MantisBT 1.2.12 - 1.2.14 Multiple Vulnerabilities

MantisBT 1.2.13 - 1.2.16 'admin\_config\_report.php' SQLi

MantisBT 1.2.x < 1.2.13 Multiple Vulnerabilities

MantisBT 1.2.x < 1.2.18 Multiple Vulnerabilities

MantisBT 1.2.x < 1.2.19 Multiple Vulnerabilities

MantisBT < 1.2.12 Multiple Vulnerabilities

MantisBT Detection

MapServer < 5.2.2 / 4.10.4 Multiple Flaws

MapServer < 5.4.2 / 5.2.3 / 4.10.5 Buffer Overflow

MapServer < 5.6.9 / 6.0.4 / 6.2.2 / 6.4.1 SQL Injection

MapServer Detection

MapServer for Windows (MS4W) Bundled Apache / PHP Configuration Local File Inclusion

MapServer for Windows (MS4W) Detection

MapServer Insecure MapServ CGI Command-line Debug Args

MapServer Multiple Remote Vulnerabilities

Marcus Xenakis directory.php Execute Arbitrary Commands

Master Index search.cgi Traversal Arbitrary File/Directory Access

mathTeX mathtex.cgi getdirective Function dpi Tag Arbitrary Code Execution

Matt Kruse calendar\_admin.pl Shell Metacharacter Arbitrary Command Execution

Matt Wright FormHandler.cgi Arbitrary File Access

Matt Wright guestbook.pl Arbitrary Command Execution

Matt Wright textcounter.pl Arbitrary Command Execution

Matthew Wright FormMail CGI (formmail.cgi) Arbitrary Mail Relay

MaxWebPortal <= 1.33 Multiple Vulnerabilities

MaxWebPortal <= 1.35 Multiple Vulnerabilities

MaxWebPortal memKey Parameter SQL Injection

McAfee Agent 4.6.x < 4.8.0.1938 / 5.0.x < 5.0.1 Log View Clickjacking (SB10094)

McAfee Cloud Single Sign On User Interface Detection

McAfee Cloud Single Sign On WebUI Default Credentials

McAfee Common Management Agent < 3.6.0.546 Multiple Vulnerabilities

McAfee Common Management Agent < 3.6.0.595 UDP Packet Handling Format String

McAfee Common Management Agent < 3.6.0.603 FrameworkService.exe AVClient DoS

McAfee Common Management Agent Traversal Arbitrary File Write

McAfee Email Gateway Appliance 7.x Multiple Vulnerabilities (SB10037)

McAfee Email Gateway Appliance 7.x Unspecified Command Injection (SB10057)

McAfee Email Gateway Multiple Vulnerabilities (SB10064)

McAfee ePolicy Orchestrator 4.6.x Multiple Vulnerabilities (SB10042)

McAfee ePolicy Orchestrator Application Server Detection

McAfee ePolicy Orchestrator SSL/TLS Certificate Validation Security Bypass Vulnerability (SB10120)

McAfee ESM SIEM Detection

McAfee LinuxShield Login Username Enumeration

McAfee Managed Agent FrameworkService.exe HTTP Request DoS (SB10055)

McAfee VirusScan Enterprise for Linux User Interface Detection

McAfee Vulnerability Manager Detect

McAfee Web Gateway User Interface Default Credentials

McAfee Web Gateway User Interface Detection

McAfee Web Reporter Detection (remote check)

McAfee WebShield UI Authentication Bypass (SB10026)

McAfee WebShield UI mui Directory Traversal (SB10026)

McAfee WebShield Web UI Detection

MDPro index.php topicid Parameter SQL Injection

MediaWiki 1.19.x < 1.19.4 / 1.20.x < 1.20.3 Multiple Vulnerabilities

MediaWiki 1.19.x < 1.19.5 / 1.20.x < 1.20.4 Multiple Vulnerabilities

MediaWiki 1.19.x < 1.19.6 / 1.20.x < 1.20.5 Multiple Vulnerabilities

MediaWiki 1.19.x < 1.19.7 / 1.20.x < 1.20.6 Arbitrary File Upload

MediaWiki 1.23.x < 1.23.14 / 1.25.x < 1.25.6 / 1.26.x < 1.26.3 Multiple Vulnerabilities

MediaWiki 1.23.x < 1.23.15 / 1.26.x < 1.26.4 / 1.27.x < 1.27.1 Multiple Vulnerabilities

MediaWiki < 1.17.3 / 1.18.2 Multiple Vulnerabilities

MediaWiki < 1.18.5 / 1.19.2 Multiple Vulnerabilities

MediaWiki < 1.18.6 / 1.19.3 / 1.20.1 Multiple Vulnerabilities

MediaWiki < 1.19.10 / 1.21.4 / 1.22.1 Multiple Vulnerabilities

MediaWiki < 1.19.11 / 1.21.5 / 1.22.2 Multiple Remote Code Execution Vulnerabilities

MediaWiki < 1.19.12 / 1.21.6 / 1.22.3 Multiple Vulnerabilities

MediaWiki < 1.19.14 / 1.21.8 / 1.22.5 ChangePassword XSRF

MediaWiki < 1.19.17 / 1.21.11 / 1.22.8 / 1.23.1 External SVG Resource

MediaWiki < 1.19.18 / 1.22.9 / 1.23.2 Multiple Vulnerabilities

MediaWiki < 1.19.22 / 1.22.14 / 1.23.7 Multiple Vulnerabilities

MediaWiki < 1.19.24 / 1.23.9 / 1.24.2 Multiple Vulnerabilities

MediaWiki < 1.19.8 / 1.20.7 / 1.21.2 Multiple Vulnerabilities

MediaWiki < 1.19.9 / 1.20.8 / 1.21.3 Multiple Vulnerabilities

MediaWiki < 1.3.11 Multiple Remote Vulnerabilities

MediaWiki < 1.3.17 / 1.4.11 / 1.5.0 Multiple Vulnerabilities

MediaWiki Detection

MediaWiki JSON Callback Crafted API Request Information Disclosure

MediaWiki Language Option eval() Function Arbitrary PHP Code Execution

MediaWiki Login Cross-Site Request Forgery

MediaWiki mwdoc-filter.php Arbitrary File Access

MediaWiki thumb.php 'w' Parameter Remote Shell Command Injection

MediaWiki Unsupported Version Detection

Meeting Room Booking System (MRBS) month.php area Parameter SQL Injection

Meeting Room Booking System Detection

Meeting Room Booking System typematch Parameter SQL Injection

Mensajeitor Tag Board Admin Bypass

Merak Webmail / IceWarp Web Mail < 5.2.8 Multiple Vulnerabilities

MERCUR WebView WebMail Server mail\_user Parameter DoS

MercuryBoard User-Agent SQL Injection

MetaCart E-Shop productsByCategory.ASP Multiple Vulnerabilities

Metasploit HTTP Server detection

Metertek pagelog.cgi Traversal Arbitrary File Access

Micro Focus Enterprise Administration Server Authentication Check

Micro Focus Enterprise Administration Server Detection

Micro Focus Operations Orchestration JMiniX Multiple Vulnerabilities

Microsoft ASP.NET Application Tracing trace.axd Information Disclosure

Microsoft ASP.NET Malformed File Request Path Disclosure

Microsoft BizTalk Server Multiple Remote Vulnerabilities

Microsoft Commerce Server 2002 authfiles/login.asp Authentication Bypass

Microsoft FrontPage htimage.exe CGI Remote Overflow

Microsoft IIS / Site Server showcode.asp source Parameter Traversal Arbitrary File Access

Microsoft IIS 6.0 PHP NTFS Stream Authentication Bypass

Microsoft IIS advsearch.asp Direct Request Remote DoS

Microsoft IIS ctss.idc ODBC Sample Arbitrary Command Execution

Microsoft IIS Dangerous Sample Files Detection

Microsoft IIS fpcount.exe CGI Remote Overflow

Microsoft IIS global.asa Remote Information Disclosure

Microsoft IIS idq.dll Traversal Arbitrary File Access

Microsoft IIS Multiple Vulnerabilities (MS02-018)

Microsoft IIS newdsn.exe Arbitrary File Creation

Microsoft IIS ODBC Tool getdrvrs.exe DSN Creation

Microsoft IIS Phone Book Service /pbserver/pbserver.dll Remote Overflow

Microsoft IIS query.asp Direct Request Remote DoS

Microsoft IIS search.asp Direct Request DoS

Microsoft IIS Translate f: ASP/ASA Source Disclosure

Microsoft IIS Translate f: ASP/ASA Source Disclosure (IIS 5.1)

Microsoft Outlook Web Access (OWA) Anonymous Access

Microsoft Outlook Web Access (OWA) owalogon.asp Redirection Account Enumeration

Microsoft Outlook Web Access (OWA) Version Detection

Microsoft Personal Web Server Multiple Dot Request Arbitrary File Access

Microsoft Remote Desktop Web Access Detection

Microsoft SharePoint Service Help.aspx 'tid' Parameter DoS

Microsoft Site Server Multiple Script Information Disclosure

Microsoft UDDI Services Detection

Microsoft W3Who ISAPI w3who.dll Multiple Remote Vulnerabilities

Mike Bobbitt's album.pl Alternative Configuration File Remote Command Execution

Mingle Forum Plugin for WordPress 'topic' parameter SQL Injection

Mini SQL CGI content-length Field Remote Overflow

Mini SQL w3-msql Arbitrary Directory Access

miniBB bb\_func\_txt.php pathToFiles Parameter Remote File Inclusion

miniBB index.php user Parameter SQL Injection

miniPortail admin.php Cookie Manipulation Security Bypass

Minis minis.php month Parameter Traversal Arbitrary File Access

MiniVend view\_page.html Shell Metacharacter Arbitrary Command Execution

Missing Function Level Access Control

Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Missing or Permissive X-Frame-Options HTTP Response Header

Miva htmlscript Traversal Arbitrary File Access

mnoGoSearch Detection

mnoGoSearch search.cgi Multiple Parameter Remote Overflows

mnoGoSearch search.cgi QUERY\_STRING Parameter Parsing Arbitrary File Access

Mobius DocumentDirect ddicgi.exe Long GET Request Overflow

Mod\_auth\_mysql Multibyte Encoding SQL Injection

ModernBill <= 4.3.0 Multiple Vulnerabilities

Module Builder DownloadModule Traversal Arbitrary File Disclosure

MODx 'ucfg' Parameter Arbitrary File Access

MODx < 0.9.1a Multiple Vulnerabilities

MODx < 2.0.3-pl class\_key Parameter Local File Inclusion

MODx CMS base\_path Parameter Remote File Inclusion

MODx CMS Detection

MODx config.js.php Information Disclosure

MoinMoin 'sys.argv' Information Disclosure

MoinMoin < 1.9.6 Multiple Vulnerabilities

MoinMoin Detection

MoinMoin MOIN\_ID Cookie userform Action Traversal Arbitrary File Overwrite

MoinMoin twikidraw.py Traversal File Upload Arbitrary File Overwrite

MondoSearch MsmMask.exe Arbitrary Script Source Disclosure

Monitorix Built-in HTTP Server Remote Command Execution

Monkey HTTP Daemon (monkeyd) < 0.9.1 Multiple Vulnerabilities

Mono XSP for ASP.NET Server Crafted Request Script Source Code Disclosure

Monster Top List sources/functions.php root\_path Parameter Remote File Inclusion

Moodle 'filter/tex/texed.php' 'pathname' Parameter Remote Command Execution

Moodle 'index.php' 'tag' Parameter SQL Injection

Moodle 'lib/kses.php' 'kses\_bad\_protocol\_once' Function Arbitrary PHP Code Execution

Moodle 'moodledata/sessions' Session Files Remote Information Disclosure

Moodle < 1.4.3 Multiple Vulnerabilities

Moodle < 1.5.1 Multiple Vulnerabilities

Moodle < 1.5.3 Multiple SQL Injection Vulnerabilities

Moodle < 1.6.2 Multiple Vulnerabilities

Moodle < 1.9.6 / 1.8.10 Multiple Vulnerabilities

Moodle Detection

Moodle Forum 'post.php' Unauthorized Post Deletion CSRF

Moodle LaTeX Information Disclosure

Mort Bay Jetty URL Multiple Slash Character Information Disclosure

Mountain Network Systems webcart.cgi Arbitrary Command Execution

Movable Type 5.2.X < 5.2.6 Unspecified Vulnerability

Movable Type < 3.2 Multiple Vulnerabilities

Movable Type Detection

Movable Type mt-check.cgi System Information Disclosure

Movable Type mt-load.cgi Privilege Escalation

Movable Type mt-upgrade.cgi Remote Command Execution

Movable Type mt.cfg Information Disclosure

Movable Type User Registration Restriction Bypass

Mozilla Bonsai Mutiple Flaws (Auth Bypass, XSS, Cmd Exec, PD)

MPC SoftWeb Guestbook Multiple Vulnerabilities

MPM Guestbook Pro top.php Traversal Arbitrary File Access

MRTG mrtg.cgi cfg Parameter Traversal Arbitrary Files Access

MS04-017: Crystal Reports Web Viewer Could Allow Information Disclosure and DoS (842689) (uncredentialed check)

MS11-051: Vulnerability in Active Directory Certificate Services Web Enrollment Could Allow Elevation of Privilege (2518295) (uncredentialed check)

MS11-100: ASP.NET Could Allow Denial of Service (2638420) (uncredentialed check)

MS12-007: Vulnerability in AntiXSS Library Could Allow Information Disclosure (2607664) (uncredentialed check)

MultiHTML multihtml.pl Traversal Arbitrary File Access

Multiple Adobe Products XML External Entity (XXE) Injection (APSB10-05)

Multiple Dangerous CGI Script Detection

Multiple Server Crafted Request WEB-INF Directory Information Disclosure

Multiple Slider Plugins for WordPress 'img' Parameter Local File Inclusion Vulnerability

Multiple Vendor info2www CGI Arbitrary Command Execution

Multiple Vendor jj CGI Arbitrary Command Execution

Multiple Vendor phf CGI Arbitrary Command Execution

Multiple Vendor test-cgi Arbitrary File Access

Multiple Vendor view\_source CGI Traversal Arbitrary File Access

Multiple Web Server finger CGI Information Disclosure

Multiple Web Server printenv CGI Information Disclosure

Mura CMS Default Administrator Credentials

Mura CMS Detection

Mura CMS FILEID Parameter Directory Traversal

Muscat Empower CGI Malformed DB Parameter Path Disclosure

Mutiny < 4.5-1.12 Unspecified Network Interface Menu Remote Command Injection

Mutiny < 5.0-1.11 Multiple Directory Traversals

Mutiny Detection

MVPower DVR Remote Command Execution

My Guest Book (myGuestBk) Multiple Vulnerabilities

My\_eGallery < 3.1.1g Remote File Inclusion

my\_gallery Plugin for e107 dload.php file Parameter Arbitrary File PHP Source Disclosure

MyBB 'comma' Cookie SQLi

MyBB 1.6.4 Backdoor PHP Remote Code Execution

MyBB < 1.01 function\_upload.php SQLi

MyBB < 1.04 misc.php SQLi

MyBB < 1.6.10 Multiple Vulnerabilities

MyBB < 1.6.11 Multiple Vulnerabilities

MyBB < 1.6.12 Multiple Vulnerabilities

MyBB < 1.6.9 Multiple Vulnerabilities

MyBB <= 1.00 RC4 Multiple SQL Injection Vulnerabilities

MyBB calendar.php 'month' Parameter SQLi

MyBB Detection

MyBB forumdisplay.php 'sortby' Parameter Arbitrary PHP Code Execution

MyBB global.php 'KILL\_GLOBAL' Overwrite SQL Injection

MyBB HTTP Header 'CLIENT-IP' Field SQLi

MyBB index.php 'referrer' Parameter SQLi

MyBB member.php 'uid' Parameter SQLi

MyBB misc.php Multiple SQL Injection Vulnerabilities

MyBB ratethread.php 'rating' Parameter SQLi

MyBB search.php 'forums' Parameter SQLi

MyDMS < 1.4.3 Multiple Vulnerabilities

myEvent Multiple Remote Vulnerabilities

myGallery mygallerybrowser.php 'myPath' Parameter Remote File Inclusion

myPHPcalendar Multiple Scripts cal\_dir Parameter Remote File Inclusion

myPHPNuke My\_eGallery gallery/displayCategory.php basepath Parameter Remote File Inclusion

myPHPNuke phptonuke.php filnavn Parameter Traversal Arbitrary File Access

myphpPageTool /doc/admin/index.php ptinclude Parameter Remote File Inclusion

MyReview Admin.php email Parameter SQL Injection

MyServer 0.6.2 math\_sum.mscgi Multiple Vulnerabilities

MyServer 0.8 Multiple Vulnerabilities

MySQL Enterprise Monitor (MEM) Web Detection

MySQL Enterprise Monitor 2.3.x < 2.3.21 / 3.0.x < 3.0.23 Multiple Vulnerabilities

MySQL Enterprise Monitor 3.0.x < 3.0.11 Multiple Vulnerabilities

MySQL Enterprise Monitor 3.0.x < 3.0.19 Apache Struts Predictable Token XSRF

MySQL Enterprise Monitor 3.0.x < 3.0.26 / 3.1.x < 3.1.2 Unspecified RCE

MySQL Enterprise Monitor 3.0.x < 3.0.5 Apache Struts DMI Multiple Vulnerabilities

MySQL Enterprise Monitor 3.1.x < 3.1.4.7895 Agent Subcomponent RCE (January 2017 CPU)

MySQL Enterprise Monitor 3.1.x < 3.1.5.7958 Multiple Vulnerabilities (SWEET32) (January 2017 CPU)

MySQL Enterprise Monitor 3.1.x < 3.1.6.7959 Java Object Deserialization RCE (January 2017 CPU)

MySQL Enterprise Monitor 3.1.x < 3.1.7.8023 / 3.2.x < 3.2.7.1204 / 3.3.x < 3.3.3.1199 Multiple Vulnerabilities (April 2017 CPU)

MySQL Enterprise Monitor 3.2.x < 3.2.2.1075 Multiple Vulnerabilities (January 2017 CPU)

MySQL Enterprise Monitor 3.2.x < 3.2.5.1141 Multiple Vulnerabilities (SWEET32) (January 2017 CPU)

MySQL Enterprise Monitor 3.2.x < 3.2.8.2223 / 3.3.x < 3.3.4.3247 Multiple Vulnerabilities (July 2017 CPU)

MySQL Enterprise Monitor 3.2.x < 3.2.9.2249 / 3.3.x < 3.3.5.3292 / 3.4.x < 3.4.3.4225 Multiple Vulnerabilities (October 2017 CPU)

MySQL Enterprise Monitor 3.3.x < 3.3.1.1112 Multiple Vulnerabilities (SWEET32) (January 2017 CPU)

MySQL Enterprise Monitor 3.3.x < 3.3.7.3306 / 3.4.x < 3.4.5.4248 / 4.0.x < 4.0.2.5168 Multiple Vulnerabilities (January 2018 CPU)

MySQL Enterprise Monitor 3.3.x < 3.3.9.3339 / 3.4.x < 3.4.7.4296 / 4.0.x < 4.0.4.5233 Multiple Vulnerabilities (April 2018 CPU)

MySQL Enterprise Monitor 3.4.x < 3.4.8 / 4.0.x < 4.0.5 / 8.0.x < 8.0.1 Multiple Vulnerabilities (July 2018 CPU)

MySQL Enterprise Monitor < 2.1.2 Multiple XSRF Vulnerabilities

MySQL Enterprise Monitor < 2.3.14 Apache Struts Multiple Vulnerabilities

MySQL Enterprise Monitor < 2.3.17 Multiple Vulnerabilities

MySQL Enterprise Monitor < 2.3.20 Apache Struts Predictable Token XSRF

MySQL Eventum Detection

N/X Web Content Management Multiple Script Remote File Inclusion

Nabopoll survey.inc.php path Parameter Remote File Inclusion

Nagios Core Detection

Nagios Core history.cgi Multiple Parameter Buffer Overflow

Nagios Looking Glass Addon for Nagios server/s3\_download.php File Disclosure

Nagios XI / Fusion Detection

Nagios XI 2011R1.9 Multiple SQL Injection Vulnerabilities

Nagios XI < 2011R1.9 Multiple Vulnerabilities

Nagios XI < 2012R1.6 Multiple Vulnerabilities

Nagios XI < 2012R2.4 tfPassword Parameter SQL Injection

NagiosQL Detection

Namazu < 2.0.14 Multiple Vulnerabilities

Narcissus backend.php release Parameter Remote Command Execution

NAS4Free Web UI Default Credentials

nBill component for Joomla! 'cid' Parameter SQLi

NCDSA HTTPd nph-test-cgi Arbitrary Directory Listing

NConf delete\_attr.php id Parameter SQL Injection

NCSA Campas cgi-bin Arbitrary Command Execution

NeoMail Session ID Weakness neomail-prefs.pl Arbitrary Mail-folder Manipulation

Net Optics Director Default Credentials

Net Optics Director Web Detection

NetApp OnTAP Web Detection

Netbilling nbmember.cgi cmd Parameter Information Disclosure

NetCharts Server Default Password

NetCode NC Book book.cgi current Parameter Arbitrary Command Execution

Netdynamics ndcgi.exe Previous User Session Replay

NETFile Default Credentials

NETFile FTP/Web Server Directory Traversal Arbitrary File Access

NetGain Enterprise Manager Command Injection

NetGain Enterprise Manager Detection

NETGEAR DGN Remote Unauthenticated Command Execution

NETGEAR GS105PE Pro Safe Switch Hard-coded Credentials

NETGEAR Multiple Model cgi-bin RCE

NETGEAR Multiple Model PHP Remote Command Injection

NETGEAR ReadyNAS Remote Unauthenticated Command Execution

NETGEAR Router Default Password (password) for 'admin' Account

NETGEAR SOAP Request Handling Remote Authentication Bypass

NETGEAR Wireless Access Point Hardcoded Default Password

NetIQ Access Manager 4.0 < 4.0 SP1 Hotfix 3 Multiple Vulnerabilities

NetIQ Access Manager Detect

NetIQ Privileged User Manager Default Admin Password

NetIQ Privileged User Manager Detection

NetIQ Privileged User Manager ldapagnt\_eval() Function Remote Code Execution (intrusive check)

NetIQ Privileged User Manager ldapagnt\_eval() Function Remote Code Execution (version check)

NetIQ Privileged User Manager Password Change Authentication Bypass (intrusive check)

NetIQ Privileged User Manager Password Change Authentication Bypass (version check)

NetIQ Privileged User Manager regclnt.dll Directory Traversal

NetIQ Sentinel Detection

netOffice Dwins demoSession Parameter Authentication Bypass

Netquery <= 3.1 Multiple Vulnerabilities

Netquery <= 3.11 nquser.php host Parameter Arbitrary Command Execution

Netref cat\_for\_gen.php Arbitrary PHP Command Injection

Netscape Enterprise Default Administrative Password

Netscape Enterprise Server Default Files Present

Netscape PSCOErrPage.htm errPagePath Parameter Traversal Arbitrary File Access

NetSupport Manager Gateway Detection

NetSupport Manager Gateway HTTP Protocol Information Disclosure

NetWin CWmail.exe Item Parameter Remote Overflow

Netwin Netauth netauth.cgi Traversal Arbitrary File Access

Netwin WebNews Webnews.exe Remote Overflow

NetworkActiv Web Server Crafted Filename Request Script Source Disclosure

Newbb\_plus Module for RunCMS Client-Ip Header SQL Injection

News Desk newsdesk.cgi t Parameter Traversal Arbitrary File Access

Newsletter Plugin for WordPress 'preview.php' 'data' Parameter Directory Traversal

NewsScript newsscript.pl mode Parameter Privilege Escalation

NextApp Echo XML Parsing Information Disclosure Vulnerability

NextGEN Smooth Gallery Plugin for WordPress 'galleryID' Parameter SQL Injection

Nimda Worm Infected HTML File Detection

Noah's Classifieds <= 1.3 Multiple Vulnerabilities

NOCC <= 1.0 Multiple Vulnerabilities

Nokia IPSO Voyager WebGUI readfile.tcl file Parameter Arbitrary File Access

NolaPro Default Credentials

NolaPro Detection

Novell 'modulemanager' Servlet Arbitrary File Upload (intrusive check)

Novell 'modulemanager' Servlet Arbitrary File Upload (safe check)

Novell eDirectory iMonitor HTTP Protocol Stack (httpstk) Host HTTP Header Remote Overflow

Novell GroupWise 'FileUploadServlet' Arbitrary File Access Vulnerability

Novell GroupWise Administration Console Detection

Novell GroupWise Document Viewer Agent Arbitrary File Download

Novell GroupWise WebAccess Arbitrary File Download

Novell GroupWise WebAccess Error Handler Authentication Bypass

Novell GroupWise WebAccess User.interface Directory Traversal

Novell GroupWise WebAccess WebAccessUninstall.ini Information Disclosure

Novell Identity Manager Role Based Provisioning Module Detection

Novell Identity Manager Role Based Provisioning Module Unspecified Vulnerability

Novell iManager < 2.7 SP1 Property Book Pages Arbitrary Plug-in Studio Deletion

Novell iManager < 2.7.6 Patch 1 Multiple Vulnerabilities

Novell iManager Detection

Novell iManager Unsupported Version

Novell Sentinel Log Manager Authentication Bypass

Novell Sentinel Log Manager Web Detection

Novell Teaming Default Credentials

Novell Teaming Detection

Novell Teaming Login User Account Enumeration Weakness

Novell ZENworks Asset Management Detection

Novell ZENworks Asset Management rtrlet Component GetFile\_Password Method Hardcoded Credentials Information Disclosure

Novell ZENworks Configuration Management < 11.2.4 Multiple Vulnerabilities

Novell ZENworks Configuration Management < 11.3.2 Remote Code Execution (intrusive check)

Novell ZENworks Control Center Detection

Novell ZENworks Control Center File Upload Remote Code Execution (intrusive check)

Novell ZENworks Mobile Management Detection

Novell ZENworks Mobile Management MDM.php Local File Inclusion

Nucleus CMS < 3.15 Multiple Vulnerabilities

Nucleus CMS action.php itemid Parameter SQL Injection

Nucleus CMS PLUGINADMIN.php DIR\_LIBS Parameter Remote File Inclusion

Nuked-Klan 1.2b Multiple Vulnerabilities

Nuked-Klan index.php Multiple Module Vulnerabilities

Nuked-Klan index.php user\_langue Parameter Traversal Arbitrary File Access

Nukedit utilities/login.asp email Parameter SQL Injection

Nukestyles.com viewpage.php Addon for PHP-Nuke File Parameter Traversal Arbitrary File Access

NUUO NVR Web Interface RCE

O'Reilly WebSite Pro args.bat Arbitrary Command Execution

O'Reilly WebSite uploader.exe Arbitrary File Upload

O'Reilly WebSite win-c-sample Remote Overflow

Observer <= 0.3.2.1 Multiple Remote Command Execution Vulnerabilities

Observium Detection

Observium PHP Object Unserialization Remote File Writing Vulnerability

Ocean12 ASP Calendar Administrative Access

Ocean12 ASP Guestbook Manager Database Download

ocPortal index.php req\_path Parameter Remote File Inclusion

OCS Inventory NG Server Administration Console Detection

OCS Inventory NG Server Administration Console header.php login Parameter SQL Injection

Oempro index.php FormValue\_Email Parameter SQL Injection Authentication Bypass

OmniHTTPd Encoded Space Request Script Source Disclosure

OmniHTTPd imagemap.exe CGI Remote Overflow

OmniHTTPd visadmin.exe Malformed URL DoS

OneOrZero Helpdesk default\_language Local File Inclusion

OneOrZero Helpdesk tinfo.php Arbitrary File Upload

OneOrZero Helpdesk tupdate.php sg Parameter SQL Injection

ONVIF Snapshot Username and Password Leak

ONVIF Username and Password leak

op5 Config Arbitrary Command Execution

op5 Monitor < 5.7.3 Multiple Vulnerabilities

op5 Monitor < 6.1.0 Information Disclosure and Security Bypass Vulnerabilities

op5 Monitor Credential Leak

op5 Monitor Detection

op5 Monitor Persistent Session Cookie

op5 Portal Arbitrary Command Execution

op5 Portal Detection

Open Conference System < 1.1.6 Multiple Script fullpath Parameter Remote File Inclusion

Open Redirect

Open Source Point Of Sale Default Credentials

Open Source Point Of Sale Detection

Open Source Point Of Sale Stored XSS

Open Virtual Desktop Detection

Open Web Analytics < 1.5.6 Multiple Vulnerabilities

Open Web Analytics Detection

Open Web Analytics owa\_email\_address SQL Injection

Open WebMail Detection

Open WebMail Shell Escape Arbitrary Command Execution

Open WebMail userstat.pl Arbitrary Command Execution

Open WebMail vacation.pl Arbitrary Command Execution

Open-AudIT include\_lang.php language Parameter Traversal Local File Inclusion

Open-Realty index.php select\_users\_lang Parameter Traversal Local File Inclusion

OpenAdmin Tool Detection

Openads Delivery Engine OA\_Delivery\_Cache\_store() Function name Argument Arbitrary PHP Code Execution

OpenBB < 1.0.9 Multiple Vulnerabilities

OpenBB index.php CID Parameter SQL Injection

OpenBiblio < 0.5.2 Multiple Scripts Local File Inclusion

OpenCA crypto-utils.lib libCheckSignature Function Signature Validation Weakness

OpenCA Multiple Signature Validation Bypass

OpenCart route Parameter Local File Inclusion

OpenCms < 6.2.2 Multiple Vulnerabilities

OpenConnect WebConnect < 6.5.1 Multiple Vulnerabilities

OpenDocMan Access Control Bypass

OpenEMR C\_FormEvaluation.class.php fileroot Parameter Remote File Inclusion

Openfiler Management Interface Default Administrator Credentials

Openfiler Management Interface Detection

Openfire < 3.6.3 Multiple Vulnerabilities

Openfire < 3.6.4 jabber:iq:auth Crafted password\_change Request Password Manipulation

Openfire < 3.9.2 XMPP-Layer DoS

Openfire Admin Console Detection

Openfire Admin Console Remote Privilege Escalation

Openfire AuthCheck Authentication Bypass

OpenMediaVault Default Administrator Credentials

OpenMediaVault Web Detection

OpenNetAdmin dcm.php options[desc] Parameter Arbitrary Remote PHP Code Execution

OpenNMS Web Console Default Credentials

OpenNMS Web Console Detection

OpenStack Glance Detection

OpenStack Keystone Default Credentials

OpenStack Keystone Detection

OpenWebMail < 1.90 Multiple Vulnerabilities

OpenWrt Router with a Blank Password (telnet check)

OpenX ac.php bannerid Parameter SQL Injection

OpenX fc.php MAX\_type Parameter Traversal Local File Inclusion

OpenX flowplayer-3.1.1.min.js Backdoor Remote Code Execution

OpenX install.php / install-plugin.php Admin Authentication Bypass

OpenX Open Flash Chart ofc\_upload\_image.php File Upload Arbitrary Code Execution

OpenX Source Detection

OpenX Source Unsupported Software Detection

Oracle Application Express (APEX) / REST Data Services Listener Detection

Oracle BI Publisher Default Credentials Check

Oracle BI Publisher Enterprise Detection

Oracle Business Intelligence Publisher (October 2012 CPU)

Oracle Business Intelligence Publisher April 2012 Critical Patch Update

Oracle Business Process Management Detection

Oracle Business Transaction Management 'FlashTunnelService' 'WriteToFile' Message RCE

Oracle Business Transaction Management Detection

Oracle Containers for J2EE Detection

Oracle Containers for J2EE Multiple Unspecified HTTP Vulnerabilities (April 2014 CPU)

Oracle Endeca Information Discovery Studio Detection

Oracle Endeca Information Discovery Studio Multiple Vulnerabilities (October 2014 CPU)

Oracle Enterprise Data Quality Dashboard Detection

Oracle Enterprise Data Quality Director Detection

Oracle Enterprise Data Quality Multiple Vulnerabilities (October 2014 CPU)

Oracle Enterprise Manager Database Express (EM Express) Detection

Oracle GlassFish Server Administration Console Default Credentials

Oracle GlassFish Server Administration Console GET Request Authentication Bypass

Oracle GlassFish Server Path Traversal

Oracle GlassFish Server Request Handling Remote File Disclosure

Oracle GlassFish Server URL normalization Denial of Service

Oracle Identity Analytics / Sun Role Manager Unspecified Remote Vulnerability (April 2014 CPU)

Oracle Identity Analytics Detection

Oracle Integrated Lights Out Manager (ILOM) < 3.2.6 Multiple Vulnerabilities (uncredentialed check)

Oracle Integrated Lights Out Manager (ILOM) < 4.0.2.1 Multiple Vulnerabilities (uncredentialed check)

Oracle Integrated Lights Out Manager Web Detection

Oracle JavaServer Faces Multiple Partial Directory Traversals

Oracle MapViewer Detection

Oracle MapViewer Multiple Vulnerabilities (July 2012 CPU)

Oracle OpenSSO Agent Multiple Vulnerabilities (October 2014 CPU)

Oracle OpenSSO Detection

Oracle OpenSSO Multiple Vulnerabilities (April 2014 CPU)

Oracle OpenSSO SAML Multiple Vulnerabilities (January 2015 CPU)

Oracle Policy Automation (Oracle Web Determinations) Unspecified Remote Security Vulnerability (July 2013 CPU)

Oracle Portal Demo Organization Chart Detection

Oracle Portal Demo Organization Chart SQL Injection

Oracle Portal Detection

Oracle Primavera Gateway (Apr 2020 CPU)

Oracle Primavera Gateway Multiple Vulnerabilities (Apri 2017 CPU)

Oracle Primavera Gateway Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Primavera Gateway Multiple Vulnerabilities (Jul 2019 CPU)

Oracle Primavera Gateway Multiple Vulnerabilities (July 2017 CPU)

Oracle Primavera Gateway Multiple Vulnerabilities (Oct 2018 CPU)

Oracle Primavera Gateway Multiple Vulnerabilities (Oct 2019 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (Apr 2019 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (Apr 2020 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (April 2018 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (Jan 2019 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (July 2017 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (July 2018 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (Oct 2019 CPU)

Oracle Primavera P6 Enterprise Project Portfolio Management (EPPM) Multiple Vulnerabilities (October 2018 CPU)

Oracle Primavera Unifier (Apr 2020 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (Apr 2019 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (April 2018 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (Jan 2019 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (Jan 2020 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (Jul 2019 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (July 2017 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (July 2018 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (Oct 2018 CPU)

Oracle Primavera Unifier Multiple Vulnerabilities (Oct 2019 CPU)

Oracle Primavera Unifier Platform Component Unspecified Remote Issue (January 2018 CPU)

Oracle Real User Experience Insight (Apr 2020 CPU)

Oracle Real User Experience Insight Detection

Oracle Real User Experience Insight October 2014 CPU

Oracle Reports Servlet Detection

Oracle Reports Servlet Parsequery Function Remote Database Credentials Exposure

Oracle Reports Servlet Remote File Access

Oracle Secure Backup Administration Server Authentication Bypass

Oracle Secure Backup Administration Server login.php Arbitrary Command Injection

Oracle Secure Backup Administration Server login.php Authentication Bypass

Oracle Secure Backup Administration Server login.php uname Parameter Arbitrary Command Injection

Oracle Secure Global Desktop Administration Console Detection

Oracle Traffic Director Administration Console Detection

Oracle Web Determinations Detection

Oracle WebCenter Content 'GET\_SEARCH\_RESULTS' SQL Injection

Oracle WebCenter Content (April 2013 CPU)

Oracle WebCenter Content (July 2013 CPU)

Oracle WebCenter Content Default Administration Credentials

Oracle WebCenter Content Detection

Oracle WebCenter Content Multiple Vulnerabilities (January 2018 CPU)

Oracle WebCenter Content Server Component Unspecified Issue (October 2017 CPU)

Oracle WebCenter Content Server Multiple Vulnerabilities (July 2017 CPU)

Oracle WebCenter Content Server Multiple Vulnerabilities (October 2015 CPU)

Oracle WebCenter Content Server Remote Security Vulnerability (January 2015 CPU)

Oracle WebCenter Content Server Subcomponent Remote Issue (October 2013 CPU)

Oracle WebCenter Sites Default Credentials Check

Oracle WebCenter Sites Detection

Oracle WebLogic Default Credentials

Oracle WebLogic Server Multiple Vulnerabilities (April 2013 CPU)

OraMon config/oramon.ini Information Disclosure

OrangeHRM login.php txtUserName Parameter SQL Injection

Oreon lang/index.php file Parameter Remote File Inclusion

OrientDB < 2.0.15 / 2.1.1 XSRF

OrientDB < 2.0.7 / 2.1.0 Weak Session IDs

Original inc/exif.inc.php exif\_prog Parameter Arbitrary Command Execution

Orion Application Server Crafted Filename Extension JSP Script Source Disclosure

OS Command Injection

osCommerce Customer Testimonials customer\_testimonials.php testimonial\_id Parameter SQL Injection

osCommerce Detection

osCommerce file\_manager.php Arbitrary PHP Code Injection

osCommerce file\_manager.php Arbitrary PHP Code Injection (intrusive check)

osCommerce file\_manager.php filename Parameter Traversal Arbitrary File Access

osCommerce shopping\_cart.php id Array Parameters SQL Injection

osCommerce Unprotected Admin Directory

osCommerce update.php readme\_file Parameter Arbitrary File Disclosure

OSSIM 'host/draw\_tree.php' Access Restriction Weakness Information Disclosure

OSSIM < 4.3.2 Multiple SQL Injection Vulnerabilities

OSSIM < 4.3.3.1 tele\_stats.php SQL Injection

OSSIM download.php Directory Traversal

OSSIM SOAP Service Detection

OSSIM tele\_compress.php Directory Traversal

OSSIM Web Frontend Default Credentials

osTicket <= 1.2.7 Multiple Vulnerabilities

osTicket <= 1.3.1 Multiple Vulnerabilities

osTicket Arbitrary Attachment Disclosure

osTicket Attachment Handling File Upload Arbitrary Code Execution

osTicket Detection

osTicket Form Field Modification File Upload Size Restriction Bypass

osTicket open.php Support Address Crafted Mail Loop Remote DoS

osTicket setup.php Accessibility

OTRS Authenticated Remote Code Execution (OSA-2017-07)

OTRS Authenticated Remote Code Execution (OSA-2017-09)

OTRS SOAP Interface Unauthenticated Object Manipulation

OTRS Unspecified Remote Code Execution (OSA-2017-04)

Owl < 0.74.0 Multiple Vulnerabilities

Owl browse.php Authentication Bypass

Owl Intranet Engine <= 0.91 Multiple Vulnerabilities

Owl Intranet Engine lib/OWL\_API.php xrms\_file\_root Parameter Remote File Inclusion

ownCloud Web Interface Detection

P-News p-news.php Name Field Privilege Escalation

P-Synch Password Management Multiple Vulnerabilities

Packeteer PacketShaper Web Management rpttop.htm Crafted Request Remote DoS

Packeteer Web Management Interface Authentication

Packeteer Web Management Interface Detection

Packeteer Web Management Interface Version Detection

PacketVideo TwonkyServer Detection

PacketVideo TwonkyServer Directory Traversal

paFAQ 1.0 Beta 4 Multiple Vulnerabilities

paFileDB <= 3.1 Multiple Vulnerabilities (1)

paFileDB <= 3.1 Multiple Vulnerabilities (2)

paFileDB auth.php pafiledbcookie Cookie SQL Injection

paFileDB Detection

paFileDB includes/search.php categories Parameter SQL Injection

PAFileDB Multiple Script Error Message Path Disclosure

paFileDB pafiledb.php Multiple Parameter SQL Injection

paFileDB sessions Directory Admin Hashed Password Disclosure

Pages Pro filenote Parameter Traversal Arbitrary File Modification

Pagesetter for PostNuke index.php id Parameter Traversal Arbitrary File Access

PAJAX < 0.5.2 Multiple Vulnerabilities

Palo Alto Expedition < 1.1.13 Cross-Site Scripting Vulnerability (PAN-SA-2019-0009)

Palo Alto Networks PAN-OS Management Interface RCE (PAN-SA-2017-0027)

PALS Library System WebPALS pals-cgi Multiple Vulnerabilities

Pandora FMS <= 5.0 SP2 SQLi

Pandora FMS <= 5.1 SP1 XSS

Pandora FMS Console Authentication Bypass

Pandora FMS Console Default Credentials

Pandora FMS Console Detection

paNews 2.0.4b Multiple Input Validation Vulnerabilities

paNews admin\_setup.php Multiple Parameter Arbitrary PHP Code Injection

paNews Detection

Participants Database Plugin for WordPress 'query' Parameter SQL Injection

Participants Database Plugin for WordPress < 1.5.4.9 'query' Parameter SQL Injection

PatchLink Update /dagent/downloadreport.asp Multiple Parameter SQL Injection

PatchLink Update Server checkprofile.asp checkid Parameter SQL Injection

PatchLink Update Server nwupload.asp Traversal Arbitrary File Write

PatchLink Update Server proxyreg.asp Arbitrary Proxy Manipulation

PBLang 4.65 Multiple Vulnerabilities

PBLang < 4.66z Multiple Vulnerabilities

PBLang BBS <= 4.65 Multiple Vulnerabilities

PBLang login.php lang Parameter Local File Inclusion

PCCS-Mysql User/Password Exposure

PCS Daemon (pcsd) Cookie Signing Multiple Vulnerabilities

PD9 MegaBBS Multiple Vulnerabilities

PDGSoft Shopping Cart Multiple Vulnerabilities

PerlCal cal\_make.pl p0 Parameter Traversal Arbitrary File Read

PerlDesk kb.cgi view Parameter SQL Injection

PerlDesk pdesk.cgi lang Parameter Traversal Arbitrary File Access

pfSense < 2.1.3 Remote Denial of Service Vulnerability (SA-14\_05)

pfSense < 2.1.4 Multiple Vulnerabilities (SA-14\_08 - SA-14\_12)

pfSense < 2.1.5 Multiple Vulnerabilities ( SA-14\_14 )

pfSense < 2.1.5 Multiple Vulnerabilities (SA-14\_15 - SA-14\_17)

pfSense < 2.2.1 Multiple Vulnerabilities (SA-15\_02 - SA-15\_04)

pfSense < 2.2.2 Multiple Vulnerabilities (SA-15\_05)

pfSense < 2.3.1-p1 Multiple Vulnerabilities (SA-16\_05)

pfSense < 2.3.4-p1 Multiple Vulnerabilities (SA-17\_05 / SA-17\_06)

PGPMail.pl detection

Philboard /database/philboard.mdb Direct Request Database Disclosure

Philboard philboard\_admin.ASP Authentication Bypass

Phorum common.php ForumLang Parameter Traversal Arbitrary File Access

Phorum Detection

Phorum search.php location Parameter HTTP Response Splitting

PhotoPost < 5.1 Multiple Input Validation Vulnerabilities

PhotoPost PHP < 5.0.1 Multiple Remote Vulnerabilities

PhotoPost PHP Detection

Photopost PHP Pro photo Parameter SQL Injection

PHP 4.x < 4.3.0 ZendEngine Integer Overflow

PHP 5 < 5.2.7 Multiple Vulnerabilities

PHP 5.1.x < 5.1.2 Multiple Vulnerabilities

PHP 5.1.x < 5.1.5 Multiple Vulnerabilities

PHP 5.2 < 5.2.14 Multiple Vulnerabilities

PHP 5.2 < 5.2.15 Multiple Vulnerabilities

PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS

PHP 5.2.x filter\_globals Subsequence Request Parsing Remote Code Execution

PHP 5.3 < 5.3.1 Multiple Vulnerabilities

PHP 5.3 < 5.3.3 Multiple Vulnerabilities

PHP 5.3 < 5.3.4 Multiple Vulnerabilities

PHP 5.3 < 5.3.6 Multiple Vulnerabilities

PHP 5.3 < 5.3.7 Multiple Vulnerabilities

PHP 5.3.7 crypt() MD5 Incorrect Return Value

PHP 5.3.9 'php\_register\_variable\_ex()' Code Execution (banner check)

PHP 5.3.9 'php\_register\_variable\_ex()' Code Execution (intrusive check)

PHP 5.3.x < 5.3.13 CGI Query String Code Execution

PHP 5.3.x < 5.3.14 Multiple Vulnerabilities

PHP 5.3.x < 5.3.15 Multiple Vulnerabilities

PHP 5.3.x < 5.3.21 cURL X.509 Certificate Domain Name Matching MiTM Weakness

PHP 5.3.x < 5.3.22 Multiple Vulnerabilities

PHP 5.3.x < 5.3.23 Multiple Vulnerabilities

PHP 5.3.x < 5.3.26 Multiple Vulnerabilities

PHP 5.3.x < 5.3.27 Multiple Vulnerabilities

PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities

PHP 5.3.x < 5.3.29 Multiple Vulnerabilities

PHP 5.4.x < 5.4.0 Multiple Vulnerabilities

PHP 5.4.x < 5.4.1 Multiple Vulnerabilities

PHP 5.4.x < 5.4.11 cURL X.509 Certificate Domain Name Matching MiTM Weakness

PHP 5.4.x < 5.4.12 Information Disclosure

PHP 5.4.x < 5.4.13 Information Disclosure

PHP 5.4.x < 5.4.16 Multiple Vulnerabilities

PHP 5.4.x < 5.4.17 Buffer Overflow

PHP 5.4.x < 5.4.19 Multiple Vulnerabilities

PHP 5.4.x < 5.4.23 OpenSSL openssl\_x509\_parse() Memory Corruption

PHP 5.4.x < 5.4.24 Multiple Vulnerabilities

PHP 5.4.x < 5.4.26 Multiple Vulnerabilities

PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS

PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation

PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities

PHP 5.4.x < 5.4.3 Multiple Vulnerabilities

PHP 5.4.x < 5.4.30 Multiple Vulnerabilities

PHP 5.4.x < 5.4.31 CLI Server 'header' DoS

PHP 5.4.x < 5.4.32 Multiple Vulnerabilities

PHP 5.4.x < 5.4.34 Multiple Vulnerabilities

PHP 5.4.x < 5.4.35 'donote' DoS

PHP 5.4.x < 5.4.36 'process\_nested\_data' RCE

PHP 5.4.x < 5.4.37 Multiple Vulnerabilities

PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)

PHP 5.4.x < 5.4.39 Multiple Vulnerabilities

PHP 5.4.x < 5.4.4 Multiple Vulnerabilities

PHP 5.4.x < 5.4.40 Multiple Vulnerabilities

PHP 5.4.x < 5.4.41 Multiple Vulnerabilities

PHP 5.4.x < 5.4.42 Multiple Vulnerabilities

PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)

PHP 5.4.x < 5.4.44 Multiple Vulnerabilities

PHP 5.4.x < 5.4.45 Multiple Vulnerabilities

PHP 5.4.x < 5.4.5 \_php\_stream\_scandir Overflow

PHP 5.5.x < 5.5.1 xml.c Buffer Overflow

PHP 5.5.x < 5.5.10 Multiple Vulnerabilities

PHP 5.5.x < 5.5.11 awk Magic Parsing BEGIN DoS

PHP 5.5.x < 5.5.12 FPM Unix Socket Insecure Permission Escalation

PHP 5.5.x < 5.5.13 'src/cdf.c' Multiple Vulnerabilities

PHP 5.5.x < 5.5.14 Multiple Vulnerabilities

PHP 5.5.x < 5.5.15 Multiple Vulnerabilities

PHP 5.5.x < 5.5.16 Multiple Vulnerabilities

PHP 5.5.x < 5.5.18 Multiple Vulnerabilities

PHP 5.5.x < 5.5.19 'donote' DoS

PHP 5.5.x < 5.5.20 'process\_nested\_data' RCE

PHP 5.5.x < 5.5.21 Multiple Vulnerabilities

PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)

PHP 5.5.x < 5.5.23 Multiple Vulnerabilities

PHP 5.5.x < 5.5.24 Multiple Vulnerabilities

PHP 5.5.x < 5.5.25 Multiple Vulnerabilities

PHP 5.5.x < 5.5.26 Multiple Vulnerabilities

PHP 5.5.x < 5.5.27 Multiple Vulnerabilities (BACKRONYM)

PHP 5.5.x < 5.5.28 Multiple Vulnerabilities

PHP 5.5.x < 5.5.29 Multiple Vulnerabilities

PHP 5.5.x < 5.5.3 Multiple Vulnerabilities

PHP 5.5.x < 5.5.30 Multiple Vulnerabilities

PHP 5.5.x < 5.5.32 Multiple Vulnerabilities

PHP 5.5.x < 5.5.33 Multiple Vulnerabilities

PHP 5.5.x < 5.5.34 Multiple Vulnerabilities

PHP 5.5.x < 5.5.35 Multiple Vulnerabilities

PHP 5.5.x < 5.5.36 Multiple Vulnerabilities

PHP 5.5.x < 5.5.37 Multiple Vulnerabilities

PHP 5.5.x < 5.5.38 Multiple Vulnerabilities (httpoxy)

PHP 5.5.x < 5.5.7 OpenSSL openssl\_x509\_parse() Memory Corruption

PHP 5.5.x < 5.5.8 Multiple Vulnerabilities

PHP 5.5.x < 5.5.9 GD Extension Multiple Vulnerabilities

PHP 5.6.0 Multiple Vulnerabilities

PHP 5.6.x < 5.6.1 'add\_post\_var' Code Execution

PHP 5.6.x < 5.6.10 Multiple Vulnerabilities

PHP 5.6.x < 5.6.11 Multiple Vulnerabilities (BACKRONYM)

PHP 5.6.x < 5.6.12 Multiple Vulnerabilities

PHP 5.6.x < 5.6.13 Multiple Vulnerabilities

PHP 5.6.x < 5.6.14 Multiple Vulnerabilities

PHP 5.6.x < 5.6.18 Multiple Vulnerabilities

PHP 5.6.x < 5.6.19 Multiple Vulnerabilities

PHP 5.6.x < 5.6.2 Multiple Vulnerabilities

PHP 5.6.x < 5.6.20 Multiple Vulnerabilities

PHP 5.6.x < 5.6.21 Multiple Vulnerabilities

PHP 5.6.x < 5.6.22 Multiple Vulnerabilities

PHP 5.6.x < 5.6.23 Multiple Vulnerabilities

PHP 5.6.x < 5.6.24 Multiple Vulnerabilities (httpoxy)

PHP 5.6.x < 5.6.25 Multiple Vulnerabilities

PHP 5.6.x < 5.6.26 Multiple Vulnerabilities

PHP 5.6.x < 5.6.27 Multiple Vulnerabilities

PHP 5.6.x < 5.6.28 Multiple Vulnerabilities

PHP 5.6.x < 5.6.29 Multiple Vulnerabilities

PHP 5.6.x < 5.6.3 'donote' DoS

PHP 5.6.x < 5.6.30 Multiple DoS

PHP 5.6.x < 5.6.31 Multiple Vulnerabilities

PHP 5.6.x < 5.6.32 Multiple Vulnerabilities

PHP 5.6.x < 5.6.33 Multiple Vulnerabilities

PHP 5.6.x < 5.6.34 Stack Buffer Overflow

PHP 5.6.x < 5.6.35 Security Bypass Vulnerability

PHP 5.6.x < 5.6.36 Multiple Vulnerabilities

PHP 5.6.x < 5.6.37 exif\_thumbnail\_extract() DoS

PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability

PHP 5.6.x < 5.6.39 Multiple vulnerabilities

PHP 5.6.x < 5.6.4 'process\_nested\_data' RCE

PHP 5.6.x < 5.6.40 Multiple vulnerabilities.

PHP 5.6.x < 5.6.5 Multiple Vulnerabilities

PHP 5.6.x < 5.6.6 Multiple Vulnerabilities (GHOST)

PHP 5.6.x < 5.6.7 Multiple Vulnerabilities

PHP 5.6.x < 5.6.8 Multiple Vulnerabilities

PHP 5.6.x < 5.6.9 Multiple Vulnerabilities

PHP 5.x < 5.1.0 Multiple Vulnerabilities

PHP 5.x < 5.2 Multiple Vulnerabilities

PHP 5.x < 5.2.2 Multiple vulnerabilities

PHP 7.0.x < 7.0.0 Multiple Vulnerabilities

PHP 7.0.x < 7.0.1 Multiple Vulnerabilities

PHP 7.0.x < 7.0.10 Multiple Vulnerabilities

PHP 7.0.x < 7.0.11 Multiple Vulnerabilities

PHP 7.0.x < 7.0.12 Multiple Vulnerabilities

PHP 7.0.x < 7.0.13 Multiple Vulnerabilities

PHP 7.0.x < 7.0.14 Multiple Vulnerabilities

PHP 7.0.x < 7.0.15 Multiple Vulnerabilities

PHP 7.0.x < 7.0.16 Multiple Vulnerabilities

PHP 7.0.x < 7.0.17 Denial of Service Vulnerability

PHP 7.0.x < 7.0.19 Multiple Vulnerabilities

PHP 7.0.x < 7.0.20 Multiple Vulnerabilities

PHP 7.0.x < 7.0.21 Multiple Vulnerabilities

PHP 7.0.x < 7.0.22 Denial of Service Vulnerability

PHP 7.0.x < 7.0.23 Heap-based Buffer Overflow Vulnerability

PHP 7.0.x < 7.0.25 Multiple Vulnerabilities

PHP 7.0.x < 7.0.27 Multiple Vulnerabilities

PHP 7.0.x < 7.0.28 Stack Buffer Overflow

PHP 7.0.x < 7.0.3 Multiple Vulnerabilities

PHP 7.0.x < 7.0.30 Multiple Vulnerabilities

PHP 7.0.x < 7.0.31 Use After Free Arbitrary Code Execution in EXIF

PHP 7.0.x < 7.0.32 Transfer-Encoding Parameter XSS Vulnerability

PHP 7.0.x < 7.0.33 Multiple vulnerabilities

PHP 7.0.x < 7.0.4 Multiple Vulnerabilities

PHP 7.0.x < 7.0.5 Multiple Vulnerabilities

PHP 7.0.x < 7.0.6 Multiple Vulnerabilities

PHP 7.0.x < 7.0.7 Multiple Vulnerabilities

PHP 7.0.x < 7.0.8 Multiple Vulnerabilities

PHP 7.0.x < 7.0.9 Multiple Vulnerabilities (httpoxy)

PHP 7.1.x < 7.1.0 Multiple Vulnerabilities.

PHP 7.1.x < 7.1.1 Multiple Vulnerabilities

PHP 7.1.x < 7.1.11 Multiple Vulnerabilities

PHP 7.1.x < 7.1.13 Multiple Vulnerabilities

PHP 7.1.x < 7.1.15 Stack Buffer Overflow

PHP 7.1.x < 7.1.17 Multiple Vulnerabilities

PHP 7.1.x < 7.1.2 Multiple Vulnerabilities

PHP 7.1.x < 7.1.20 exif\_thumbnail\_extract() DoS

PHP 7.1.x < 7.1.22 Transfer-Encoding Parameter XSS Vulnerability

PHP 7.1.x < 7.1.25 Multiple vulnerabilities

PHP 7.1.x < 7.1.26 Multiple vulnerabilities.

PHP 7.1.x < 7.1.27 Multiple vulnerabilities.

PHP 7.1.x < 7.1.28 Multiple vulnerabilities.

PHP 7.1.x < 7.1.29 Heap-based Buffer Overflow Vulnerability.

PHP 7.1.x < 7.1.3 Denial of Service Vulnerability

PHP 7.1.x < 7.1.30 Multiple Vulnerabilities.

PHP 7.1.x < 7.1.31 Multiple Vulnerabilities.

PHP 7.1.x < 7.1.5 Multiple Vulnerabilities

PHP 7.1.x < 7.1.6 Multiple Vulnerabilities

PHP 7.1.x < 7.1.7 Multiple Vulnerabilities

PHP 7.1.x < 7.1.8 Denial of Service Vulnerability

PHP 7.1.x < 7.1.9 Heap-based Buffer Overflow Vulnerability

PHP 7.2.x < 7.2.0 Heap-based Buffer Overflow Vulnerability

PHP 7.2.x < 7.2.1 Multiple Vulnerabilities

PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability

PHP 7.2.x < 7.2.13 Multiple vulnerabilities

PHP 7.2.x < 7.2.14 Multiple vulnerabilities.

PHP 7.2.x < 7.2.16 Multiple vulnerabilities.

PHP 7.2.x < 7.2.17 Multiple vulnerabilities.

PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability.

PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.

PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.

PHP 7.2.x < 7.2.26 Multiple Vulnerabilities

PHP 7.2.x < 7.2.27 / PHP 7.3.x < 7.3.14 / 7.4.x < 7.4.2 Multiple Vulnerabilities

PHP 7.2.x < 7.2.28 / PHP 7.3.x < 7.3.15 / 7.4.x < 7.4.3 Multiple Vulnerabilities

PHP 7.2.x < 7.2.29 Multiple Vulnerabilities

PHP 7.2.x < 7.2.3 Stack Buffer Overflow

PHP 7.2.x < 7.2.5 Stack Buffer Overflow

PHP 7.2.x < 7.2.8 Use After Free Arbitrary Code Execution in EXIF

PHP 7.3.0 [alpha|beta] < 7.3.0 Multiple vulnerabilities

PHP 7.3.x < 7.3.1 Multiple vulnerabilities.

PHP 7.3.x < 7.3.10 Heap-Based Buffer Overflow Vulnerability.

PHP 7.3.x < 7.3.13 / 7.4.x < 7.4.1 Multiple Vulnerabilities

PHP 7.3.x < 7.3.16 Multiple Vulnerabilities

PHP 7.3.x < 7.3.2 Information Disclosure.

PHP 7.3.x < 7.3.3 Multiple vulnerabilities.

PHP 7.3.x < 7.3.4 Multiple vulnerabilities.

PHP 7.3.x < 7.3.5 Heap-based Buffer Overflow Vulnerability.

PHP 7.3.x < 7.3.6 Multiple Vulnerabilities.

PHP 7.3.x < 7.3.7 Multiple Vulnerabilities.

PHP 7.3.x < 7.3.8 Multiple Vulnerabilities.

PHP 7.3.x < 7.3.9 Multiple Vulnerabilities.

PHP 7.4.x < 7.4.0 Multiple Vulnerabilities.

PHP 7.x < 7.0.2 Multiple Vulnerabilities

PHP < 3.0 mylog.html/mlog.html Arbitrary File Access

PHP < 4.0.4 IMAP Module imap\_open() Function Overflow

PHP < 4.2.x mail Function CRLF Injection

PHP < 4.3.1 CGI Module Force Redirect Settings Bypass Arbitrary File Access

PHP < 4.3.10 / 5.0.3 Multiple Vulnerabilities

PHP < 4.3.11 / 5.0.3 Multiple Unspecified Vulnerabilities

PHP < 4.3.3 Multiple Vulnerabilities

PHP < 4.3.3 php\_check\_safe\_mode\_include\_dir Function Safemode Bypass

PHP < 4.3.8 Multiple Vulnerabilities

PHP < 4.4.1 / 5.0.6 Multiple Vulnerabilities

PHP < 4.4.3 / 5.1.4 Multiple Vulnerabilities

PHP < 4.4.4 Multiple Vulnerabilities

PHP < 4.4.5 Multiple Vulnerabilities

PHP < 4.4.7 / 5.2.2 Multiple Vulnerabilities

PHP < 4.4.8 Multiple Vulnerabilities

PHP < 4.4.9 Multiple Vulnerabilities

PHP < 5.2.1 Multiple Vulnerabilities

PHP < 5.2.10 Multiple Vulnerabilities

PHP < 5.2.11 Multiple Vulnerabilities

PHP < 5.2.12 Multiple Vulnerabilities

PHP < 5.2.3 Multiple Vulnerabilities

PHP < 5.2.4 Multiple Vulnerabilities

PHP < 5.2.5 Multiple Vulnerabilities

PHP < 5.2.6 Multiple Vulnerabilities

PHP < 5.2.8 Multiple Vulnerabilities

PHP < 5.2.9 Multiple Vulnerabilities

PHP < 5.3.11 Multiple Vulnerabilities

PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution

PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities

PHP < 5.3.9 Multiple Vulnerabilities

PHP < 5.6.37 or 7.2.x < 7.2.8 Multiple Vulnerabilities (Deprecated)

PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

PHP Advanced Transfer Manager <= 1.21 Multiple Vulnerabilities

PHP Advanced Transfer Manager <= 1.30 Multiple Vulnerabilities

PHP Doc System index.php show Parameter Local File Inclusion

PHP Easy Download admin/save.php moreinfo Parameter Code Injection

PHP Error Log Format String Command Injection

PHP Foreign Function Interface Arbitrary DLL Loading safe\_mode Restriction Bypass

PHP iCalendar Cookie Data Traversal Local File Inclusion

PHP iCalendar index.php phpicalendar Parameter Remote File Inclusion

PHP iCalendar Multiple Script Remote File Inclusion

PHP iCalendar publish.ical.php Arbitrary File Upload

PHP ip2long Function String Validation Weakness

PHP Live Helper Multiple Remote File Inclusions

PHP Live! directory/conf File Include Unspecified Issue

PHP Mail Function Header Spoofing

PHP mb\_send\_mail() Function Parameter Security Bypass

PHP Multiple Image Processing Functions File Handling DoS

PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

PHP PHP\_RSHUTDOWN\_FUNCTION Security Bypass

PHP php\_variables.c Multiple Variable Open Bracket Memory Disclosure

PHP prior to 5.5.x < 5.5.31 / 5.6.x < 5.6.17 Multiple Vulnerabilities

PHP rfc1867.c $\_FILES Array Crafted MIME Header Arbitrary File Upload

PHP Rocket for FrontPage phprocketaddin page Parameter Traversal Arbitrary File Access

PHP Safe Mode mail Function 5th Parameter Arbitrary Command Execution

PHP socket\_iovec\_alloc() Function Overflow

PHP Support Tickets index.php Multiple Parameter SQL Injection

PHP Surveyor Multiple Vulnerabilities

PHP Symlink Function Race Condition open\_basedir Bypass

PHP Topsites counter.php count\_log\_file Parameter Arbitrary File Overwrite

PHP TopSites setup.php Administration Authentication Bypass

PHP Unsupported Version Detection

PHP Upload Center index.php filename Parameter Directory Traversal Arbitrary File Access

PHP Version 5 Hash Collision Form Parameter Parsing Remote DoS

PHP Xdebug Module Unauthenticated RCE (exploit)

PHP-Blogger pref.db Database Information Disclosure

PHP-Calendar includes/search.php Multiple Parameter SQL Injection

PHP-Calendar Multiple Script phpc\_root\_path Parameter Remote File Inclusion

php-Charts Detection

php-Charts url.php Remote PHP Code Execution

php-Charts wizard/index.php PHP Execution

PHP-Fusion 4.01 Multiple Vulnerabilities

PHP-Fusion < 5.00 viewthread.php Arbitrary Message Thread / Forum Access

PHP-Fusion < 6.00.110 Multiple Scripts SQL Injection

PHP-Fusion <= 6.00.105 Multiple Vulnerabilities

PHP-Fusion <= 6.00.106 Multiple Vulnerabilities

PHP-Fusion Authenticate.class.php Multiple Cookie SQL Injection

PHP-Fusion Database Backup Disclosure

PHP-Fusion Detection

PHP-Fusion extract() Global Variable Overwriting

PHP-Kit <= 1.6.1 RC2 Multiple Vulnerabilities

PHP-Nuke Detection

PHP-Nuke Gallery Add-on modules.php include Parameter Traversal Arbitrary File Access

PHP-Nuke Network Tools Add-On Arbitrary Command Execution

PHP-Nuke opendir.php Traversal Arbitrary File Read

PHP-Nuke sql\_debug Information Disclosure

PHP-Ping index.php pingto Parameter Arbitrary Code Execution

PHP-Ping php-ping.php count Parameter Arbitrary Command Execution

php-proxima autohtml.php Arbitrary File Retrieval

PHP-Update blog.php Variable Overwriting Arbitrary Code Execution

PHP/FI php.cgi Traversal Arbitrary File Access

PHP3 Physical Path Disclosure via POST Requests

phpAdsNew / phpPgAds < 2.0.6 Multiple Vulnerabilities

phpAdsNew helperfunction.php Remote File Inclusion

phpAdsNew XML-RPC Library Remote Code Injection

phpAlbum language.php data\_dir Parameter Remote File Inclusion

Phpauction <= 2.5 Multiple Vulnerabilities

PHPAuction Admin Authentication Bypass

PHPAuction Multiple Script include\_path Parameter File Inclusion

phPay admin/phpinfo.php Information Disclosure

phpBannerExchange Template Class Local File Inclusion

phpBB < 2.0.11 Multiple Vulnerabilities (ESMARKCONANT)

phpBB < 2.0.16 viewtopic.php Highlighting Feature Arbitrary PHP Code Execution

phpBB < 2.0.17 Nested BBCode URL Tags XSS

phpBB < 2.0.19 Multiple XSS

phpBB < 2.0.22 Multiple Vulnerabilities

phpBB < 2.0.7 Multiple Script SQL Injection

phpBB < 2.0.9 Multiple Vulnerabilities

phpBB <= 2.0.11 Multiple Vulnerabilities

phpBB <= 2.0.12 Multiple Vulnerabilities

phpBB <= 2.0.13 Multiple Vulnerabilities

phpBB <= 2.0.14 Multiple Vulnerabilities

phpBB <= 2.0.17 Multiple Vulnerabilities

phpBB Advanced GuestBook addentry.php phpbb\_root\_path Parameter Remote File Inclusion

phpBB Cash\_Mod admin\_cash.php Arbitrary Command Execution

phpBB Detection

phpBB Fetch All < 2.0.12 Multiple Scripts SQL Injection

phpBB Knowledge Base Module kb.php cat Parameter SQL Injection

phpBB Multiple Module phpbb\_root\_path Parameter Remote File Inclusion

phpBB Photo Album Module <= 2.0.53 Multiple Vulnerabilities

phpBB up.php Arbitrary File Upload

phpBB viewtopic.php highlight Parameter SQL Injection (ESMARKCONANT)

phpBB viewtopic.php topic\_id Parameter SQL Injection

PHPCatalog id Parameter SQL Injection

phpCOIN < 1.2.2 2005-12-13 Fix-File Multiple Vulnerabilities

phpCOIN <= 1.2.1b Multiple Vulnerabilities

phpCOIN <= 1.2.2 Multiple SQL Injection Vulnerabilities

phpCOIN Multiple Script \_CCFG Parameter Remote File Inclusion

PhpDig < 1.8.5 Unspecified Vulnerability

PhpDig config.php relative\_script\_path Parameter Remote File Inclusion

phpDocumentor <= 1.3.0 RC4 Local And Remote File Inclusion

PHPFM Arbitrary File Upload

phpFormGenerator Arbitrary File Upload

phpGedView Arbitrary File Access / Remote File Inclusion

PhpGedView Detection

PhpGedView module.php pgvaction Parameter Traversal Local File Inclusion

PhpGedView PGV\_BASE\_DIRECTORY Parameter Remote File Inclusion

phpGroupWare < 0.9.16 Addressbook Unspecified Vulnerability

phpGroupWare <= 0.9.16.003 Multiple Vulnerabilities

phpGroupWare Admin/Setup Password Plaintext Cookie Storage

phpGroupWare Calendar Module Holiday File Save Extension Feature Arbitrary File Execution

phpGroupWare Detection

phpGroupWare index.php Addressbook XSS

phpGroupWare Multiple Module SQL Injection

phpGroupWare phpgw.inc.php phpgw\_info Parameter Remote File Inclusion

phpGroupWare Unspecified Remote File Inclusion

PHPix album Parameter Encoded Traversal Arbitrary File/Directory Access

PHPix index.phtml Multiple Parameter Arbitrary Command Execution

phpLDAPadmin Anonymous Bind Security Bypass Vulnerability

phpLDAPadmin cmd.php cmd Parameter Local File Inclusion

phpLDAPadmin custom\_welcome\_page Parameter File Include Vulnerability

phpLDAPadmin Detection

phpLDAPadmin orderby Parameter Arbitrary PHP Code Execution

PHPLinks Multiple Input Validation Vulnerabilities

phpList <= 2.10.8 Variable Overwriting

phpList <= 2.6.3 Multiple Vulnerabilities

phpList cline Parameter Array Remote File Inclusion

phpList Detection

phpList index.php database\_module Parameter Local File Inclusion

phpListPro Multiple Script returnpath Parameter Remote File Inclusions

phpMoAdmin Detection

phpMoAdmin saveObject Remote Command Execution

phpMyAdmin 2.11.x / 3.3.x < 2.11.11.3 / 3.3.9.2 SQL Query Bookmarks Arbitrary SQL Query Execution (PMASA-2011-02)

phpMyAdmin 3.3.x / 3.4.x < 3.3.10.2 / 3.4.3.1 Multiple Vulnerabilities (PMASA-2011-5 - PMASA-2011-8)

phpMyAdmin 3.5.x / 4.x < 4.0.5 'Header.class.php' Clickjacking Bypass (PMASA-2013-10)

phpMyAdmin 3.5.x < 3.5.8.1 / 4.x < 4.0.0-rc3 Multiple Vulnerabilities (PMASA-2013-2 - PMASA-2013-5

phpMyAdmin 3.5.x < 3.5.8.2 / 4.0.x < 4.0.4.2 Multiple Vulnerabilities (PMASA-2013-8 - PMASA-2013-15

phpMyAdmin 4.0 < 4.8.5 Multiple Vulnerabilities (PMASA-2019-1), (PMASA-2019-2)

phpMyAdmin 4.0.x < 4.0.10.1 / 4.1.x < 4.1.14.2 / 4.2.x < 4.2.6 Multiple Vulnerabilities (PMASA-2014-4 - PMASA-2014-7)

phpMyAdmin 4.0.x < 4.0.10.10 / 4.2.x < 4.2.13.3 / 4.3.x < 4.3.13.1 / 4.4.x < 4.4.6.1 Multiple Vulnerabilities (PMASA-2015-2, PMASA-2015-3)

phpMyAdmin 4.0.x < 4.0.10.13 / 4.4.x < 4.4.15.3 / 4.5.x < 4.5.4 Multiple Vulnerabilities (PMASA-2016-1 - PMASA-2016-5)

phpMyAdmin 4.0.x < 4.0.10.16 Multiple Vulnerabilities (PMASA-2016-17, PMASA-2016-22 - PMASA-2016-24, PMASA-2016-26 - PMASA-2016-28)

phpMyAdmin 4.0.x < 4.0.10.17 / 4.4.x < 4.4.15.8 / 4.6.x < 4.6.4 Multiple Vulnerabilities (PMASA-2016-29 - PMASA-2016-56)

phpMyAdmin 4.0.x < 4.0.10.19 / 4.4.x < 4.4.15.10 / 4.6.x < 4.6.6 Multiple Vulnerabilities (PMASA-2017-1 - PMASA-2017-7)

phpMyAdmin 4.0.x < 4.0.10.3 / 4.1.x < 4.1.14.4 / 4.2.x < 4.2.8.1 Micro History XSS and XSRF Vulnerabilities (PMASA-2014-10)

phpMyAdmin 4.0.x < 4.0.10.6 / 4.1.x < 4.1.14.7 / 4.2.x < 4.2.12 Multiple Vulnerabilities (PMASA-2014-13 - PMASA-2014-16)

phpMyAdmin 4.0.x < 4.0.10.7 / 4.1.x < 4.1.14.8 / 4.2.x < 4.2.13.1 Multiple Vulnerabilities (PMASA-2014-17 - PMASA-2014-18)

phpMyAdmin 4.0.x < 4.0.10.9 / 4.2.x < 4.2.13.2 / 4.3.x < 4.3.11.1 Information Disclosure Vulnerability (PMASA-2015-1)

phpMyAdmin 4.3.x < 4.3.13.2 / 4.4.x < 4.4.14.1 reCaptcha Bypass (PMASA-2015-4)

phpMyAdmin 4.4.x < 4.4.15.3 / 4.5.x < 4.5.4 Multiple Vulnerabilities (PMASA-2016-6, PMASA-2016-7)

phpMyAdmin 4.4.x < 4.4.15.7 Multiple Vulnerabilities (PMASA-2016-17, PMASA-2016-19, PMASA-2016-21 - PMASA-2016-24, PMASA-2016-26 - PMASA-2016-28)

phpMyAdmin 4.5.x < 4.5.4 Multiple Vulnerabilities (PMASA-2016-8, PMASA-2016-9)

phpMyAdmin 4.6.x < 4.6.3 Multiple Vulnerabilities (PMASA-2016-17 - PMASA-2016-28)

phpMyAdmin 4.7.7 < 4.9.2 SQLi (PMASA-2019-5)

phpMyAdmin 4.7.x <= 4.7.6 / 4.8.x < 4.8.4 Multiple XSRF/CSRF Vulnerabilities (PMASA-2018-7)

phpMyAdmin 4.8.x < 4.8.2 Vulnerability (PMASA-2018-4)

phpMyAdmin 4.x < 4.0.4.1 import.php GLOBALS Variable Injection Configuration Parameter Manipulation (PMASA-2013-7)

phpMyAdmin 4.x < 4.8.4 Multiple Vulnerabilities (PMASA-2018-6) (PMASA-2018-8)

phpMyAdmin 4.x < 4.8.5 Multiple Vulnerabilities (PMASA-2019-1) (PMASA-2019-2)

phpMyAdmin 4.x < 4.9.0 CSRF vulnerablity (PMASA-2019-4)

phpMyAdmin < 2.5.2 Multiple Vulnerabilities

phpMyAdmin < 2.6.0-pl2 Unspecified Arbitrary Command Execution

phpMyAdmin < 2.6.1 pl1 Multiple Script File Inclusions

phpMyAdmin < 2.6.1-rc1 Multiple Remote Vulnerabilities

phpMyAdmin < 2.6.4-pl3 Multiple Vulnerabilities

phpMyAdmin < 2.9.1 Multiple Vulnerabilities

phpMyAdmin < 3.3.10.1 / 3.4.1 Multiple Vulnerabilities (PMASA-2011-03 - PMASA-2011-04

phpMyAdmin <= 4.9.1 Cross-Site Request Forgery Vulnerability

phpMyAdmin Detection

phpMyAdmin export.php what Parameter Traversal Arbitrary File Access

phpMyAdmin file\_path Parameter Vulnerabilities (PMASA-2009-1)

phpMyAdmin grab\_globals.lib.php subform Parameter Traversal Local File Inclusion

phpMyAdmin import\_blacklist Variable Overwriting

phpMyAdmin Installation Not Password Protected

phpMyAdmin Multiple Path Disclosure Vulnerabilities (PMASA-2016-1, PMASA-2016-6, PMASA-2016-8)

phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

phpMyAdmin server\_sync.php Backdoor (PMASA-2012-5)

phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

phpMyAdmin setup.php Arbitrary PHP Code Execution (PMASA-2010-4)

phpMyAdmin setup.php save Action Arbitrary PHP Code Injection (PMASA-2009-3)

phpMyAdmin setup.php unserialize() Arbitrary PHP Code Execution (PMASA-2010-3)

phpMyAdmin simplexml\_load\_string() Function Information Disclosure (PMASA-2011-17)

phpMyAdmin sql.php Traversal Arbitrary File Access

phpMyAdmin url.php Redirect (PMASA-2011-4)

phpMyAgenda rootagenda Parameter File Include Vulnerability

phpMyBackupPro < 1.0.0 Unspecified Input Validation Issues

phpMyConferences menus.inc.php lvc\_include\_dir Parameter Remote File Inclusion

PhpMyExplorer index.php chemin Parameter Encoded Traversal Arbitrary File Access

phpMyFAQ < 1.5.2 Multiple Vulnerabilities

phpMyFAQ < 1.6.10 Multiple Script Arbitrary File Upload

phpMyFAQ < 1.6.8 Multiple SQL Injection Vulnerabilities

phpMyFAQ Detection

phpMyFAQ Forum Message username Field SQL Injection

phpMyFAQ Image Upload Authentication Bypass

phpMyFAQ index.php action Parameter Local File Inclusion

phpMyWebHosting Authentication SQL Injection

PHPNews auth.php Multiple Parameter SQL Injection

PHPNews auth.php path Parameter Remote File Inclusion

PHPNews news.php prevnext Parameter SQL Injection

PHPNews sendtofriend.php 'mid' Parameter SQLi

phpPgAdmin index.php \_language Parameter Local File Inclusion

phpPgAdmin index.php formLanguage Parameter Local File Inclusion

phpPgAdmin sql.php goto Parameter Traversal Arbitrary File Access

phpPgAds dest Parameter HTTP Response Splitting

PHProjekt <= 5.1 Multiple Remote File Inclusions

PHProjekt authform.inc.php path\_pre Parameter Remote File Inclusion

PHProjekt setup.php Authentication Bypass Arbitrary Code Execution

PHProxy Detection

phpRPC Library rpc\_decoder.php decode() Function Arbitrary Code Execution

phpSANE file\_save Parameter Remote File Include

phpScheduleIt < 1.0.1 Reservation.class.php Arbitrary Reservation Modification

phpScheduleIt Detection

phpScheduleIt reserve.php start\_date Parameter Arbitrary Command Injection

phpSecurePages cfgProgDir Variable File Include Vulnerabilities

phpShop Default Credentials

phpShop Detection

phpShop shop/flypage SQL Injection

phpSlash fields Parameter PHP Code Injection

PHPSurveyor Multiple SQL Injections

phpSysInfo < 2.4.1 Multiple Vulnerabilities

phpwcms 1.2.5 Multiple Vulnerabilities

phpwcms Detection

phpwcms spaw\_control.class.php spaw\_root Parameter Remote File Inclusion

PHPWebAdmin for hMailServer Multiple File Inclusions

phpWebFTP index.php language Parameter Local File Inclusion

PhpWebGallery comments.php sort\_by Parameter SQL Injection

phpWebNotes core/api.php t\_path\_core Parameter File Inclusion

phpWebSite < 0.9.x Multiple Vulnerabilities

phpWebSite <= 0.10.1 Multiple Vulnerabilities

phpWebSite Detection

phpWebSite Image Announcement Upload Arbitrary Command Execution

phpWebSite index.php hub\_dir Parameter Local File Inclusion

phpWebSite index.php Search Module SQL Injection

phpWebThings core/editor.php editor\_insert\_bottom Parameter Remote File Inclusion

phpWebThings Multiple Scripts SQL Injection

PHPWind Board faq.php skin Parameter Remote File Inclusion

PHPX admin/index.php username Parameter SQL Injection

PineApp Mail-SeCure admin/confnetworking.html Multiple Parameter Remote Command Injection

PineApp Mail-SeCure Default Credentials

PineApp Mail-SeCure Detection

PineApp Mail-SeCure test\_li\_connection.php Remote Command Injection

ping.asp CGI Arbitrary Command Execution

Pinnacle ShowCenter Skin DoS

Piranha's RH6.2 default password

Pivotal RabbitMQ Management Plugin 3.4.x / 3.5.x / 3.6.x < 3.6.9 Multiple Vulnerabilities

Pivotal RabbitMQ Management Plugin Detection

Piwigo Detection

Piwigo install.php dl Parameter Traversal Arbitrary File Access

Piwik < 2.16.1-rc1 Multiple Vulnerabilities

Piwik core/Loader.php Trojaned Distribution

Piwik Detection

Pixelpost < 1.5 RC1 showimage Parameter SQL Injection

Pixelpost index.php category Parameter SQL Injection

Pixelpost index.php parent\_id Parameter SQL Injection

PJ CGI Neo PJreview\_Neo.cgi p Parameter Traversal Arbitrary File Access

Plain Old Webserver URI Traversal Arbitrary File Access

Plesk Horde Detection

Plesk Multiple Script locale\_id Parameter Traversal Arbitrary File Access

Plesk Panel Apache Arbitrary PHP Code Injection

Pligg Detection

Pligg evb/check\_url.php url Parameter SQL Injection

Pligg login.php return Parameter Arbitrary Site Redirect

Pligg settemplate.php template Parameter Local File Inclusion

Plogger plog-admin-functions.php config Parameter Remote File Inclusion

Plogger plog-download.php checked[] Parameter SQL Injection

Plogger plog-rss.php id Parameter SQL Injection

Plone Detection

Plone PloneFormGen Unspecified Arbitrary Code Execution

Plone Request Parsing Remote Command Execution

Plone Security Bypass

Plone Unprotected MembershipTool Methods Arbitrary Portrait Manipulation

pluck < 4.5.3 Multiple Local File Include Vulnerabilities

Pluck update.php Remote Privilege Escalation

Plume CMS < 1.0.3 Remote File Inclusion

Plumtree Portal Default Credentials

Plumtree Portal User Object User Enumeration

PlusMail plusmail CGI Arbitrary Command Execution

pMachine <= 2.2.1 Multiple Vulnerabilities

pMachine lib.inc.php pm\_path Parameter Remote File Inclusion

pMachine mail\_autocheck.php Arbitrary Code Execution

PMOS Help Desk form.php Arbitrary Code Execution

PmWiki < 2.1 beta 21 Multiple Vulnerabilities

PmWiki < 2.1.21 Global Variables Overwriting

PNphpBB2 index.php c Parameter SQL Injection

Polar HelpDesk Authentication Bypass

Poll It CGI data\_dir Parameter Arbitrary File Access

Polycom SoundPoint IP Phone Default Password

Polycom SoundPoint IP Phones reg\_1.html SIP Information Disclosure

popper\_mod PHP Administration Script Authentication Bypass

Portable phpMyAdmin Plugin for WordPress 'wp-pma-mod' Authentication Bypass

PortalApp forums.asp sortby Parameter SQL Injection

Poster version.two index.php Account Manipulation Privilege Escalation

Postfix Admin Detection

PostNuke < 0.762 Multiple Vulnerabilities

PostNuke <= 0.760 RC2 Multiple Vulnerabilities

PostNuke <= 0.760 RC4a Multiple Vulnerabilities

PostNuke <= 0.760 RC4b Multiple Vulnerabilities

PostNuke AutoTheme Module Multiple Unspecified Vulnerabilities

PostNuke Detection

PostNuke Glossary Module page Parameter SQL Injection

PostNuke Install Script Admin Password Disclosure

PostNuke Members\_List Module Information Disclosure

PostNuke PNphpBB2 includes/functions\_admin.php phpbb\_root\_path Parameter Remote File Inclusion

PostNuke pnTresMailer codebrowserpntm.php Traversal Arbitrary File Access

PostNuke Rating System DoS

PostNuke Sections Module Information Disclosure

PowerPortal index.php index\_page Parameter SQL Injection

Powershell Empire Detection

PPA functions.inc.php config[ppa\_root\_path] Parameter Remote File Inclusion

Prado Framework sr Parameter Directory Traversal

Prizm Content Connect default.aspx document Parameter Remote File Inclusion

processit CGI Environment Variable Remote Information Disclosure

ProductCart Multiple Input Validation Vulnerabilities

ProductCart Multiple Scripts SQL Injection

ProductCart Multiple Vulnerabilities

Profense Web Application Firewall Default Credentials

Properties Component for Joomla! 'aid' Parameter SQLi

PRTG Network Monitor Default Credentials

PRTG Network Monitor Detection

PRTG Traffic Grapher Detection

PSCS VPOP3 messagelist.html msglistlen Parameter DoS

Psunami.CGI Command Execution

PT News Unauthorized Administrative Access

Pulse Connect Secure Detection

Pulse Policy Secure Detection

Pulse Secure Pulse Connect Secure SSL VPN Unauthenticated Path Traversal (CVE-2019-11510)

PunBB < 1.2.2 Multiple Input Validation Vulnerabilities

PunBB < 1.2.6 Multiple Vulnerabilities

PunBB < 1.2.7 Multiple Vulnerabilities

PunBB < 1.2.8 Multiple Vulnerabilities

PunBB Detection

PunBB include/common.php language Parameter Local File Inclusion

PunBB profile.php id Parameter SQL Injection

PunBB Search Dropdown Private Forum Disclosure

PunBB search.php old\_searches Parameter SQL Injection

Puppet 2.7.x / 3.2.x < 2.7.23 / 3.2.4 and Enterprise 2.8.x / 3.0.x < 2.8.3 / 3.0.1 Multiple Vulnerabilities

Puppet < 2.7.26 / 3.6.2 and Enterprise 2.8.x < 2.8.7 Multiple Vulnerabilities

Puppet Enterprise 2.8.x / 3.2.x Multiple Vulnerabilities

Puppet Enterprise 2.x < 2.6.1 Session Handling Weakness

Puppet Enterprise 2015.x / 2016.x < 2016.4.0 Multiple Vulnerabilities

Puppet Enterprise 2015.x / 2016.x < 2016.4.0 Multiple Vulnerabilities

Puppet Enterprise 2015.x < 2015.3.3 Multiple Vulnerabilities

Puppet Enterprise 2015.x < 2016.4.0 Denial of Service Vulnerability

Puppet Enterprise 2016.x < 2016.4.12 / 2017.x < 2017.3.7 / 2018.x < 2018.1.1 Arbitrary Code Execution Vulnerability

Puppet Enterprise 2016.x < 2016.4.15 / 2017.x < 2017.3.10 / 2018.x < 2018.1.4 Plaintext Credential Vulnerability

Puppet Enterprise 2017.x < 2017.3.6 Cross-site Scripting Vulnerability

Puppet Enterprise 2018.x < 2018.1.1 Code Execution Vulnerability

Puppet Enterprise 3.3.0 Bundled Oracle Java Vulnerabilities

Puppet Enterprise 3.7.x < 3.8.1 / 3.8.x < 3.8.1 Multiple Vulnerabilities

Puppet Enterprise 3.x < 3.1.1 Multiple Vulnerabilities

Puppet Enterprise 3.x < 3.1.2 DTLS Retransmission DoS

Puppet Enterprise 3.x < 3.1.3 LibYAML Heap-Based Buffer Overflow

Puppet Enterprise 3.x < 3.2.0 Multiple Vulnerabilities

Puppet Enterprise 3.x < 3.8.1 Multiple Vulnerabilities (Logjam)

Puppet Enterprise < 2015.3.0 Information Disclosure Vulnerability

Puppet Enterprise < 2015.3.1 Information Disclosure Vulnerability

Puppet Enterprise < 2016.2.1 Multiple Vulnerabilities

Puppet Enterprise < 2016.4.0 Multiple Vulnerabilities

Puppet Enterprise < 2016.4.5 / 2016.5.x / 2017.1.x Multiple Vulnerabilities

Puppet Enterprise < 2017.2.2 Arbitrary Code Execution Vulnerability

Puppet Enterprise < 2017.3.4 Code Execution Vulnerability

Puppet Enterprise < 3.0.1 Multiple Vulnerabilities

Puppet Enterprise < 3.1.0 Multiple Vulnerabilities

Puppet Enterprise Console Authentication Bypass (intrusive check)

Puppet Enterprise Console Detection

Puppet Enterprise Installation Process Local CA Key Disclosure

Puppet Enterprise Multiple OpenSSL Vulnerabilities (FREAK)

Puppet Enterprise x < 2018.1.9 / 2019.x.x < 2019.0.3 Default Password Vulnerabilities

Puppet Multiple Vulnerabilities (2013/03/12)

Puppet REST API Detection

Puppet Symlink File Overwrite

Puppet Unauthenticated Remote Code Execution

Puppet Unsafe YAML Unserialization

QlikView Server AccessPoint XML External Entity Injection

QNAP Photo Station WebUI Detection

QNAP Signage Station Arbitrary File Upload Vulnerability

QNAP Signage Station Server Detection

Qualiteam X-Cart Multiple Script perl\_binary Parameter Arbitrary Command Execution

Qualiteam X-Cart Multiple Vulnerabilities

Quantum vmPRO Default Credentials Check

Quantum vmPRO Web Administration Interface Detection

Quest DR Series Appliance Web Default Administrator Credentials

Quest DR Series Appliance Web Detection

QuickEStore insertorder.cfm CFTOKEN Parameter SQL Injection

Quikstore Shopping Cart quikstore.cgi Multiple Vulnerabilities

QuikStore Shopping Cart quikstore.cgi template Parameter Traversal Arbitrary File Access

r57shell Backdoor Detection

RabidHamster R4 Detection

RabidHamster R4 left\_console.html cmd Parameter loadfile() Function Traversal Arbitrary File Access

RaidenHTTPD check.php SoftParserFileXml Parameter Remote File Inclusion

RaidenHTTPD workspace.php ulang Parameter Local File Inclusion

RCBlog index.php post Parameter Traversal Arbitrary File Access

RealServer /admin/Docs/default.cfg Information Disclosure

RealVNC Java Viewer Detection

Red Hat Administration Server (redhat-ds-admin) Multiple Remote Vulnerabilities

Red Hat JBoss Enterprise Application Platform 6.x < 6.4.22 Multiple Vulnerabilities

Red Hat JBoss Enterprise Application Platform 7.x < 7.2.2 Multiple Vulnerabilities

Red Hat JBoss Enterprise Application Platform 7.x < 7.2.4 Authorization Bypass

Red Hat JBoss Enterprise Application Platform 7.x < 7.2.5 Multiple Vulnerabilities

Redhat Stronghold status / info Request Information Disclosure

RegistrationMagic Plugin for WordPress < 3.7.9.3 PHP Object Injection

Remote Help Default Credentials

Request Tracker 3.8.x < 3.8.17 / 4.x < 4.0.13 Multiple Vulnerabilities

Request Tracker 3.x < 3.8.12 / 4.x < 4.0.6 Multiple Vulnerabilities

Request Tracker 3.x < 3.8.15 / 4.x < 4.0.8 Multiple Vulnerabilities

Request Tracker 3.x < 3.8.9 Security Bypass and Information Disclosure

Request Tracker 4.0.x < 4.0.23 / 4.2.x < 4.2.10 Multiple Vulnerabilities

Request Tracker 4.2.x < 4.2.5 Email::Address:List Module String Handling DoS

Request Tracker Default Credentials

Request Tracker Detection

Request Tracker Session Fixation Vulnerability

Request Tracker Unsupported Version Detection

Resin viewfile Servlet Arbitrary File Disclosure

ReviewPost PHP Pro Multiple Script SQL Injections

Revive Adserver 'www/delivery/axmlrpc.php' 'what' Parameter SQL Injection

Revive Adserver < 3.0.5 Multiple CSRF Vulnerabilities

Revive Adserver Detection

RiSearch show.pl Arbitrary File Access

RiSearch show.pl Open Proxy Relay

Riverbed SteelApp (Stingray) Traffic Manager Web UI Detection

ROADS search.pl form Parameter Traversal Arbitrary File Access

RokModule Component for Joomla! 'moduleid' Parameter SQi

rot13sj.cgi Arbitrary File Access

RoundCube Webmail bin/html2text.php Post Request Remote PHP Code Execution

Roxen Web Server Counter Module Crafted Request Saturation DoS

rpm\_query CGI System Information Disclosure

RSA Operations Console Detection

RSA Security Console Detection

RSA Self-Service Console Detection

RSForm! Component for Joomla! 'lang' Parameter Local File Include

RTH login.php uname Parameter SQL Injection

Ruby cgi.rb Malformed HTTP Request CPU Utilization DoS

Ruby on Rails HTTP Digest Authentication Bypass

Ruby on Rails Routing Code URL Code Evaluation DoS

RunCMS < 1.5.3 debug\_show.php Multiple Vulnerabilities

RunCMS <= 1.2 Multiple Vulnerabilities

RunCMS Detection

RunCMS Multiple Script bbPath Parameter Remote File Inclusion

RunCMS Multiple Script lid Parameter SQL Injection

RunCMS Remote Arbitrary File Upload

RunCMS xoopsOption Parameter Local File Inclusion

RWCards Component for Joomla! 'category\_id' Parameter SQLi

RWCards Component for Joomla! 'mosConfig\_absolute\_path' Parameter Remote File Include

SalesLogix eViewer slxweb.dll Request Remote DoS

Samba Web Administration Tool (SWAT) Detection

Samba Web Administration Tool (SWAT) Error Message Username Enumeration

Sambar Server /cgi-bin/mailit.pl Arbitrary Mail Relay

Sambar Server /session/sendmail Arbitrary Mail Relay

Sambar Server /sysadmin Default Accounts

Sambar Server cgitest.exe Remote Overflow

Sambar Server dumpenv.pl Information Disclosure

Sambar Server ISAPI Search Utility search.dll Arbitrary Directory Listing

Sambar Server Multiple CGI Environment Variable Disclosure

Sambar Server Multiple CGI Remote Overflow

Sambar Server Multiple Script Arbitrary Code Execution

Sambar Server pagecount CGI Traversal Arbitrary File Overwrite

Sambar Server search.pl results.stm Overflow DoS

SandSurfer < 1.7.0 User Authentication Bypass

SAP BusinessObjects 'HappyAxis2.jsp' Information Disclosure

SAP BusinessObjects Detection

SAP Control SOAP Web Service Detection

SAP Control SOAP Web Service Remote Code Execution (SAP Note 1414444)

SAP DB / MaxDB Web Server DBM\_INTERN\_TEST Event Buffer Overflow

SAP DB / MaxDB WebDBM Client Database Name Remote Overflow

SAP Host Agent SOAP Web Service Information Disclosure (SAP Note 1816536)

SAP Host Control SOAP Web Service 'Database/Name' Command Execution (SAP Note 1341333)

SAP Host Control SOAP Web Service Detection

SAP Internet Graphics Server (IGS) Directory Traversal Vulnerability

Savant Web Server cgitest.exe Overflow

SaveWebPortal <= 3.4 Multiple Vulnerabilities

Sawmill 8.x < 8.1.7.3 Arbitrary File Disclosure

Sawmill < 7.1.6 Multiple Vulnerabilities

Sawmill Detection

Sawmill File Access Information Disclosure

Sawmill Weak Password Encryption Scheme Information Disclosure

SAXoPRESS pbcs.dll url Parameter Traversal Arbitrary File Access

sBLOG search.php keyword Parameter SQL Injection

Scout Portal Toolkit SPT--ForumTopics.php forumid Parameter SQL Injection

ScozBook scozbook/add.php Multiple Parameter XSS

Scriptegrator Plugin for Joomla! 'files[]' Parameter Remote File Include

Scrutinizer < 10.1.2 Multiple Vulnerabilities

Scrutinizer < 9.0.1 d4d/alarms.php Multiple Parameters SQLi

Scrutinizer < 9.5.2 d4d/statusFilter.php q Parameter SQL Injection

Scrutinizer < 9.5.2 Multiple Vulnerabilities

Scrutinizer Default Credentials Check

Scrutinizer NetFlow & sFlow Analyzer Detection

Security Center < 3.4.2.1 Directory Traversal Arbitrary File Access

SecurityReporter < 4.6.3p1 Multiple Vulnerabilities

Seditio Detection

Seditio plug.php pag\_sub Parameter SQL Injection

Segue CMS themesettings.inc.php themesdir Parameter Remote File Inclusion

Sendcard sendcard.php id Parameter SQL Injection

Sensitive File Disclosure

SEO Tools Plugin for WordPress 'file' Parameter Arbitrary File Access

Serendipity < 0.7.0beta3 Multiple Vulnerabilities

Serendipity < 0.8.1 Multiple Vulnerabilities

Serendipity < 2.1.1 Multiple Vulnerabilities

Serendipity comment.php url Parameter SQL Injection

Serendipity Detection

Serendipity exit.php Multiple Parameter SQL Injection

Serendipity Multiple Script HTTP Response Splitting

Serendipity serendipity\_event\_bbcode.php Script serendipity[charset] Parameter Local File Inclusion

Serendipity XML-RPC for PHP Remote Code Injection

ServerView Servername Parameter Arbitrary Command Execution

ServletExec 4.1 / JRun ISAPI Multiple DoS

ServletExec 4.1 ISAPI com.newatlanta.servletexec.JSP10Servlet Path Disclosure

ServletExec 4.1 ISAPI com.newatlanta.servletexec.JSP10Servlet Traversal Arbitrary File Access

SGDynamo sgdynamo.exe HTNAME Parameter Path Disclosure

SGI InfoSearch infosrch.cgi fname Parameter Arbitrary Command Execution

Shop-Script admin.php Admin Panel Security Bypass

ShopCartCGI Multiple Script Traversal Arbitrary File Access

SHOUTcast Server admin.cgi Long Argument Overflow

SHOUTcast Server Filename Handling Format String

SHOUTcast Server User-Agent / Host Header DoS

Silent-Storm Portal Multiple Input Validation Vulnerabilities

Silex USB Device Server Web Configuration Page Empty Password

Silver Peak NX Detection

Silver Peak VX < 6.2.4 XSS

Silver Peak VX Default Credentials

Silver Peak VX Detection

SilverNews < 2.0.4 Multiple Vulnerabilities

SilverStream Database Structure Disclosure

SilverStripe CMS Detection

SilverStripe CMS Running in Development Mode

SilverStripe debug\_profile Parameter Information Disclosure

SimpGB guestbook.php quote Parameter SQL Injection

Simple Form Multiple Parameter Arbitrary Mail Relaying

Simple Form Subject Tags Arbitrary Mail Relay

Simple Machines Forum Avatar Information Disclosure Vulnerability

Simple Machines Forum Detection

Simple Machines Forum msg Parameter SQL Injection Vulnerability

Simple Machines Forum Search.php SQL Injection

Simple Machines Forum Validation Code Prediction Arbitrary Password Reset

Simple PHP Blog <= 0.4.0 Multiple Vulnerabilities

Simple PHP Blog comments.php Traversal Arbitrary File Access

Simple PHP Blog config/users.php Arbitrary User Password Hash Disclosure

Simple PHP Blog Detection

Simple PHP Blog install05.php blog\_language Parameter Local File Inclusion

Simple Web Counter swc ctr Parameter Remote Overflow

Simple:Press Plugin for WordPress 'value' parameter SQL Injection

SimpleBBS topics.php name Parameter Arbitrary Command Execution

SimpleBBS users disclosure

SimpleBoard / Joomlaboard 'sbp' Parameter Remote File Include

SimpleChat Information Disclosure

SimpleFAQ Component for Joomla! 'aid' Parameter SQLi

SimpleSAMLphp Detection

Simplicity oF Upload download.php language Parameter Local File Inclusion

Simplog <= 0.9.2 Multiple Vulnerabilities

Singapore Gallery < 0.9.11 Multiple Vulnerabilities

SIR GNUBoard Remote File Inclusion

Site Documentation Module for Drupal Database Tables Access Content Permission Information Disclosure

Site Sift Listings detail.php id Parameter SQL Injection

Site@School Multiple Script cmsdir Parameter Remote File Inclusion

Site@School slideshow\_full.php album\_name Parameter SQL Injection

SiteBuilder-FX top.php admindir Parameter Remote File Inclusion

Sitecore CMS < 5.3.2 rev. 090212 Web Service Security Database Information Disclosure

Sitecore CMS < 6.4.1 rev.110720 'url' Parameter URI Redirection

Sitecore CMS Detection

SiteEnable Multiple Input Validation Vulnerabilities

Sitefinity CMS Arbitrary File Upload

Sitefinity CMS Detection

Siteframe siteframe.php LOCAL\_PATH Parameter Remote File Inclusion

Siteman < 1.1.11 Multiple Vulnerabilities

SiteMinder smpwservicescgi.exe Arbitrary Site Redirect

SiteScope Web Service Unpassworded Access

SiteX photo.php albumid Parameter SQL Injection

SIX-webboard generate.cgi 'content' Parameter Traversal Arbitrary File Access

Slimstat Analytics Plugin for WordPress < 4.7.1 PHP Object Injection

SLMail WebMail Multiple Remote Overflows

Smart Publisher index.php filedata Parameter Arbitrary Command Execution

smb2www Proxy Bypass

smb2www Unspecified Arbitrary Remote Command Execution

Smush Image Plugin for WordPress < 2.7.6 Directory Traversal

Snare Agent Detection

Snare Agent for Linux < 1.7.0 / 2.0.0 Multiple Vulnerabilities

Sniplets Plugin for WordPress execute.php 'text' Parameter Arbitrary Command Execution

Snitz Forums 2000 3.4.03 Multiple Vulnerabilities

Snitz Forums 2000 < 3.4.03 register.asp Email Parameter SQL Injection

Snitz Forums 2000 <= 3.4.07 register.asp 'Email' Parameter SQL Injection

Snitz Forums 2000 active.asp HTTP X-Forwarded-For Header SQL Injection

Snitz Forums 2000 Detection

Snitz Forums 2000 register.asp Email Parameter SQL Injection

SnortReport nmap.php target Parameter Arbitrary Command Execution

SocialEngine Blog Plugin category\_id Parameter SQL Injection

Sojourn Search Engine sojourn.cgi cat Parameter Traversal Arbitrary File Access

SolarWinds Log and Event Manager < 6.0.1 HyperSQL Remote Code Execution

SolarWinds Log and Event Manager < 6.2.0 Multiple Remote Command Execution Vulnerabilities

SolarWinds Log and Event Manager < 6.3.1 Hotfix 3 Jailbreak and Privilege Escalation

SolarWinds Log and Event Manager < 6.3.1 Hotfix 4 Insecure HTTP Update Download MitM Code Execution

SolarWinds Log and Event Manager Default Credentials

SolarWinds Log and Event Manager Detection

SolarWinds Log and Event Manager Unsupported Version Detection

SolarWinds Orion Multiple SQLi Vulnerabilities

SolarWinds Orion NPM < 10.3.1 Multiple Vulnerabilities

SolarWinds Orion NPM < 10.7 Multiple Vulnerabilities

SolarWinds Orion NPM < 9.5 Login.asp SQLi

SolarWinds Orion Product Detection

SolarWinds Server & Application Monitor (SAM) Detection

SolarWinds Storage Manager AuthenticationFilter Script Upload RCE

SolarWinds Storage Manager Detection

SolarWinds Storage Manager Server LoginServlet loginName Parameter SQL Injection

SolarWinds Virtualization Manager Detection

SolusVM Default Administrator Credentials

SolusVM Detection

SonicWALL Global Management System (GMS) / Analyzer GMC Service XML External Entity (XXE) Injection

SonicWALL Global Management System (GMS) / Analyzer sgms Webapp File Deletion

SonicWALL Global Management System (GMS) / Analyzer Universal Management Appliance or Host (UMA / UMH) Information Disclosure

SonicWALL Global Management System (GMS) 8.x < 8.2 Multiple Vulnerabilities

SonicWALL Universal Management Suite Detection

SonicWALL ViewPoint Server Default Credentials

SonicWALL ViewPoint Server Detection

Sophos Web Appliance < 4.3.1 Multiple Remote Command Injection Vulnerabilities

Sophos Web Protection Appliance Multiple Vulnerabilities

Sophos Web Protection Appliance Open Redirect Vulnerability

Sophos Web Protection Appliance patience.cgi 'id' Parameter Directory Traversal

Sophos Web Protection Detection

Sourcefire Defense Center Multiple Security Vulnerabilities

Sphider configset.php settings\_dir Parameter Remote File Inclusion

Spiceworks HTTP Response Accept Header Handling Overflow DoS

SPiD lang.php lang\_path Remote File Inclusion

SpiderSales Shopping Cart SQL injection

spin\_client.cgi Remote Overflow

SPIP < 1.8.2-g Multiple Vulnerabilities

Splunk 4.0.x < 4.0.11 / 4.1.x < 4.1.2 Directory Traversal

Splunk 4.3.x < 4.3.6 Unspecified XSS

Splunk 5.0.x < 5.0.3 Multiple Vulnerabilities

Splunk < 5.0.4 X-FRAME-OPTIONS Clickjacking Vulnerability

Splunk < 5.0.5 Multiple Code Execution Vulnerabilities

Splunk Default Administrator Credentials (Splunk Web)

Splunk Default Administrator Credentials (splunkd)

Splunk Enterprise 5.0.x < 5.0.10 / 6.1.x < 6.1.4 Multiple Vulnerabilities

Splunk Enterprise 5.0.x < 5.0.13 / 6.0.x < 6.0.9 / 6.1.x < 6.1.8 OpenSSL Vulnerabilities (FREAK)

Splunk Enterprise 6.0.x < 6.0.14 / 6.1.x < 6.1.13 / 6.2.x < 6.2.14 / 6.3.x < 6.3.11 / 6.4.x < 6.4.8 / 6.5.x < 6.5.3 or Splunk Light < 6.6.0 Multiple Vulnerabilities

Splunk Enterprise 6.0.x < 6.0.6 Multiple Vulnerabilities

Splunk Enterprise 6.0.x < 6.0.7 Multiple Vulnerabilities (POODLE)

Splunk Enterprise 6.1.x < 6.1.3 Multiple Vulnerabilities

Splunk Enterprise 6.2.x < 6.2.2 Multiple Vulnerabilities (FREAK)

Splunk Enterprise 6.3.x < 6.3.12 / 6.4.x < 6.4.9 / 6.5.x < 6.5.6 / 6.6 < 6.6.3.2 or 6.6.4 / 7.0.x < 7.0.0.1 Multiple SAML Implementation Vulnerabilities

Splunk Enterprise 6.4.x < 6.4.6 Stored XSS Vulnerability

Splunk Enterprise 6.4.x < 6.4.7 Multiple Vulnerabilities

Splunk Enterprise < 5.0.14 / 6.0.10 / 6.1.9 / 6.2.5 or Splunk Light < 6.2.5 Multiple Vulnerabilities

Splunk Enterprise < 5.0.15 / 6.0.11 / 6.1.10 / 6.2.9 / 6.3.3.4 or Splunk Light < 6.2.9 / 6.3.3.4 Multiple Vulnerabilities (DROWN)

Splunk Enterprise < 5.0.16 / 6.0.12 / 6.1.11 / 6.2.10 / 6.3.6 / 6.4.3 or Splunk Light < 6.4.3 Cross-Site Redirection

Splunk Enterprise < 5.0.16 / 6.0.12 / 6.1.11 / 6.2.11 / 6.3.6 / 6.4.2 or Splunk Light < 6.4.2 Multiple Vulnerabilities

Splunk Enterprise < 5.0.17 / 6.0.13 / 6.1.12 / 6.2.12 / 6.3.8 / 6.4.4 or Splunk Light < 6.5.0 Multiple Vulnerabilities

Splunk Enterprise < 5.0.17 / 6.0.13 / 6.1.12 / 6.2.13 / 6.3.9 / 6.4.5 / 6.5.2 or Splunk Light < 6.5.2 Multiple Vulnerabilities

Splunk Enterprise < 5.0.18 / 6.0.14 / 6.1.13 / 6.2.13.1 / 6.3.10 / 6.4.6 / 6.5.3 / Splunk Light < 6.5.3 Multiple Vulnerabilities

Splunk Enterprise < 5.0.19 / 6.0.15 / 6.1.14 / 6.2.14 / 6.3.11 Error Message Spoofing

Splunk Free Detection

Splunk Information Disclosure Vulnerability (SP-CAAAP5E)

Splunk Information Exposure (SP-CAAAP5E

Spreecommerce api/orders.json Search Function Arbitrary Command Execution

Spyke Multiple Remote Vulnerabilities

SQL Dump Files Disclosed via Web Server

SQL-Ledger 'admin.pl' Empty Credentials

SQLi scanner

SQLiteManager confirm.php spaw\_root Parameter Remote File Inclusion

SQLiteManager SQLiteManager\_currentTheme Cookie Traversal Local File Inclusion

Squid cachemgr.cgi Proxied Port Scanning

SquidClamav Detection

SquidClamav Specially Crafted Character Parsing Remote DoS

Squirrelcart cart\_content.php cart\_isp\_root Parameter Remote File Inclusion

Squirrelcart index.php Multiple Parameter SQL Injection

SquirrelMail < 1.4.3 Multiple Vulnerabilities

SquirrelMail < 1.4.4 Multiple Vulnerabilities

SquirrelMail < 1.4.6 Multiple Vulnerabilities

SquirrelMail < 1.45 Multiple Vulnerabilities

SquirrelMail compose.php session\_expired\_post Arbitrary Variable Overwriting

SquirrelMail decodeHeader Arbitrary HTML Injection

SquirrelMail Detection

SquirrelMail HTTPS Session Cookie Secure Flag Weakness

SquirrelMail map\_yp\_alias Username Mapping Alias Arbitrary Code Execution

SquirrelMail Multiple Remote Vulnerabilities

SquirrelMail plugin.php plugins Parameter Local File Inclusion

SquirrelMail S/MIME Plug-in Remote Command Execution

SquirrelMail strings.php base\_uri Parameter Information Disclosure

Stadtaus Gaestebuch-Script index.php include\_files Parameter Remote File Inclusion

Stadtaus PHP Form Mail formmail.inc.php Remote File Inclusion

Stalkerlab Mailers CGIMail.exe Arbitrary File Retrieval

Stellar Docs Malformed Query Path Disclosure

StockMan Shopping Cart shop.plx page Parameter Arbitrary Command Execution

StockMan Shopping Cart shop.plx Path Disclosure

Stronghold swish Search Script Information Disclosure

SugarCRM <= 4.0 beta acceptDecline.php Remote File Inclusion

SugarCRM <= 4.2.0a Multiple Script sugarEntry Parameter Remote File Inclusion

SugarCRM Detection

SugarCRM on Apache / Windows .htaccess Direct Request Arbitrary File Access

SugarSales Multiple Module Traversal Arbitrary File Access

Sun Java ASP Server Default Admin Password

Sun Java System ASP < 4.0.3 Multiple Vulnerabilities

Sun Java System Directory Server Online Help Feature Information Disclosure

Sun Java System Identity Manager Account Disclosure

Sun Java System Identity Manager Default Credentials

Sun Java System Identity Manager Detection

Sun Java System Identity Manager ext Parameter Arbitrary File Retrieval

Sun Java Web Server bboard Servlet Command Execution

Sun JavaServer Default Admin Password

Sun ONE (iPlanet) Application Server Detection

Sun ONE Application Server Upper Case Request JSP Source Disclosure

Sun OpenSSO / Java System Access Manager Login Module User Account Enumeration Weakness

Sun Server Console Authentication Bypass

Sun Sunsolve CD Pack sscd\_suncourier.pl email Parameter Arbitrary Command Execution

Super Guestbook superguestconfig Admin Password Disclosure

Super Simple Blog Script Detection

Super Simple Blog Script entry Parameter SQL Injection

Super-M Son hServer URI Traversal Arbitrary File Access

SuSE Support Data Base sbsearch.cgi Arbitrary Command Execution

SWAT Unauthenticated Access (Demo Mode)

Sybase EAServer 6.3.1 < 6.3.1.07 Build 63107 / 6.2 < 6.2.0.12 Build 62012 Multiple Vulnerabilities

Sybase EAServer 6.x < 6.3.1 ESD#3 Multiple Code Execution Vulnerabilities

Sybase EAServer Detect

Sybase EAServer WebConsole jaqadmin Default Password

Sybase EAServer XML External Entity (XXE) Arbitrary File Disclosure

Symantec (Blue Coat) Reporter CLI OS Command Injection Vulnerability (SYMSA1465)

Symantec (Blue Coat) Reporter Denial of Service vulnerability (SYMSA1280)

Symantec (Blue Coat) Reporter Multiple Vulnerabilities (SA158)

Symantec (Blue Coat) Reporter UI Information Disclosure Vulnerability (SYMSA1489)

Symantec AntiVirus Scan Engine Web Interface Multiple Remote Vulnerabilities

Symantec Backup Exec System Recovery Manager FileUpload Class Unauthorized File Upload

Symantec Backup Exec System Recovery Manager Traversal Arbitrary File Access

Symantec Data Center Security Manager Privilege Escalation

Symantec Data Center Security Server 'environment.jsp' Information Disclosure (SYM15-001)

Symantec Data Center Security Server SQLi (SYM15-001)

Symantec Data Center Security Web Administration Interface Detection

Symantec Data Center Security Web Console Interface Detection

Symantec Data Insight < 4.5 Multiple Vulnerabilities (SYM14-012)

Symantec Endpoint Protection Manager < 12.1 RU6 MP1 Multiple Vulnerabilities (SYM15-007)

Symantec Endpoint Protection Manager Detection

Symantec LiveUpdate Administrator < 2.3 CSRF (SYM11-005)

Symantec LiveUpdate Administrator < 2.3.2 Privilege Escalation (SYM12-009)

Symantec LiveUpdate Administrator < 2.3.2.110 Multiple Vulnerabilities (SYM14-005)

Symantec LiveUpdate Administrator Web Detection

Symantec Mail Security for SMTP Admin Center Default Credentials

Symantec Message Filter Management Interface Default Credentials

Symantec Message Filter Management Interface Detection

Symantec Message Filter Multiple Vulnerabilities (SYM12-010)

Symantec Messaging Gateway 10.x < 10.6.1 Management Console Multiple Vulnerabilities (SYM16-005)

Symantec Messaging Gateway 10.x < 10.6.1-4 Multiple Vulnerabilities (SYM16-010)

Symantec Messaging Gateway 10.x < 10.6.2 Multiple Vulnerabilities (SYM16-015) (SYM16-016)

Symantec Messaging Gateway 10.x < 10.6.3-266 Multiple Vulnerabilities (SYM17-004)

Symantec Messaging Gateway 10.x < 10.6.3-267 Multiple Vulnerabilities (SYM17-006)

Symantec Messaging Gateway 10.x < 10.6.4 Directory Traversal Vulnerability (SYM17-016)

Symantec Messaging Gateway 10.x < 10.6.6 Multiple Vulnerabilities (SYMSA1461)

Symantec Messaging Gateway 10.x < 10.7.0 Information Disclosure Vulnerability (SYMSA1482)

Symantec Messaging Gateway 10.x < 10.7.1 Privilege Escalation Vulnerability (SYMSA1486)

Symantec Messaging Gateway 10.x < 10.7.3 Multiple Vulnerabilities (SYMSA1501)

Symantec Messaging Gateway 9.5.x Multiple Vulnerabilities (SYM12-013)

Symantec Messaging Gateway 9.5.x Multiple Vulnerabilities (SYM12-018)

Symantec Messaging Gateway Detection

Symantec Reporting Server < 1.0.224.0 Multiple Vulnerabilities

Symantec Reporting Server Improper URL Handling Exposure

Symantec Web Gateway < 5.0.3 Multiple Vulnerabilities (SYM12-006) (version check)

Symantec Web Gateway < 5.1.1 Multiple Vulnerabilities (SYM13-008)

Symantec Web Gateway < 5.2.1 Multiple Vulnerabilities (SYM14-010)

Symantec Web Gateway < 5.2.2 Authenticated OS Command Injection (SYM14-016)

Symantec Web Gateway < 5.2.5 Management Console Command Injection (SYM16-017)

Symantec Web Gateway <= 5.1.1 Multiple Vulnerabilities (SYM14-003)

Symantec Web Gateway Anti-Virus Definition < 20160628.037 Multiple Vulnerabilities (SYM16-010) (credentialed check)

Symantec Web Gateway Database < 5.0.0.1277 Multiple Vulnerabilities (SYM15-009) (credentialed check)

Symantec Web Gateway Detection

Symantec Web Gateway forget.php Blind SQL Injection (SYM11-008)

Symantec Web Gateway ipchange.php Shell Command Injection (SYM12-006) (intrusive check)

Symantec Web Gateway login.php Blind SQL Injection (SYM11-001)

Symantec Web Gateway Multiple Script Shell Command Execution (SYM12-011)

Symantec Web Gateway search.php SQL Injection (SYM12-011)

Symantec Web Gateway upload\_file() Remote Code Execution (SYM12-006) (intrusive check)

Symantec Web Security (SWS) Multiple Vulnerabilities

Symantec Web Security Detection

Sympa Detection

Sympa Malformed Content-Type Header Remote DoS

Sympa src/queue.c queue Utility Local Overflow

Sympa wwsympa do\_search\_list Overflow DoS

Sympa wwsympa Invalid LDAP Password Remote DoS

Sympa wwsympa.fcgi Unauthorised List Creation

Symphony 2.0.6 mode Parameter Local File Inclusion

Symphony Detection

Symphony sym\_auth Cookie SQL Injection

Symphony token Parameter SQL Injection

Sync Breeze HTTP POST Request Handling Remote Stack Buffer Overflow

Synchrologic Email Accelerator aggregate.asp User Account Disclosure

Syncrify < 2.1 Build 420 Multiple Security Bypass Vulnerabilities

Syncrify Detection

Synology DiskStation Manager (DSM) Detection

Synology DiskStation Manager (DSM) Web Administration Interface Default Credentials

Synology DiskStation Manager 4.0-x < 4.0-2259 / 4.1-x / 4.2-x < 4.2-3243 SLICEUPLOAD Function Remote Code Execution

Synology DiskStation Manager 4.3-x < 4.3-3810 Update 1 Multiple Vulnerabilities

Synology DiskStation Manager < 4.3-3776 Update 2 Multiple Vulnerabilities

Synology DiskStation Manager < 4.3-3810 Update 3 Multiple FileBrowser Component Directory Traversal Vulnerabilities

Synology DiskStation Manager uistrings.cgi lang Parameter Directory Traversal

SysCP < 1.2.11 Multiple Script Command Execution Vulnerabilities

Sysinfo name Parameter Arbitrary Code Execution

TalentSoft Web+ webplus CGI Traversal Arbitrary File Access

TalentSoft Web+ webplus.exe Path Disclosure

Tarantella Enterprise ttawebtop.cgi pg Parameter Traversal Arbitrary File Access

TaskFreak! Default Credentials

TaskFreak! Detection

TaskFreak! loadByKey() SQL Injection

Technote main.cgi filename Parameter Traversal Arbitrary File Access

Tektronix PhaserLink Multiple Admin Page Unauthenticated Configuration Manipulation

Tektronix PhaserLink Printer Web Server Direct Request Administrator Access

Temenos T24 Detection

Tenable Appliance < 4.5.0 Web UI simpleupload.py Remote Command Execution (TNS-2017-07)

Tenable Appliance Web Authentication Bypass

Tenable Appliance Web Detection

Tenable Nessus 6.0.x < 6.6 Multiple Vulnerabilities

Tenable Nessus 6.x < 6.8 Multiple Vulnerabilities

Tenable Security Center Default Credentials

Tenable SecurityCenter Detection

Terminal Services Web Detection

TestDirector (TD) for Mercury Quality Center SPIDERLib.Loader ActiveX Control (Spider90.ocx) ProgColor Property Overflow (2)

Textor Webmasters Ltd listrec.pl TEMPLATE Parameter Arbitrary Command Execution

TextPortal Default Passwords

The Includer includer.cgi Arbitrary Command Execution

TheCartPress Plugin for WordPress 'tcp\_class\_path' Parameter Remote File Inclusion

TheServer server.ini Direct Request Plaintext Credentials Disclosure

ThinClientServer Admin Account Creation Privilege Escalation

Thinking Arts ES.One store.cgi StartID Parameter Traversal Arbitrary File Access

ThinkPHP Multiple Parameter RCE

thttpd ssi Servlet Encoded Traversal Arbitrary File Access

Thunderstone Software Texis Crafted Request Information Disclosure

Thunderstone Software TEXIS Nonexistent File Request Path Disclosure

Thyme event\_view.php eid Parameter SQL Injection

TIBCO Spotfire Analytics Server Authentication Module Unspecified Information Disclosure

TIBCO Spotfire Analytics Server Web Application Multiple Vulnerabilities

TIBCO Spotfire Server Authentication Module Unspecified Privilege Escalation

TIBCO Spotfire Server Authentication Module Unspecified Remote Code Execution

TIBCO Spotfire Server Detection

TIBCO Spotfire Server Unsupported Version Detection

TigerVNC < 1.3.1 ZRLE Heap-based Buffer Overflow

TigerVNC Java Viewer Detection

TightVNC Java Viewer Detection

TikiWiki < 1.8.2 Multiple Input Validation Vulnerabilities

TikiWiki < 1.8.6 / 1.9.1 Multiple Vulnerabilities

TikiWiki < 1.9.8.2 Multiple Scripts Local File Inclusion

TikiWiki Detection

TikiWiki File Upload temp Directory Arbitrary Script Execution

TikiWiki jhot.php Arbitrary File Upload

TikiWiki tiki-graph\_formula.php f Parameter Arbitrary Command Execution

TikiWiki tiki-lastchanges.php Empty sort\_mode Parameter Information Disclosure

Tikiwiki tiki-listmovies.php movie Parameter Traversal Arbitrary File Access

TikiWiki Unauthorized Page Access

TikiWiki unserialize() Function Arbitrary Code Execution

TimThumb 'timthumb.php' < 2.8.14 WebShot 'src' Parameter Remote Command Execution

TimThumb 'timthumb.php' WebShot 'src' Parameter Remote Command Execution

TimThumb Cache Directory 'src' Parameter Arbitrary PHP File Upload

TimThumb Detection

TinyBrowser Component for Joomla! 'tinybrowser\_lang' Cookie Local File Include

TinyWebGallery lang Parameter Local File Inclusion

Tivoli Directory Server ldacgi.exe Template Parameter Traversal Arbitrary File Access

Tivoli Provisioning Manager Express for Software Distribution Detection

Tivoli Provisioning Manager Express for Software Distribution Multiple SQL Injections

toendaCMS < 0.6.2.1 Multiple Vulnerabilities

Topsec Firewall Cookie Command Injection (ELIGIBLECANDIDATE)

TorrentTrader download.php id Parameter SQL Injection

TP-Link Unauthenticated CGI Cross-Site Request Forgery (Remote)

Trac quickjump Search Script q Parameter Arbitrary Site Redirect

Trac Ticket Query Module group Parameter SQL Injection

TrackerCam Multiple Remote Vulnerabilities

TrailScout Module For Drupal Session Cookie SQL Injection

Trapeze Service Shell - Admin Service Accessible

Traq admincp/common.php authenticate() Function Authentication Bypass Remote Code Execution

Traq Detection

Trend Micro Control Manager cgiShowClientAdm Security Bypass

Trend Micro Control Manager download.php File Disclosure

Trend Micro Control Manager GetPassword() SQLi

Trend Micro ControlManager < 3.0 SP5 Multiple Vulnerabilities

Trend Micro Data Loss Prevention Virtual Appliance Encoded Traversal Arbitrary File Access

Trend Micro Data Loss Prevention Virtual Appliance Web Console Detection

Trend Micro Emanager Detection

Trend Micro IMSS Console Management Detection

Trend Micro InterScan VirusWall /interscan/cgi-bin/FtpSave.dll Unauthenticated Remote Configuration Manipulation

Trend Micro InterScan VirusWall catinfo CGI Overflow

Trend Micro InterScan Web Security Suite Default Credentials

Trend Micro IWSS Console Management Detection

Trend Micro OfficeScan 7.3 Multiple Vulnerabilities

Trend Micro OfficeScan ofcscan.ini Configuration File Disclosure

Trend Micro OfficeScan Server CGI Modules Multiple Vulnerabilities

Trend Micro Scanmail for Domino nsf File Information Disclosure

Trend Micro ScanMail for Exchange Web Console Detection

Trend Micro ServerProtect for Linux splx\_2376\_info Cookie Authentication Bypass

Trend Micro Smart Protection Server Session Hijacking Via Log File Disclosure

Trend Micro Threat Intelligence Manager sampleReporting.php 'fakename' Parameter File Disclosure

Trend Micro Threat Intelligence Manager Web Console Detection

Trend Micro TMCM Console Management Detection

Trend Micro Virus Buster cgiWebupdate.exe Arbitrary File Retrieval

Tripwire for Webpages Installation Disclosure

trixbox Cisco Phone Services PhoneDirectory.php ID Parameter SQL Injection

trixbox Dashboard user/index.php langChoice Parameter Local File Inclusion

trixbox maint Web Interface Default Credentials

trixbox Web Detection

Trouble Ticket Express fid Parameter Arbitrary Remote Code Execution

Truegalerie admin.php loggedin Parameter Admin Authentication Bypass

TrustPort WebFilter help.php hf Parameter Directory Traversal

ttCMS 2.2 Multiple Vulnerabilities

ttforum Multiple Vulnerabilities

Turbo Seek tseekdir.cgi location Parameter Arbitrary File Access

TUTOS < 1.1.20040412 Multiple Input Validation Issues

TUTOS < 1.2 Multiple Input Validation Vulnerabilities

TWiki %INCLUDE Parameter Arbitrary Command Injection

TWiki 'debugenableplugins' Parameter RCE

TWiki 'filename' Parameter Traversal Arbitrary File Access

TWiki 'rev' Parameter Arbitrary Command Execution

TWiki < 5.1.3 Multiple Vulnerabilities

TWiki < 5.1.4 MAKETEXT Variable Tilde Character Command Injection

TWiki bin/configure 'image' Parameter Traversal Arbitrary File Access/Execution

TWiki configure Script Arbitrary Command Execution

TWiki Detection

TWiki ImageGalleryPlugin Shell Command Injection

TYPO3 'AbstractController.php' 'BACK\_PATH' Parameter Remote File Inclusion

TYPO3 'cmw\_linklist Extension' 'category\_uid' Parameter SQL Injection

TYPO3 'jumpUrl' Mechanism Information Disclosure

TYPO3 'spell-check-logic.php' 'userUid' Parameter Arbitrary Command Execution

TYPO3 < 3.5.0 Multiple Vulnerabilities

TYPO3 Anchor-only Links Remote Spoofing Vulnerability

TYPO3 Back-end 'index.php' 'redirect\_url' Redirect

TYPO3 Default Credentials

TYPO3 Detection

TYPOlight < 2.2.5 Unspecified Vulnerability

UBB.threads < 6.5.2 beta Multiple Vulnerabilities

UBB.threads addpost\_newpoll.php thispath Parameter Remote File Inclusion

UBB.threads Detection

UBB.threads doeditconfig Arbitrary Command Injection

UBB.threads dosearch.php SQL injection

UBB.threads editpost.php Number Parameter SQL Injection

Ubuntu Drupal Theme - Brown images/layout/gradient.php File Disclosure

UebiMiau Multiple Input Validation Vulnerabilities

Ultimate Form Builder Lite for WordPress < 1.3.7 SQL Injection

Ultimate PHP Board < 1.9.7 viewforum.php Multiple Vulnerabilities

Ultimate PHP Board add.php Direct Request Information Disclosure

Ultimate PHP Board admin\_iplog.php Arbitrary Code Execution

Ultimate PHP Board chat/login.php username Parameter Arbitrary Command Execution

Ultimate PHP Board users.dat Multiple Vulnerabilities

Ultimate Product Catalog Plugin for WordPress < 4.2.26 PHP Object Injection

UltraVNC Java Viewer Detection

Umbraco codeEditorSave.asmx SaveDLRScript Operation Traversal File Upload Arbitrary Command Execution

Umbraco Detection

Unify eWave ServletExec 3.0C UploadServlet Unprivileged File Upload

Untangle NG Firewall Captive Portal RCE

Untangle NG Firewall Detection

Upload Lite upload.cgi Arbitrary File Upload

Uploader Plugin for WordPress File Upload Arbitrary Code Execution

US Robotics Broadband Router 8003 menu.htm Admin Password Disclosure

Usermin 'miniserv.pl' Arbitrary File Disclosure

Usermin 'miniserv.pl' Base-64 String Metacharacter Handling Session Spoofing

Usermin Detection

Usermin Null Byte Filtering Information Disclosure

UserPro Plugin for WordPress up\_auto\_log Parameter Remote Authentication Bypass

uStorekeeper ustorekeeper.pl file Parameter Traversal Arbitrary File Access

Vanilla Forum p Parameter Local File Inclusion

Vanilla Forums Header Injection Remote Code Execution

vBulletin 'widget\_php' Command Execution

vBulletin <= 3.0.9 Multiple Vulnerabilities

vBulletin authorize.php x\_invoice\_num Parameter SQL Injection

vBulletin calendar.php eventid Parameter SQL Injection

vBulletin Database Credentials Information Disclosure

vBulletin Detection

vBulletin Email Field XSS

vBulletin forumdisplay.php comma Parameter Arbitrary Command Execution

vBulletin includes/init.php Unspecified Vulnerability

vBulletin misc.php template Parameter PHP Code Injection

vBulletin upgrade.php Accessible

vCard define.inc.php match Parameter Remote File Inclusion

VChat Multiple Remote Vulnerabilities

Veri-NAC Appliance unauthenticated URL Directory Traversal

Veritas NetBackup Appliance 2.6.0.x / 2.6.1.x / 2.7.x RCE (VTS16-002)

Veritas NetBackup Appliance 2.7.x / 3.0.x Remote Command Execution (VTS17-005)

Veritas NetBackup Appliance 2.7.x / 3.0.x Remote Command Execution (VTS17-005) (exploit)

Veritas NetBackup Appliance < 2.7.2 / 3.1.0 Multiple Vulnerabilities (VTS17-003)

Veritas NetBackup Appliance Web Console Detection

Verity UltraSeek 3.1.x Malformed URL Remote DoS

Verity Ultraseek < 5.7 Multiple Vulnerabilities

VHCS include/sql.php include\_path Parameter Remote File Inclusion

VHCS login.php check\_login() Function Authentication Bypass

VHCS PHPSESSID Cookie Session Fixation

ViArt Shop Detection

ViArt Shop sips\_response.php DATA Parameter Request Parsing Remote Shell Command Execution

VICIDIAL Call Center Suite admin.php SQL Injection

VICIDIAL Call Center Suite Default Administrative Credentials

VideoDB < 2.0.2 Multiple Vulnerabilities

ViewCVS < 1.0.0 Multiple Vulnerabilities

ViewVC Detection

ViewVC Direct Request CVSROOT Information Disclosure

Vignette Application Portal Diagnostic Utility Information Disclosure

Vignette StoryServer < 6.0.4 Arbitrary TCL Code Execution

Vignette StoryServer TCL Server Crash Information Disclosure

Viralator CGI Script Arbitrary Command Execution

ViRobot Linux Server addschup Multiple Overflows

ViRobot Linux Server filescan Authentication Bypass

Virtual Visions FTP ftp.pl dir Parameter Traversal Arbitrary File Access

Virtualizor < 2.3.1 Unspecified SQL Injection

Virtualizor < 2.3.2 PDNS Domain Deletion Security Bypass

Virtualizor Detection

Visitor Data Module for Joomla! X-Forwarded-For Header RCE

VisNetic / Merak Mail Server Multiple Remote Vulnerabilities

Visual Mining NetCharts Server Arbitrary File Upload

Visual Mining NetCharts Server Default Credentials (Web UI)

Visual Mining NetCharts Server Web UI Detection

Visualware MyConnection Server Web Detection

VLC Web Interface Detection

VLC Web Interface XML Services Remote Command Execution

VMware AirWatch Console HTTP Detection

VMware ESX / ESXi host Directory Configuration Files Information Disclosure

VMware ESX / ESXi Remotely Accessible Method Object Browser API

VMware ESX / ESXi Web-Based Datastore Browser Default Credentials

VMware Horizon Workspace Detection

VMware Host Agent Directory Traversal (VMSA-2009-0015)

VMware Host Agent Web Detection

VMware vCenter Operations Manager Web UI Default Credentials

VMware vCenter Update Manager Detection

VMware vCenter Update Manager Directory Traversal (VMSA-2011-0014)

VMware vRealize Log Insight 2.x / 3.x < 3.6.0 Directory Traversal File Disclosure (VMSA-2016-0011)

VMware vRealize Log Insight 4.6.x < 4.6.2 / 4.7.x < 4.7.1 Authorization Bypass Vulnerability (VMSA-2018-0028)

VMware vRealize Operations Manager ver 6.x < 6.40 Suite API CollectorHttpRelayController RelayRequest Object DiskFileItem Deserialization DoS

VMware vRealize Operations Manager Web UI Detection

Vocran NVR Remote Command Execution

VP-ASP Multiple Script SQL Injection

VP-ASP shopexd.asp catalogid Parameter SQL Injection

VP-ASP shopsearch SQL Injection

VPOPMail for SquirrelMail vpopmail.php Arbitrary Command Execution

vpopmail-CGIApps vpasswd.cgi Remote Command Execution

vTiger < 4.5a2 Multiple Vulnerabilities

vTiger CRM Directory File Disclosure

Vtiger CRM graph.php Directory Traversal

vtiger CRM phprint.php lang\_crm Parameter Local File Inclusion

VX Search HTTP POST Request Handling Remote Stack Buffer Overflow

w-Agora 4.1.6a Multiple Input Validation Vulnerabilities

w-Agora <= 4.2.0 Multiple Vulnerabilities

w-Agora inc\_dir Parameter Remote File Inclusion

w-Agora index.php site Parameter Traversal Arbitrary File Access

w-Agora Multiple Script Traversal Arbitrary File Access

W3 Total Cache Plugin for WordPress Cache File Direct Request Information Disclosure

W3 Total Cache Plugin for WordPress Multiple Insecure PHP Code Inclusion Macros Remote Code Execution

W3.org Anaya Web sendtemp.pl 'templ' Parameter Traversal Arbitrary File Access

WANem Detection

WANem result.php pc Parameter Remote Command Execution

WaveMaker < 6.4.6 Security Bypass

WaveMaker Studio Detection

WaveMaker Studio Requires No Authentication

Way-board way-board.cgi db Parameter Arbitrary File Access

Web Accessible Backups

Web Application Information Disclosure

Web Application Potentially Sensitive CGI Parameter Detection

Web Application SQL Backend Identification

Web Common Credentials

Web Common Credentials (HTML form)

Web Server /cgi-bin Perl Interpreter Access

Web Server /cgi-bin Shell Access

Web Server Generic 3xx Redirect

Web Server Generic Cookie Injection

Web Server info.php / phpinfo.php Detection

Web Server Malicious JavaScript Link Detection

Web Server Office File Inventory

Web Service Description Language File Detected

Web Site Client Access Policy File Detection

Web Site Cross-Domain Policy File Detection

Web Site sitemap.xml File and Directory Disclosure

Web Tests Session Expiration Errors

Web Wiz check\_user.asp txtUserName Parameter SQL Injection

Web Wiz Forums wwforum.mdb Direct Request Database Disclosure

Web Wiz Site News / Compulsive Media CNU5 news.mdb Direct Request Database Disclosure

web-app.org WebAPP Encoded Request .dat File Disclosure

web.config File Information Disclosure

WebActive HTTP Server active.log Remote Information Disclosure

WebAdmin < 3.2.5 Multiple Vulnerabilities

WebAdmin < 3.2.6 MDaemon Account Hijacking

webadmin.php show Parameter Arbitrary File Access

WEBalbum skin2 Cookie Parameter Traversal Local File Inclusion

WebAPP apage.cgi f Parameter Arbitrary Command Execution

WebAPP Detection

WebAPP Directory Traversal

Webapp.org WebAPP < 0.9.9.6 Multiple Vulnerabilities

WebCalendar < 1.0.2 Multiple Vulnerabilities

WebCalendar assistant\_edit.php Unauthorized Access

WebCalendar Detection

WebCalendar includes/functions.php noSet Variable Overwrite

WebCalendar Login Error Message User Account Enumeration

WebCalendar login.php webcalendar\_session Cookie SQL Injection

WebCalendar long.php user\_inc Parameter Traversal Arbitrary File Access

WebCalendar send\_reminders.php includedir Parameter Remote File Inclusion

Webcart Default Install Configuration Disclosure

WebChat defines.php WEBCHATPATH Parameter Remote File Inclusion

webERP Configuration File Remote Access

Webfroot shoutbox.php conf Parameter Traversal Local File Inclusion

WebGais webgais CGI Arbitrary Command Execution

WebGais websendmail CGI Arbitrary Command Execution

WebGlimpse Detection

WebGlimpse query Parameter Command Injection

WebGUI < 6.7.3 Multiple Command Execution Vulnerabilities

WebGUI < 6.7.6 Asset.pm Asset Addition Arbitrary Code Execution

WebGUI user profile Unspecified Vulnerability

WebHints hints.pl Arbitrary Command Execution

Webhosting Component for Joomla! 'catid' Parameter SQLi

WEBInsta CMS index.php templates\_dir Parameter Remote File Inclusion

WebLogic < 8.1 SP3 Multiple Vulnerabilities

WebLogic Multiple Method Cleartext Password Disclosure

WebLogic Servlets Multiple Vulnerabilities

Webman I-Mall i-mall.cgi Arbitrary Command Execution

WebMatic Unspecified Login Function Access Vulnerability

Webmin 'miniserv.pl' 'username' Parameter Format String

Webmin 'miniserv.pl' Arbitrary File Disclosure

Webmin 'miniserv.pl' Base-64 String Metacharacter Handling Session Spoofing

Webmin 0.21 <= 1.0 Multiple Vulnerabilities

Webmin 0.80 / 0.88 world-writable files

Webmin 0.91 Directory Traversal

Webmin 0.92 Multiple Vulnerabilities

Webmin 0.96 Multiple Vulnerabilities

Webmin 0.99 Remote Code Exection

Webmin 1.140 Multiple Vulnerabilities

Webmin 1.720 Read Mail Symlink Vulnerability

Webmin 1.840 / 1.880 Local File Inclusion Vulnerability

Webmin 1.850 Multiple Vulnerabilities

Webmin 1.890 - 1.920 Remote Command Execution (CVE-2019-15107, CVE-2019-15231)

Webmin 1.x < 1.160 Remote Code Execution

Webmin < 0.5 Brute Force Vulnerability

Webmin < 0.85 Multiple Vulnerabilities

Webmin < 1.070 authentication bypass

Webmin < 1.200 Unauthorized Configuration File Access

Webmin < 1.230 miniserv.pl Authentication Bypass

Webmin < 1.250 miniserv.pl Remote Code Execution

Webmin < 1.280 Directory Traversal

Webmin <= 1.590 Multiple Vulnerabilities

Webmin Detection

Webmin Null Byte Filtering Information Disclosure

Webmin Unspecified Command Execution Vulnerability (< 1.370)

WebPagetest < 2.7.2 file Parameter Traversal Arbitrary File Access

WebPagetest Detection

WEBrick Encoded Traversal Arbitrary CGI Source Disclosure

Websense Reporting Console Detection

Websense TRITON 7.8 Source Code Disclosure

Websense TRITON Unauthorized File Disclosure

Webserver 4D Plaintext Password Storage

WebShield Appliance Detection

Website Baker Admin Login SQL Injection

Website Baker REMEMBER\_KEY Cookie SQL Injection

WebSite Pro Malformed URL Path Disclosure

WebSite Pro webfind.exe keywords Parameter Remote Overflow

WebsitePro Remote Request Overflow

WebSpeed Development Mode Check

WebSpeed Messenger Administration Utility Unauthenticated Access

WebSpeed Workshop Arbitrary Command Execution

WebSPIRS webspirs.cgi Traversal Arbitrary File Access

WebStores 2000 browse\_item\_details.asp SQL Injection

WebTitan 'categories-x.php' 'sortkey' Parameter SQL Injection

WebTitan Detect

WebTitan Web Interface Default Credentials

WebWho+ whois.pl time Parameter Arbitrary Command Execution

WebYaST Host Modification MiTM

WebYaST Web Client Detection

WePresent file\_transfer.cgi Remote Command Execution

West Wind Web Connection Unprotected Configuration Editor Application

Western Digital Arkeia 10.1.x < 10.1.19 / 10.2.x < 10.2.9 Multiple Vulnerabilities (Heartbleed)

Western Digital Arkeia lang Cookie Crafted Local File Inclusion

Western Digital Arkeia lang Cookie Local File Inclusion

Western Digital Arkeia Virtual Appliance Blank Password

Western Digital Arkeia Virtual Appliance Detection

Western Digital Arkeia Virtual Appliance Unsupported Version Detection

Western Digital My Net Router main\_internet.php Admin Credential Disclosure

Western Digital MyCloud Unauthenticated File Upload

Western Digital ShareSpace Detection

Western Digital ShareSpace WEB GUI Information Disclosure

Western Digital TV Multiple Vulnerabilities

WF-Chat User Account Disclosure

WHM AutoPilot < 2.5.20 Multiple Remote Vulnerabilities

WihPhoto sendphoto.php Traversal Arbitrary File Access

Wikka wikka.php Local File Inclusion

Windmail.exe Shell Metacharacter Arbitrary Command Execution

Winmail Server <= 4.2 Build 0824 Multiple Vulnerabilities

Winmail Server Webmail Unspecified Vulnerability

Woltlab Burning Board Detection

WoltLab Burning Board Lite thread.php decode\_cookie Function threadvisit Cookie Parameter SQL Injection

WoltLab Burning Board Lite wbb\_userid Parameter PHP Unset SQL Injection

Woltlab Burning Board modcp.php Multiple Parameter SQL Injection

Woltlab Burning Board Multiple SQL Injections

WoltLab Burning Board search.php Multiple Parameter SQL Injection

Woltlab Burning Board verify\_email Function SQL Injection

Woppoware PostMaster <= 4.2.2 Multiple Vulnerabilities

Wordit Logbook logbook.pl file Parameter Arbitrary File Access

WordPress 'blog.header.php' Multiple Parameter SQL Injection

WordPress 'press-this.php' Security Bypass

WordPress 'query.php' is\_admin() Function Information Disclosure

WordPress 'template-functions-category.php' 'cat\_ID' Parameter SQL Injection

WordPress 'wp-login.php' HTTP Response Splitting

WordPress 'xmlrpc.php' pingback.ping Server-Side Request Forgery

WordPress 2.3.0 - 4.8.3 Unauthorized Password Reset

WordPress 3.3.x < 3.3.1 XSS Vulnerability

WordPress 4.7.x < 4.7.2 REST API 'id' Parameter Privilege Escalation

WordPress < 0.72 RC1 Multiple Vulnerabilities

WordPress < 1.2.2 Multiple Vulnerabilities

WordPress < 1.5.1 Multiple Vulnerabilities

WordPress < 1.5.1 Multiple XSS and SQL Injection Vulnerabilities

WordPress < 1.5.1.3 XMLRPC SQL Injection

WordPress < 2.0.2 Multiple Cross-Site Scripting (XSS) Vulnerabilities

WordPress < 2.1.1 Multiple Script Backdoors

WordPress < 2.8.3 'wp-admin' Multiple Security Bypass Vulnerabilities

WordPress < 2.8.4 'wp-login.php' 'key' Parameter Remote Administrator Password Reset (uncredentialed check)

WordPress < 2.8.4 Password Reset

WordPress < 2.8.6 Multiple Vulnerabilities

WordPress < 3.0.1 Security Bypass

WordPress < 3.0.2 Multiple Vulnerabilities

WordPress < 3.0.3 XML-RPC Interface Access Restriction Bypass

WordPress < 3.0.4 Multiple XSS Vulnerabilities

WordPress < 3.0.5 Multiple Vulnerabilities

WordPress < 3.1.1 Multiple Vulnerabilities

WordPress < 3.1.3 Multiple Vulnerabilities

WordPress < 3.1.4 / 3.2-RC3 Multiple Blind SQL Injection Vulnerabilities

WordPress < 3.3.2 Multiple Vulnerabilities

WordPress < 3.3.3 / 3.4.0 Multiple Vulnerabilities

WordPress < 3.4.1 Multiple Vulnerabilities

WordPress < 3.4.2 Multiple Vulnerabilities

WordPress < 3.5.1 Multiple Vulnerabilities

WordPress < 3.5.2 Multiple Vulnerabilities

WordPress < 3.6.1 Multiple Vulnerabilities

WordPress < 3.7.2 / 3.8.2 Multiple Vulnerabilities

WordPress < 3.7.4 / 3.8.4 / 3.9.2 Multiple Vulnerabilities

WordPress < 3.7.5 / 3.8.5 / 3.9.3 / 4.0.1 Multiple Vulnerabilities

WordPress < 3.7.6 / 3.8.6 / 3.9.4 / 4.1.2 Multiple Vulnerabilities

WordPress < 3.7.9 / 3.8.9 / 3.9.7 / 4.1.6 / 4.2.3 Multiple Vulnerabilities

WordPress < 4.2.4 Multiple Vulnerabilities

WordPress < 4.3.1 Multiple Vulnerabilities

WordPress < 4.4.1 class-wp-theme.php XSS

WordPress < 4.4.2 Multiple Vulnerabilities

WordPress < 4.5.0 Multiple Vulnerabilities

WordPress < 4.5.2 Multiple Vulnerabilities (ImageTragick)

WordPress < 4.5.3 Multiple Vulnerabilities

WordPress < 4.6 Multiple Vulnerabilities

WordPress < 4.6.1 Multiple Vulnerabilities

WordPress < 4.7.1 Multiple Vulnerabilities

WordPress < 4.7.2 Multiple Vulnerabilities

WordPress < 4.7.3 Multiple Vulnerabilities

WordPress < 4.7.5 Multiple Vulnerabilities

WordPress < 4.8.2 Multiple Vulnerabilities

WordPress < 4.8.3 Multiple Vulnerabilities

WordPress < 4.9.1 Multiple Vulnerabilities

WordPress < 4.9.2 MediaElement.js Flash Fallback XSS

WordPress < 4.9.5 Multiple Vulnerabilities

WordPress < 4.9.7 Arbitrary File Deletion Vulnerability

WordPress < 4.9.9 / 5.x < 5.0.1 Cross-site Scripting Vulnerability

WordPress < 4.9.9 Remote Code Execution Vulnerabilities

WordPress < 5.0.4 Directory Traversal Vulnerability

WordPress < 5.1.1 Multiple Vulnerabilities

WordPress < 5.2.4 Multiple Vulnerabilities

WordPress < 5.3.1

WordPress <= 3.6.1 / 3.7.x < 3.7.30 / 3.8.x < 3.8.30 / 3.9.x < 3.9.28 / 4.0.x < 4.0.27 / 4.1.x < 4.1.27 / 4.2.x < 4.2.24 / 4.3.x < 4.3.20 / 4.4.x < 4.4.19 / 4.5.x < 4.5.18 / 4.6.x < 4.6.15 / 4.7.x < 4.7.14 / 4.8.x < 4.8.10 / 4.9.x < 4.9.11 / 5.0.x < 5.0.6 / 5.1.x < 5.1.2 / 5.2.x < 5.2.3 Multiple Vulnerabilities

WordPress <= 3.9.5 / 4.1.x < 4.1.4 / 4.2.x < 4.2.1 Comments Stored XSS

WordPress A Page Flip Book Plugin for WordPress 'pageflipbook\_language' Parameter Arbitrary Code Execution

WordPress AdServe 'adclick.php' 'id' Parameter SQL Injection

WordPress check\_ajax\_referer() Function SQL Injection

WordPress Cookie 'cache\_lastpostdate' Parameter PHP Code Injection

WordPress Detection

WordPress fGallery 'fim\_rss.php' 'album' Parameter SQL Injection

WordPress index.php 'cat' Parameter Local File Inclusion

WordPress Outdated Plugin Detection

WordPress Pingback File Information Disclosure

WordPress Plugin 'AMP for WP - Accelerated Mobile Pages' < 0.9.97.20 Multiple Vulnerabilities

WordPress Plugin 'Duplicator' < 1.3.28 Unauthenticated Arbitrary File Download

WordPress Plugin 'ThemeGrill Demo Importer' 1.3.4 < 1.6.3 Database Wipe and Auth Bypass

WordPress Plugin 'WP GDPR Compliance' < 1.4.3 Privilege Escalation

WordPress Plugin Detection

WordPress Poll Plugin 'poll\_id' Parameter SQL Injection

WordPress ToolsPack Plugin Backdoor

WordPress Trackback 'wp-trackback.php' 'tb\_id' Parameter SQL Injection

WordPress Trackback Charset Decoding SQL Injection

WordPress Unsupported Version Detection

WordPress User Enumeration

Wordtrans-web exec\_wordtrans Function Arbitrary Command Execution

WowBB <= 1.61 Multiple Vulnerabilities

WowBB view\_user.php Multiple Parameter SQL Injection

WP Forum Server Plugin for WordPress 'topic' Parameter SQL Injection

WP Google Maps for WordPress < 7.11.17 Unauthenticated SQL Injection (CVE-2019-10692)

WP Mobile Detector Plugin for WordPress File Upload RCE

WP Online Store Plugin for WordPress Multiple Parameter File Disclosure

WP Smart Security Plugin for WordPress PHP Object Injection

WP Source Control Plugin for WordPress Directory Traversal

WP Statistics Plugin for WordPress 'functions.php' wp\_statistics\_searchengine\_query() SQLi

WP Statistics Plugin for WordPress < 12.0.8 'functions.php' wp\_statistics\_searchengine\_query() SQLi

WP Statistics Plugin for WordPress < 12.6.7 Blind SQL Injection

WP Super Cache Plugin for WordPress Multiple Insecure PHP Code Inclusion Macros Remote Code Execution

WP Symposium Plugin Arbitrary File Upload

WP Symposium Plugin for WordPress 'symposium\_groups\_functions.php' 'gid' Parameter SQL Injection

WP Symposium Plugin for WordPress forum.php 'show' Parameter SQL Injection

WP Symposium Plugin for WordPress forum.php 'show' Parameter SQL Injection (Version Check)

WP Symposium Plugin for WordPress forum\_functions.php 'topic\_id' Parameter SQLi

WP-Forum Plugin for WordPress 'forum\_feed.php' 'thread' Parameter SQL Injection

WP-Lytebox 'pg' Parameter Local File Inclusion

WP-Syntax Plugin for WordPress 'apply\_filters' function Command Execution

WPS Web-Portal-System wps\_shop.cgi art Parameter Arbitrary Command Injection

WPtouch Plugin for WordPress 'wptouch\_redirect' Parameter URL Redirection

WWWBoard passwd.txt Authentication Credential Disclosure

wwwcount Count.cgi Remote Overflow

wwwwais QUERY\_STRING Parameter Remote Overflow

X-News Password MD5 Hash Authentication Bypass

X2Engine < 3.5.1 Multiple Vulnerabilities

X2Engine < 3.7.4 Multiple Vulnerabilities

X2Engine < 4.0 ProfileController.php Unrestricted File Upload Vulnerability

X2Engine < 4.2 Multiple Vulnerabilities

X2Engine Detection

X7 Chat help/index.php help\_file Parameter Local File Inclusion

X7 Chat index.php day Parameter SQL Injection

X7 Chat upgradev1.php old\_prefix Parameter SQL Injection

XAMPP < 1.4.14 Multiple Vulnerabilities

XAMPP ADOdb mssql\_connect Remote Buffer Overflow

XAMPP Example Pages Detection

Xaraya index.php module Parameter Traversal Arbitrary File/Directory Manipulation

Xaraya Software/Version Detection

Xerox CentreWare Web < 4.6.46 Multiple Vulnerabilities (XRX08-008)

Xerver Double Slash Authentication Bypass

XMB Forum < 1.9.10 Multiple Vulnerabilities

XMB member.php Multiple Parameter SQL Injection

XOOPS 1.0 RC1 Multiple Vulnerabilities

XOOPS < 2.0.12 Multiple Vulnerabilities

XOOPS Article Module article.php id Parameter SQL Injection

XOOPS Articles Module print.php id Parameter SQL Injection

XOOPS Detection

XOOPS Dictionary Module print.php id Parameter SQL Injection

Xoops Incontent Module Traversal Arbitrary PHP File Source Disclosure

XOOPS Jobs Module index.php cid Parameter SQL Injection

XOOPS Multiple Modules spaw\_control.class.php spaw\_root Parameter Remote File Inclusion

XOOPS Multiple Scripts mydirname Parameter Arbitrary Command Injection

XOOPS WF-Section Module print.php articleid Parameter SQL Injection

XOOPS XFSection Module modify.php dir\_module Parameter Remote File Inclusion

XOOPS xoopsConfig Parameter Variable Overwrite Local File Inclusion

XOOPS xoopsConfig[language] Parameter Local File Inclusion (DSECRG-08-040)

XOOPS xoopsConfig[language] Parameter Local File Inclusion (XOOPS\_WFd205\_xpl)

XoopsGallery init\_basic.php GALLERY\_BASEDIR Parameter Remote File Inclusion

Xpressions Interactive Multiple Products login.asp SQL Injection

XStandard Lite Plugin for Joomla! X\_CMS\_LIBRARY\_PATH Header Directory Traversal

XTreme ASP Photo Gallery adminlogin.asp Multiple Parameter SQL Injection

Xylogics Annex Terminal Service ping CGI Program DoS

YaBB 1 Gold < 1.3.2 Multiple Input Validation Vulnerabilities

YaBB 1 GOLD SP 1.3.2 Multiple Vulnerabilities

YaBB SE < 1.5.2 Multiple Vulnerabilities

YaBB SE Cookie Authentication Bypass

YaBB YaBB.pl num Parameter Traversal Arbitrary File Access

YaNC Component for Joomla! 'listid' Parameter SQLi

YaPiG < 0.92.2 Multiple Scripts Arbitrary Command Execution

YaPiG < 0.95b Multiple Vulnerabilities

YaPiG <= 0.9.5b Multiple Vulnerabilities

YaPiG Password Protected Directory Bypass

yappa-ng < 2.3.2 Multiple Vulnerabilities

yappa-ng index.php album Parameter Local File Inclusion

Zabbix 1.9.x < 1.9.4 zabbix\_agentd DoS

Zabbix 2.0.x < 2.0.21 / 2.2.x < 2.2.18 / 3.0.x < 3.0.9 / 3.2.x < 3.2.5 Multiple Vulnerabilities

Zabbix 3.0.x < 3.0.13 / 3.2.x < 3.2.10 / 3.4.x < 3.4.4 Multiple Vulnerabilities

Zabbix 3.2.x < 3.2.7 Multiple Vulnerabilities

Zabbix < 1.8.16 / 2.0.5 / 2.1.0 user.login cnf Parameter Authentication Bypass

Zabbix < 1.8.18rc1 / 2.0.9rc1 / 2.1.7 Multiple SQL Injections

Zabbix < 1.8.20 / 2.0.11 / 2.2.2 Multiple Vulnerabilities

Zabbix < 1.8.6 Multiple Vulnerabilities

Zabbix < 2.0.18 / 2.2.13 / 3.0.3 'mysql.size' Parameter Command Injection

Zabbix < 2.2.12 / 2.4.8 / 3.0.1 charts.php 'stime' Parameter Resource Consumption Remote DoS

Zabbix Web Interface Default Administrator Credentials

Zabbix Web Interface Detection

Zabbix Web Interface extlang[] Parameter Remote Code Execution

Zabbix Web Interface popup\_bitem.php itemid Parameter SQL Injection

Zanfi CMS Lite index.php inc Parameter Remote File Inclusion

Zen Cart autoload\_func.php autoLoadConfig Array Remote File Inclusion

Zen Cart Detection

Zen Cart extras/curltest.php Information Disclosure

Zen Cart index.php typefilter Parameter Traversal Local File Inclusion

Zen Cart ipn\_main\_handler.php custom SQL Injection

Zen Cart password\_forgotten.php Admin Access Bypass

Zen Cart password\_forgotten.php admin\_email Parameter SQL Injection

Zen Cart products\_id[] Array SQL Injection

ZEN Load Balancer global.conf Information Disclosure

Zenphoto < 1.4.2.1 Multiple Vulnerabilities

Zenphoto Detection

Zenphoto rss.php albumnr Parameter SQL Injection

Zenphoto viewer\_size\_image\_saved Cookie Value eval() Call Remote PHP Code Execution

zenTrack index.php configFile Parameter Traversal Arbitrary Files Access

zenTrack index.php Multiple Parameter Remote File Inclusion

ZeroBoard < 4.1pl5 Multiple Remote Vulnerabilities

ZeroBoard Multiple Scripts dir Parameter Remote File Inclusion

zFeeder admin.php Direct Request Admin Authentication Bypass

Zimbra Collaboration Server 8.7.x < 8.7.11p10 XML External Entity injection (XXE) vulnerability

Zimbra Collaboration Server < 7.2.6 / 8.0.6 Unspecified Vulnerability

Zimbra Collaboration Server Aspell Spell Check Service Detection

Zimbra Collaboration Server skin Parameter Traversal Local File Inclusion

Zimbra Collaboration Server Web Detection

Zinwave Series 3000 DAS Web Interface Default Credentials

ZixForum ZixForum.mdb DIrect Request Database Disclosure

Zmanda Recovery Manager for MySQL socket-server.pl MYSQL\_BINPATH Variable Command Execution

zml.cgi Directory Traversal

Zoho ManageEngine OpManager 'OPM\_BVNAME' Multiple Vulnerabilities

Zorum <= 3.5 Multiple Remote Vulnerabilities

ZPanel 2.0 Multiple Script Remote File Inclusion

# CentOS Local Security Checks

CentOS 3 / 4 / 5 : acpid (CESA-2009:0474)

CentOS 3 / 4 / 5 : bind (CESA-2007:0740)

CentOS 3 / 4 / 5 : bind (CESA-2009:0020)

CentOS 3 / 4 / 5 : bind / selinux-policy (CESA-2008:0533)

CentOS 3 / 4 / 5 : bzip2 (CESA-2008:0893)

CentOS 3 / 4 / 5 : bzip2 (CESA-2010:0703)

CentOS 3 / 4 / 5 : cups (CESA-2007:0123)

CentOS 3 / 4 / 5 : cups (CESA-2007:0720)

CentOS 3 / 4 / 5 : cups (CESA-2008:0498)

CentOS 3 / 4 / 5 : cups (CESA-2008:0937)

CentOS 3 / 4 / 5 : cups (CESA-2010:0490)

CentOS 3 / 4 / 5 : e2fsprogs (CESA-2008:0003)

CentOS 3 / 4 / 5 : ed (CESA-2008:0946)

CentOS 3 / 4 / 5 : expat (CESA-2009:1625)

CentOS 3 / 4 / 5 : fetchmail (CESA-2007:0385)

CentOS 3 / 4 / 5 : fetchmail (CESA-2009:1427)

CentOS 3 / 4 / 5 : freeradius (CESA-2007:0338)

CentOS 3 / 4 / 5 : freetype (CESA-2007:0150)

CentOS 3 / 4 / 5 : freetype (CESA-2008:0556)

CentOS 3 / 4 / 5 : freetype (CESA-2010:0607)

CentOS 3 / 4 / 5 : gcc / gcc4 (CESA-2010:0039)

CentOS 3 / 4 / 5 : ghostscript (CESA-2008:0155)

CentOS 3 / 4 / 5 : gimp (CESA-2007:0343)

CentOS 3 / 4 / 5 : gimp (CESA-2007:0513)

CentOS 3 / 4 / 5 : gzip (CESA-2010:0061)

CentOS 3 / 4 / 5 : httpd (CESA-2008:0967)

CentOS 3 / 4 / 5 : ImageMagick (CESA-2008:0145)

CentOS 3 / 4 / 5 : ipsec-tools (CESA-2008:0849)

CentOS 3 / 4 / 5 : kdebase (CESA-2007:0494)

CentOS 3 / 4 / 5 : krb5 (CESA-2010:0029)

CentOS 3 / 4 / 5 : krb5 (CESA-2010:0423)

CentOS 3 / 4 / 5 : libpng (CESA-2007:0356)

CentOS 3 / 4 / 5 : libpng (CESA-2007:0992)

CentOS 3 / 4 / 5 : libpng / libpng10 (CESA-2010:0534)

CentOS 3 / 4 / 5 : libtool (CESA-2009:1646)

CentOS 3 / 4 / 5 : libvorbis (CESA-2007:0845)

CentOS 3 / 4 / 5 : libvorbis (CESA-2008:0270)

CentOS 3 / 4 / 5 : libvorbis (CESA-2009:1561)

CentOS 3 / 4 / 5 : libxml2 (CESA-2008:0032)

CentOS 3 / 4 / 5 : libxml2 (CESA-2008:0836)

CentOS 3 / 4 / 5 : libxml2 (CESA-2008:0884)

CentOS 3 / 4 / 5 : libxml2 (CESA-2008:0988)

CentOS 3 / 4 / 5 : libxslt (CESA-2008:0287)

CentOS 3 / 4 / 5 : lynx (CESA-2008:0965)

CentOS 3 / 4 / 5 : mikmod (CESA-2010:0720)

CentOS 3 / 4 / 5 : mod\_perl (CESA-2007:0395)

CentOS 3 / 4 / 5 : mutt (CESA-2007:0386)

CentOS 3 / 4 / 5 : net-snmp (CESA-2008:0529)

CentOS 3 / 4 / 5 : net-snmp (CESA-2008:0971)

CentOS 3 / 4 / 5 : newt (CESA-2009:1463)

CentOS 3 / 4 / 5 : openoffice / openoffice.org (CESA-2007:0406)

CentOS 3 / 4 / 5 : openoffice.org (CESA-2007:0848)

CentOS 3 / 4 / 5 : openoffice.org (CESA-2010:0101)

CentOS 3 / 4 / 5 : openssl (CESA-2009:0004)

CentOS 3 / 4 / 5 : pango (CESA-2009:0476)

CentOS 3 / 4 / 5 : pango (CESA-2010:0140)

CentOS 3 / 4 / 5 : perl (CESA-2007:0966)

CentOS 3 / 4 / 5 : perl (CESA-2008:0522)

CentOS 3 / 4 / 5 : php (CESA-2010:0040)

CentOS 3 / 4 / 5 : pidgin (CESA-2008:0584)

CentOS 3 / 4 / 5 : postfix (CESA-2008:0839)

CentOS 3 / 4 / 5 : postgresql (CESA-2007:0336)

CentOS 3 / 4 / 5 : qt (CESA-2007:0721)

CentOS 3 / 4 / 5 : qt (CESA-2007:0883)

CentOS 3 / 4 / 5 : quagga (CESA-2007:0389)

CentOS 3 / 4 / 5 : samba (CESA-2007:0354)

CentOS 3 / 4 / 5 : samba (CESA-2007:1114)

CentOS 3 / 4 / 5 : samba (CESA-2010:0697)

CentOS 3 / 4 / 5 : samba / samba3x (CESA-2010:0488)

CentOS 3 / 4 / 5 : squid (CESA-2007:1130)

CentOS 3 / 4 / 5 : squid (CESA-2008:0214)

CentOS 3 / 4 / 5 : squirrelmail (CESA-2007:0358)

CentOS 3 / 4 / 5 : squirrelmail (CESA-2009:0010)

CentOS 3 / 4 / 5 : squirrelmail (CESA-2009:0057)

CentOS 3 / 4 / 5 : star (CESA-2007:0873)

CentOS 3 / 4 / 5 : tetex (CESA-2007:0731)

CentOS 3 / 4 / 5 : vixie-cron (CESA-2007:0345)

CentOS 3 / 4 / 5 : wget (CESA-2009:1549)

CentOS 3 / 4 / 5 : wireshark (CESA-2008:0890)

CentOS 3 / 4 / 5 : wireshark (CESA-2010:0360)

CentOS 3 / 4 / 5 : xterm (CESA-2009:0018)

CentOS 3 / 4 : 4Suite (CESA-2009:1572)

CentOS 3 / 4 : bind (CESA-2007:0044)

CentOS 3 / 4 : bzip2 (CESA-2005:474)

CentOS 3 / 4 : cpio (CESA-2005:378)

CentOS 3 / 4 : cups (CESA-2005:706)

CentOS 3 / 4 : cups (CESA-2005:878)

CentOS 3 / 4 : cups (CESA-2006:0163)

CentOS 3 / 4 : cups (CESA-2008:0153)

CentOS 3 / 4 : cups (CESA-2008:0206)

CentOS 3 / 4 : cups (CESA-2009:0308)

CentOS 3 / 4 : cups (CESA-2009:1083)

CentOS 3 / 4 : curl (CESA-2005:340)

CentOS 3 / 4 : curl (CESA-2005:807)

CentOS 3 / 4 : curl (CESA-2009:0341)

CentOS 3 / 4 : curl (CESA-2010:0329)

CentOS 3 / 4 : cvs (CESA-2005:387)

CentOS 3 / 4 : cvs (CESA-2005:756)

CentOS 3 / 4 : enscript (CESA-2008:1021)

CentOS 3 / 4 : ethereal (CESA-2005:427)

CentOS 3 / 4 : ethereal (CESA-2005:687)

CentOS 3 / 4 : ethereal (CESA-2005:809)

CentOS 3 / 4 : ethereal (CESA-2006:0156)

CentOS 3 / 4 : ethereal (CESA-2006:0420)

CentOS 3 / 4 : Evolution (CESA-2005:267)

CentOS 3 / 4 : evolution (CESA-2007:0353)

CentOS 3 / 4 : evolution (CESA-2007:0509)

CentOS 3 / 4 : evolution (CESA-2008:0516)

CentOS 3 / 4 : fetchmail (CESA-2005:640)

CentOS 3 / 4 : fetchmail (CESA-2007:0018)

CentOS 3 / 4 : firefox / seamonkey (CESA-2008:0223)

CentOS 3 / 4 : freeradius (CESA-2005:524)

CentOS 3 / 4 : freeradius (CESA-2006:0271)

CentOS 3 / 4 : freetype (CESA-2006:0500)

CentOS 3 / 4 : freetype (CESA-2007:0403)

CentOS 3 / 4 : freetype (CESA-2009:0329)

CentOS 3 / 4 : gaim (CESA-2005:365)

CentOS 3 / 4 : gaim (CESA-2005:429)

CentOS 3 / 4 : gaim (CESA-2005:518)

CentOS 3 / 4 : gaim (CESA-2005:627)

CentOS 3 / 4 : gdk-pixbuf (CESA-2005:343)

CentOS 3 / 4 : gdk-pixbuf (CESA-2005:810)

CentOS 3 / 4 : gedit (CESA-2005:499)

CentOS 3 / 4 : gftp (CESA-2005:410)

CentOS 3 / 4 : ghostscript (CESA-2009:0345)

CentOS 3 / 4 : ghostscript (CESA-2009:0420)

CentOS 3 / 4 : gnome-vfs2 (CESA-2009:0005)

CentOS 3 / 4 : gnomemeeting (CESA-2007:0086)

CentOS 3 / 4 : gnu / gnupg (CESA-2006:0266)

CentOS 3 / 4 : gnupg (CESA-2006:0571)

CentOS 3 / 4 : gnupg (CESA-2006:0615)

CentOS 3 / 4 : gnupg (CESA-2006:0754)

CentOS 3 / 4 : gnupg (CESA-2007:0106)

CentOS 3 / 4 : gtk2 (CESA-2005:344)

CentOS 3 / 4 : gtk2 (CESA-2005:811)

CentOS 3 / 4 : gzip (CESA-2005:357)

CentOS 3 / 4 : gzip (CESA-2006:0667)

CentOS 3 / 4 : httpd (CESA-2005:582)

CentOS 3 / 4 : httpd (CESA-2005:608)

CentOS 3 / 4 : httpd (CESA-2006:0159)

CentOS 3 / 4 : httpd (CESA-2006:0619)

CentOS 3 / 4 : httpd (CESA-2007:0662)

CentOS 3 / 4 : ImageMagick (CESA-2005:413)

CentOS 3 / 4 : ImageMagick (CESA-2005:480)

CentOS 3 / 4 : ImageMagick (CESA-2006:0178)

CentOS 3 / 4 : ImageMagick (CESA-2006:0633)

CentOS 3 / 4 : ImageMagick (CESA-2007:0015)

CentOS 3 / 4 : ipsec-tools (CESA-2006:0267)

CentOS 3 / 4 : kdelibs (CESA-2005:307)

CentOS 3 / 4 : kdelibs (CESA-2006:0720)

CentOS 3 / 4 : kernel (CESA-2005:366)

CentOS 3 / 4 : krb5 (CESA-2007:0095)

CentOS 3 / 4 : libgsf (CESA-2007:0011)

CentOS 3 / 4 : libtiff (CESA-2006:0425)

CentOS 3 / 4 : libtiff (CESA-2006:0603)

CentOS 3 / 4 : libungif (CESA-2005:828)

CentOS 3 / 4 : lynx (CESA-2005:803)

CentOS 3 / 4 : lynx (CESA-2005:839)

CentOS 3 / 4 : mailman (CESA-2006:0204)

CentOS 3 / 4 : mailman (CESA-2006:0486)

CentOS 3 / 4 : mailman (CESA-2006:0600)

CentOS 3 / 4 : mikmod (CESA-2005:506)

CentOS 3 / 4 : mod\_auth\_pgsql (CESA-2006:0164)

CentOS 3 / 4 : mozilla (CESA-2005:435)

CentOS 3 / 4 : mozilla (CESA-2005:587)

CentOS 3 / 4 : mozilla (CESA-2005:769)

CentOS 3 / 4 : Mozilla (CESA-2005:789)

CentOS 3 / 4 : mozilla (CESA-2006:0199)

CentOS 3 / 4 : mozilla (CESA-2006:0329)

CentOS 3 / 4 : mutt (CESA-2006:0577)

CentOS 3 / 4 : nasm (CESA-2005:381)

CentOS 3 / 4 : ncompress (CESA-2006:0663)

CentOS 3 / 4 : net-snmp (CESA-2007:1045)

CentOS 3 / 4 : netpbm (CESA-2005:743)

CentOS 3 / 4 : netpbm (CESA-2008:0131)

CentOS 3 / 4 : openmotif (CESA-2005:412)

CentOS 3 / 4 : openmotif (CESA-2006:0272)

CentOS 3 / 4 : OpenOffice.org (CESA-2005:375)

CentOS 3 / 4 : openoffice.org (CESA-2006:0573)

CentOS 3 / 4 : openoffice.org (CESA-2007:0001)

CentOS 3 / 4 : openoffice.org (CESA-2007:0033)

CentOS 3 / 4 : openoffice.org (CESA-2008:0176)

CentOS 3 / 4 : openoffice.org (CESA-2008:0538)

CentOS 3 / 4 : openoffice.org (CESA-2009:1426)

CentOS 3 / 4 : openoffice.org (CESA-2010:0643)

CentOS 3 / 4 : openssh (CESA-2006:0738)

CentOS 3 / 4 : openssh / openssl (CESA-2006:0697)

CentOS 3 / 4 : openssl (CESA-2005:476)

CentOS 3 / 4 : openssl (CESA-2005:800)

CentOS 3 / 4 : openssl (CESA-2006:0661)

CentOS 3 / 4 : openssl (CESA-2006:0695)

CentOS 3 / 4 : openssl (CESA-2010:0163)

CentOS 3 / 4 : openssl096b (CESA-2005:830)

CentOS 3 / 4 : openssl096b (CESA-2010:0173)

CentOS 3 / 4 : pcre (CESA-2005:761)

CentOS 3 / 4 : php (CESA-2005:564)

CentOS 3 / 4 : php (CESA-2005:748)

CentOS 3 / 4 : php (CESA-2005:831)

CentOS 3 / 4 : php (CESA-2006:0276)

CentOS 3 / 4 : php (CESA-2006:0568)

CentOS 3 / 4 : php (CESA-2006:0669)

CentOS 3 / 4 : php (CESA-2006:0730)

CentOS 3 / 4 : php (CESA-2007:0076)

CentOS 3 / 4 : php (CESA-2007:0155)

CentOS 3 / 4 : php (CESA-2009:0337)

CentOS 3 / 4 : postgresql (CESA-2005:433)

CentOS 3 / 4 : postgresql (CESA-2006:0526)

CentOS 3 / 4 : postgresql (CESA-2007:0064)

CentOS 3 / 4 : python (CESA-2006:0197)

CentOS 3 / 4 : python (CESA-2006:0713)

CentOS 3 / 4 : python (CESA-2007:1076)

CentOS 3 / 4 : qt (CESA-2006:0725)

CentOS 3 / 4 : quagga (CESA-2006:0525)

CentOS 3 / 4 : ruby (CESA-2005:799)

CentOS 3 / 4 : ruby (CESA-2006:0604)

CentOS 3 / 4 : ruby (CESA-2006:0729)

CentOS 3 / 4 : samba (CESA-2006:0591)

CentOS 3 / 4 : samba (CESA-2007:0060)

CentOS 3 / 4 : samba (CESA-2008:0288)

CentOS 3 / 4 : seamonkey (CESA-2006:0676)

CentOS 3 / 4 : seamonkey (CESA-2006:0734)

CentOS 3 / 4 : seamonkey (CESA-2006:0759)

CentOS 3 / 4 : seamonkey (CESA-2007:0077)

CentOS 3 / 4 : seamonkey (CESA-2007:0402)

CentOS 3 / 4 : seamonkey (CESA-2007:0722)

CentOS 3 / 4 : seamonkey (CESA-2007:0980)

CentOS 3 / 4 : seamonkey (CESA-2007:1084)

CentOS 3 / 4 : seamonkey (CESA-2008:0104)

CentOS 3 / 4 : seamonkey (CESA-2008:0208)

CentOS 3 / 4 : seamonkey (CESA-2008:0547)

CentOS 3 / 4 : seamonkey (CESA-2008:0599)

CentOS 3 / 4 : seamonkey (CESA-2008:0882)

CentOS 3 / 4 : seamonkey (CESA-2008:0977)

CentOS 3 / 4 : seamonkey (CESA-2008:1037)

CentOS 3 / 4 : seamonkey (CESA-2009:0257)

CentOS 3 / 4 : seamonkey (CESA-2009:0325)

CentOS 3 / 4 : seamonkey (CESA-2009:0437)

CentOS 3 / 4 : seamonkey (CESA-2009:1531)

CentOS 3 / 4 : seamonkey (CESA-2010:0113)

CentOS 3 / 4 : seamonkey (CESA-2010:0333)

CentOS 3 / 4 : seamonkey (CESA-2010:0499)

CentOS 3 / 4 : seamonkey (CESA-2010:0557)

CentOS 3 / 4 : seamonkey (CESA-2010:0680)

CentOS 3 / 4 : seamonkey (CESA-2010:0781)

CentOS 3 / 4 : seamonkey (CESA-2010:0810)

CentOS 3 / 4 : sendmail (CESA-2006:0264)

CentOS 3 / 4 : sendmail (CESA-2006:0515)

CentOS 3 / 4 : sharutils (CESA-2005:377)

CentOS 3 / 4 : squid (CESA-2005:415)

CentOS 3 / 4 : squid (CESA-2005:766)

CentOS 3 / 4 : SquirrelMail (CESA-2005:595)

CentOS 3 / 4 : SquirrelMail (CESA-2005:595-02)

CentOS 3 / 4 : squirrelmail (CESA-2006:0283)

CentOS 3 / 4 : squirrelmail (CESA-2006:0547)

CentOS 3 / 4 : squirrelmail (CESA-2006:0668)

CentOS 3 / 4 : squirrelmail (CESA-2007:0022)

CentOS 3 / 4 : squirrelmail (CESA-2009:1490)

CentOS 3 / 4 : sudo (CESA-2005:535)

CentOS 3 / 4 : sysreport (CESA-2005:502)

CentOS 3 / 4 : sysreport (CESA-2005:598)

CentOS 3 / 4 : tar (CESA-2006:0749)

CentOS 3 / 4 : tcpdump (CESA-2005:417)

CentOS 3 / 4 : telnet (CESA-2005:504)

CentOS 3 / 4 : tetex (CESA-2006:0160)

CentOS 3 / 4 : texinfo (CESA-2006:0727)

CentOS 3 / 4 : texinfo (CESA-2006:0727-1)

CentOS 3 / 4 : util-linux (CESA-2007:0969)

CentOS 3 / 4 : util-linux / mount (CESA-2005:782)

CentOS 3 / 4 : vim (CESA-2005:745)

CentOS 3 / 4 : vim (CESA-2008:0617)

CentOS 3 / 4 : vnc (CESA-2009:0261)

CentOS 3 / 4 : wget (CESA-2005:771)

CentOS 3 / 4 : wget (CESA-2005:812)

CentOS 3 / 4 : wireshark (CESA-2006:0602)

CentOS 3 / 4 : wireshark (CESA-2006:0658)

CentOS 3 / 4 : wireshark (CESA-2006:0726)

CentOS 3 / 4 : wireshark (CESA-2007:0066)

CentOS 3 / 4 : wireshark (CESA-2009:0313)

CentOS 3 / 4 : xloadimage (CESA-2005:332)

CentOS 3 / 4 : xloadimage (CESA-2005:802)

CentOS 3 / 4 : xpdf (CESA-2005:840)

CentOS 3 / 4 : xpdf (CESA-2007:0735)

CentOS 3 / 4 : xpdf (CESA-2009:0430)

CentOS 3 / 5 : curl (CESA-2009:1209)

CentOS 3 / 5 : httpd (CESA-2009:1579)

CentOS 3 / 5 : libtiff (CESA-2009:1159)

CentOS 3 / 5 : libvorbis (CESA-2009:1219)

CentOS 3 / 5 : libxml / libxml2 (CESA-2009:1206)

CentOS 3 / 5 : openoffice.org (CESA-2008:0939)

CentOS 3 / 5 : perl-Net-DNS (CESA-2007:0674)

CentOS 3 / 5 : php (CESA-2008:0544)

CentOS 3 / 5 : pidgin (CESA-2009:1218)

CentOS 3 / 5 : squirrelmail (CESA-2009:1066)

CentOS 3 / 5 : wireshark (CESA-2009:1100)

CentOS 3 : bind (CESA-2009:1181)

CentOS 3 : binutils (CESA-2005:659)

CentOS 3 : cpio (CESA-2010:0145)

CentOS 3 : cscope (CESA-2009:1101)

CentOS 3 : cups (CESA-2005:571)

CentOS 3 : cups (CESA-2007:1023)

CentOS 3 : cups (CESA-2008:1028)

CentOS 3 : cups (CESA-2009:0428)

CentOS 3 : cups (CESA-2010:0754)

CentOS 3 : cyrus-sasl (CESA-2007:0878)

CentOS 3 : dhcp (CESA-2009:1154)

CentOS 3 : elfutils (CESA-2006:0368)

CentOS 3 : evolution (CESA-2005:238)

CentOS 3 : evolution (CESA-2009:0358)

CentOS 3 : freetype (CESA-2010:0577)

CentOS 3 : freetype (CESA-2010:0736)

CentOS 3 : gcc (CESA-2007:0473)

CentOS 3 : gd (CESA-2004:638)

CentOS 3 : gdb (CESA-2007:0469)

CentOS 3 : ghostscript (CESA-2005:081)

CentOS 3 : glibc (CESA-2005:256)

CentOS 3 : gstreamer-plugins (CESA-2009:0269)

CentOS 3 : httpd (CESA-2007:0533)

CentOS 3 : httpd (CESA-2008:0005)

CentOS 3 : httpd (CESA-2009:1108)

CentOS 3 : httpd (CESA-2009:1205)

CentOS 3 : imap (CESA-2005:850)

CentOS 3 : imap (CESA-2009:0275)

CentOS 3 : initscripts (CESA-2006:0015)

CentOS 3 : kdebase (CESA-2006:0576)

CentOS 3 : kdegraphics (CESA-2005:021)

CentOS 3 : kdegraphics (CESA-2006:0648)

CentOS 3 : kdelibs (CESA-2009:1128)

CentOS 3 : kernel (CESA-2005:293)

CentOS 3 : kernel (CESA-2005:294)

CentOS 3 : kernel (CESA-2005:472)

CentOS 3 : kernel (CESA-2005:663)

CentOS 3 : kernel (CESA-2006:0140)

CentOS 3 : kernel (CESA-2006:0144)

CentOS 3 : kernel (CESA-2006:0437)

CentOS 3 : kernel (CESA-2006:0710)

CentOS 3 : kernel (CESA-2007:0436)

CentOS 3 : kernel (CESA-2007:0671)

CentOS 3 : kernel (CESA-2007:0938)

CentOS 3 : kernel (CESA-2007:1049)

CentOS 3 : kernel (CESA-2008:0211)

CentOS 3 : kernel (CESA-2008:0973)

CentOS 3 : kernel (CESA-2009:1233)

CentOS 3 : kernel (CESA-2009:1550)

CentOS 3 : krb5 (CESA-2005:330)

CentOS 3 : krb5 (CESA-2005:562)

CentOS 3 : krb5 (CESA-2007:0384)

CentOS 3 : krb5 (CESA-2008:0181)

CentOS 3 : krb5 (CESA-2009:0410)

CentOS 3 : libpng (CESA-2009:0340)

CentOS 3 : libtiff (CESA-2008:0863)

CentOS 3 : libtiff (CESA-2010:0520)

CentOS 3 : libxml (CESA-2004:650)

CentOS 3 : mozilla (CESA-2005:384)

CentOS 3 : mysql-server (CESA-2005:348)

CentOS 3 : net-snmp (CESA-2005:373)

CentOS 3 : net-snmp (CESA-2009:0295)

CentOS 3 : net-snmp (CESA-2009:1124)

CentOS 3 : netpbm (CESA-2005:843)

CentOS 3 : ntp (CESA-2009:1651)

CentOS 3 : openldap (CESA-2007:0430)

CentOS 3 : openldap / nss\_ldap (CESA-2005:751)

CentOS 3 : openssh (CESA-2005:106)

CentOS 3 : openssh (CESA-2005:550)

CentOS 3 : openssh (CESA-2006:0298)

CentOS 3 : openssl (CESA-2007:0813)

CentOS 3 : pam (CESA-2007:0465)

CentOS 3 : pcre (CESA-2007:1063)

CentOS 3 : perl (CESA-2005:881)

CentOS 3 : PHP (CESA-2005:405)

CentOS 3 : php (CESA-2007:0889)

CentOS 3 : pidgin (CESA-2009:1059)

CentOS 3 : pidgin (CESA-2009:1535)

CentOS 3 : postgresql (CESA-2008:0039)

CentOS 3 : postgresql (CESA-2009:1485)

CentOS 3 : postgresql (CESA-2010:0427)

CentOS 3 : python (CESA-2009:1178)

CentOS 3 : rdesktop (CESA-2008:0576)

CentOS 3 : rsh (CESA-2005:074)

CentOS 3 : ruby (CESA-2008:0562)

CentOS 3 : ruby (CESA-2008:0896)

CentOS 3 : samba (CESA-2007:1013)

CentOS 3 : samba (CESA-2009:1528)

CentOS 3 : seamonkey (CESA-2006:0608)

CentOS 3 : seamonkey (CESA-2009:0398)

CentOS 3 : seamonkey (CESA-2009:1096)

CentOS 3 : seamonkey (CESA-2009:1134)

CentOS 3 : seamonkey (CESA-2009:1163)

CentOS 3 : seamonkey (CESA-2009:1185)

CentOS 3 : seamonkey (CESA-2009:1432)

CentOS 3 : seamonkey (CESA-2010:0546)

CentOS 3 : shadow-utils (CESA-2007:0431)

CentOS 3 : slocate (CESA-2005:345)

CentOS 3 : squid (CESA-2006:0045)

CentOS 3 : tar (CESA-2006:0195)

CentOS 3 : tar (CESA-2010:0142)

CentOS 3 : tcltk (CESA-2008:0134)

CentOS 3 : tcpdump (CESA-2005:421)

CentOS 3 : tetex (CESA-2005:354)

CentOS 3 : tetex (CESA-2007:1028)

CentOS 3 : tetex (CESA-2010:0401)

CentOS 3 : unzip (CESA-2008:0196)

CentOS 3 : vixie-cron (CESA-2006:0117)

CentOS 3 : vsftpd (CESA-2008:0579)

CentOS 3 : wireshark (CESA-2008:0059)

CentOS 3 : XFree86 (CESA-2005:331)

CentOS 3 : XFree86 (CESA-2005:501)

CentOS 3 : XFree86 (CESA-2005:787)

CentOS 3 : XFree86 (CESA-2006:0635)

CentOS 3 : XFree86 (CESA-2006:0666)

CentOS 3 : XFree86 (CESA-2007:0002)

CentOS 3 : XFree86 (CESA-2007:0125)

CentOS 3 : XFree86 (CESA-2008:0029)

CentOS 3 : XFree86 (CESA-2008:0502)

CentOS 3 : xloadimage (CESA-2005:332-01)

CentOS 3 : xpdf (CESA-2007:1030)

CentOS 3 : xpdf (CESA-2009:1500)

CentOS 3 : xpdf (CESA-2010:0750)

CentOS 3 : xscreensaver (CESA-2006:0498)

CentOS 3 : xscreensaver (CESA-2007:0322)

CentOS 4 / 5 / 6 : firefox (CESA-2012:0079)

CentOS 4 / 5 / 6 : libpng / libpng10 (CESA-2012:0317)

CentOS 4 / 5 / 6 : libvorbis (CESA-2012:0136)

CentOS 4 / 5 / 6 : php (CESA-2012:0093)

CentOS 4 / 5 : apr (CESA-2011:0507)

CentOS 4 / 5 : apr (CESA-2011:0844)

CentOS 4 / 5 : bluez-libs / bluez-utils (CESA-2008:0581)

CentOS 4 / 5 : cups (CESA-2009:0429)

CentOS 4 / 5 : curl (CESA-2011:0918)

CentOS 4 / 5 : cyrus-imapd (CESA-2009:1459)

CentOS 4 / 5 : cyrus-imapd (CESA-2011:0859)

CentOS 4 / 5 : cyrus-imapd (CESA-2011:1317)

CentOS 4 / 5 : cyrus-imapd (CESA-2011:1508)

CentOS 4 / 5 : devhelp / firefox / yelp (CESA-2007:0400)

CentOS 4 / 5 : device-mapper-multipath (CESA-2009:0411)

CentOS 4 / 5 : dhcp (CESA-2011:0428)

CentOS 4 / 5 : dhcp (CESA-2011:1160)

CentOS 4 / 5 : dovecot (CESA-2011:1187)

CentOS 4 / 5 : elinks (CESA-2007:0933)

CentOS 4 / 5 : elinks (CESA-2009:1471)

CentOS 4 / 5 : evolution (CESA-2008:0177)

CentOS 4 / 5 : exim (CESA-2011:0153)

CentOS 4 / 5 : file (CESA-2007:0391)

CentOS 4 / 5 : firefox (CESA-2007:0724)

CentOS 4 / 5 : firefox (CESA-2007:0979)

CentOS 4 / 5 : firefox (CESA-2008:0103)

CentOS 4 / 5 : firefox (CESA-2008:0207)

CentOS 4 / 5 : firefox (CESA-2008:0222)

CentOS 4 / 5 : firefox (CESA-2008:0879)

CentOS 4 / 5 : firefox (CESA-2008:0978)

CentOS 4 / 5 : firefox (CESA-2008:1036)

CentOS 4 / 5 : firefox (CESA-2009:0256)

CentOS 4 / 5 : firefox (CESA-2009:0315)

CentOS 4 / 5 : firefox (CESA-2009:0397)

CentOS 4 / 5 : firefox (CESA-2009:0436)

CentOS 4 / 5 : firefox (CESA-2009:0449)

CentOS 4 / 5 : firefox (CESA-2009:1674)

CentOS 4 / 5 : firefox (CESA-2010:0112)

CentOS 4 / 5 : firefox (CESA-2010:0547)

CentOS 4 / 5 : firefox (CESA-2010:0681)

CentOS 4 / 5 : firefox (CESA-2010:0782)

CentOS 4 / 5 : firefox (CESA-2011:0471)

CentOS 4 / 5 : firefox (CESA-2011:0885)

CentOS 4 / 5 : firefox (CESA-2011:1341)

CentOS 4 / 5 : firefox (CESA-2011:1437)

CentOS 4 / 5 : firefox / seamonkey (CESA-2009:1430)

CentOS 4 / 5 : firefox / xulrunner (CESA-2011:0373)

CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)

CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1242)

CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1268)

CentOS 4 / 5 : flac (CESA-2007:0975)

CentOS 4 / 5 : foomatic (CESA-2011:1109)

CentOS 4 / 5 : freetype (CESA-2010:0578)

CentOS 4 / 5 : freetype (CESA-2010:0737)

CentOS 4 / 5 : freetype (CESA-2010:0889)

CentOS 4 / 5 : freetype (CESA-2011:1402)

CentOS 4 / 5 : freetype (CESA-2011:1455)

CentOS 4 / 5 : gd (CESA-2008:0146)

CentOS 4 / 5 : gd (CESA-2010:0003)

CentOS 4 / 5 : gnutls (CESA-2009:1232)

CentOS 4 / 5 : htdig (CESA-2007:1095)

CentOS 4 / 5 : httpd (CESA-2011:1392)

CentOS 4 / 5 : kdebase (CESA-2007:0905)

CentOS 4 / 5 : kdebase (CESA-2010:0348)

CentOS 4 / 5 : kdegraphics (CESA-2007:0729)

CentOS 4 / 5 : kdegraphics (CESA-2009:0431)

CentOS 4 / 5 : kdegraphics (CESA-2010:0753)

CentOS 4 / 5 : kdelibs (CESA-2007:0909)

CentOS 4 / 5 : kdelibs (CESA-2009:1601)

CentOS 4 / 5 : kdelibs (CESA-2011:1385)

CentOS 4 / 5 : kernel (CESA-2008:0154)

CentOS 4 / 5 : krb5 (CESA-2007:0562)

CentOS 4 / 5 : krb5 (CESA-2010:0926)

CentOS 4 / 5 : krb5 (CESA-2011:1851)

CentOS 4 / 5 : libexif (CESA-2007:0501)

CentOS 4 / 5 : libtiff (CESA-2010:0519)

CentOS 4 / 5 : libtiff (CESA-2011:0318)

CentOS 4 / 5 : libtiff (CESA-2011:0392)

CentOS 4 / 5 : libuser (CESA-2011:0170)

CentOS 4 / 5 : libwmf (CESA-2009:0457)

CentOS 4 / 5 : libxslt (CESA-2008:0649)

CentOS 4 / 5 : mailman (CESA-2011:0307)

CentOS 4 / 5 : mysql (CESA-2007:0875)

CentOS 4 / 5 : mysql (CESA-2007:1155)

CentOS 4 / 5 : neon (CESA-2009:1452)

CentOS 4 / 5 : netpbm (CESA-2011:1811)

CentOS 4 / 5 : nspr / nss (CESA-2011:1282)

CentOS 4 / 5 : nss (CESA-2010:0165)

CentOS 4 / 5 : nss (CESA-2011:0472)

CentOS 4 / 5 : nss (CESA-2011:1444)

CentOS 4 / 5 : ntp (CESA-2009:0046)

CentOS 4 / 5 : ntp (CESA-2009:1648)

CentOS 4 / 5 : openldap (CESA-2008:0110)

CentOS 4 / 5 : openldap (CESA-2008:0583)

CentOS 4 / 5 : openoffice.org / openoffice.org2 (CESA-2008:0175)

CentOS 4 / 5 : openssh (CESA-2008:0855)

CentOS 4 / 5 : perl (CESA-2011:1797)

CentOS 4 / 5 : perl-Archive-Tar (CESA-2010:0505)

CentOS 4 / 5 : php (CESA-2007:0890)

CentOS 4 / 5 : php (CESA-2010:0919)

CentOS 4 / 5 : pidgin (CESA-2008:1023)

CentOS 4 / 5 : pidgin (CESA-2009:1060)

CentOS 4 / 5 : pidgin (CESA-2009:1453)

CentOS 4 / 5 : pidgin (CESA-2009:1536)

CentOS 4 / 5 : pidgin (CESA-2010:0044)

CentOS 4 / 5 : pidgin (CESA-2010:0115)

CentOS 4 / 5 : pidgin (CESA-2010:0788)

CentOS 4 / 5 : pidgin (CESA-2011:1371)

CentOS 4 / 5 : pidgin (CESA-2011:1820)

CentOS 4 / 5 : postfix (CESA-2011:0422)

CentOS 4 / 5 : postfix (CESA-2011:0843)

CentOS 4 / 5 : postgresql (CESA-2008:0038)

CentOS 4 / 5 : postgresql (CESA-2009:1484)

CentOS 4 / 5 : postgresql (CESA-2011:0197)

CentOS 4 / 5 : postgresql (CESA-2011:1377)

CentOS 4 / 5 : postgresql / postgresql84 (CESA-2010:0742)

CentOS 4 / 5 : PyXML (CESA-2010:0002)

CentOS 4 / 5 : quagga (CESA-2010:0785)

CentOS 4 / 5 : rpm (CESA-2011:1349)

CentOS 4 / 5 : ruby (CESA-2008:0561)

CentOS 4 / 5 : ruby (CESA-2008:0897)

CentOS 4 / 5 : ruby (CESA-2008:0981)

CentOS 4 / 5 : ruby (CESA-2012:0070)

CentOS 4 / 5 : samba (CESA-2009:1529)

CentOS 4 / 5 : samba (CESA-2011:0305)

CentOS 4 / 5 : samba (CESA-2011:1219)

CentOS 4 / 5 : spamassassin (CESA-2007:0492)

CentOS 4 / 5 : speex (CESA-2008:0235)

CentOS 4 / 5 : squirrelmail (CESA-2012:0103)

CentOS 4 / 5 : system-config-printer (CESA-2011:1196)

CentOS 4 / 5 : systemtap (CESA-2009:0373)

CentOS 4 / 5 : tar (CESA-2007:0860)

CentOS 4 / 5 : tar (CESA-2010:0141)

CentOS 4 / 5 : thunderbird (CESA-2007:0401)

CentOS 4 / 5 : thunderbird (CESA-2007:0723)

CentOS 4 / 5 : thunderbird (CESA-2007:0981)

CentOS 4 / 5 : thunderbird (CESA-2007:1083)

CentOS 4 / 5 : thunderbird (CESA-2008:0105)

CentOS 4 / 5 : thunderbird (CESA-2008:0209)

CentOS 4 / 5 : thunderbird (CESA-2008:0224)

CentOS 4 / 5 : thunderbird (CESA-2008:0616)

CentOS 4 / 5 : thunderbird (CESA-2008:0908)

CentOS 4 / 5 : thunderbird (CESA-2008:0976)

CentOS 4 / 5 : thunderbird (CESA-2009:0002)

CentOS 4 / 5 : thunderbird (CESA-2009:0258)

CentOS 4 / 5 : thunderbird (CESA-2010:0682)

CentOS 4 / 5 : thunderbird (CESA-2010:0780)

CentOS 4 / 5 : thunderbird (CESA-2010:0812)

CentOS 4 / 5 : thunderbird (CESA-2011:0474)

CentOS 4 / 5 : thunderbird (CESA-2011:0887)

CentOS 4 / 5 : thunderbird (CESA-2011:1165)

CentOS 4 / 5 : thunderbird (CESA-2011:1243)

CentOS 4 / 5 : thunderbird (CESA-2011:1267)

CentOS 4 / 5 : thunderbird (CESA-2011:1343)

CentOS 4 / 5 : thunderbird (CESA-2011:1438)

CentOS 4 / 5 : thunderbird (CESA-2012:0085)

CentOS 4 / 5 : tog-pegasus (CESA-2008:0002)

CentOS 4 / 5 : vsftpd (CESA-2011:0337)

CentOS 4 / 5 : wireshark (CESA-2008:0058)

CentOS 4 / 5 : wireshark (CESA-2010:0625)

CentOS 4 / 5 : wireshark (CESA-2011:0370)

CentOS 4 / 5 : xmlsec1 (CESA-2009:1428)

CentOS 4 / 5 : xmlsec1 (CESA-2011:0486)

CentOS 4 : apache (CESA-2006:0618)

CentOS 4 : apr-util (CESA-2010:0950)

CentOS 4 : autofs5 (CESA-2007:1129)

CentOS 4 : autofs5 (CESA-2007:1177)

CentOS 4 : bind (CESA-2009:1180)

CentOS 4 : bind (CESA-2010:1000)

CentOS 4 : bind (CESA-2011:1496)

CentOS 4 : binutils (CESA-2005:673)

CentOS 4 : bluez-utils (CESA-2007:0065)

CentOS 4 : busybox (CESA-2007:0244)

CentOS 4 : cpio (CESA-2007:0245)

CentOS 4 : cpio (CESA-2010:0143)

CentOS 4 : cups (CESA-2005:772)

CentOS 4 : cups (CESA-2007:1022)

CentOS 4 : cups (CESA-2008:0161)

CentOS 4 : cups (CESA-2010:0755)

CentOS 4 : curl (CESA-2005:875)

CentOS 4 : cyrus-imapd (CESA-2005:408)

CentOS 4 : cyrus-sasl (CESA-2007:0795)

CentOS 4 : dbus (CESA-2005:102)

CentOS 4 : dbus (CESA-2007:0008)

CentOS 4 : dia (CESA-2006:0280)

CentOS 4 : dia (CESA-2006:0541)

CentOS 4 : elfutils (CESA-2006:0354)

CentOS 4 : elinks (CESA-2006:0742)

CentOS 4 : Evolution (CESA-2005:397)

CentOS 4 : evolution / evolution-data-server (CESA-2009:0355)

CentOS 4 : evolution-data-server (CESA-2009:0354)

CentOS 4 : evolution28 (CESA-2008:0515)

CentOS 4 : evolution28-pango (CESA-2011:1325)

CentOS 4 : exim (CESA-2005:358)

CentOS 4 : exim (CESA-2010:0970)

CentOS 4 : file (CESA-2007:0124)

CentOS 4 : Firefox (CESA-2005:383)

CentOS 4 : firefox (CESA-2005:434)

CentOS 4 : firefox (CESA-2005:586)

CentOS 4 : firefox (CESA-2005:768)

CentOS 4 : firefox (CESA-2005:785)

CentOS 4 : firefox (CESA-2006:0200)

CentOS 4 : firefox (CESA-2006:0328)

CentOS 4 : Firefox (CESA-2006:0610)

CentOS 4 : firefox (CESA-2006:0675)

CentOS 4 : firefox (CESA-2006:0733)

CentOS 4 : Firefox (CESA-2006:0758)

CentOS 4 : firefox (CESA-2007:0079)

CentOS 4 : firefox (CESA-2007:1082)

CentOS 4 : firefox (CESA-2008:0549)

CentOS 4 : firefox (CESA-2008:0598)

CentOS 4 : firefox (CESA-2009:1530)

CentOS 4 : firefox (CESA-2010:0332)

CentOS 4 : firefox (CESA-2010:0500)

CentOS 4 : firefox (CESA-2010:0558)

CentOS 4 : firefox (CESA-2010:0808)

CentOS 4 : firefox (CESA-2010:0966)

CentOS 4 : firefox (CESA-2011:0310)

CentOS 4 : firefox (CESA-2012:0142)

CentOS 4 : freetype (CESA-2011:1161)

CentOS 4 : frysk (CESA-2011:1327)

CentOS 4 : gcc (CESA-2007:0220)

CentOS 4 : gd (CESA-2006:0194)

CentOS 4 : gdb (CESA-2005:709)

CentOS 4 : gdb (CESA-2007:0229)

CentOS 4 : gdm (CESA-2010:0657)

CentOS 4 : gdm / openldap (CESA-2007:0310)

CentOS 4 : ghostscript (CESA-2012:0096)

CentOS 4 : gimp (CESA-2006:0598)

CentOS 4 : gimp (CESA-2011:0837)

CentOS 4 : glibc (CESA-2012:0125)

CentOS 4 : gnutls (CESA-2005:430)

CentOS 4 : gnutls (CESA-2006:0207)

CentOS 4 : gnutls (CESA-2006:0680)

CentOS 4 : gnutls (CESA-2008:0492)

CentOS 4 : gnutls (CESA-2010:0167)

CentOS 4 : gpdf (CESA-2005:708)

CentOS 4 : gpdf (CESA-2005:867)

CentOS 4 : gpdf (CESA-2006:0177)

CentOS 4 : gpdf (CESA-2007:0730)

CentOS 4 : gpdf (CESA-2007:1025)

CentOS 4 : gpdf (CESA-2008:0262)

CentOS 4 : gpdf (CESA-2009:0458)

CentOS 4 : gpdf (CESA-2009:1503)

CentOS 4 : gpdf (CESA-2009:1681)

CentOS 4 : gpdf (CESA-2010:0752)

CentOS 4 : gstreamer-plugins (CESA-2009:0270)

CentOS 4 : gstreamer-plugins (CESA-2011:0477)

CentOS 4 : gstreamer-plugins (CESA-2011:1264)

CentOS 4 : gtk2 (CESA-2007:0019)

CentOS 4 : Helix / Player (CESA-2005:788)

CentOS 4 : HelixPlayer (CESA-2005:392)

CentOS 4 : HelixPlayer (CESA-2005:517)

CentOS 4 : HelixPlayer (CESA-2007:0605)

CentOS 4 : HelixPlayer (CESA-2010:0094)

CentOS 4 : HelixPlayer removal (CESA-2010:0981)

CentOS 4 : Horde (CESA-2006:0412-001)

CentOS 4 : httpd (CESA-2007:0534)

CentOS 4 : httpd (CESA-2007:0747)

CentOS 4 : httpd (CESA-2008:0006)

CentOS 4 : httpd (CESA-2009:1580)

CentOS 4 : httpd (CESA-2010:0175)

CentOS 4 : httpd (CESA-2011:1245)

CentOS 4 : ImageMagick (CESA-2010:0653)

CentOS 4 : kdebase (CESA-2006:0548)

CentOS 4 : kdebase (CESA-2006:0582)

CentOS 4 : kdegraphics (CESA-2005:671)

CentOS 4 : kdegraphics (CESA-2005:868)

CentOS 4 : kdegraphics (CESA-2006:0206)

CentOS 4 : kdegraphics (CESA-2006:0262)

CentOS 4 : kdegraphics (CESA-2007:1024)

CentOS 4 : kdegraphics (CESA-2008:0238)

CentOS 4 : kdegraphics (CESA-2009:1512)

CentOS 4 : kdegraphics (CESA-2009:1682)

CentOS 4 : kdelibs (CESA-2005:393)

CentOS 4 : kdelibs (CESA-2005:612)

CentOS 4 : kdelibs (CESA-2006:0184)

CentOS 4 : kdenetwork (CESA-2005:639)

CentOS 4 : kernel (CESA-2005:420)

CentOS 4 : kernel (CESA-2005:514)

CentOS 4 : kernel (CESA-2005:808)

CentOS 4 : kernel (CESA-2006:0101)

CentOS 4 : kernel (CESA-2006:0132)

CentOS 4 : kernel (CESA-2006:0493)

CentOS 4 : kernel (CESA-2006:0574)

CentOS 4 : kernel (CESA-2006:0575)

CentOS 4 : kernel (CESA-2006:0617)

CentOS 4 : kernel (CESA-2006:0689)

CentOS 4 : kernel (CESA-2007:0014)

CentOS 4 : kernel (CESA-2007:0085)

CentOS 4 : kernel (CESA-2007:0488)

CentOS 4 : kernel (CESA-2007:0774)

CentOS 4 : kernel (CESA-2007:0937)

CentOS 4 : kernel (CESA-2007:0939)

CentOS 4 : kernel (CESA-2007:1104)

CentOS 4 : kernel (CESA-2008:0055)

CentOS 4 : kernel (CESA-2008:0167)

CentOS 4 : kernel (CESA-2008:0237)

CentOS 4 : kernel (CESA-2008:0508)

CentOS 4 : kernel (CESA-2008:0607)

CentOS 4 : kernel (CESA-2008:0972)

CentOS 4 : kernel (CESA-2009:0014)

CentOS 4 : kernel (CESA-2009:0331)

CentOS 4 : kernel (CESA-2009:0459)

CentOS 4 : kernel (CESA-2009:1223)

CentOS 4 : kernel (CESA-2009:1438)

CentOS 4 : kernel (CESA-2009:1522)

CentOS 4 : kernel (CESA-2009:1541)

CentOS 4 : kernel (CESA-2009:1671)

CentOS 4 : kernel (CESA-2010:0020)

CentOS 4 : kernel (CESA-2010:0076)

CentOS 4 : kernel (CESA-2010:0146)

CentOS 4 : kernel (CESA-2010:0394)

CentOS 4 : kernel (CESA-2010:0474)

CentOS 4 : kernel (CESA-2010:0606)

CentOS 4 : kernel (CESA-2010:0676)

CentOS 4 : kernel (CESA-2010:0718)

CentOS 4 : kernel (CESA-2010:0779)

CentOS 4 : kernel (CESA-2010:0936)

CentOS 4 : kernel (CESA-2011:0162)

CentOS 4 : krb5 (CESA-2005:567)

CentOS 4 : krb5 (CESA-2006:0612)

CentOS 4 : krb5 (CESA-2008:0180)

CentOS 4 : krb5 (CESA-2009:0409)

CentOS 4 : libc-client (CESA-2005:848)

CentOS 4 : libexif (CESA-2007:1166)

CentOS 4 : libgtop2 (CESA-2007:0765)

CentOS 4 : libpng (CESA-2006:0205)

CentOS 4 : libpng (CESA-2009:0333)

CentOS 4 : libpng (CESA-2011:1103)

CentOS 4 : libsoup (CESA-2009:0344)

CentOS 4 : libtiff (CESA-2008:0848)

CentOS 4 : libwmf (CESA-2006:0597)

CentOS 4 : libxml2 (CESA-2012:0016)

CentOS 4 : lm\_sensors (CESA-2005:825)

CentOS 4 : mailman (CESA-2007:0779)

CentOS 4 : mod\_auth\_kerb (CESA-2006:0746)

CentOS 4 : mozilla (CESA-2005:386)

CentOS 4 : mysql (CESA-2005:685)

CentOS 4 : mysql (CESA-2006:0544)

CentOS 4 : mysql (CESA-2007:0152)

CentOS 4 : mysql (CESA-2007:1222-001)

CentOS 4 : mysql (CESA-2010:0110)

CentOS 4 : mysql (CESA-2010:0824)

CentOS 4 : net-snmp (CESA-2005:395)

CentOS 4 : netpbm (CESA-2005:793)

CentOS 4 : netpbm (CESA-2009:0012)

CentOS 4 : NetworkManager (CESA-2009:0362)

CentOS 4 : nfs-utils (CESA-2009:0955)

CentOS 4 : nfs-utils-lib (CESA-2007:0913)

CentOS 4 : nss\_ldap (CESA-2006:0719)

CentOS 4 : ntp (CESA-2006:0393)

CentOS 4 : ntp (CESA-2009:1040)

CentOS 4 : openldap (CESA-2007:1038)

CentOS 4 : openldap (CESA-2010:0543)

CentOS 4 : openldap / nss\_ldap (CESA-2005:767)

CentOS 4 : openoffice.org / openoffice.org2 (CESA-2011:0181)

CentOS 4 : openoffice.org2 (CESA-2008:0537)

CentOS 4 : openssh (CESA-2005:527)

CentOS 4 : openssh (CESA-2006:0044)

CentOS 4 : openssh (CESA-2007:0257)

CentOS 4 : openssh (CESA-2007:0703)

CentOS 4 : openssl (CESA-2007:1003)

CentOS 4 : openssl (CESA-2010:0977)

CentOS 4 : openssl (CESA-2012:0086)

CentOS 4 : pam (CESA-2005:805)

CentOS 4 : pam (CESA-2007:0737)

CentOS 4 : pango (CESA-2011:0180)

CentOS 4 : pcre (CESA-2007:0968)

CentOS 4 : pcre (CESA-2007:1052)

CentOS 4 : pcre (CESA-2007:1068)

CentOS 4 : perl (CESA-2005:674)

CentOS 4 : perl (CESA-2005:880)

CentOS 4 : perl (CESA-2006:0605)

CentOS 4 : perl-Net-DNS (CESA-2007:0675)

CentOS 4 : PHP (CESA-2005:406)

CentOS 4 : php (CESA-2007:0349)

CentOS 4 : php (CESA-2008:0545)

CentOS 4 : php (CESA-2012:0071)

CentOS 4 : postgresql (CESA-2010:0428)

CentOS 4 : python (CESA-2011:0491)

CentOS 4 : rpm (CESA-2010:0678)

CentOS 4 : rsh (CESA-2005:165)

CentOS 4 : ruby (CESA-2005:543)

CentOS 4 : ruby (CESA-2006:0427)

CentOS 4 : ruby (CESA-2007:0961)

CentOS 4 : ruby (CESA-2011:0908)

CentOS 4 : samba (CESA-2007:1016)

CentOS 4 : samba (CESA-2012:0332)

CentOS 4 : sblim (CESA-2008:0497)

CentOS 4 : seamonkey (CESA-2006:0609)

CentOS 4 : seamonkey (CESA-2009:1431)

CentOS 4 : seamonkey (CESA-2009:1673)

CentOS 4 : seamonkey (CESA-2010:0967)

CentOS 4 : seamonkey (CESA-2011:0313)

CentOS 4 : seamonkey (CESA-2011:0375)

CentOS 4 : seamonkey (CESA-2011:0473)

CentOS 4 : seamonkey (CESA-2011:0888)

CentOS 4 : seamonkey (CESA-2011:1167)

CentOS 4 : seamonkey (CESA-2011:1244)

CentOS 4 : seamonkey (CESA-2011:1266)

CentOS 4 : seamonkey (CESA-2011:1344)

CentOS 4 : seamonkey (CESA-2011:1440)

CentOS 4 : seamonkey (CESA-2012:0084)

CentOS 4 : seamonkey (CESA-2012:0141)

CentOS 4 : sendmail (CESA-2007:0252)

CentOS 4 : shadow-utils (CESA-2007:0276)

CentOS 4 : slocate (CESA-2005:346)

CentOS 4 : spamassassin (CESA-2005:498)

CentOS 4 : spamassassin (CESA-2006:0129)

CentOS 4 : spamassassin (CESA-2006:0543)

CentOS 4 : spamassassin (CESA-2007:0074)

CentOS 4 : squid (CESA-2006:0052)

CentOS 4 : subversion (CESA-2011:0861)

CentOS 4 : systemtap (CESA-2010:0125)

CentOS 4 : systemtap (CESA-2010:0895)

CentOS 4 : tar (CESA-2006:0232)

CentOS 4 : tcpdump (CESA-2005:505)

CentOS 4 : tcpdump (CESA-2007:0387)

CentOS 4 : tetex (CESA-2007:1027)

CentOS 4 : tetex (CESA-2010:0399)

CentOS 4 : thunderbird (CESA-2005:601)

CentOS 4 : thunderbird (CESA-2005:791)

CentOS 4 : thunderbird (CESA-2006:0330)

CentOS 4 : thunderbird (CESA-2006:0611)

CentOS 4 : thunderbird (CESA-2006:0677)

CentOS 4 : thunderbird (CESA-2006:0735)

CentOS 4 : Thunderbird (CESA-2006:0760)

CentOS 4 : thunderbird (CESA-2007:0078)

CentOS 4 : thunderbird (CESA-2010:0154)

CentOS 4 : thunderbird (CESA-2010:0544)

CentOS 4 : thunderbird (CESA-2010:0968)

CentOS 4 : thunderbird (CESA-2011:0312)

CentOS 4 : thunderbird (CESA-2011:0374)

CentOS 4 : tk (CESA-2008:0135)

CentOS 4 : udev (CESA-2005:864)

CentOS 4 : unzip (CESA-2007:0203)

CentOS 4 : util-linux (CESA-2007:0235)

CentOS 4 : util-linux (CESA-2009:0981)

CentOS 4 : vixie-cron (CESA-2005:361)

CentOS 4 : vixie-cron (CESA-2006:0539)

CentOS 4 : w3c-libwww (CESA-2007:0208)

CentOS 4 : wireshark (CESA-2007:0709)

CentOS 4 : wireshark (CESA-2011:0013)

CentOS 4 : xorg (CESA-2007:0126)

CentOS 4 : xorg-x11 (CESA-2005:198)

CentOS 4 : xorg-x11 (CESA-2005:396)

CentOS 4 : xorg-x11 (CESA-2006:0451)

CentOS 4 : xorg-x11 (CESA-2006:0634)

CentOS 4 : xorg-x11 (CESA-2006:0665)

CentOS 4 : xorg-x11 (CESA-2007:0003)

CentOS 4 : xorg-x11 (CESA-2007:0519)

CentOS 4 : xorg-x11 (CESA-2007:0898)

CentOS 4 : xorg-x11 (CESA-2008:0030)

CentOS 4 : xorg-x11 (CESA-2008:0503)

CentOS 4 : xorg-x11 (CESA-2011:0432)

CentOS 4 : xorg-x11 (CESA-2011:1155)

CentOS 4 : xorg-x11 (CESA-2011:1360)

CentOS 4 : xpdf (CESA-2005:670)

CentOS 4 : xpdf (CESA-2006:0201)

CentOS 4 : xpdf (CESA-2007:1029)

CentOS 4 : xpdf (CESA-2008:0240)

CentOS 4 : xpdf (CESA-2009:1501)

CentOS 4 : xpdf (CESA-2009:1680)

CentOS 4 : xpdf (CESA-2010:0751)

CentOS 4 : xterm (CESA-2007:0701)

CentOS 4 : zlib (CESA-2005:569)

CentOS 4 : zlib (CESA-2005:584)

CentOS 5 / 6 / 7 : bash (CESA-2014:1293) (Shellshock)

CentOS 5 / 6 / 7 : bash (CESA-2014:1306)

CentOS 5 / 6 / 7 : bind (CESA-2014:1984)

CentOS 5 / 6 / 7 : bind (CESA-2016:0073)

CentOS 5 / 6 / 7 : bind (CESA-2016:0459)

CentOS 5 / 6 / 7 : bind (CESA-2016:1944)

CentOS 5 / 6 / 7 : firefox (CESA-2014:1635)

CentOS 5 / 6 / 7 : firefox (CESA-2014:1919)

CentOS 5 / 6 / 7 : firefox (CESA-2015:0265)

CentOS 5 / 6 / 7 : firefox (CESA-2015:0718)

CentOS 5 / 6 / 7 : firefox (CESA-2015:0988)

CentOS 5 / 6 / 7 : firefox (CESA-2015:1207)

CentOS 5 / 6 / 7 : firefox (CESA-2015:1581)

CentOS 5 / 6 / 7 : firefox (CESA-2015:1586)

CentOS 5 / 6 / 7 : firefox (CESA-2015:1693)

CentOS 5 / 6 / 7 : firefox (CESA-2015:1834)

CentOS 5 / 6 / 7 : firefox (CESA-2015:1982)

CentOS 5 / 6 / 7 : firefox (CESA-2015:2657)

CentOS 5 / 6 / 7 : firefox (CESA-2016:0071)

CentOS 5 / 6 / 7 : firefox (CESA-2016:0197)

CentOS 5 / 6 / 7 : firefox (CESA-2016:0373)

CentOS 5 / 6 / 7 : firefox (CESA-2016:0695)

CentOS 5 / 6 / 7 : firefox (CESA-2016:1217)

CentOS 5 / 6 / 7 : firefox (CESA-2016:1551)

CentOS 5 / 6 / 7 : firefox (CESA-2016:1912)

CentOS 5 / 6 / 7 : firefox (CESA-2016:2843)

CentOS 5 / 6 / 7 : firefox (CESA-2016:2946)

CentOS 5 / 6 / 7 : firefox (CESA-2017:0190)

CentOS 5 / 6 / 7 : firefox / xulrunner (CESA-2014:0919)

CentOS 5 / 6 / 7 : firefox / xulrunner (CESA-2014:1144)

CentOS 5 / 6 / 7 : firefox / xulrunner (CESA-2015:0046)

CentOS 5 / 6 / 7 : firefox / xulrunner (CESA-2015:0766)

CentOS 5 / 6 / 7 : glibc (CESA-2014:1110)

CentOS 5 / 6 / 7 : jakarta-commons-httpclient (CESA-2014:1166)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2014:0907)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2014:1634)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2015:0085) (POODLE)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2015:0808)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2015:1526) (Bar Mitzvah) (Logjam)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2015:2086)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2016:0067)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2016:0723)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2016:1776)

CentOS 5 / 6 / 7 : java-1.6.0-openjdk (CESA-2017:0061)

CentOS 5 / 6 / 7 : java-1.7.0-openjdk (CESA-2016:1504)

CentOS 5 / 6 / 7 : java-1.7.0-openjdk (CESA-2016:2658)

CentOS 5 / 6 / 7 : java-1.7.0-openjdk (CESA-2017:0269)

CentOS 5 / 6 / 7 : nss (CESA-2014:1307)

CentOS 5 / 6 / 7 : nss (CESA-2014:1948) (POODLE)

CentOS 5 / 6 / 7 : nss / nss-util (CESA-2016:2779)

CentOS 5 / 6 / 7 : openldap (CESA-2015:1840)

CentOS 5 / 6 / 7 : procmail (CESA-2014:1172)

CentOS 5 / 6 / 7 : setroubleshoot (CESA-2015:0729)

CentOS 5 / 6 / 7 : thunderbird (CESA-2015:1012)

CentOS 5 / 6 / 7 : thunderbird (CESA-2015:1455)

CentOS 5 / 6 / 7 : thunderbird (CESA-2015:1682)

CentOS 5 / 6 / 7 : thunderbird (CESA-2015:1852)

CentOS 5 / 6 / 7 : thunderbird (CESA-2015:2519)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:0001)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:0258)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:0460)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:1041)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:1392)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:1809)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:1985)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:2825)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:2850)

CentOS 5 / 6 / 7 : thunderbird (CESA-2016:2973)

CentOS 5 / 6 / 7 : thunderbird (CESA-2017:0238)

CentOS 5 / 6 / 7 : thunderbird (CESA-2017:0498)

CentOS 5 / 6 : axis (CESA-2014:1193)

CentOS 5 / 6 : bind (CESA-2012:0716)

CentOS 5 / 6 : bind (CESA-2012:1123)

CentOS 5 / 6 : bind (CESA-2012:1363)

CentOS 5 / 6 : bind (CESA-2016:2093)

CentOS 5 / 6 : bind (CESA-2016:2141)

CentOS 5 / 6 : bind (CESA-2017:0063)

CentOS 5 / 6 : boost (CESA-2013:0668)

CentOS 5 / 6 : cups (CESA-2013:0580)

CentOS 5 / 6 : curl (CESA-2013:0771)

CentOS 5 / 6 : curl (CESA-2013:0983)

CentOS 5 / 6 : cvs (CESA-2012:0321)

CentOS 5 / 6 : dbus-glib (CESA-2013:0568)

CentOS 5 / 6 : devhelp / firefox / libproxy / xulrunner / yelp (CESA-2013:0271)

CentOS 5 / 6 : elinks (CESA-2013:0250)

CentOS 5 / 6 : expat (CESA-2012:0731)

CentOS 5 / 6 : firefox (CESA-2012:0387)

CentOS 5 / 6 : firefox (CESA-2012:0515)

CentOS 5 / 6 : firefox (CESA-2012:0710)

CentOS 5 / 6 : firefox (CESA-2012:1088)

CentOS 5 / 6 : firefox (CESA-2012:1210)

CentOS 5 / 6 : firefox (CESA-2012:1350)

CentOS 5 / 6 : firefox (CESA-2012:1407)

CentOS 5 / 6 : firefox (CESA-2012:1482)

CentOS 5 / 6 : firefox (CESA-2013:0820)

CentOS 5 / 6 : firefox (CESA-2013:1140)

CentOS 5 / 6 : firefox (CESA-2013:1268)

CentOS 5 / 6 : firefox (CESA-2013:1476)

CentOS 5 / 6 : firefox (CESA-2013:1812)

CentOS 5 / 6 : firefox (CESA-2014:0132)

CentOS 5 / 6 : firefox (CESA-2014:0310)

CentOS 5 / 6 : firefox (CESA-2014:0448)

CentOS 5 / 6 : firefox (CESA-2014:0741)

CentOS 5 / 6 : firefox (CESA-2016:2780)

CentOS 5 / 6 : firefox (CESA-2017:0459)

CentOS 5 / 6 : firefox / thunderbird (CESA-2012:0516)

CentOS 5 / 6 : firefox / xulrunner (CESA-2013:0144)

CentOS 5 / 6 : firefox / xulrunner (CESA-2013:0696)

CentOS 5 / 6 : firefox / xulrunner (CESA-2013:0981)

CentOS 5 / 6 : freetype (CESA-2012:0467)

CentOS 5 / 6 : freetype (CESA-2013:0216)

CentOS 5 / 6 : ghostscript (CESA-2012:0095)

CentOS 5 / 6 : ghostscript (CESA-2012:1256)

CentOS 5 / 6 : gimp (CESA-2013:1778)

CentOS 5 / 6 : gnupg2 (CESA-2013:1459)

CentOS 5 / 6 : gnutls (CESA-2013:0588)

CentOS 5 / 6 : gnutls (CESA-2013:0883)

CentOS 5 / 6 : httpd (CESA-2013:0815)

CentOS 5 / 6 : httpd (CESA-2013:1156)

CentOS 5 / 6 : httpd (CESA-2014:0920)

CentOS 5 / 6 : httpd (CESA-2016:1421) (httpoxy)

CentOS 5 / 6 : icu (CESA-2011:1815)

CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)

CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)

CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1505)

CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2014:0097)

CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2014:0408)

CentOS 5 / 6 : java-1.7.0-openjdk (CESA-2013:0165)

CentOS 5 / 6 : java-1.7.0-openjdk (CESA-2013:0247)

CentOS 5 / 6 : java-1.7.0-openjdk (CESA-2013:0275)

CentOS 5 / 6 : krb5 (CESA-2013:0942)

CentOS 5 / 6 : libexif (CESA-2012:1255)

CentOS 5 / 6 : libgcrypt (CESA-2013:1457)

CentOS 5 / 6 : libpng (CESA-2012:0407)

CentOS 5 / 6 : libpng (CESA-2012:0523)

CentOS 5 / 6 : libtiff (CESA-2012:0468)

CentOS 5 / 6 : libtiff (CESA-2012:1054)

CentOS 5 / 6 : libtiff (CESA-2012:1590)

CentOS 5 / 6 : libXfont (CESA-2014:0018)

CentOS 5 / 6 : libxml2 (CESA-2012:1288)

CentOS 5 / 6 : libxml2 (CESA-2012:1512)

CentOS 5 / 6 : libxml2 (CESA-2013:0581)

CentOS 5 / 6 : libxslt (CESA-2012:1265)

CentOS 5 / 6 : mod\_nss (CESA-2013:1779)

CentOS 5 / 6 : nss (CESA-2013:1861)

CentOS 5 / 6 : openoffice.org (CESA-2012:0705)

CentOS 5 / 6 : openssl (CESA-2012:0426)

CentOS 5 / 6 : openssl (CESA-2012:0518)

CentOS 5 / 6 : openssl (CESA-2012:0699)

CentOS 5 / 6 : openssl (CESA-2013:0587)

CentOS 5 / 6 : openssl097a / openssl098e (CESA-2014:0626)

CentOS 5 / 6 : openswan (CESA-2013:0827)

CentOS 5 / 6 : openswan (CESA-2014:0185)

CentOS 5 / 6 : perl (CESA-2013:0685)

CentOS 5 / 6 : perl-DBD-Pg (CESA-2012:1116)

CentOS 5 / 6 : php (CESA-2012:0546)

CentOS 5 / 6 : php (CESA-2013:1049)

CentOS 5 / 6 : php / php53 (CESA-2012:0019)

CentOS 5 / 6 : php / php53 (CESA-2013:1813)

CentOS 5 / 6 : php / php53 (CESA-2014:1012)

CentOS 5 / 6 : php / php53 (CESA-2014:1326)

CentOS 5 / 6 : pidgin (CESA-2012:1102)

CentOS 5 / 6 : pidgin (CESA-2013:0646)

CentOS 5 / 6 : pidgin (CESA-2014:0139)

CentOS 5 / 6 : pixman (CESA-2013:1869)

CentOS 5 / 6 : postgresql / postgresql84 (CESA-2012:0678)

CentOS 5 / 6 : postgresql / postgresql84 (CESA-2012:1037)

CentOS 5 / 6 : postgresql / postgresql84 (CESA-2012:1263)

CentOS 5 / 6 : postgresql / postgresql84 (CESA-2013:1475)

CentOS 5 / 6 : postgresql / postgresql84 (CESA-2014:0211)

CentOS 5 / 6 : rpm (CESA-2012:0451)

CentOS 5 / 6 : rpm (CESA-2014:1974)

CentOS 5 / 6 : rsyslog / rsyslog5 (CESA-2014:1671)

CentOS 5 / 6 : ruby (CESA-2013:1090)

CentOS 5 / 6 : samba (CESA-2012:0465)

CentOS 5 / 6 : samba / samba3x (CESA-2012:0533)

CentOS 5 / 6 : samba / samba3x (CESA-2013:1806)

CentOS 5 / 6 : samba / samba3x (CESA-2014:0330)

CentOS 5 / 6 : samba / samba3x (CESA-2014:0866)

CentOS 5 / 6 : squid (CESA-2014:1148)

CentOS 5 / 6 : subversion (CESA-2013:0737)

CentOS 5 / 6 : subversion (CESA-2014:0255)

CentOS 5 / 6 : sudo (CESA-2012:1081)

CentOS 5 / 6 : systemtap (CESA-2012:0376)

CentOS 5 / 6 : thunderbird (CESA-2012:0388)

CentOS 5 / 6 : thunderbird (CESA-2012:0715)

CentOS 5 / 6 : thunderbird (CESA-2012:1089)

CentOS 5 / 6 : thunderbird (CESA-2012:1211)

CentOS 5 / 6 : thunderbird (CESA-2012:1351)

CentOS 5 / 6 : thunderbird (CESA-2012:1362)

CentOS 5 / 6 : thunderbird (CESA-2012:1413)

CentOS 5 / 6 : thunderbird (CESA-2012:1483)

CentOS 5 / 6 : thunderbird (CESA-2013:0145)

CentOS 5 / 6 : thunderbird (CESA-2013:0272)

CentOS 5 / 6 : thunderbird (CESA-2013:0627)

CentOS 5 / 6 : thunderbird (CESA-2013:0697)

CentOS 5 / 6 : thunderbird (CESA-2013:0821)

CentOS 5 / 6 : thunderbird (CESA-2013:0982)

CentOS 5 / 6 : thunderbird (CESA-2013:1142)

CentOS 5 / 6 : thunderbird (CESA-2013:1269)

CentOS 5 / 6 : thunderbird (CESA-2013:1480)

CentOS 5 / 6 : thunderbird (CESA-2013:1823)

CentOS 5 / 6 : thunderbird (CESA-2014:0133)

CentOS 5 / 6 : thunderbird (CESA-2014:0316)

CentOS 5 / 6 : thunderbird (CESA-2014:0449)

CentOS 5 / 6 : thunderbird (CESA-2014:0742)

CentOS 5 / 6 : thunderbird (CESA-2014:0918)

CentOS 5 / 6 : thunderbird (CESA-2014:1145)

CentOS 5 / 6 : thunderbird (CESA-2014:1647)

CentOS 5 / 6 : thunderbird (CESA-2014:1924)

CentOS 5 / 6 : thunderbird (CESA-2015:0047)

CentOS 5 / 6 : thunderbird (CESA-2015:0266)

CentOS 5 / 6 : vino (CESA-2013:1452)

CentOS 5 / 6 : xalan-j2 (CESA-2014:0348)

CentOS 5 / 6 : xinetd (CESA-2013:1409)

CentOS 5 / 6 : xorg-x11-server (CESA-2013:1426)

CentOS 5 / 6 : xorg-x11-server (CESA-2013:1868)

CentOS 5 / 6 : xulrunner (CESA-2012:0143)

CentOS 5 / 6 : xulrunner (CESA-2012:1361)

CentOS 5 / 6 : xulrunner (CESA-2013:0614)

CentOS 5 / 7 : java-1.7.0-openjdk (CESA-2016:0054) (SLOTH)

CentOS 5 / 7 : java-1.7.0-openjdk (CESA-2016:0512)

CentOS 5 / 7 : java-1.7.0-openjdk (CESA-2016:0676)

CentOS 5 / 7 : nspr / nss (CESA-2014:0916)

CentOS 5 / 7 : thunderbird (CESA-2015:0771)

CentOS 5 : acpid (CESA-2009:1642)

CentOS 5 : aide (CESA-2007:0539)

CentOS 5 : apr (CESA-2009:1204)

CentOS 5 : apr-util (CESA-2009:1107)

CentOS 5 : autofs (CESA-2007:1128)

CentOS 5 : autofs (CESA-2007:1176)

CentOS 5 : autofs (CESA-2013:0132)

CentOS 5 : automake (CESA-2014:1243)

CentOS 5 : avahi (CESA-2009:0013)

CentOS 5 : avahi (CESA-2010:0528)

CentOS 5 : avahi (CESA-2011:0436)

CentOS 5 : axis (CESA-2013:0683)

CentOS 5 : bash (CESA-2011:1073)

CentOS 5 : bind (CESA-2009:1179)

CentOS 5 : bind (CESA-2009:1620)

CentOS 5 : bind (CESA-2010:0062)

CentOS 5 : bind (CESA-2010:0976)

CentOS 5 : bind (CESA-2011:1458)

CentOS 5 : bind (CESA-2012:1267)

CentOS 5 : bind (CESA-2015:1514)

CentOS 5 : bind (CESA-2015:1706)

CentOS 5 : bind (CESA-2015:2656)

CentOS 5 : bind97 (CESA-2011:0845)

CentOS 5 : bind97 (CESA-2011:0926)

CentOS 5 : bind97 (CESA-2011:1459)

CentOS 5 : bind97 (CESA-2012:0717)

CentOS 5 : bind97 (CESA-2012:1122)

CentOS 5 : bind97 (CESA-2012:1266)

CentOS 5 : bind97 (CESA-2012:1364)

CentOS 5 : bind97 (CESA-2013:0690)

CentOS 5 : bind97 (CESA-2013:1115)

CentOS 5 : bind97 (CESA-2014:1244)

CentOS 5 : bind97 (CESA-2014:1985)

CentOS 5 : bind97 (CESA-2015:1515)

CentOS 5 : bind97 (CESA-2015:1707)

CentOS 5 : bind97 (CESA-2015:2658)

CentOS 5 : bind97 (CESA-2016:0074)

CentOS 5 : bind97 (CESA-2016:0458)

CentOS 5 : bind97 (CESA-2016:1945)

CentOS 5 : bind97 (CESA-2016:2094)

CentOS 5 : bind97 (CESA-2016:2142)

CentOS 5 : bind97 (CESA-2017:0064)

CentOS 5 : ccid (CESA-2013:1323)

CentOS 5 : cman (CESA-2007:0559)

CentOS 5 : cman (CESA-2009:1341)

CentOS 5 : conga (CESA-2011:0394)

CentOS 5 : conga (CESA-2013:0128)

CentOS 5 : conga (CESA-2014:1194)

CentOS 5 : cpio (CESA-2010:0144)

CentOS 5 : cscope (CESA-2009:1102)

CentOS 5 : cups (CESA-2007:1020)

CentOS 5 : cups (CESA-2008:0157)

CentOS 5 : cups (CESA-2008:0192)

CentOS 5 : cups (CESA-2008:1029)

CentOS 5 : cups (CESA-2009:1082)

CentOS 5 : cups (CESA-2009:1513)

CentOS 5 : cups (CESA-2009:1595)

CentOS 5 : cups (CESA-2010:0129)

CentOS 5 : cups (CESA-2010:0811)

CentOS 5 : cyrus-imapd (CESA-2009:1116)

CentOS 5 : dbus (CESA-2008:0159)

CentOS 5 : dbus (CESA-2009:0008)

CentOS 5 : dbus (CESA-2010:0018)

CentOS 5 : dbus (CESA-2011:0376)

CentOS 5 : dbus (CESA-2011:1132)

CentOS 5 : dhcp (CESA-2012:1140)

CentOS 5 : dnsmasq (CESA-2009:1238)

CentOS 5 : dstat (CESA-2009:1619)

CentOS 5 : ecryptfs-utils (CESA-2009:1307)

CentOS 5 : ecryptfs-utils (CESA-2011:1241)

CentOS 5 : enscript (CESA-2008:1016)

CentOS 5 : evolution (CESA-2008:0514)

CentOS 5 : evolution-data-server (CESA-2007:0344)

CentOS 5 : evolution-data-server (CESA-2007:0510)

CentOS 5 : firefox (CESA-2008:0569)

CentOS 5 : firefox (CESA-2008:0597)

CentOS 5 : firefox (CESA-2009:1095)

CentOS 5 : firefox (CESA-2009:1162)

CentOS 5 : firefox (CESA-2010:0501)

CentOS 5 : firefox (CESA-2010:0556)

CentOS 5 : freeradius (CESA-2009:1451)

CentOS 5 : freeradius2 (CESA-2012:1327)

CentOS 5 : freeradius2 (CESA-2013:0134)

CentOS 5 : freetype (CESA-2009:1061)

CentOS 5 : gdm (CESA-2007:0777)

CentOS 5 : gdm (CESA-2009:1364)

CentOS 5 : gdm / initscripts (CESA-2013:1213)

CentOS 5 : gfs2-utils (CESA-2009:1337)

CentOS 5 : ghostscript (CESA-2009:0421)

CentOS 5 : giflib (CESA-2009:0444)

CentOS 5 : gimp (CESA-2011:0838)

CentOS 5 : gimp (CESA-2012:1181)

CentOS 5 : glibc (CESA-2010:0787)

CentOS 5 : glibc (CESA-2010:0793)

CentOS 5 : glibc (CESA-2011:0412)

CentOS 5 : glibc (CESA-2012:0126)

CentOS 5 : glibc (CESA-2012:0397)

CentOS 5 : glibc (CESA-2012:1097)

CentOS 5 : glibc (CESA-2012:1207)

CentOS 5 : glibc (CESA-2013:0769)

CentOS 5 : glibc (CESA-2013:1411)

CentOS 5 : glibc (CESA-2015:0090) (GHOST)

CentOS 5 : glibc (CESA-2015:1627)

CentOS 5 : gnome-screensaver (CESA-2008:0197)

CentOS 5 : gnome-vfs2 (CESA-2013:0131)

CentOS 5 : gnupg (CESA-2013:1458)

CentOS 5 : gnupg (CESA-2014:0016)

CentOS 5 : gnupg2 (CESA-2010:0603)

CentOS 5 : gnutls (CESA-2008:0489)

CentOS 5 : gnutls (CESA-2008:0982)

CentOS 5 : gnutls (CESA-2010:0166)

CentOS 5 : gnutls (CESA-2012:0428)

CentOS 5 : gnutls (CESA-2014:0247)

CentOS 5 : gnutls (CESA-2014:0594)

CentOS 5 : gstreamer-plugins-base (CESA-2009:0352)

CentOS 5 : gstreamer-plugins-good (CESA-2009:1123)

CentOS 5 : gtk2 (CESA-2013:0135)

CentOS 5 : hplip (CESA-2007:0960)

CentOS 5 : hplip (CESA-2008-0818)

CentOS 5 : hplip / hplip3 (CESA-2011:0154)

CentOS 5 : hplip3 (CESA-2013:0133)

CentOS 5 : httpd (CESA-2007:0556)

CentOS 5 : httpd (CESA-2008:0008)

CentOS 5 : httpd (CESA-2009:1075)

CentOS 5 : httpd (CESA-2009:1148)

CentOS 5 : httpd (CESA-2010:0168)

CentOS 5 : httpd (CESA-2010:0659)

CentOS 5 : httpd (CESA-2013:0130)

CentOS 5 : httpd (CESA-2014:0369)

CentOS 5 : hypervkvpd (CESA-2013:0807)

CentOS 5 : icu (CESA-2008:0090)

CentOS 5 : icu (CESA-2009:1122)

CentOS 5 : ImageMagick (CESA-2010:0652)

CentOS 5 : ImageMagick (CESA-2012:0545)

CentOS 5 : ipa-client (CESA-2013:0189)

CentOS 5 : ipsec-tools (CESA-2007:0342)

CentOS 5 : ipsec-tools (CESA-2009:1036)

CentOS 5 : iscsi-initiator-utils (CESA-2007:0497)

CentOS 5 : jakarta-commons-collections (CESA-2015:2671)

CentOS 5 : jakarta-commons-httpclient (CESA-2013:0270)

CentOS 5 : java-1.6.0-openjdk (CESA-2009:0377)

CentOS 5 : java-1.6.0-openjdk (CESA-2009:1201)

CentOS 5 : java-1.6.0-openjdk (CESA-2009:1584)

CentOS 5 : java-1.6.0-openjdk (CESA-2010:0339)

CentOS 5 : java-1.6.0-openjdk (CESA-2010:0768)

CentOS 5 : java-1.6.0-openjdk (CESA-2011:0176)

CentOS 5 : java-1.6.0-openjdk (CESA-2011:0214)

CentOS 5 : java-1.6.0-openjdk (CESA-2011:0281)

CentOS 5 : java-1.6.0-openjdk (CESA-2011:0857)

CentOS 5 : java-1.6.0-openjdk (CESA-2011:1380) (BEAST)

CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)

CentOS 5 : java-1.6.0-openjdk (CESA-2012:1222)

CentOS 5 : java-1.6.0-openjdk (CESA-2012:1385) (ROBOT)

CentOS 5 : java-1.6.0-openjdk (CESA-2013:0246)

CentOS 5 : java-1.6.0-openjdk (CESA-2013:0274)

CentOS 5 : java-1.6.0-openjdk (CESA-2013:0604)

CentOS 5 : java-1.7.0-openjdk (CESA-2013:0603)

CentOS 5 : java-1.7.0-openjdk (CESA-2013:0752)

CentOS 5 : java-1.7.0-openjdk (CESA-2013:0958)

CentOS 5 : java-1.7.0-openjdk (CESA-2013:1447)

CentOS 5 : java-1.7.0-openjdk (CESA-2014:0027)

CentOS 5 : java-1.7.0-openjdk (CESA-2014:0407)

CentOS 5 : java-1.7.0-openjdk (CESA-2014:0890)

CentOS 5 : java-1.7.0-openjdk (CESA-2014:1633)

CentOS 5 : java-1.7.0-openjdk (CESA-2015:0068) (POODLE)

CentOS 5 : java-1.7.0-openjdk (CESA-2015:0807)

CentOS 5 : java-1.7.0-openjdk (CESA-2015:1230) (Bar Mitzvah) (Logjam)

CentOS 5 : java-1.7.0-openjdk (CESA-2015:1921)

CentOS 5 : kdegraphics (CESA-2009:1130)

CentOS 5 : kdegraphics (CESA-2009:1502)

CentOS 5 : kdelibs (CESA-2009:1127)

CentOS 5 : Kernel (CESA-2007:0169)

CentOS 5 : kernel (CESA-2007:0347)

CentOS 5 : kernel (CESA-2007:0376)

CentOS 5 : kernel (CESA-2007:0595)

CentOS 5 : kernel (CESA-2007:0705)

CentOS 5 : kernel (CESA-2007:0936)

CentOS 5 : kernel (CESA-2007:0940)

CentOS 5 : kernel (CESA-2008:0089)

CentOS 5 : kernel (CESA-2008:0129)

CentOS 5 : kernel (CESA-2008:0233)

CentOS 5 : kernel (CESA-2008:0275)

CentOS 5 : kernel (CESA-2008:0519)

CentOS 5 : kernel (CESA-2008:0612)

CentOS 5 : kernel (CESA-2008:0885)

CentOS 5 : kernel (CESA-2008:0957)

CentOS 5 : kernel (CESA-2008:1017)

CentOS 5 : kernel (CESA-2009:0326)

CentOS 5 : kernel (CESA-2009:0473)

CentOS 5 : kernel (CESA-2009:1106)

CentOS 5 : kernel (CESA-2009:1193)

CentOS 5 : kernel (CESA-2009:1222)

CentOS 5 : kernel (CESA-2009:1243)

CentOS 5 : kernel (CESA-2009:1455)

CentOS 5 : kernel (CESA-2009:1548)

CentOS 5 : kernel (CESA-2009:1670)

CentOS 5 : kernel (CESA-2010:0019)

CentOS 5 : kernel (CESA-2010:0046)

CentOS 5 : kernel (CESA-2010:0147)

CentOS 5 : kernel (CESA-2010:0398)

CentOS 5 : kernel (CESA-2010:0504)

CentOS 5 : kernel (CESA-2010:0610)

CentOS 5 : kernel (CESA-2010:0661)

CentOS 5 : kernel (CESA-2010:0704)

CentOS 5 : kernel (CESA-2010:0723)

CentOS 5 : kernel (CESA-2010:0792)

CentOS 5 : kernel (CESA-2010:0839)

CentOS 5 : kernel (CESA-2011:0004)

CentOS 5 : kernel (CESA-2011:0163)

CentOS 5 : kernel (CESA-2011:0303)

CentOS 5 : kernel (CESA-2011:0429)

CentOS 5 : kernel (CESA-2011:0833)

CentOS 5 : kernel (CESA-2011:0927)

CentOS 5 : kernel (CESA-2011:1065)

CentOS 5 : kernel (CESA-2011:1212)

CentOS 5 : kernel (CESA-2011:1386)

CentOS 5 : kernel (CESA-2011:1479)

CentOS 5 : kernel (CESA-2012:0007)

CentOS 5 : kernel (CESA-2012:0107)

CentOS 5 : kernel (CESA-2012:0480)

CentOS 5 : kernel (CESA-2012:0690)

CentOS 5 : kernel (CESA-2012:0721)

CentOS 5 : kernel (CESA-2012:1061)

CentOS 5 : kernel (CESA-2012:1174)

CentOS 5 : kernel (CESA-2012:1323)

CentOS 5 : kernel (CESA-2012:1445)

CentOS 5 : kernel (CESA-2012:1540)

CentOS 5 : kernel (CESA-2013:0168)

CentOS 5 : kernel (CESA-2013:0594)

CentOS 5 : kernel (CESA-2013:0621)

CentOS 5 : kernel (CESA-2013:0747)

CentOS 5 : kernel (CESA-2013:0847)

CentOS 5 : kernel (CESA-2013:1034)

CentOS 5 : kernel (CESA-2013:1166)

CentOS 5 : kernel (CESA-2013:1292)

CentOS 5 : kernel (CESA-2013:1348)

CentOS 5 : kernel (CESA-2013:1449)

CentOS 5 : kernel (CESA-2013:1790)

CentOS 5 : kernel (CESA-2014:0108)

CentOS 5 : kernel (CESA-2014:0285)

CentOS 5 : kernel (CESA-2014:0433)

CentOS 5 : kernel (CESA-2014:0740)

CentOS 5 : kernel (CESA-2014:0926)

CentOS 5 : kernel (CESA-2014:1143)

CentOS 5 : kernel (CESA-2014:1959)

CentOS 5 : kernel (CESA-2014:2008)

CentOS 5 : kernel (CESA-2015:0164)

CentOS 5 : kernel (CESA-2015:0783)

CentOS 5 : kernel (CESA-2015:1042)

CentOS 5 : kernel (CESA-2016:0045)

CentOS 5 : kernel (CESA-2016:0450)

CentOS 5 : kernel (CESA-2016:2124) (Dirty COW)

CentOS 5 : kernel (CESA-2016:2962)

CentOS 5 : kernel (CESA-2017:0323)

CentOS 5 : krb5 (CESA-2007:0858)

CentOS 5 : krb5 (CESA-2007:0892)

CentOS 5 : krb5 (CESA-2008:0164)

CentOS 5 : krb5 (CESA-2009:0408)

CentOS 5 : krb5 (CESA-2010:0343)

CentOS 5 : krb5 (CESA-2011:0199)

CentOS 5 : krb5 (CESA-2014:1245)

CentOS 5 : krb5 (CESA-2014:1255)

CentOS 5 : kvm (CESA-2009:1465)

CentOS 5 : kvm (CESA-2009:1659)

CentOS 5 : kvm (CESA-2010:0088)

CentOS 5 : kvm (CESA-2010:0126)

CentOS 5 : kvm (CESA-2010:0627)

CentOS 5 : kvm (CESA-2010:0898)

CentOS 5 : kvm (CESA-2012:0051)

CentOS 5 : kvm (CESA-2012:0676)

CentOS 5 : kvm (CESA-2012:1235)

CentOS 5 : kvm (CESA-2013:0608)

CentOS 5 : kvm (CESA-2013:0727)

CentOS 5 : kvm (CESA-2014:0163)

CentOS 5 : kvm (CESA-2015:0869)

CentOS 5 : kvm (CESA-2015:1003) (Venom)

CentOS 5 : kvm (CESA-2015:1189)

CentOS 5 : kvm (CESA-2015:1925)

CentOS 5 : kvm (CESA-2016:1943)

CentOS 5 : kvm (CESA-2017:0454)

CentOS 5 : lcms (CESA-2009:0011)

CentOS 5 : lftp (CESA-2009:1278)

CentOS 5 : lftp (CESA-2010:0585)

CentOS 5 : libexif (CESA-2007:1165)

CentOS 5 : libjpeg (CESA-2013:1804)

CentOS 5 : libpng (CESA-2011:1104)

CentOS 5 : libtiff (CESA-2008:0847)

CentOS 5 : libtiff (CESA-2014:0223)

CentOS 5 : libvirt (CESA-2010:0615)

CentOS 5 : libvirt (CESA-2011:0391)

CentOS 5 : libvirt (CESA-2011:1019)

CentOS 5 : libvirt (CESA-2013:0127)

CentOS 5 : libvirt / libvirt.test (CESA-2011:0478)

CentOS 5 : libwpd (CESA-2012:1043)

CentOS 5 : libXfont (CESA-2008:0064)

CentOS 5 : libXfont (CESA-2011:1154)

CentOS 5 : libXfont (CESA-2014:1893)

CentOS 5 : libxml2 (CESA-2012:0017)

CentOS 5 : libxml2 (CESA-2014:1885)

CentOS 5 : logwatch (CESA-2011:0324)

CentOS 5 : lvm2-cluster (CESA-2010:0567)

CentOS 5 : mesa (CESA-2013:0898)

CentOS 5 : mysql (CESA-2009:1289)

CentOS 5 : mysql (CESA-2010:0109)

CentOS 5 : mysql (CESA-2010:0442)

CentOS 5 : mysql (CESA-2010:0825)

CentOS 5 : mysql (CESA-2012:0127)

CentOS 5 : mysql (CESA-2013:0121)

CentOS 5 : mysql (CESA-2013:0180)

CentOS 5 : mysql55-mysql (CESA-2014:0186)

CentOS 5 : mysql55-mysql (CESA-2014:0536)

CentOS 5 : mysql55-mysql (CESA-2014:1859)

CentOS 5 : mysql55-mysql (CESA-2015:1628)

CentOS 5 : net-snmp (CESA-2013:0124)

CentOS 5 : net-snmp (CESA-2014:0322)

CentOS 5 : NetworkManager (CESA-2009:0361)

CentOS 5 : NetworkManager (CESA-2010:0108)

CentOS 5 : NetworkManager / dbus-glib (CESA-2010:0616)

CentOS 5 : nfs-utils (CESA-2008:0486)

CentOS 5 : nfs-utils (CESA-2009:1321)

CentOS 5 : nfs-utils-lib (CESA-2007:0951)

CentOS 5 : nspr / nss (CESA-2013:1791)

CentOS 5 : nspr / nss (CESA-2015:1980)

CentOS 5 : nspr / nss (CESA-2016:0684)

CentOS 5 : nss (CESA-2012:1090)

CentOS 5 : nss (CESA-2013:0214)

CentOS 5 : nss (CESA-2013:1135)

CentOS 5 : nss (CESA-2014:1246)

CentOS 5 : nss (CESA-2015:1664)

CentOS 5 : nss (CESA-2016:0371)

CentOS 5 : nss\_db (CESA-2010:0347)

CentOS 5 : ntp (CESA-2009:1039)

CentOS 5 : ntp (CESA-2014:2025)

CentOS 5 : opal (CESA-2007:0957)

CentOS 5 : OpenIPMI (CESA-2013:0123)

CentOS 5 : openldap (CESA-2010:0542)

CentOS 5 : openldap (CESA-2011:0346)

CentOS 5 : openldap (CESA-2014:0206)

CentOS 5 : openoffice.org (CESA-2008:0835)

CentOS 5 : openoffice.org (CESA-2010:0459)

CentOS 5 : openoffice.org (CESA-2011:0182)

CentOS 5 : openoffice.org (CESA-2012:0411)

CentOS 5 : openoffice.org (CESA-2012:1136)

CentOS 5 : openoffice.org / hsqldb (CESA-2007:1048)

CentOS 5 : openssh (CESA-2009:1287)

CentOS 5 : openssh (CESA-2009:1470)

CentOS 5 : openssl (CESA-2007:0964)

CentOS 5 : openssl (CESA-2009:1335)

CentOS 5 : openssl (CESA-2010:0054)

CentOS 5 : openssl (CESA-2010:0162)

CentOS 5 : openssl (CESA-2010:0978)

CentOS 5 : openssl (CESA-2012:0060)

CentOS 5 : openssl (CESA-2014:0624)

CentOS 5 : openssl (CESA-2014:1053)

CentOS 5 : openssl (CESA-2014:1653) (POODLE)

CentOS 5 : openssl (CESA-2015:0800) (FREAK)

CentOS 5 : openssl (CESA-2015:1197) (Logjam)

CentOS 5 : openssl (CESA-2015:2616)

CentOS 5 : openssl (CESA-2016:0302) (DROWN)

CentOS 5 : openssl (CESA-2016:1137)

CentOS 5 : openssl097a (CESA-2010:0164)

CentOS 5 : openswan (CESA-2009:0402)

CentOS 5 : openswan (CESA-2009:1138)

CentOS 5 : openswan (CESA-2011:1422)

CentOS 5 : pam (CESA-2010:0819)

CentOS 5 : pam\_krb5 (CESA-2008:0907)

CentOS 5 : pango (CESA-2011:1326)

CentOS 5 : pcre (CESA-2007:0967)

CentOS 5 : pcsc-lite (CESA-2010:0533)

CentOS 5 : perl (CESA-2010:0458)

CentOS 5 : perl-DBD-Pg (CESA-2009:0479)

CentOS 5 : php (CESA-2007:0153)

CentOS 5 : php (CESA-2007:0348)

CentOS 5 : php (CESA-2009:0338)

CentOS 5 : php (CESA-2012:0033)

CentOS 5 : php (CESA-2012:1045)

CentOS 5 : php (CESA-2013:1814)

CentOS 5 : php (CESA-2014:0311)

CentOS 5 : php (CESA-2014:1824)

CentOS 5 : php53 (CESA-2011:0196)

CentOS 5 : php53 (CESA-2011:1423)

CentOS 5 : php53 (CESA-2012:0092)

CentOS 5 : php53 (CESA-2012:0547)

CentOS 5 : php53 (CESA-2012:1047)

CentOS 5 : php53 (CESA-2013:1050)

CentOS 5 : php53 (CESA-2013:1307)

CentOS 5 : php53 (CESA-2014:1768)

CentOS 5 : pidgin (CESA-2009:1139)

CentOS 5 : piranha (CESA-2014:0174)

CentOS 5 : poppler (CESA-2007:0732)

CentOS 5 : poppler (CESA-2008:0239)

CentOS 5 : poppler (CESA-2009:0480)

CentOS 5 : poppler (CESA-2009:1504)

CentOS 5 : poppler (CESA-2010:0749)

CentOS 5 : postgresql (CESA-2010:0429)

CentOS 5 : postgresql (CESA-2012:0677)

CentOS 5 : postgresql (CESA-2012:1036)

CentOS 5 : postgresql (CESA-2012:1264)

CentOS 5 : postgresql (CESA-2014:0249)

CentOS 5 : postgresql84 (CESA-2010:0430)

CentOS 5 : postgresql84 (CESA-2011:0198)

CentOS 5 : postgresql84 (CESA-2011:1378)

CentOS 5 : pwlib (CESA-2007:0932)

CentOS 5 : python (CESA-2009:1176)

CentOS 5 : python (CESA-2011:0492)

CentOS 5 : python (CESA-2012:0745)

CentOS 5 : qspice (CESA-2010:0633)

CentOS 5 : qspice (CESA-2013:1474)

CentOS 5 : qspice-client (CESA-2010:0632)

CentOS 5 : qt4 (CESA-2011:1324)

CentOS 5 : quagga (CESA-2012:1258)

CentOS 5 : quota (CESA-2013:0120)

CentOS 5 : rdesktop (CESA-2008:0575)

CentOS 5 : rdesktop (CESA-2011:0506)

CentOS 5 : rgmanager (CESA-2009:1339)

CentOS 5 : rgmanager (CESA-2011:1000)

CentOS 5 : rpm (CESA-2010:0679)

CentOS 5 : rsync (CESA-2011:0999)

CentOS 5 : ruby (CESA-2009:1140)

CentOS 5 : ruby (CESA-2011:0909)

CentOS 5 : ruby (CESA-2013:0129)

CentOS 5 : ruby (CESA-2013:0611)

CentOS 5 : samba (CESA-2008:0290)

CentOS 5 : samba (CESA-2014:0305)

CentOS 5 : samba (CESA-2016:0621) (Badlock)

CentOS 5 : samba3x (CESA-2010:0698)

CentOS 5 : samba3x (CESA-2011:0306)

CentOS 5 : samba3x (CESA-2011:1220)

CentOS 5 : samba3x (CESA-2012:0466)

CentOS 5 : samba3x (CESA-2013:1310)

CentOS 5 : samba3x (CESA-2015:0249)

CentOS 5 : samba3x (CESA-2016:0613) (Badlock)

CentOS 5 : scsi-target-utils (CESA-2010:0362)

CentOS 5 : scsi-target-utils (CESA-2010:0518)

CentOS 5 : scsi-target-utils (CESA-2011:0332)

CentOS 5 : sos (CESA-2012:0153)

CentOS 5 : sos (CESA-2013:1121)

CentOS 5 : spice-xpi (CESA-2010:0651)

CentOS 5 : spice-xpi (CESA-2011:0427)

CentOS 5 : squirrelmail (CESA-2013:0126)

CentOS 5 : sssd (CESA-2011:0975)

CentOS 5 : sssd (CESA-2013:1319)

CentOS 5 : struts (CESA-2014:0474)

CentOS 5 : subversion (CESA-2009:1203)

CentOS 5 : subversion (CESA-2011:0257)

CentOS 5 : subversion (CESA-2011:0327)

CentOS 5 : subversion (CESA-2011:0862)

CentOS 5 : sudo (CESA-2010:0122)

CentOS 5 : sudo (CESA-2010:0361)

CentOS 5 : sudo (CESA-2010:0475)

CentOS 5 : sudo (CESA-2010:0675)

CentOS 5 : sudo (CESA-2012:1149)

CentOS 5 : sudo (CESA-2013:1353)

CentOS 5 : sudo (CESA-2014:0266)

CentOS 5 : sysstat (CESA-2011:1005)

CentOS 5 : systemtap (CESA-2010:0124)

CentOS 5 : systemtap (CESA-2010:0894)

CentOS 5 : systemtap (CESA-2011:0841)

CentOS 5 : systemtap (CESA-2011:1089)

CentOS 5 : tcl (CESA-2013:0122)

CentOS 5 : tetex (CESA-2010:0400)

CentOS 5 : tetex (CESA-2012:1201)

CentOS 5 : thunderbird (CESA-2009:1126)

CentOS 5 : thunderbird (CESA-2010:0153)

CentOS 5 : thunderbird (CESA-2010:0545)

CentOS 5 : tk (CESA-2008:0136)

CentOS 5 : tog-pegasus (CESA-2008:1001)

CentOS 5 : tomcat (CESA-2007:0327)

CentOS 5 : tomcat (CESA-2007:0569)

CentOS 5 : tomcat (CESA-2007:0871)

CentOS 5 : tomcat (CESA-2008:0042)

CentOS 5 : tomcat (CESA-2009:1164)

CentOS 5 : tomcat5 (CESA-2008:0648)

CentOS 5 : tomcat5 (CESA-2010:0580)

CentOS 5 : tomcat5 (CESA-2011:0336)

CentOS 5 : tomcat5 (CESA-2011:1845)

CentOS 5 : tomcat5 (CESA-2012:0474)

CentOS 5 : tomcat5 (CESA-2013:0640)

CentOS 5 : tomcat5 (CESA-2013:0870)

CentOS 5 : udev (CESA-2009:0427)

CentOS 5 : vim (CESA-2007:0346)

CentOS 5 : vim (CESA-2008:0580)

CentOS 5 : w3m (CESA-2010:0565)

CentOS 5 : wireshark (CESA-2013:0125)

CentOS 5 : wireshark (CESA-2014:0341)

CentOS 5 : wireshark (CESA-2014:1677)

CentOS 5 : xen (CESA-2007:0323)

CentOS 5 : xen (CESA-2008:0194)

CentOS 5 : xen (CESA-2008:0892)

CentOS 5 : xen (CESA-2009:0003)

CentOS 5 : xen (CESA-2009:1472)

CentOS 5 : xen (CESA-2011:0496)

CentOS 5 : xen (CESA-2011:1401)

CentOS 5 : xen (CESA-2012:1130)

CentOS 5 : xen (CESA-2012:1236)

CentOS 5 : xen (CESA-2013:0241)

CentOS 5 : xen (CESA-2013:0599)

CentOS 5 : xen (CESA-2015:1002) (Venom)

CentOS 5 : xen (CESA-2015:2065)

CentOS 5 : xen (CESA-2016:2963)

CentOS 5 : xerces-j2 (CESA-2009:1615)

CentOS 5 : xinetd (CESA-2013:1302)

CentOS 5 : xorg-x11-apps / libX11 (CESA-2007:0157)

CentOS 5 : xorg-x11-server (CESA-2008:0031)

CentOS 5 : xorg-x11-server (CESA-2008:0504)

CentOS 5 : xorg-x11-server (CESA-2010:0382)

CentOS 5 : xorg-x11-server (CESA-2011:1359)

CentOS 5 : xorg-x11-server (CESA-2014:1982)

CentOS 5 : xorg-x11-server-utils (CESA-2011:0433)

CentOS 5 : xorg-x11-xfs (CESA-2007:0520)

CentOS 5 : xulrunner (CESA-2010:0809)

CentOS 5 : yum-updatesd (CESA-2014:1004)

CentOS 6 / 7 : 389-ds-base (CESA-2014:1031)

CentOS 6 / 7 : apr (CESA-2017:3270)

CentOS 6 / 7 : bind (CESA-2015:0672)

CentOS 6 / 7 : bind (CESA-2015:1513)

CentOS 6 / 7 : bind (CESA-2015:1705)

CentOS 6 / 7 : bind (CESA-2015:2655)

CentOS 6 / 7 : bluez (CESA-2017:2685) (BlueBorne)

CentOS 6 / 7 : cups (CESA-2015:1123)

CentOS 6 / 7 : expat (CESA-2016:2824)

CentOS 6 / 7 : firefox (CESA-2017:1440)

CentOS 6 / 7 : firefox (CESA-2017:2456)

CentOS 6 / 7 : firefox (CESA-2017:2831)

CentOS 6 / 7 : firefox (CESA-2017:3247)

CentOS 6 / 7 : firefox (CESA-2017:3382)

CentOS 6 / 7 : firefox (CESA-2018:0122)

CentOS 6 / 7 : firefox (CESA-2018:0549)

CentOS 6 / 7 : flac (CESA-2015:0767)

CentOS 6 / 7 : freetype (CESA-2015:0696)

CentOS 6 / 7 : gdk-pixbuf2 (CESA-2015:1694)

CentOS 6 / 7 : ghostscript (CESA-2017:1230)

CentOS 6 / 7 : git (CESA-2016:0496)

CentOS 6 / 7 : glibc (CESA-2015:0092) (GHOST)

CentOS 6 / 7 : gnutls (CESA-2016:0012) (SLOTH)

CentOS 6 / 7 : haproxy (CESA-2015:1741)

CentOS 6 / 7 : ImageMagick (CESA-2016:0726) (ImageTragick)

CentOS 6 / 7 : ImageMagick (CESA-2016:1237)

CentOS 6 / 7 : ipa (CESA-2016:1797)

CentOS 6 / 7 : ipa / libldb / libtalloc / libtdb / libtevent / openchange / samba / samba4 (CESA-2016:0612) (Badlock)

CentOS 6 / 7 : jakarta-taglibs-standard (CESA-2015:1695)

CentOS 6 / 7 : jasper (CESA-2014:2021)

CentOS 6 / 7 : jasper (CESA-2015:0074)

CentOS 6 / 7 : jasper (CESA-2017:1208)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2014:0889)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2014:1620)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2015:0067) (POODLE)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2015:0806)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2015:1229) (Bar Mitzvah) (Logjam)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2015:1920)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2017:1204)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2017:2424)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2017:3392)

CentOS 6 / 7 : java-1.7.0-openjdk (CESA-2018:0349)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2015:0809)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2015:1228) (Bar Mitzvah) (Logjam)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2015:1919)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2016:1458)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2016:2079)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2017:0180)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2017:1789)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2017:2998)

CentOS 6 / 7 : java-1.8.0-openjdk (CESA-2018:0095)

CentOS 6 / 7 : libgcrypt (CESA-2016:2674)

CentOS 6 / 7 : libldb (CESA-2016:0009)

CentOS 6 / 7 : libreoffice (CESA-2015:2619)

CentOS 6 / 7 : libssh2 (CESA-2016:0428)

CentOS 6 / 7 : libtiff (CESA-2017:0225)

CentOS 6 / 7 : libvncserver (CESA-2014:1826)

CentOS 6 / 7 : libwmf (CESA-2015:1917)

CentOS 6 / 7 : libXfont (CESA-2014:1870)

CentOS 6 / 7 : libXfont (CESA-2015:1708)

CentOS 6 / 7 : libxml2 (CESA-2014:1655)

CentOS 6 / 7 : libxml2 (CESA-2016:1292)

CentOS 6 / 7 : libyaml (CESA-2015:0100)

CentOS 6 / 7 : lzo (CESA-2014:0861)

CentOS 6 / 7 : mailx (CESA-2014:1999)

CentOS 6 / 7 : mercurial (CESA-2017:1576)

CentOS 6 / 7 : microcode\_ctl (CESA-2018:0093) (Spectre)

CentOS 6 / 7 : mutt (CESA-2018:2526)

CentOS 6 / 7 : net-snmp (CESA-2015:1636)

CentOS 6 / 7 : nspr / nss / nss-util (CESA-2015:1981)

CentOS 6 / 7 : nss (CESA-2016:0007) (SLOTH)

CentOS 6 / 7 : nss (CESA-2017:2832)

CentOS 6 / 7 : nss / nss-util (CESA-2015:1185) (Logjam)

CentOS 6 / 7 : nss / nss-util (CESA-2017:1100)

CentOS 6 / 7 : nss-softokn (CESA-2015:1699)

CentOS 6 / 7 : nss-util (CESA-2016:0370)

CentOS 6 / 7 : ntp (CESA-2014:2024)

CentOS 6 / 7 : ntp (CESA-2015:1930)

CentOS 6 / 7 : ntp (CESA-2016:0063)

CentOS 6 / 7 : ntp (CESA-2016:1141)

CentOS 6 / 7 : ntp (CESA-2017:0252)

CentOS 6 / 7 : openssl (CESA-2014:1052)

CentOS 6 / 7 : openssl (CESA-2014:1652)

CentOS 6 / 7 : openssl (CESA-2015:0066)

CentOS 6 / 7 : openssl (CESA-2015:1072) (Logjam)

CentOS 6 / 7 : openssl (CESA-2015:1115)

CentOS 6 / 7 : openssl (CESA-2015:2617)

CentOS 6 / 7 : openssl (CESA-2016:0008) (SLOTH)

CentOS 6 / 7 : openssl (CESA-2016:0301) (DROWN)

CentOS 6 / 7 : openssl (CESA-2016:1940)

CentOS 6 / 7 : openssl (CESA-2017:0286)

CentOS 6 / 7 : openssl098e (CESA-2016:0372) (DROWN)

CentOS 6 / 7 : pam (CESA-2015:1640)

CentOS 6 / 7 : pcs (CESA-2015:1700)

CentOS 6 / 7 : php (CESA-2014:1767)

CentOS 6 / 7 : policycoreutils (CESA-2016:2702)

CentOS 6 / 7 : postgresql (CESA-2015:0750)

CentOS 6 / 7 : postgresql (CESA-2015:1194)

CentOS 6 / 7 : python (CESA-2016:1626) (httpoxy)

CentOS 6 / 7 : python-twisted-web (CESA-2016:1978)

CentOS 6 / 7 : rpcbind (CESA-2016:0005)

CentOS 6 / 7 : samba (CESA-2016:0448)

CentOS 6 / 7 : samba (CESA-2017:1270) (SambaCry)

CentOS 6 / 7 : sudo (CESA-2016:2872)

CentOS 6 / 7 : sudo (CESA-2017:1382)

CentOS 6 / 7 : sudo (CESA-2017:1574)

CentOS 6 / 7 : thunderbird (CESA-2017:1201)

CentOS 6 / 7 : thunderbird (CESA-2017:1561)

CentOS 6 / 7 : thunderbird (CESA-2017:2534)

CentOS 6 / 7 : thunderbird (CESA-2017:2885)

CentOS 6 / 7 : thunderbird (CESA-2017:3372)

CentOS 6 / 7 : thunderbird (CESA-2018:0061)

CentOS 6 / 7 : thunderbird (CESA-2018:0262)

CentOS 6 / 7 : unzip (CESA-2015:0700)

CentOS 6 / 7 : vim (CESA-2016:2972)

CentOS 6 / 7 : wget (CESA-2014:1764)

CentOS 6 / 7 : wireshark (CESA-2014:1676)

CentOS 6 / 7 : xerces-j2 (CESA-2014:1319)

CentOS 6 / 7 : xorg-x11-server (CESA-2014:1983)

CentOS 6 / 7 : xorg-x11-server (CESA-2015:0797)

CentOS 6 : 389-ds-base (CESA-2012:0813)

CentOS 6 : 389-ds-base (CESA-2012:0997)

CentOS 6 : 389-ds-base (CESA-2013:0503)

CentOS 6 : 389-ds-base (CESA-2013:0628)

CentOS 6 : 389-ds-base (CESA-2013:0742)

CentOS 6 : 389-ds-base (CESA-2013:1119)

CentOS 6 : 389-ds-base (CESA-2013:1182)

CentOS 6 : 389-ds-base (CESA-2013:1752)

CentOS 6 : 389-ds-base (CESA-2014:0292)

CentOS 6 : 389-ds-base (CESA-2016:2765)

CentOS 6 : 389-ds-base (CESA-2017:0893)

CentOS 6 : 389-ds-base (CESA-2018:0515)

CentOS 6 : 389-ds-base (CESA-2018:1364)

CentOS 6 : abrt (CESA-2012:0841)

CentOS 6 : abrt / libreport (CESA-2013:0215)

CentOS 6 : augeas (CESA-2013:1537)

CentOS 6 : augeas (CESA-2014:0044)

CentOS 6 : autofs (CESA-2015:1344)

CentOS 6 : automake (CESA-2013:0526)

CentOS 6 : bash (CESA-2017:0725)

CentOS 6 : bind (CESA-2012:1268)

CentOS 6 : bind (CESA-2012:1549)

CentOS 6 : bind (CESA-2013:0550)

CentOS 6 : bind (CESA-2013:0689)

CentOS 6 : bind (CESA-2013:1114)

CentOS 6 : bind (CESA-2014:0043)

CentOS 6 : bind (CESA-2015:1471)

CentOS 6 : bind (CESA-2017:1105)

CentOS 6 : bind (CESA-2017:1202)

CentOS 6 : bind (CESA-2017:1679)

CentOS 6 : bind (CESA-2018:0101)

CentOS 6 : bind (CESA-2018:2571)

CentOS 6 : bind (CESA-2019:1492)

CentOS 6 : bind-dyndb-ldap (CESA-2012:0683)

CentOS 6 : bind-dyndb-ldap (CESA-2012:1139)

CentOS 6 : busybox (CESA-2012:0810)

CentOS 6 : busybox (CESA-2013:1732)

CentOS 6 : ca-certificates (CESA-2013:1866)

CentOS 6 : ccid (CESA-2013:0523)

CentOS 6 : cheese / control-center / ekiga / evolution / evolution-data-server / etcgnome-panel / etc (CESA-2013:1540)

CentOS 6 : cifs-utils (CESA-2012:0902)

CentOS 6 : coreutils (CESA-2013:1652)

CentOS 6 : coreutils (CESA-2017:0654)

CentOS 6 : cups (CESA-2014:1388)

CentOS 6 : curl (CESA-2014:0561)

CentOS 6 : curl (CESA-2015:1254)

CentOS 6 : dbus (CESA-2012:1261)

CentOS 6 : dbus (CESA-2019:1726)

CentOS 6 : dhcp (CESA-2011:1819)

CentOS 6 : dhcp (CESA-2012:1141)

CentOS 6 : dhcp (CESA-2013:0504)

CentOS 6 : dhcp (CESA-2018:0469)

CentOS 6 : dhcp (CESA-2018:1454)

CentOS 6 : ding-libs / sssd (CESA-2018:1877)

CentOS 6 : dnsmasq (CESA-2013:0277)

CentOS 6 : dnsmasq (CESA-2017:2838)

CentOS 6 : dovecot (CESA-2013:0520)

CentOS 6 : dovecot (CESA-2014:0790)

CentOS 6 : dovecot (CESA-2019:2885)

CentOS 6 : evolution (CESA-2013:0516)

CentOS 6 : evolution-mapi / openchange (CESA-2013:0515)

CentOS 6 : file (CESA-2014:1606)

CentOS 6 : file (CESA-2016:0760)

CentOS 6 : firefox (CESA-2017:1104)

CentOS 6 : firefox (CESA-2018:0526)

CentOS 6 : firefox (CESA-2018:1098)

CentOS 6 : firefox (CESA-2018:1414)

CentOS 6 : firefox (CESA-2018:2112)

CentOS 6 : firefox (CESA-2018:2693)

CentOS 6 : firefox (CESA-2018:2834)

CentOS 6 : firefox (CESA-2018:2881)

CentOS 6 : firefox (CESA-2018:3006)

CentOS 6 : firefox (CESA-2018:3831)

CentOS 6 : firefox (CESA-2019:0218)

CentOS 6 : firefox (CESA-2019:0373)

CentOS 6 : firefox (CESA-2019:0623)

CentOS 6 : firefox (CESA-2019:0672)

CentOS 6 : firefox (CESA-2019:1267)

CentOS 6 : firefox (CESA-2019:1604)

CentOS 6 : firefox (CESA-2019:1765)

CentOS 6 : firefox (CESA-2019:2694)

CentOS 6 : firefox (CESA-2019:3281)

CentOS 6 : firefox (CESA-2019:4108)

CentOS 6 : firefox (CESA-2020:0086)

CentOS 6 : firefox (CESA-2020:0521)

CentOS 6 : firefox (CESA-2020:0816)

CentOS 6 : firefox (CESA-2020:1339)

CentOS 6 : foomatic (CESA-2016:0491)

CentOS 6 : freeradius (CESA-2012:1326)

CentOS 6 : freeradius (CESA-2015:1287)

CentOS 6 : freeradius (CESA-2017:1759)

CentOS 6 : freetype (CESA-2019:4254)

CentOS 6 : gc (CESA-2013:1500)

CentOS 6 : gdb (CESA-2013:0522)

CentOS 6 : gegl (CESA-2012:1455)

CentOS 6 : ghostscript (CESA-2017:0014)

CentOS 6 : ghostscript (CESA-2018:3760)

CentOS 6 : gimp (CESA-2012:1180)

CentOS 6 : git (CESA-2013:0589)

CentOS 6 : git (CESA-2017:2485)

CentOS 6 : git (CESA-2020:0316)

CentOS 6 : glibc (CESA-2012:0058)

CentOS 6 : glibc (CESA-2012:0393)

CentOS 6 : glibc (CESA-2012:1098)

CentOS 6 : glibc (CESA-2012:1208)

CentOS 6 : glibc (CESA-2013:1605)

CentOS 6 : glibc (CESA-2014:1391)

CentOS 6 : glibc (CESA-2015:0016)

CentOS 6 : glibc (CESA-2015:0863)

CentOS 6 : glibc (CESA-2016:0175)

CentOS 6 : glibc (CESA-2017:0680)

CentOS 6 : glibc (CESA-2017:1480) (Stack Clash)

CentOS 6 : glibc (CESA-2018:1879)

CentOS 6 : glusterfs (CESA-2018:2892)

CentOS 6 : gnupg2 (CESA-2018:2180)

CentOS 6 : gnutls (CESA-2012:0429)

CentOS 6 : gnutls (CESA-2014:0246)

CentOS 6 : gnutls (CESA-2014:0595)

CentOS 6 : gnutls (CESA-2015:1457)

CentOS 6 : gnutls (CESA-2017:0574)

CentOS 6 : grep (CESA-2015:1447)

CentOS 6 : gstreamer-plugins-bad-free (CESA-2016:2974)

CentOS 6 : gstreamer-plugins-good (CESA-2016:2975)

CentOS 6 : haproxy (CESA-2013:0868)

CentOS 6 : haproxy (CESA-2013:1120)

CentOS 6 : hivex (CESA-2015:1378)

CentOS 6 : hplip (CESA-2013:0500)

CentOS 6 : hplip (CESA-2013:1274)

CentOS 6 : httpd (CESA-2012:0128)

CentOS 6 : httpd (CESA-2013:0512)

CentOS 6 : httpd (CESA-2014:0370)

CentOS 6 : httpd (CESA-2015:1249)

CentOS 6 : httpd (CESA-2015:1668)

CentOS 6 : httpd (CESA-2017:1721)

CentOS 6 : httpd (CESA-2017:2478)

CentOS 6 : httpd (CESA-2017:2972) (Optionsbleed)

CentOS 6 : ibacm / ibsim / ibutils / infiniband-diags / infinipath-psm / libibmad / libibumad / etc (CESA-2013:0509)

CentOS 6 : ibutils / infinipath-psm / libibverbs / libmlx4 / librdmacm / mpitests / mstflint / etc (CESA-2013:1661)

CentOS 6 : icedtea-web (CESA-2012:1132)

CentOS 6 : icedtea-web (CESA-2012:1434)

CentOS 6 : icedtea-web (CESA-2013:0753)

CentOS 6 : icedtea-web (CESA-2016:0778)

CentOS 6 : icu (CESA-2020:0896)

CentOS 6 : ImageMagick (CESA-2012:0544)

CentOS 6 : Important: / ruby193-libyaml (CESA-2014:0355)

CentOS 6 : ipa (CESA-2013:0188)

CentOS 6 : ipa (CESA-2013:0528)

CentOS 6 : ipa (CESA-2015:1462)

CentOS 6 : ipmitool (CESA-2011:1814)

CentOS 6 : ipmitool (CESA-2020:1331)

CentOS 6 : jakarta-commons-collections (CESA-2015:2521)

CentOS 6 : jasper (CESA-2011:1807)

CentOS 6 : java-1.6.0-openjdk (CESA-2012:0135)

CentOS 6 : java-1.6.0-openjdk (CESA-2012:0729)

CentOS 6 : java-1.6.0-openjdk (CESA-2012:1221)

CentOS 6 : java-1.6.0-openjdk (CESA-2012:1384) (ROBOT)

CentOS 6 : java-1.6.0-openjdk (CESA-2013:0245)

CentOS 6 : java-1.6.0-openjdk (CESA-2013:0273)

CentOS 6 : java-1.6.0-openjdk (CESA-2013:0605)

CentOS 6 : java-1.7.0-openjdk (CESA-2012:1009)

CentOS 6 : java-1.7.0-openjdk (CESA-2012:1223)

CentOS 6 : java-1.7.0-openjdk (CESA-2012:1386) (ROBOT)

CentOS 6 : java-1.7.0-openjdk (CESA-2013:0602)

CentOS 6 : java-1.7.0-openjdk (CESA-2013:0751)

CentOS 6 : java-1.7.0-openjdk (CESA-2013:0957)

CentOS 6 : java-1.7.0-openjdk (CESA-2013:1451)

CentOS 6 : java-1.7.0-openjdk (CESA-2014:0026)

CentOS 6 : java-1.7.0-openjdk (CESA-2014:0406)

CentOS 6 : java-1.7.0-openjdk (CESA-2016:0053) (SLOTH)

CentOS 6 : java-1.7.0-openjdk (CESA-2016:0511)

CentOS 6 : java-1.7.0-openjdk (CESA-2016:0675)

CentOS 6 : java-1.7.0-openjdk (CESA-2018:1270)

CentOS 6 : java-1.7.0-openjdk (CESA-2018:1647) (Spectre)

CentOS 6 : java-1.7.0-openjdk (CESA-2018:2283)

CentOS 6 : java-1.7.0-openjdk (CESA-2018:3409)

CentOS 6 : java-1.7.0-openjdk (CESA-2019:0462)

CentOS 6 : java-1.7.0-openjdk (CESA-2019:0790)

CentOS 6 : java-1.7.0-openjdk (CESA-2019:1840)

CentOS 6 : java-1.7.0-openjdk (CESA-2019:3158)

CentOS 6 : java-1.7.0-openjdk (CESA-2020:0632)

CentOS 6 : java-1.8.0-openjdk (CESA-2014:1636)

CentOS 6 : java-1.8.0-openjdk (CESA-2015:0069) (POODLE)

CentOS 6 : java-1.8.0-openjdk (CESA-2016:0050) (SLOTH)

CentOS 6 : java-1.8.0-openjdk (CESA-2016:0514)

CentOS 6 : java-1.8.0-openjdk (CESA-2016:0651)

CentOS 6 : java-1.8.0-openjdk (CESA-2017:1109)

CentOS 6 : java-1.8.0-openjdk (CESA-2018:1188)

CentOS 6 : java-1.8.0-openjdk (CESA-2018:1650) (Spectre)

CentOS 6 : java-1.8.0-openjdk (CESA-2018:2241)

CentOS 6 : java-1.8.0-openjdk (CESA-2018:2943)

CentOS 6 : java-1.8.0-openjdk (CESA-2019:0416)

CentOS 6 : java-1.8.0-openjdk (CESA-2019:0774)

CentOS 6 : java-1.8.0-openjdk (CESA-2019:1811)

CentOS 6 : java-1.8.0-openjdk (CESA-2019:3136)

CentOS 6 : java-1.8.0-openjdk (CESA-2020:0157)

CentOS 6 : kdelibs (CESA-2012:1416)

CentOS 6 : kdelibs (CESA-2012:1418)

CentOS 6 : kernel (CESA-2011:1849)

CentOS 6 : kernel (CESA-2012:0052)

CentOS 6 : kernel (CESA-2012:0350)

CentOS 6 : kernel (CESA-2012:0481)

CentOS 6 : kernel (CESA-2012:0571)

CentOS 6 : kernel (CESA-2012:0743)

CentOS 6 : kernel (CESA-2012:0862)

CentOS 6 : kernel (CESA-2012:1064)

CentOS 6 : kernel (CESA-2012:1156)

CentOS 6 : kernel (CESA-2012:1304)

CentOS 6 : kernel (CESA-2012:1366)

CentOS 6 : kernel (CESA-2012:1426)

CentOS 6 : kernel (CESA-2012:1580)

CentOS 6 : kernel (CESA-2013:0223)

CentOS 6 : kernel (CESA-2013:0496)

CentOS 6 : kernel (CESA-2013:0567)

CentOS 6 : kernel (CESA-2013:0630)

CentOS 6 : kernel (CESA-2013:0744)

CentOS 6 : kernel (CESA-2013:0830)

CentOS 6 : kernel (CESA-2013:0911)

CentOS 6 : kernel (CESA-2013:1051)

CentOS 6 : kernel (CESA-2013:1173)

CentOS 6 : kernel (CESA-2013:1436)

CentOS 6 : kernel (CESA-2013:1645)

CentOS 6 : kernel (CESA-2013:1801)

CentOS 6 : kernel (CESA-2014:0159)

CentOS 6 : kernel (CESA-2014:0328)

CentOS 6 : kernel (CESA-2014:0475)

CentOS 6 : kernel (CESA-2014:0771)

CentOS 6 : kernel (CESA-2014:0924)

CentOS 6 : kernel (CESA-2014:0981)

CentOS 6 : kernel (CESA-2014:1167)

CentOS 6 : kernel (CESA-2014:1392)

CentOS 6 : kernel (CESA-2014:1843)

CentOS 6 : kernel (CESA-2014:1997)

CentOS 6 : kernel (CESA-2015:0087)

CentOS 6 : kernel (CESA-2015:0674)

CentOS 6 : kernel (CESA-2015:0864)

CentOS 6 : kernel (CESA-2015:1081)

CentOS 6 : kernel (CESA-2015:1221)

CentOS 6 : kernel (CESA-2015:1272)

CentOS 6 : kernel (CESA-2015:1623)

CentOS 6 : kernel (CESA-2015:2636)

CentOS 6 : kernel (CESA-2016:0494)

CentOS 6 : kernel (CESA-2016:0715)

CentOS 6 : kernel (CESA-2016:0855)

CentOS 6 : kernel (CESA-2016:1406)

CentOS 6 : kernel (CESA-2016:1664)

CentOS 6 : kernel (CESA-2016:2006)

CentOS 6 : kernel (CESA-2016:2105) (Dirty COW)

CentOS 6 : kernel (CESA-2016:2766)

CentOS 6 : kernel (CESA-2017:0036)

CentOS 6 : kernel (CESA-2017:0293)

CentOS 6 : kernel (CESA-2017:0307)

CentOS 6 : kernel (CESA-2017:0817)

CentOS 6 : kernel (CESA-2017:0892)

CentOS 6 : kernel (CESA-2017:1372)

CentOS 6 : kernel (CESA-2017:1486) (Stack Clash)

CentOS 6 : kernel (CESA-2017:1723)

CentOS 6 : kernel (CESA-2017:2681) (BlueBorne)

CentOS 6 : kernel (CESA-2017:2795)

CentOS 6 : kernel (CESA-2017:2863)

CentOS 6 : kernel (CESA-2017:3200)

CentOS 6 : kernel (CESA-2018:0008) (Meltdown) (Spectre)

CentOS 6 : kernel (CESA-2018:0169)

CentOS 6 : kernel (CESA-2018:0512) (Meltdown) (Spectre)

CentOS 6 : kernel (CESA-2018:1319) (Meltdown)

CentOS 6 : kernel (CESA-2018:1651) (Spectre)

CentOS 6 : kernel (CESA-2018:1854) (Spectre)

CentOS 6 : kernel (CESA-2018:2164) (Spectre)

CentOS 6 : kernel (CESA-2018:2390) (Foreshadow)

CentOS 6 : kernel (CESA-2018:2846)

CentOS 6 : kernel (CESA-2019:0415)

CentOS 6 : kernel (CESA-2019:0717)

CentOS 6 : kernel (CESA-2019:1169) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

CentOS 6 : kernel (CESA-2019:1488) (SACK Panic) (SACK Slowness)

CentOS 6 : kernel (CESA-2019:2473)

CentOS 6 : kernel (CESA-2019:2736)

CentOS 6 : kernel (CESA-2019:2863)

CentOS 6 : kernel (CESA-2019:3836)

CentOS 6 : kernel (CESA-2019:3878)

CentOS 6 : kernel (CESA-2019:4256)

CentOS 6 : kernel (CESA-2020:0790)

CentOS 6 : krb5 (CESA-2011:1790)

CentOS 6 : krb5 (CESA-2012:1131)

CentOS 6 : krb5 (CESA-2013:0656)

CentOS 6 : krb5 (CESA-2013:0748)

CentOS 6 : krb5 (CESA-2014:1389)

CentOS 6 : krb5 (CESA-2015:0794)

CentOS 6 : krb5 (CESA-2016:0493)

CentOS 6 : krb5-appl (CESA-2011:1852)

CentOS 6 : krb5-appl (CESA-2020:1349)

CentOS 6 : ksh (CESA-2020:0515)

CentOS 6 : libarchive (CESA-2016:1850)

CentOS 6 : libguestfs (CESA-2012:0774)

CentOS 6 : libguestfs (CESA-2013:1536)

CentOS 6 : libguestfs (CESA-2017:0564)

CentOS 6 : libjpeg-turbo (CESA-2013:1803)

CentOS 6 : libpng (CESA-2015:2594)

CentOS 6 : libproxy (CESA-2012:1461)

CentOS 6 : librelp (CESA-2018:1225)

CentOS 6 : libreoffice (CESA-2012:1135)

CentOS 6 : libreoffice (CESA-2015:1458)

CentOS 6 : libreoffice (CESA-2017:0979)

CentOS 6 : libreoffice (CESA-2018:0517)

CentOS 6 : libreport (CESA-2015:2504)

CentOS 6 : librsvg2 (CESA-2014:0127)

CentOS 6 : libssh2 (CESA-2019:1652)

CentOS 6 : libtar (CESA-2013:1418)

CentOS 6 : libtasn1 (CESA-2012:0427)

CentOS 6 : libtasn1 (CESA-2014:0596)

CentOS 6 : libtiff (CESA-2014:0222)

CentOS 6 : libtiff (CESA-2016:1547)

CentOS 6 : libtirpc (CESA-2013:0884)

CentOS 6 : libtirpc (CESA-2017:1268)

CentOS 6 : libuser (CESA-2015:1482)

CentOS 6 : libvirt (CESA-2012:0748)

CentOS 6 : libvirt (CESA-2012:1202)

CentOS 6 : libvirt (CESA-2012:1359)

CentOS 6 : libvirt (CESA-2013:0199)

CentOS 6 : libvirt (CESA-2013:0276)

CentOS 6 : libvirt (CESA-2013:0831)

CentOS 6 : libvirt (CESA-2013:1272)

CentOS 6 : libvirt (CESA-2014:0103)

CentOS 6 : libvirt (CESA-2014:0560)

CentOS 6 : libvirt (CESA-2014:1873)

CentOS 6 : libvirt (CESA-2018:0030) (Spectre)

CentOS 6 : libvirt (CESA-2018:1669) (Spectre)

CentOS 6 : libvirt (CESA-2018:1929)

CentOS 6 : libvirt (CESA-2019:1180) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

CentOS 6 : libvirt (CESA-2019:1578)

CentOS 6 : libvorbis (CESA-2018:0649)

CentOS 6 : libX11 / libXcursor / libXext / libXfixes / libXi / libXinerama / libXp / libXrandr / etc (CESA-2014:1436)

CentOS 6 : libxml2 (CESA-2012:0018)

CentOS 6 : libxml2 (CESA-2012:0324)

CentOS 6 : libxml2 (CESA-2014:0513)

CentOS 6 : libxml2 (CESA-2015:1419)

CentOS 6 : libxml2 (CESA-2015:2549)

CentOS 6 : luci (CESA-2013:1603)

CentOS 6 : luci (CESA-2014:1390)

CentOS 6 : mailman (CESA-2015:1417)

CentOS 6 : mailman (CESA-2018:0504)

CentOS 6 : mariadb55-mariadb (CESA-2014:0189)

CentOS 6 : memcached (CESA-2016:2820)

CentOS 6 : mesa (CESA-2013:0897)

CentOS 6 : microcode\_ctl (CESA-2018:0013) (Spectre)

CentOS 6 : mingw32-libxml2 (CESA-2013:0217)

CentOS 6 : mod\_auth\_mellon (CESA-2014:1803)

CentOS 6 : mod\_perl (CESA-2018:2737)

CentOS 6 : mod\_wsgi (CESA-2014:0788)

CentOS 6 : Moderate: / mariadb55-mariadb (CESA-2014:0522)

CentOS 6 : Moderate: / mysql55-mysql (CESA-2014:0537)

CentOS 6 : Moderate: / ruby193-rubygem-actionpack (CESA-2014:0510)

CentOS 6 : mutt (CESA-2014:0304)

CentOS 6 : mysql (CESA-2012:0105)

CentOS 6 : mysql (CESA-2012:0874)

CentOS 6 : mysql (CESA-2012:1462)

CentOS 6 : mysql (CESA-2012:1551)

CentOS 6 : mysql (CESA-2013:0219)

CentOS 6 : mysql (CESA-2013:0772)

CentOS 6 : mysql (CESA-2014:0164)

CentOS 6 : mysql (CESA-2017:0184)

CentOS 6 : mysql55-mysql (CESA-2014:0173)

CentOS 6 : net-snmp (CESA-2012:0876)

CentOS 6 : net-snmp (CESA-2014:0321)

CentOS 6 : net-snmp (CESA-2015:1385)

CentOS 6 : nspluginwrapper (CESA-2012:1459)

CentOS 6 : nspr (CESA-2013:0213)

CentOS 6 : nspr / nss / nss-util (CESA-2013:1829)

CentOS 6 : nspr / nss / nss-util (CESA-2014:0917)

CentOS 6 : nspr / nss / nss-util (CESA-2016:0591)

CentOS 6 : nss (CESA-2012:0973)

CentOS 6 : nss (CESA-2012:1091)

CentOS 6 : nss (CESA-2017:1364)

CentOS 6 : nss (CESA-2018:2898)

CentOS 6 : nss / nss-util / nss-softokn / nspr (CESA-2013:1144)

CentOS 6 : nss-pam-ldapd (CESA-2013:0590)

CentOS 6 : nss-softokn (CESA-2019:4152)

CentOS 6 : ntp (CESA-2015:1459)

CentOS 6 : ntp (CESA-2016:0780)

CentOS 6 : ntp (CESA-2017:3071)

CentOS 6 : ntp (CESA-2018:3854)

CentOS 6 : ocaml (CESA-2017:0565)

CentOS 6 : openjpeg (CESA-2012:1068)

CentOS 6 : openjpeg (CESA-2012:1283)

CentOS 6 : openjpeg (CESA-2013:1850)

CentOS 6 : openjpeg (CESA-2017:0559)

CentOS 6 : openldap (CESA-2012:0899)

CentOS 6 : openldap (CESA-2012:1151)

CentOS 6 : openldap (CESA-2014:0126)

CentOS 6 : openslp (CESA-2018:2308)

CentOS 6 : openslp (CESA-2020:0199)

CentOS 6 : openssh (CESA-2012:0884)

CentOS 6 : openssh (CESA-2013:0519)

CentOS 6 : openssh (CESA-2013:1591)

CentOS 6 : openssh (CESA-2014:1552)

CentOS 6 : openssh (CESA-2016:0466)

CentOS 6 : openssh (CESA-2016:0741)

CentOS 6 : openssh (CESA-2017:0641)

CentOS 6 : openssh (CESA-2017:2563)

CentOS 6 : openssh (CESA-2019:0711)

CentOS 6 : openssl (CESA-2012:0059)

CentOS 6 : openssl (CESA-2014:0015)

CentOS 6 : openssl (CESA-2014:0376)

CentOS 6 : openssl (CESA-2014:0625)

CentOS 6 : openssl (CESA-2015:0715)

CentOS 6 : openssl (CESA-2016:0996)

CentOS 6 : openssl (CESA-2019:2471)

CentOS 6 : pacemaker (CESA-2013:1635)

CentOS 6 : pacemaker (CESA-2015:1424)

CentOS 6 : pacemaker (CESA-2016:2675)

CentOS 6 : pam (CESA-2013:0521)

CentOS 6 : patch (CESA-2018:1199)

CentOS 6 : pcs (CESA-2015:0990)

CentOS 6 : pcs (CESA-2018:1927)

CentOS 6 : pcsc-lite (CESA-2013:0525)

CentOS 6 : php (CESA-2012:1046)

CentOS 6 : php (CESA-2013:0514)

CentOS 6 : php (CESA-2013:1615)

CentOS 6 : php (CESA-2015:1218)

CentOS 6 : php (CESA-2016:1609) (httpoxy)

CentOS 6 : php (CESA-2019:3287)

CentOS 6 : php-pecl-apc (CESA-2012:0811)

CentOS 6 : pidgin (CESA-2011:1821)

CentOS 6 : piranha (CESA-2014:0175)

CentOS 6 : pixman (CESA-2013:0687)

CentOS 6 : pki-core (CESA-2013:0511)

CentOS 6 : pki-core (CESA-2015:1347)

CentOS 6 : polkit (CESA-2013:1270)

CentOS 6 : polkit (CESA-2019:0420)

CentOS 6 : poppler (CESA-2017:2550)

CentOS 6 : postgresql (CESA-2015:2081)

CentOS 6 : postgresql (CESA-2016:0347)

CentOS 6 : postgresql (CESA-2017:2860)

CentOS 6 : postgresql92-postgresql (CESA-2014:0221)

CentOS 6 : ppp (CESA-2020:0631)

CentOS 6 : procps (CESA-2018:1777)

CentOS 6 : python (CESA-2012:0744)

CentOS 6 : python (CESA-2013:1582)

CentOS 6 : python (CESA-2015:1330)

CentOS 6 : python (CESA-2019:1467)

CentOS 6 : python-imaging (CESA-2020:0898)

CentOS 6 : python-jinja2 (CESA-2014:0747)

CentOS 6 : python-paramiko (CESA-2018:1124)

CentOS 6 : python-paramiko (CESA-2018:3406)

CentOS 6 : python-paste-script (CESA-2012:1206)

CentOS 6 : python-reportlab (CESA-2020:0197)

CentOS 6 : python-sqlalchemy (CESA-2012:0369)

CentOS 6 : qemu-kvm (CESA-2011:1777)

CentOS 6 : qemu-kvm (CESA-2011:1801)

CentOS 6 : qemu-kvm (CESA-2012:0050)

CentOS 6 : qemu-kvm (CESA-2012:1234)

CentOS 6 : qemu-kvm (CESA-2013:0609)

CentOS 6 : qemu-kvm (CESA-2013:0896)

CentOS 6 : qemu-kvm (CESA-2013:1100)

CentOS 6 : qemu-kvm (CESA-2013:1553)

CentOS 6 : qemu-kvm (CESA-2014:0420)

CentOS 6 : qemu-kvm (CESA-2014:0743)

CentOS 6 : qemu-kvm (CESA-2014:1075)

CentOS 6 : qemu-kvm (CESA-2015:0867)

CentOS 6 : qemu-kvm (CESA-2015:0998) (Venom)

CentOS 6 : qemu-kvm (CESA-2015:1087)

CentOS 6 : qemu-kvm (CESA-2015:1833)

CentOS 6 : qemu-kvm (CESA-2015:1924)

CentOS 6 : qemu-kvm (CESA-2015:2694)

CentOS 6 : qemu-kvm (CESA-2016:0082)

CentOS 6 : qemu-kvm (CESA-2016:0997)

CentOS 6 : qemu-kvm (CESA-2016:1585)

CentOS 6 : qemu-kvm (CESA-2017:0309)

CentOS 6 : qemu-kvm (CESA-2017:0352)

CentOS 6 : qemu-kvm (CESA-2017:0621)

CentOS 6 : qemu-kvm (CESA-2017:1206)

CentOS 6 : qemu-kvm (CESA-2018:0516)

CentOS 6 : qemu-kvm (CESA-2018:1660) (Spectre)

CentOS 6 : qemu-kvm (CESA-2018:2162) (Spectre)

CentOS 6 : qemu-kvm (CESA-2019:1181) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

CentOS 6 : qemu-kvm (CESA-2019:1650)

CentOS 6 : qemu-kvm (CESA-2019:2892)

CentOS 6 : qemu-kvm (CESA-2020:0775)

CentOS 6 : qpid (CESA-2012:1269)

CentOS 6 : qt (CESA-2012:0880)

CentOS 6 : qt (CESA-2013:0669)

CentOS 6 : quagga (CESA-2012:1259)

CentOS 6 : quagga (CESA-2017:0794)

CentOS 6 : raptor (CESA-2012:0410)

CentOS 6 : rpcbind (CESA-2017:1267)

CentOS 6 : rsyslog (CESA-2012:0796)

CentOS 6 : rsyslog7 (CESA-2014:1654)

CentOS 6 : rtkit (CESA-2013:1282)

CentOS 6 : ruby (CESA-2012:0069)

CentOS 6 : ruby (CESA-2013:0612)

CentOS 6 : ruby (CESA-2013:1764)

CentOS 6 : ruby (CESA-2014:1911)

CentOS 6 : ruby193-rubygem-actionpack (CESA-2014:0306)

CentOS 6 : rubygems (CESA-2013:1441)

CentOS 6 : samba (CESA-2013:1542)

CentOS 6 : samba (CESA-2015:0251)

CentOS 6 : samba (CESA-2016:0011)

CentOS 6 : samba (CESA-2016:0611) (Badlock)

CentOS 6 : samba (CESA-2017:0662)

CentOS 6 : samba (CESA-2017:2789)

CentOS 6 : samba (CESA-2018:1860)

CentOS 6 : samba4 (CESA-2013:0506)

CentOS 6 : samba4 (CESA-2013:1543)

CentOS 6 : samba4 (CESA-2013:1805)

CentOS 6 : samba4 (CESA-2014:0383)

CentOS 6 : samba4 (CESA-2014:1009)

CentOS 6 : samba4 (CESA-2015:0250)

CentOS 6 : samba4 (CESA-2016:0010)

CentOS 6 : samba4 (CESA-2016:0449)

CentOS 6 : samba4 (CESA-2016:1487)

CentOS 6 : samba4 (CESA-2017:0744)

CentOS 6 : samba4 (CESA-2017:1271) (SambaCry)

CentOS 6 : samba4 (CESA-2017:2791)

CentOS 6 : samba4 (CESA-2018:1883)

CentOS 6 : sblim-cim-client2 (CESA-2012:0987)

CentOS 6 : setroubleshoot / setroubleshoot-plugins (CESA-2016:1267)

CentOS 6 : sos (CESA-2012:0958)

CentOS 6 : sos (CESA-2016:0152)

CentOS 6 : spice-gtk (CESA-2012:1284)

CentOS 6 : spice-gtk (CESA-2013:1273)

CentOS 6 : spice-gtk (CESA-2020:0471)

CentOS 6 : spice-gtk / spice-server (CESA-2018:2732)

CentOS 6 : spice-server (CESA-2013:1192)

CentOS 6 : spice-server (CESA-2013:1473)

CentOS 6 : spice-server (CESA-2015:1715)

CentOS 6 : spice-server (CESA-2015:1889)

CentOS 6 : spice-server (CESA-2016:1204)

CentOS 6 : spice-server (CESA-2017:0253)

CentOS 6 : spice-server (CESA-2018:3522)

CentOS 6 : spice-server (CESA-2019:0232)

CentOS 6 : sqlite (CESA-2015:1634)

CentOS 6 : squid (CESA-2011:1791)

CentOS 6 : squid (CESA-2013:0505)

CentOS 6 : squid (CESA-2014:0597)

CentOS 6 : squid (CESA-2016:1138)

CentOS 6 : squid (CESA-2016:1573)

CentOS 6 : squid34 (CESA-2016:1140)

CentOS 6 : squid34 (CESA-2017:0183)

CentOS 6 : sssd (CESA-2013:0508)

CentOS 6 : sssd (CESA-2013:0663)

CentOS 6 : sssd (CESA-2015:2019)

CentOS 6 : stunnel (CESA-2013:0714)

CentOS 6 : subversion (CESA-2015:0165)

CentOS 6 : subversion (CESA-2015:1633)

CentOS 6 : sudo (CESA-2013:1701)

CentOS 6 : sudo (CESA-2015:1409)

CentOS 6 : sudo (CESA-2019:3755)

CentOS 6 : sudo (CESA-2020:0726)

CentOS 6 : t1lib (CESA-2012:0062)

CentOS 6 : telnet (CESA-2020:1335)

CentOS 6 : texlive (CESA-2012:0137)

CentOS 6 : thunderbird (CESA-2012:0080)

CentOS 6 : thunderbird (CESA-2012:0140)

CentOS 6 : thunderbird (CESA-2018:0647)

CentOS 6 : thunderbird (CESA-2018:1726)

CentOS 6 : thunderbird (CESA-2018:2251)

CentOS 6 : thunderbird (CESA-2018:3403)

CentOS 6 : thunderbird (CESA-2018:3531)

CentOS 6 : thunderbird (CESA-2019:0159)

CentOS 6 : thunderbird (CESA-2019:0269)

CentOS 6 : thunderbird (CESA-2019:0680)

CentOS 6 : thunderbird (CESA-2019:1310)

CentOS 6 : thunderbird (CESA-2019:1624)

CentOS 6 : thunderbird (CESA-2019:1777)

CentOS 6 : thunderbird (CESA-2019:3756)

CentOS 6 : thunderbird (CESA-2019:4205)

CentOS 6 : thunderbird (CESA-2020:0123)

CentOS 6 : thunderbird (CESA-2020:0574)

CentOS 6 : thunderbird (CESA-2020:0914)

CentOS 6 : tigervnc (CESA-2017:0630)

CentOS 6 : tomcat6 (CESA-2011:1780)

CentOS 6 : tomcat6 (CESA-2012:0475)

CentOS 6 : tomcat6 (CESA-2013:0623)

CentOS 6 : tomcat6 (CESA-2013:0869)

CentOS 6 : tomcat6 (CESA-2013:0964)

CentOS 6 : tomcat6 (CESA-2014:0429)

CentOS 6 : tomcat6 (CESA-2014:0865)

CentOS 6 : tomcat6 (CESA-2014:1038)

CentOS 6 : tomcat6 (CESA-2015:0991)

CentOS 6 : tomcat6 (CESA-2016:0492)

CentOS 6 : tomcat6 (CESA-2016:2045) (httpoxy)

CentOS 6 : tomcat6 (CESA-2017:0527)

CentOS 6 : tomcat6 (CESA-2017:3080)

CentOS 6 : tomcat6 (CESA-2020:0912)

CentOS 6 : trousers (CESA-2014:1507)

CentOS 6 : udisks (CESA-2014:0293)

CentOS 6 : util-linux-ng (CESA-2013:0517)

CentOS 6 : vim (CESA-2019:1774)

CentOS 6 : vino (CESA-2013:0169)

CentOS 6 : wget (CESA-2014:0151)

CentOS 6 : wireshark (CESA-2012:0509)

CentOS 6 : wireshark (CESA-2013:1569)

CentOS 6 : wireshark (CESA-2014:0342)

CentOS 6 : wireshark (CESA-2015:1460)

CentOS 6 : wireshark (CESA-2017:0631)

CentOS 6 : wpa\_supplicant (CESA-2015:1439)

CentOS 6 : wpa\_supplicant (CESA-2017:2911) (KRACK)

CentOS 6 : xerces-c (CESA-2020:0702)

CentOS 6 : xinetd (CESA-2013:0499)

CentOS 6 : xmlrpc3 (CESA-2018:1779)

CentOS 6 : xorg-x11-apps / xorg-x11-server-utils / xorg-x11-utils (CESA-2013:0502)

CentOS 6 : xorg-x11-drv-qxl (CESA-2013:0218)

CentOS 6 : xorg-x11-server (CESA-2012:0939)

CentOS 6 : xorg-x11-server (CESA-2013:1620)

CentOS 6 : yum-utils (CESA-2018:2284)

CentOS 6 : zsh (CESA-2018:1932)

CentOS 6 : zsh (CESA-2020:0892)

CentOS 7 : 389-ds-base (CESA-2015:0416)

CentOS 7 : 389-ds-base (CESA-2015:0895)

CentOS 7 : 389-ds-base (CESA-2016:0204)

CentOS 7 : 389-ds-base (CESA-2016:2594)

CentOS 7 : 389-ds-base (CESA-2017:0920)

CentOS 7 : 389-ds-base (CESA-2017:2569)

CentOS 7 : 389-ds-base (CESA-2018:0163)

CentOS 7 : 389-ds-base (CESA-2018:0414)

CentOS 7 : 389-ds-base (CESA-2018:1380)

CentOS 7 : 389-ds-base (CESA-2018:2757)

CentOS 7 : 389-ds-base (CESA-2018:3127)

CentOS 7 : 389-ds-base (CESA-2019:1896)

CentOS 7 : 389-ds-base (CESA-2019:3981)

CentOS 7 : abrt (CESA-2015:1083)

CentOS 7 : abrt / libreport (CESA-2015:2505)

CentOS 7 : advancecomp (CESA-2019:2332)

CentOS 7 : advancecomp (CESA-2020:1037)

CentOS 7 : apache-commons-beanutils (CESA-2020:0194)

CentOS 7 : apache-commons-collections (CESA-2015:2522)

CentOS 7 : atk / evolution / evolution-data-server / evolution-ews (CESA-2020:1080)

CentOS 7 : augeas (CESA-2017:2788)

CentOS 7 : authconfig (CESA-2017:2285)

CentOS 7 : autofs (CESA-2015:2417)

CentOS 7 : avahi (CESA-2020:1176)

CentOS 7 : bash (CESA-2017:1931)

CentOS 7 : bash (CESA-2020:1113)

CentOS 7 : bind (CESA-2015:1443)

CentOS 7 : bind (CESA-2016:2615)

CentOS 7 : bind (CESA-2017:0062)

CentOS 7 : bind (CESA-2017:0276)

CentOS 7 : bind (CESA-2017:1095)

CentOS 7 : bind (CESA-2017:1680)

CentOS 7 : bind (CESA-2018:0102)

CentOS 7 : bind (CESA-2018:2570)

CentOS 7 : bind (CESA-2019:0194)

CentOS 7 : bind (CESA-2019:1294)

CentOS 7 : bind (CESA-2019:2057)

CentOS 7 : bind (CESA-2020:1061)

CentOS 7 : binutils (CESA-2015:2079)

CentOS 7 : binutils (CESA-2018:3032)

CentOS 7 : binutils (CESA-2019:2075)

CentOS 7 : blktrace (CESA-2019:2162)

CentOS 7 : bluez (CESA-2020:1101)

CentOS 7 : chrony (CESA-2015:2241)

CentOS 7 : cloud-init (CESA-2019:0597)

CentOS 7 : clutter (CESA-2015:1510)

CentOS 7 : clutter / cogl / gnome-shell / mutter (CESA-2015:0535)

CentOS 7 : clutter-gst2 / gnome-video-effects / gstreamer-plugins-bad-free / etcgstreamer1 / etc (CESA-2017:2060)

CentOS 7 : cockpit (CESA-2019:0482)

CentOS 7 : compat-libtiff3 (CESA-2019:2051)

CentOS 7 : corosync (CESA-2018:1169)

CentOS 7 : cpio (CESA-2015:2108)

CentOS 7 : cups (CESA-2020:1050)

CentOS 7 : cups-filters (CESA-2014:1795)

CentOS 7 : cups-filters (CESA-2015:2360)

CentOS 7 : curl (CESA-2015:2159)

CentOS 7 : curl (CESA-2016:2575)

CentOS 7 : curl (CESA-2017:2016)

CentOS 7 : curl (CESA-2017:3263)

CentOS 7 : curl (CESA-2019:1880)

CentOS 7 : curl (CESA-2019:2181)

CentOS 7 : curl (CESA-2020:1020)

CentOS 7 : curl / nss-pem (CESA-2018:3157)

CentOS 7 : dhcp (CESA-2016:2590)

CentOS 7 : dhcp (CESA-2018:0158)

CentOS 7 : dhcp (CESA-2018:0483)

CentOS 7 : dhcp (CESA-2018:1453)

CentOS 7 : dhcp (CESA-2019:2060)

CentOS 7 : dnsmasq (CESA-2017:2836)

CentOS 7 : dovecot (CESA-2019:2836)

CentOS 7 : dovecot (CESA-2020:1062)

CentOS 7 : doxygen (CESA-2020:1034)

CentOS 7 : elfutils (CESA-2019:2197)

CentOS 7 : emacs (CESA-2017:2771)

CentOS 7 : evince (CESA-2017:2388)

CentOS 7 : evince / okular / poppler (CESA-2019:2022)

CentOS 7 : evince / poppler (CESA-2020:1074)

CentOS 7 : exempi (CESA-2019:2048)

CentOS 7 : exiv2 (CESA-2019:2101)

CentOS 7 : expat (CESA-2020:1011)

CentOS 7 : fence-agents (CESA-2019:2037)

CentOS 7 : file (CESA-2015:2155)

CentOS 7 : file (CESA-2020:1022)

CentOS 7 : firefox (CESA-2017:0461)

CentOS 7 : firefox (CESA-2017:0558)

CentOS 7 : firefox (CESA-2017:1106)

CentOS 7 : firefox (CESA-2018:0527)

CentOS 7 : firefox (CESA-2018:1099)

CentOS 7 : firefox (CESA-2018:1415)

CentOS 7 : firefox (CESA-2018:2113)

CentOS 7 : firefox (CESA-2018:2692)

CentOS 7 : firefox (CESA-2018:2835)

CentOS 7 : firefox (CESA-2018:2884)

CentOS 7 : firefox (CESA-2018:3005)

CentOS 7 : firefox (CESA-2018:3833)

CentOS 7 : firefox (CESA-2019:0219)

CentOS 7 : firefox (CESA-2019:0374)

CentOS 7 : firefox (CESA-2019:0622)

CentOS 7 : firefox (CESA-2019:0671)

CentOS 7 : firefox (CESA-2019:1265)

CentOS 7 : firefox (CESA-2019:1603)

CentOS 7 : firefox (CESA-2019:1763)

CentOS 7 : firefox (CESA-2019:2729)

CentOS 7 : firefox (CESA-2019:3193)

CentOS 7 : firefox (CESA-2019:4107)

CentOS 7 : firefox (CESA-2020:0085)

CentOS 7 : firefox (CESA-2020:0520)

CentOS 7 : firefox (CESA-2020:0815)

CentOS 7 : firewalld (CESA-2016:2597)

CentOS 7 : flatpak (CESA-2018:2766)

CentOS 7 : flatpak (CESA-2019:0375)

CentOS 7 : flatpak (CESA-2019:1024)

CentOS 7 : fltk / tigervnc (CESA-2017:2000)

CentOS 7 : fontconfig (CESA-2016:2601)

CentOS 7 : freeglut / libX11 / libXcursor / libXfont / libXfont2 / libXres / libdrm / libepoxy / etc (CESA-2018:3059)

CentOS 7 : freeradius (CESA-2017:1581)

CentOS 7 : freeradius (CESA-2017:2389)

CentOS 7 : freeradius (CESA-2019:1131)

CentOS 7 : freerdp (CESA-2019:0697)

CentOS 7 : freerdp / vinagre (CESA-2019:2157)

CentOS 7 : fribidi (CESA-2019:4326)

CentOS 7 : fuse (CESA-2018:3324)

CentOS 7 : gcab (CESA-2018:0350)

CentOS 7 : gcc (CESA-2018:0849)

CentOS 7 : gdm / gnome-session (CESA-2017:2128)

CentOS 7 : gdm / libX11 / libxkbcommon / xorg-x11-drv-ati / xorg-x11-drv-vesa / etc (CESA-2019:2079)

CentOS 7 : gettext (CESA-2020:1138)

CentOS 7 : ghostscript (CESA-2017:0013)

CentOS 7 : ghostscript (CESA-2017:2180)

CentOS 7 : ghostscript (CESA-2018:2918)

CentOS 7 : ghostscript (CESA-2018:3650)

CentOS 7 : ghostscript (CESA-2018:3761)

CentOS 7 : ghostscript (CESA-2018:3834)

CentOS 7 : ghostscript (CESA-2019:0229)

CentOS 7 : ghostscript (CESA-2019:0633)

CentOS 7 : ghostscript (CESA-2019:1017)

CentOS 7 : ghostscript (CESA-2019:2281)

CentOS 7 : ghostscript (CESA-2019:2586)

CentOS 7 : ghostscript (CESA-2019:3888)

CentOS 7 : gimp / gimp-help (CESA-2016:2589)

CentOS 7 : git (CESA-2015:2561)

CentOS 7 : git (CESA-2017:2004)

CentOS 7 : git (CESA-2017:2484)

CentOS 7 : git (CESA-2018:1957)

CentOS 7 : git (CESA-2018:3408)

CentOS 7 : git (CESA-2020:0124)

CentOS 7 : glibc (CESA-2014:2023)

CentOS 7 : glibc (CESA-2015:0327)

CentOS 7 : glibc (CESA-2015:2172)

CentOS 7 : glibc (CESA-2015:2199)

CentOS 7 : glibc (CESA-2016:0176)

CentOS 7 : glibc (CESA-2016:2573)

CentOS 7 : glibc (CESA-2017:1481) (Stack Clash)

CentOS 7 : glibc (CESA-2017:1916)

CentOS 7 : glibc (CESA-2018:0805)

CentOS 7 : glibc (CESA-2018:3092)

CentOS 7 : glibc (CESA-2019:2118)

CentOS 7 : glusterfs (CESA-2018:2607)

CentOS 7 : gnupg2 (CESA-2018:2181)

CentOS 7 : gnutls (CESA-2014:1846)

CentOS 7 : gnutls (CESA-2017:2292)

CentOS 7 : gnutls (CESA-2018:3050)

CentOS 7 : golang (CESA-2016:1538) (httpoxy)

CentOS 7 : golang (CESA-2017:1859)

CentOS 7 : golang (CESA-2018:0878)

CentOS 7 : graphite2 (CESA-2016:0594)

CentOS 7 : graphite2 (CESA-2017:1793)

CentOS 7 : grep (CESA-2015:2111)

CentOS 7 : groovy (CESA-2017:2486)

CentOS 7 : grub2 (CESA-2015:2401)

CentOS 7 : grub2 (CESA-2015:2623)

CentOS 7 : gstreamer-plugins-bad-free (CESA-2017:0018)

CentOS 7 : gstreamer-plugins-good (CESA-2017:0019)

CentOS 7 : gstreamer1-plugins-bad-free (CESA-2017:0021)

CentOS 7 : gstreamer1-plugins-good (CESA-2017:0020)

CentOS 7 : gtk-vnc (CESA-2017:2258)

CentOS 7 : gvfs (CESA-2019:2145)

CentOS 7 : haproxy (CESA-2014:1292)

CentOS 7 : hivex (CESA-2015:0301)

CentOS 7 : http-parser (CESA-2019:2258)

CentOS 7 : http-parser (CESA-2020:0703)

CentOS 7 : httpcomponents-client (CESA-2014:1146)

CentOS 7 : httpd (CESA-2014:0921)

CentOS 7 : httpd (CESA-2015:0325)

CentOS 7 : httpd (CESA-2015:1667)

CentOS 7 : httpd (CESA-2016:1422) (httpoxy)

CentOS 7 : httpd (CESA-2017:0906)

CentOS 7 : httpd (CESA-2017:2479)

CentOS 7 : httpd (CESA-2017:2882) (Optionsbleed)

CentOS 7 : httpd (CESA-2019:1898)

CentOS 7 : httpd (CESA-2019:2343)

CentOS 7 : httpd (CESA-2020:1121)

CentOS 7 : icedtea-web (CESA-2019:2003)

CentOS 7 : icoutils (CESA-2017:0837)

CentOS 7 : icu (CESA-2020:0897)

CentOS 7 : ImageMagick / autotrace / emacs / inkscape (CESA-2020:1180)

CentOS 7 : ipa (CESA-2015:0442)

CentOS 7 : ipa (CESA-2017:0001)

CentOS 7 : ipa (CESA-2017:0388)

CentOS 7 : ipa / slapi-nis (CESA-2015:0728)

CentOS 7 : ipsilon (CESA-2016:2809)

CentOS 7 : jasper (CESA-2018:3253)

CentOS 7 : java-1.7.0-openjdk (CESA-2018:1278)

CentOS 7 : java-1.7.0-openjdk (CESA-2018:1648) (Spectre)

CentOS 7 : java-1.7.0-openjdk (CESA-2018:2286)

CentOS 7 : java-1.7.0-openjdk (CESA-2018:3350)

CentOS 7 : java-1.7.0-openjdk (CESA-2019:0464)

CentOS 7 : java-1.7.0-openjdk (CESA-2019:0791)

CentOS 7 : java-1.7.0-openjdk (CESA-2019:1839)

CentOS 7 : java-1.7.0-openjdk (CESA-2019:3157)

CentOS 7 : java-1.7.0-openjdk (CESA-2020:0541)

CentOS 7 : java-1.8.0-openjdk (CESA-2016:0049) (SLOTH)

CentOS 7 : java-1.8.0-openjdk (CESA-2016:0513)

CentOS 7 : java-1.8.0-openjdk (CESA-2016:0650)

CentOS 7 : java-1.8.0-openjdk (CESA-2017:1108)

CentOS 7 : java-1.8.0-openjdk (CESA-2018:1191)

CentOS 7 : java-1.8.0-openjdk (CESA-2018:1649) (Spectre)

CentOS 7 : java-1.8.0-openjdk (CESA-2018:2242)

CentOS 7 : java-1.8.0-openjdk (CESA-2018:2942)

CentOS 7 : java-1.8.0-openjdk (CESA-2019:0775)

CentOS 7 : java-1.8.0-openjdk (CESA-2019:1815)

CentOS 7 : java-1.8.0-openjdk (CESA-2019:3128)

CentOS 7 : java-1.8.0-openjdk (CESA-2020:0196)

CentOS 7 : java-11-openjdk (CESA-2018:3521)

CentOS 7 : java-11-openjdk (CESA-2019:0436)

CentOS 7 : java-11-openjdk (CESA-2019:0778)

CentOS 7 : java-11-openjdk (CESA-2019:1810)

CentOS 7 : java-11-openjdk (CESA-2019:3127)

CentOS 7 : java-11-openjdk (CESA-2020:0122)

CentOS 7 : jss (CESA-2019:3067)

CentOS 7 : kde-settings / kde-workspace / kdelibs / kmag / virtuoso-opensource (CESA-2019:2141)

CentOS 7 : kde-settings / kdelibs (CESA-2019:2606)

CentOS 7 : kdelibs (CESA-2017:1264)

CentOS 7 : kdenetwork (CESA-2014:1827)

CentOS 7 : keepalived (CESA-2019:0022)

CentOS 7 : keepalived (CESA-2019:2285)

CentOS 7 : kernel (CESA-2014:0923)

CentOS 7 : kernel (CESA-2014:1023)

CentOS 7 : kernel (CESA-2014:1281)

CentOS 7 : kernel (CESA-2014:1724)

CentOS 7 : kernel (CESA-2014:1971)

CentOS 7 : kernel (CESA-2014:2010)

CentOS 7 : kernel (CESA-2015:0102)

CentOS 7 : kernel (CESA-2015:0290)

CentOS 7 : kernel (CESA-2015:0726)

CentOS 7 : kernel (CESA-2015:0987)

CentOS 7 : kernel (CESA-2015:1137)

CentOS 7 : kernel (CESA-2015:1534)

CentOS 7 : kernel (CESA-2015:1778)

CentOS 7 : kernel (CESA-2015:1978)

CentOS 7 : kernel (CESA-2015:2152)

CentOS 7 : kernel (CESA-2015:2552)

CentOS 7 : kernel (CESA-2016:0064)

CentOS 7 : kernel (CESA-2016:0185)

CentOS 7 : kernel (CESA-2016:1033)

CentOS 7 : kernel (CESA-2016:1277)

CentOS 7 : kernel (CESA-2016:1539)

CentOS 7 : kernel (CESA-2016:1633)

CentOS 7 : kernel (CESA-2016:1847)

CentOS 7 : kernel (CESA-2016:2047)

CentOS 7 : kernel (CESA-2016:2098) (Dirty COW)

CentOS 7 : kernel (CESA-2016:2574)

CentOS 7 : kernel (CESA-2017:0086)

CentOS 7 : kernel (CESA-2017:0294)

CentOS 7 : kernel (CESA-2017:0386)

CentOS 7 : kernel (CESA-2017:0933)

CentOS 7 : kernel (CESA-2017:1308)

CentOS 7 : kernel (CESA-2017:1484) (Stack Clash)

CentOS 7 : kernel (CESA-2017:1615)

CentOS 7 : kernel (CESA-2017:1842) (Stack Clash)

CentOS 7 : kernel (CESA-2017:2473)

CentOS 7 : kernel (CESA-2017:2679) (BlueBorne)

CentOS 7 : kernel (CESA-2017:2930)

CentOS 7 : kernel (CESA-2017:3315)

CentOS 7 : kernel (CESA-2018:0007) (Meltdown) (Spectre)

CentOS 7 : kernel (CESA-2018:0151) (Meltdown) (Spectre)

CentOS 7 : kernel (CESA-2018:0395)

CentOS 7 : kernel (CESA-2018:1062)

CentOS 7 : kernel (CESA-2018:1318)

CentOS 7 : kernel (CESA-2018:1629) (Spectre)

CentOS 7 : kernel (CESA-2018:1852)

CentOS 7 : kernel (CESA-2018:1965) (Spectre)

CentOS 7 : kernel (CESA-2018:2384) (Foreshadow)

CentOS 7 : kernel (CESA-2018:2748)

CentOS 7 : kernel (CESA-2018:3083)

CentOS 7 : kernel (CESA-2018:3651)

CentOS 7 : kernel (CESA-2019:0163)

CentOS 7 : kernel (CESA-2019:0512)

CentOS 7 : kernel (CESA-2019:0818)

CentOS 7 : kernel (CESA-2019:1168) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

CentOS 7 : kernel (CESA-2019:1481) (SACK Panic) (SACK Slowness)

CentOS 7 : kernel (CESA-2019:1873)

CentOS 7 : kernel (CESA-2019:2029)

CentOS 7 : kernel (CESA-2019:2600)

CentOS 7 : kernel (CESA-2019:2829)

CentOS 7 : kernel (CESA-2019:3055)

CentOS 7 : kernel (CESA-2019:3834)

CentOS 7 : kernel (CESA-2019:3872)

CentOS 7 : kernel (CESA-2019:3979)

CentOS 7 : kernel (CESA-2020:0374)

CentOS 7 : kernel (CESA-2020:0375) (deprecated)

CentOS 7 : kernel (CESA-2020:0839)

CentOS 7 : kernel (CESA-2020:1016)

CentOS 7 : kexec-tools (CESA-2014:0943)

CentOS 7 : kexec-tools (CESA-2015:0986)

CentOS 7 : keycloak-httpd-client-install (CESA-2019:2137)

CentOS 7 : krb5 (CESA-2015:0439)

CentOS 7 : krb5 (CESA-2015:2154)

CentOS 7 : krb5 (CESA-2016:0532)

CentOS 7 : krb5 (CESA-2016:2591)

CentOS 7 : krb5 (CESA-2018:0666)

CentOS 7 : krb5 (CESA-2018:3071)

CentOS 7 : ksh (CESA-2020:0568)

CentOS 7 : lftp (CESA-2020:1045)

CentOS 7 : libabw / libcmis / libetonyek / libfreehand / liblangtag / libmwaw / libodfgen / etc (CESA-2015:0377)

CentOS 7 : libarchive (CESA-2016:1844)

CentOS 7 : libarchive (CESA-2019:2298)

CentOS 7 : libarchive (CESA-2020:0203)

CentOS 7 : libcdio (CESA-2018:3246)

CentOS 7 : libcgroup (CESA-2019:2047)

CentOS 7 : libcmis / libpagemaker / libreoffice / mdds (CESA-2016:2579)

CentOS 7 : libgovirt / spice-gtk / spice-vdagent / virt-viewer (CESA-2019:2229)

CentOS 7 : libguestfs (CESA-2016:2576)

CentOS 7 : libguestfs-winsupport (CESA-2019:2308)

CentOS 7 : libICE / libX11 / libXaw / libXcursor / libXdmcp / libXfixes / libXfont / libXfont2 / etc (CESA-2017:1865)

CentOS 7 : libjpeg-turbo (CESA-2019:2052)

CentOS 7 : libkdcraw (CESA-2018:3065)

CentOS 7 : liblouis (CESA-2017:3111)

CentOS 7 : liblouis (CESA-2017:3384)

CentOS 7 : libmspack (CESA-2018:3327)

CentOS 7 : libmspack (CESA-2019:2049)

CentOS 7 : libndp (CESA-2016:1086)

CentOS 7 : libosinfo (CESA-2020:1051)

CentOS 7 : libpng (CESA-2015:2596)

CentOS 7 : libpng12 (CESA-2015:2595)

CentOS 7 : libqb (CESA-2020:1189)

CentOS 7 : LibRaw / accountsservice / colord / control-center / gdm / gnome-online-accounts / etc (CESA-2020:1021)

CentOS 7 : librelp (CESA-2018:1223)

CentOS 7 : libreoffice (CESA-2017:0914)

CentOS 7 : libreoffice (CESA-2017:1975)

CentOS 7 : libreoffice (CESA-2018:0418)

CentOS 7 : libreoffice (CESA-2019:2130)

CentOS 7 : libreoffice (CESA-2020:1151)

CentOS 7 : libreswan (CESA-2015:1154)

CentOS 7 : libreswan (CESA-2015:1979)

CentOS 7 : libreswan (CESA-2016:2603)

CentOS 7 : libsndfile (CESA-2020:1185)

CentOS 7 : libsolv (CESA-2019:2290)

CentOS 7 : libsoup (CESA-2017:2459)

CentOS 7 : libssh2 (CESA-2015:2140)

CentOS 7 : libssh2 (CESA-2019:0679)

CentOS 7 : libssh2 (CESA-2019:1884)

CentOS 7 : libssh2 (CESA-2019:2136)

CentOS 7 : libtasn1 (CESA-2017:1860)

CentOS 7 : libtiff (CESA-2016:1546)

CentOS 7 : libtiff (CESA-2019:2053)

CentOS 7 : libtirpc (CESA-2017:1263)

CentOS 7 : libuser (CESA-2015:1483)

CentOS 7 : libvirt (CESA-2014:0914)

CentOS 7 : libvirt (CESA-2014:1352)

CentOS 7 : libvirt (CESA-2015:0008)

CentOS 7 : libvirt (CESA-2015:0323)

CentOS 7 : libvirt (CESA-2016:2577)

CentOS 7 : libvirt (CESA-2018:0029) (Spectre)

CentOS 7 : libvirt (CESA-2018:1396)

CentOS 7 : libvirt (CESA-2018:1632) (Spectre)

CentOS 7 : libvirt (CESA-2018:1997) (Spectre)

CentOS 7 : libvirt (CESA-2018:3113)

CentOS 7 : libvirt (CESA-2019:1177) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

CentOS 7 : libvirt (CESA-2019:1264)

CentOS 7 : libvirt (CESA-2019:1579)

CentOS 7 : libvirt (CESA-2019:2294)

CentOS 7 : libvncserver (CESA-2018:1055)

CentOS 7 : libvncserver (CESA-2019:0059)

CentOS 7 : libvncserver (CESA-2020:0913)

CentOS 7 : libvorbis (CESA-2018:1058)

CentOS 7 : libwpd (CESA-2019:2126)

CentOS 7 : libxml2 (CESA-2015:0749)

CentOS 7 : libxml2 (CESA-2015:2550)

CentOS 7 : libxml2 (CESA-2020:1190)

CentOS 7 : linux-firmware (CESA-2018:0014) (Spectre)

CentOS 7 : linux-firmware (CESA-2018:0094) (Spectre)

CentOS 7 : linux-firmware (CESA-2019:2169)

CentOS 7 : log4j (CESA-2017:2423)

CentOS 7 : mailman (CESA-2015:1153)

CentOS 7 : mailman (CESA-2018:0505)

CentOS 7 : mailman (CESA-2020:1054)

CentOS 7 : mariadb (CESA-2014:1861)

CentOS 7 : mariadb (CESA-2015:0118)

CentOS 7 : mariadb (CESA-2015:1665) (BACKRONYM)

CentOS 7 : mariadb (CESA-2016:0534)

CentOS 7 : mariadb (CESA-2016:1602)

CentOS 7 : mariadb (CESA-2016:2595)

CentOS 7 : mariadb (CESA-2017:2192)

CentOS 7 : mariadb (CESA-2018:2439)

CentOS 7 : mariadb (CESA-2019:2327)

CentOS 7 : mariadb (CESA-2020:1100)

CentOS 7 : memcached (CESA-2016:2819)

CentOS 7 : mercurial (CESA-2016:0706)

CentOS 7 : mercurial (CESA-2017:2489)

CentOS 7 : mercurial (CESA-2019:2276)

CentOS 7 : microcode\_ctl (CESA-2018:0012) (Spectre)

CentOS 7 : mod\_auth\_mellon (CESA-2019:0766)

CentOS 7 : mod\_auth\_mellon (CESA-2020:1003)

CentOS 7 : mod\_auth\_openidc (CESA-2019:2112)

CentOS 7 : mod\_nss (CESA-2016:2602)

CentOS 7 : mod\_wsgi (CESA-2014:1091)

CentOS 7 : ModemManager / NetworkManager / NetworkManager-libreswan / network-manager-applet (CESA-2015:2315)

CentOS 7 : mutt (CESA-2020:1126)

CentOS 7 : nautilus (CESA-2018:0223)

CentOS 7 : nbdkit (CESA-2020:1167)

CentOS 7 : net-snmp (CESA-2015:2345)

CentOS 7 : net-snmp (CESA-2020:1081)

CentOS 7 : netcf (CESA-2015:2248)

CentOS 7 : nettle (CESA-2016:2582)

CentOS 7 : NetworkManager (CESA-2018:3665)

CentOS 7 : NetworkManager / NetworkManager-libreswan / libnl3 / network-manager-applet (CESA-2016:2581)

CentOS 7 : NetworkManager / NetworkManager-libreswan / libnl3 / network-manager-applet (CESA-2017:2299)

CentOS 7 : nspr / nss / nss-softokn / nss-util (CESA-2016:0685)

CentOS 7 : nspr / nss / nss-softokn / nss-util (CESA-2019:2237)

CentOS 7 : nss (CESA-2017:1365)

CentOS 7 : nss (CESA-2018:2768)

CentOS 7 : nss / nss-softokn / nss-util (CESA-2014:1073)

CentOS 7 : nss / nss-softokn / nss-util (CESA-2019:4190)

CentOS 7 : ntp (CESA-2015:2231)

CentOS 7 : ntp (CESA-2016:2583)

CentOS 7 : ntp (CESA-2018:0855)

CentOS 7 : ntp (CESA-2019:2077)

CentOS 7 : ocaml (CESA-2016:1296)

CentOS 7 : okular (CESA-2020:1173)

CentOS 7 : openhpi (CESA-2015:2369)

CentOS 7 : openjpeg (CESA-2017:0838)

CentOS 7 : openjpeg2 (CESA-2020:0262)

CentOS 7 : openjpeg2 (CESA-2020:0550)

CentOS 7 : openldap (CESA-2015:2131)

CentOS 7 : openldap (CESA-2017:1852)

CentOS 7 : opensc (CESA-2019:2154)

CentOS 7 : openslp (CESA-2018:2240)

CentOS 7 : openslp (CESA-2019:4240)

CentOS 7 : openssh (CESA-2015:0425)

CentOS 7 : openssh (CESA-2015:2088)

CentOS 7 : openssh (CESA-2016:0043)

CentOS 7 : openssh (CESA-2016:0465)

CentOS 7 : openssh (CESA-2016:2588)

CentOS 7 : openssh (CESA-2017:2029)

CentOS 7 : openssh (CESA-2018:0980)

CentOS 7 : openssh (CESA-2019:2143)

CentOS 7 : openssl (CESA-2015:0716)

CentOS 7 : openssl (CESA-2016:0722)

CentOS 7 : openssl (CESA-2018:0998)

CentOS 7 : openssl (CESA-2018:3221)

CentOS 7 : openssl (CESA-2019:0483)

CentOS 7 : openssl (CESA-2019:2304)

CentOS 7 : openwsman (CESA-2019:0638)

CentOS 7 : ovmf (CESA-2018:3090)

CentOS 7 : ovmf (CESA-2019:0809)

CentOS 7 : ovmf (CESA-2019:2125)

CentOS 7 : pacemaker (CESA-2015:2383)

CentOS 7 : pacemaker (CESA-2016:2578)

CentOS 7 : pacemaker (CESA-2016:2614)

CentOS 7 : PackageKit (CESA-2018:1224)

CentOS 7 : PackageKit / accountsservice / adwaita-icon-theme / appstream-data / at-spi2-atk / etc (CESA-2018:3140)

CentOS 7 : pango (CESA-2019:2571)

CentOS 7 : patch (CESA-2018:1200)

CentOS 7 : patch (CESA-2019:2033)

CentOS 7 : patch (CESA-2019:2964)

CentOS 7 : pcre (CESA-2015:0330)

CentOS 7 : pcre (CESA-2016:1025)

CentOS 7 : pcs (CESA-2015:0980)

CentOS 7 : pcs (CESA-2015:2290)

CentOS 7 : pcs (CESA-2016:2596)

CentOS 7 : pcs (CESA-2018:1060)

CentOS 7 : perl (CESA-2019:0109)

CentOS 7 : perl-Archive-Tar (CESA-2019:2097)

CentOS 7 : php (CESA-2014:1013)

CentOS 7 : php (CESA-2014:1327)

CentOS 7 : php (CESA-2015:1135)

CentOS 7 : php (CESA-2016:1613) (httpoxy)

CentOS 7 : php (CESA-2016:2598)

CentOS 7 : php (CESA-2017:3221)

CentOS 7 : php (CESA-2018:0406)

CentOS 7 : php (CESA-2019:3286)

CentOS 7 : php (CESA-2020:1112)

CentOS 7 : pidgin (CESA-2017:1854)

CentOS 7 : pki-core (CESA-2018:1979)

CentOS 7 : plexus-archiver (CESA-2018:1836)

CentOS 7 : policycoreutils (CESA-2018:0913)

CentOS 7 : polkit (CESA-2016:0189)

CentOS 7 : polkit (CESA-2019:0230)

CentOS 7 : polkit (CESA-2019:2046)

CentOS 7 : polkit (CESA-2020:1135)

CentOS 7 : polkit-qt (CESA-2014:1359)

CentOS 7 : poppler (CESA-2016:2580)

CentOS 7 : poppler (CESA-2017:2551)

CentOS 7 : postgresql (CESA-2015:2078)

CentOS 7 : postgresql (CESA-2016:0346)

CentOS 7 : postgresql (CESA-2016:2606)

CentOS 7 : postgresql (CESA-2017:1983)

CentOS 7 : postgresql (CESA-2017:2728)

CentOS 7 : postgresql (CESA-2017:3402)

CentOS 7 : postgresql (CESA-2018:2557)

CentOS 7 : ppp (CESA-2020:0630)

CentOS 7 : procmail (CESA-2017:3269)

CentOS 7 : procps-ng (CESA-2018:1700)

CentOS 7 : procps-ng (CESA-2019:2189)

CentOS 7 : python (CESA-2015:2101)

CentOS 7 : python (CESA-2016:2586)

CentOS 7 : python (CESA-2017:1868)

CentOS 7 : python (CESA-2018:2123)

CentOS 7 : python (CESA-2018:3041)

CentOS 7 : python (CESA-2019:0710)

CentOS 7 : python (CESA-2019:1587)

CentOS 7 : python (CESA-2019:2030)

CentOS 7 : python (CESA-2020:1131)

CentOS 7 : python-jinja2 (CESA-2019:1022)

CentOS 7 : python-paramiko (CESA-2018:3347)

CentOS 7 : python-pillow (CESA-2020:0578)

CentOS 7 : python-pip (CESA-2020:0850)

CentOS 7 : python-reportlab (CESA-2020:0195)

CentOS 7 : python-requests (CESA-2019:2035)

CentOS 7 : python-rhsm / subscription-manager (CESA-2016:2592)

CentOS 7 : python-twisted-web (CESA-2020:1091)

CentOS 7 : python-urllib3 (CESA-2019:2272)

CentOS 7 : python-virtualenv (CESA-2020:0851)

CentOS 7 : python3 (CESA-2020:1132)

CentOS 7 : qemu-kvm (CESA-2014:0927)

CentOS 7 : qemu-kvm (CESA-2014:1669)

CentOS 7 : qemu-kvm (CESA-2015:0349)

CentOS 7 : qemu-kvm (CESA-2015:0999) (Venom)

CentOS 7 : qemu-kvm (CESA-2015:1507)

CentOS 7 : qemu-kvm (CESA-2015:1793)

CentOS 7 : qemu-kvm (CESA-2015:1943)

CentOS 7 : qemu-kvm (CESA-2016:0083)

CentOS 7 : qemu-kvm (CESA-2016:0724)

CentOS 7 : qemu-kvm (CESA-2016:1606)

CentOS 7 : qemu-kvm (CESA-2016:2585)

CentOS 7 : qemu-kvm (CESA-2017:0083)

CentOS 7 : qemu-kvm (CESA-2017:0396)

CentOS 7 : qemu-kvm (CESA-2017:0987)

CentOS 7 : qemu-kvm (CESA-2017:1430)

CentOS 7 : qemu-kvm (CESA-2017:1681)

CentOS 7 : qemu-kvm (CESA-2017:1856)

CentOS 7 : qemu-kvm (CESA-2017:2445)

CentOS 7 : qemu-kvm (CESA-2017:3368)

CentOS 7 : qemu-kvm (CESA-2018:0023) (Spectre)

CentOS 7 : qemu-kvm (CESA-2018:0816)

CentOS 7 : qemu-kvm (CESA-2018:1416)

CentOS 7 : qemu-kvm (CESA-2018:1633) (Spectre)

CentOS 7 : qemu-kvm (CESA-2018:2001) (Spectre)

CentOS 7 : qemu-kvm (CESA-2018:2462)

CentOS 7 : qemu-kvm (CESA-2019:1178) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

CentOS 7 : qemu-kvm (CESA-2019:1883)

CentOS 7 : qemu-kvm (CESA-2019:2078)

CentOS 7 : qemu-kvm (CESA-2019:2607)

CentOS 7 : qemu-kvm (CESA-2020:0366)

CentOS 7 : qemu-kvm (CESA-2020:1116)

CentOS 7 : qt (CESA-2020:1172)

CentOS 7 : qt5-qt3d / qt5-qtbase / qt5-qtcanvas3d / qt5-qtconnectivity / qt5-qtdeclarative / etc (CESA-2019:2135)

CentOS 7 : quagga (CESA-2018:0377)

CentOS 7 : realmd (CESA-2015:2184)

CentOS 7 : rest (CESA-2015:2237)

CentOS 7 : resteasy-base (CESA-2014:1011)

CentOS 7 : resteasy-base (CESA-2016:2604)

CentOS 7 : rpcbind (CESA-2017:1262)

CentOS 7 : rpm (CESA-2014:1976)

CentOS 7 : rsyslog (CESA-2014:1397)

CentOS 7 : rsyslog (CESA-2019:2110)

CentOS 7 : rsyslog (CESA-2020:1000)

CentOS 7 : ruby (CESA-2014:1912)

CentOS 7 : ruby (CESA-2018:0378)

CentOS 7 : ruby (CESA-2018:3738)

CentOS 7 : ruby (CESA-2019:1235)

CentOS 7 : ruby (CESA-2019:2028)

CentOS 7 : rubygem-bundler / rubygem-thor (CESA-2015:2180)

Centos 7 : runc

CentOS 7 : samba (CESA-2014:0867)

CentOS 7 : samba (CESA-2014:1008)

CentOS 7 : samba (CESA-2015:0252)

CentOS 7 : samba (CESA-2016:0006)

CentOS 7 : samba (CESA-2016:1486)

CentOS 7 : samba (CESA-2017:1265)

CentOS 7 : samba (CESA-2017:1950)

CentOS 7 : samba (CESA-2017:2790)

CentOS 7 : samba (CESA-2017:3260)

CentOS 7 : samba (CESA-2018:3056)

CentOS 7 : samba (CESA-2019:2099)

CentOS 7 : samba (CESA-2020:1084)

CentOS 7 : SDL (CESA-2019:4024)

CentOS 7 : setroubleshoot / setroubleshoot-plugins (CESA-2016:1293)

CentOS 7 : setup (CESA-2018:3249)

CentOS 7 : slf4j (CESA-2018:0592)

CentOS 7 : sos (CESA-2016:0188)

CentOS 7 : sos-collector (CESA-2018:3663)

CentOS 7 : sox (CESA-2019:2283)

CentOS 7 : spamassassin (CESA-2018:2916)

CentOS 7 : spice (CESA-2015:1714)

CentOS 7 : spice (CESA-2015:1890)

CentOS 7 : spice (CESA-2016:1205)

CentOS 7 : spice (CESA-2017:0254)

CentOS 7 : spice (CESA-2017:2471)

CentOS 7 : spice (CESA-2019:0231)

CentOS 7 : spice / spice-gtk (CESA-2018:2731)

CentOS 7 : sqlite (CESA-2015:1635)

CentOS 7 : sqlite (CESA-2020:0227)

CentOS 7 : squid (CESA-2014:1147)

CentOS 7 : squid (CESA-2015:2378)

CentOS 7 : squid (CESA-2016:1139)

CentOS 7 : squid (CESA-2016:2600)

CentOS 7 : squid (CESA-2017:0182)

CentOS 7 : squid (CESA-2020:1068)

CentOS 7 : sssd (CESA-2015:2355)

CentOS 7 : sssd (CESA-2017:3379)

CentOS 7 : sssd (CESA-2018:3158)

CentOS 7 : sssd (CESA-2019:2177)

CentOS 7 : subversion (CESA-2015:0166)

CentOS 7 : subversion (CESA-2015:1742)

CentOS 7 : subversion (CESA-2017:2480)

CentOS 7 : sudo (CESA-2016:2593)

CentOS 7 : sudo (CESA-2019:3197)

CentOS 7 : sudo (CESA-2020:0540)

CentOS 7 : systemd (CESA-2018:0260)

CentOS 7 : systemd (CESA-2019:0049)

CentOS 7 : systemd (CESA-2019:0201)

CentOS 7 : systemd (CESA-2019:0368)

CentOS 7 : systemd (CESA-2019:2091)

CentOS 7 : taglib (CESA-2020:1175)

CentOS 7 : tcpdump (CESA-2017:1871)

CentOS 7 : tcpdump (CESA-2019:3976)

CentOS 7 : texlive (CESA-2020:1036)

CentOS 7 : thunderbird (CESA-2015:0642)

CentOS 7 : thunderbird (CESA-2018:0648)

CentOS 7 : thunderbird (CESA-2018:1725)

CentOS 7 : thunderbird (CESA-2018:2252)

CentOS 7 : thunderbird (CESA-2018:3532)

CentOS 7 : thunderbird (CESA-2019:0160)

CentOS 7 : thunderbird (CESA-2019:0270)

CentOS 7 : thunderbird (CESA-2019:0681)

CentOS 7 : thunderbird (CESA-2019:1309)

CentOS 7 : thunderbird (CESA-2019:1626)

CentOS 7 : thunderbird (CESA-2019:1775)

CentOS 7 : thunderbird (CESA-2019:2773)

CentOS 7 : thunderbird (CESA-2019:3210)

CentOS 7 : thunderbird (CESA-2019:4148)

CentOS 7 : thunderbird (CESA-2020:0120)

CentOS 7 : thunderbird (CESA-2020:0576)

CentOS 7 : thunderbird (CESA-2020:0905)

CentOS 7 : tigervnc (CESA-2015:2233)

CentOS 7 : tomcat (CESA-2014:1034)

CentOS 7 : tomcat (CESA-2015:0983)

CentOS 7 : tomcat (CESA-2016:2046) (httpoxy)

CentOS 7 : tomcat (CESA-2016:2599)

CentOS 7 : tomcat (CESA-2017:0935)

CentOS 7 : tomcat (CESA-2017:1809)

CentOS 7 : tomcat (CESA-2017:2247)

CentOS 7 : tomcat (CESA-2017:3081)

CentOS 7 : tomcat (CESA-2018:2921)

CentOS 7 : tomcat (CESA-2019:0485)

CentOS 7 : tomcat (CESA-2019:2205)

CentOS 7 : tomcat (CESA-2020:0855)

CentOS 7 : udisks2 (CESA-2019:2178)

CentOS 7 : unbound (CESA-2015:2455)

CentOS 7 : unixODBC (CESA-2019:2336)

CentOS 7 : unzip (CESA-2019:2159)

CentOS 7 : unzip (CESA-2020:1181)

CentOS 7 : uriparser (CESA-2019:2280)

CentOS 7 : util-linux (CESA-2016:2605)

CentOS 7 : util-linux (CESA-2017:0907)

CentOS 7 : vim (CESA-2019:1619)

CentOS 7 : virt-who (CESA-2015:0430)

CentOS 7 : wget (CESA-2016:2587)

CentOS 7 : wget (CESA-2017:3075)

CentOS 7 : wget (CESA-2018:3052)

CentOS 7 : wget (CESA-2019:1228)

CentOS 7 : wireshark (CESA-2015:2393)

CentOS 7 : wireshark (CESA-2020:1047)

CentOS 7 : wpa\_supplicant (CESA-2014:1956)

CentOS 7 : wpa\_supplicant (CESA-2015:1090)

CentOS 7 : wpa\_supplicant (CESA-2017:2907) (KRACK)

CentOS 7 : wpa\_supplicant (CESA-2018:3107)

CentOS 7 : xdg-user-dirs (CESA-2018:0842)

CentOS 7 : xerces-c (CESA-2015:1193)

CentOS 7 : xerces-c (CESA-2016:0430)

CentOS 7 : xerces-c (CESA-2018:3335)

CentOS 7 : xerces-c (CESA-2020:0704)

CentOS 7 : xfsprogs (CESA-2015:2151)

CentOS 7 : xmlrpc (CESA-2018:1780)

CentOS 7 : xmlsec1 (CESA-2017:2492)

CentOS 7 : xorg-x11-server (CESA-2018:3410)

CentOS 7 : yum-utils (CESA-2018:2285)

CentOS 7 : zsh (CESA-2018:3073)

CentOS 7 : zsh (CESA-2019:2017)

CentOS 7 : zsh (CESA-2020:0853)

CentOS 7 : zziplib (CESA-2018:3229)

CentOS 7 : zziplib (CESA-2019:2196)

CentOS 7 : zziplib (CESA-2020:1178)

CentOS Update Set

# Backdoors

4553 Parasite Mothership Backdoor Detection

Agobot.FO Backdoor Detection

alya.cgi CGI Backdoor Detection

Arugizer Backdoor Detection

ASUS Router 'infosvr' Remote Command Execution

BackOrifice Software Detection

Bagle Worm Removal

Bagle.B Worm Detection

Bind Shell Backdoor Detection

Bugbear Worm Detection

Bugbear.B Web Backdoor Detection

Bugbear.B Worm Detection

Cart32 Backdoor Password Arbitrary Command Execution

CDK Backdoor Detection

Cisco IOS SYNful Knock Implant

Compromised Windows System (hosts File Check)

Conficker P2P Service Detection

Conficker Worm Detection (uncredentialed check)

CYDOOR Software Detection

Dansie Shopping Cart Backdoor Detection

DeepThroat Backdoor Detection

Desktop Orbiter Server Detection

Desktop Orbiter Unpassworded Access Remote Reboot DoS

DNSChanger Malware Detection

DOWNLOADWARE Software Detection

Energizer DUO USB Battery Charger Software Backdoor (credentialed check)

Fake SMTP/FTP Server Detection (possible backdoor)

Finger Backdoor Detection

Fluxay Sensor Detection

FsSniffer Backdoor Detection

G\_Door Malware Detection

GateCrasher Backdoor Detection

Generic Backdoor Detection (banner check)

GirlFriend Backdoor Detection

Hacker Defender Backdoor Detection

Here You Have Email Worm Detection

Hikit Backdoor Detection

HP StoreVirtual Storage Remote Unauthorized Access

IRC Bot Detection

IRC Bot ident Server Detection

Kibuv Worm Detection

KINS Banking Trojan/Data Theft (credentialed check)

Korgo Worm Detection

Kuang2 the Virus Detection

Linux FTP Server Backdoor Detection

Linux Malicious File Detection

Linux Malicious File Detection: User Defined Malware

Linux Malicious Process Detection

Linux/Cdorked.A Backdoor

Lion Worm Detection

Lovgate Virus Detection

LusyPOS Malware Detection

Mac OS X Malicious Process Detection

MacOS Malicious File Detection

MacOS Malicious File Detection: User Defined Malware

Malicious Process Detection: User Defined Malware Running (Linux)

Malicious Process Detection: User Defined Malware Running (Mac OS X)

Malware Payload Code detection

Microsoft IE FRAME/IFRAME/EMBED Tag Overflow (Bofra Worm Detection)

Microsoft IIS Download.Ject Trojan Detection

Microsoft IIS Potentially Compromised Host Detection

MoonLit Virus Backdoor Detection

MS03-039 Exploitation Backdoor Account Detection

MS04-028 Exploitation Backdoor Account Detection

mstream DDoS Agent Detection

mstream DDoS Handler Detection

MyDoom Virus Backdoor Detection

NCASE Software Detection

Ncat TLS Listener

NetBus 1.x Software Detection

NetBus 2.x Software Detection

NetSphere Backdoor Detection

NetSpy Malware Services Detection

PhatBOT Backdoor Detection

Piriform CCleaner 5.33.6162 Backdoor

Portal of Doom Backdoor Detection

PostNuke Trojaned Distribution

Radmin (Remote Administrator) Port 10002 - Possible GDI Compromise

Radmin (Remote Administrator) Port 4899 Detection

RemotelyAnywhere SSH Detection

RemotelyAnywhere WWW Detection

RemoteNC Backdoor Detection

Reputation of Linux Executables: Never seen process(es)

Reputation of macOS Executables: Never seen process(es)

Sasser Virus Detection

ScMM DSL Modem/Router Backdoor Detection

Shaft Trojan Detection

SingTel Backdoor Detection (ForgotDoor)

SMTP Server Non-standard Port Detection

Stacheldraht Trojan Detection

Stuxnet Worm Detection

Stuxnet Worm Detection (uncredentialed check)

SubSeven Trojan Detection

SYAC DigiEye Backdoor Detection

SyGate Backdoor Detection

TCP Port 0 Open: Possible Backdoor

TFN (Tribe Flood Network) Trojan Detection

TFTP Backdoor Detection

TIMESINK Spyware Detection

Trin00 for Windows Trojan Detection

Trin00 Trojan Detection

Trinity v3 Trojan Detection

Trojan Horse Detection

Unmanarc Remote Control Server (URCS) Detection

Unpassworded 'bash' Backdoor Account

UnrealIRCd Backdoor Detection

VCATCH Spyware Detection

W32.Dabber Worm Detection

w32.spybot.fcd Worm Infection Detection

WinSATAN Backdoor Detection

WinShell Trojan Detection

Wollf Backdoor Detection

YARA File Scan (Linux)

YARA Memory Scan (Linux)

YARA Scan Cleanup (Linux)

YARA Scan Setup (Linux)

Zeus/Zbot Banking Trojan/Data Theft (credentialed check)

Zincite.A (MyDoom.M) Backdoor Detection

Zotob Worm Detection

ZTE F460 / F660 Cable Modems web\_shell\_cmd.gch Administrative Backdoor

ZXShell Malware Services Detection

# Amazon Linux Local Security Checks

Amazon Linux 2 : 389-ds-base (ALAS-2018-1036)

Amazon Linux 2 : 389-ds-base (ALAS-2018-1094)

Amazon Linux 2 : 389-ds-base (ALAS-2018-1106)

Amazon Linux 2 : 389-ds-base (ALAS-2018-955)

Amazon Linux 2 : 389-ds-base (ALAS-2018-980)

Amazon Linux 2 : 389-ds-base (ALAS-2019-1262)

Amazon Linux 2 : 389-ds-base (ALAS-2020-1381)

Amazon Linux 2 : advancecomp (ALAS-2019-1319)

Amazon Linux 2 : apache-commons-beanutils (ALAS-2020-1395)

Amazon Linux 2 : bind (ALAS-2018-1082)

Amazon Linux 2 : bind (ALAS-2018-954)

Amazon Linux 2 : bind (ALAS-2019-1170)

Amazon Linux 2 : bind (ALAS-2019-1187)

Amazon Linux 2 : bind (ALAS-2019-1231)

Amazon Linux 2 : binutils (ALAS-2019-1138)

Amazon Linux 2 : binutils (ALAS-2019-1185)

Amazon Linux 2 : binutils (ALAS-2019-1358)

Amazon Linux 2 : blktrace (ALAS-2019-1320)

Amazon Linux 2 : compat-libtiff3 (ALAS-2019-1345)

Amazon Linux 2 : corosync (ALAS-2018-1014)

Amazon Linux 2 : curl (ALAS-2018-1029)

Amazon Linux 2 : curl (ALAS-2018-1052)

Amazon Linux 2 : curl (ALAS-2018-1135)

Amazon Linux 2 : curl (ALAS-2018-951)

Amazon Linux 2 : curl (ALAS-2018-995)

Amazon Linux 2 : curl (ALAS-2019-1162)

Amazon Linux 2 : curl (ALAS-2019-1233)

Amazon Linux 2 : curl (ALAS-2019-1340)

Amazon Linux 2 : dhcp (ALAS-2018-1021)

Amazon Linux 2 : dhcp (ALAS-2018-963)

Amazon Linux 2 : dhcp (ALAS-2018-984)

Amazon Linux 2 : dhcp (ALAS-2019-1346)

Amazon Linux 2 : dnsmasq (ALAS-2019-1251)

Amazon Linux 2 : dovecot (ALAS-2019-1347)

Amazon Linux 2 : edk2 (ALAS-2019-1273)

Amazon Linux 2 : edk2 (ALAS-2019-1290)

Amazon Linux 2 : elfutils (ALAS-2019-1337)

Amazon Linux 2 : exempi (ALAS-2019-1321)

Amazon Linux 2 : exiv2 (ALAS-2019-1339)

Amazon Linux 2 : fence-agents (ALAS-2019-1348)

Amazon Linux 2 : file (ALAS-2019-1370)

Amazon Linux 2 : filesystem (ALAS-2019-1175)

Amazon Linux 2 : filesystem (ALAS-2019-1190)

Amazon Linux 2 : flatpak (ALAS-2018-1096)

Amazon Linux 2 : flatpak (ALAS-2019-1183)

Amazon Linux 2 : flatpak (ALAS-2019-1219)

Amazon Linux 2 : freeradius (ALAS-2019-1218)

Amazon Linux 2 : freerdp (ALAS-2019-1191)

Amazon Linux 2 : freerdp (ALAS-2019-1365)

Amazon Linux 2 : fuse (ALAS-2018-1123)

Amazon Linux 2 : ghostscript (ALAS-2018-1022)

Amazon Linux 2 : ghostscript (ALAS-2018-1088)

Amazon Linux 2 : git (ALAS-2018-1035)

Amazon Linux 2 : git (ALAS-2018-1093)

Amazon Linux 2 : git (ALAS-2018-1136)

Amazon Linux 2 : git (ALAS-2019-1371)

Amazon Linux 2 : git (ALAS-2020-1409)

Amazon Linux 2 : glib2 (ALAS-2019-1289)

Amazon Linux 2 : glibc (ALAS-2018-1048)

Amazon Linux 2 : glibc (ALAS-2018-1131)

Amazon Linux 2 : glibc (ALAS-2018-992)

Amazon Linux 2 : glibc (ALAS-2019-1140)

Amazon Linux 2 : glusterfs (ALAS-2018-1128)

Amazon Linux 2 : gnupg2 (ALAS-2018-1045)

Amazon Linux 2 : gnupg2 (ALAS-2019-1203)

Amazon Linux 2 : gnutls (ALAS-2018-1120)

Amazon Linux 2 : golang (ALAS-2018-1011)

Amazon Linux 2 : golang (ALAS-2019-1172)

Amazon Linux 2 : golang (ALAS-2019-1272) (Ping Flood) (Reset Flood)

Amazon Linux 2 : golang (ALAS-2019-1309)

Amazon Linux 2 : golang (ALAS-2019-1335)

Amazon Linux 2 : golang (ALAS-2020-1383)

Amazon Linux 2 : http-parser (ALAS-2019-1322)

Amazon Linux 2 : httpd (ALAS-2018-1062)

Amazon Linux 2 : httpd (ALAS-2019-1155)

Amazon Linux 2 : httpd (ALAS-2019-1189)

Amazon Linux 2 : httpd (ALAS-2019-1341)

Amazon Linux 2 : jasper (ALAS-2019-1150)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2018-1007)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2018-1037) (Spectre)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2018-1064)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2018-1111)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2019-1209)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2019-1268)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2019-1372)

Amazon Linux 2 : java-1.7.0-openjdk (ALAS-2020-1403)

Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2018-1002)

Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2018-1039) (Spectre)

Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2018-1054)

Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2018-1097)

Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2018-949)

Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2019-1269)

Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2020-1396)

Amazon Linux 2 : java-1.8.0-openjdk / java-1.7.0-openjdk (ALAS-2019-1177)

Amazon Linux 2 : java-11-amazon-corretto (ALAS-2019-1228)

Amazon Linux 2 : java-11-amazon-corretto (ALAS-2019-1246)

Amazon Linux 2 : java-11-amazon-corretto (ALAS-2019-1316)

Amazon Linux 2 : java-11-amazon-corretto (ALAS-2020-1387)

Amazon Linux 2 : java-11-amazon-corretto (ALAS-2020-1410)

Amazon Linux 2 : java-11-openjdk (ALAS-2019-1338) (Spectre)

Amazon Linux 2 : keepalived (ALAS-2019-1154)

Amazon Linux 2 : keepalived (ALAS-2019-1323)

Amazon Linux 2 : kernel (ALAS-2018-1023)

Amazon Linux 2 : kernel (ALAS-2018-1038) (Spectre)

Amazon Linux 2 : kernel (ALAS-2018-1044)

Amazon Linux 2 : kernel (ALAS-2018-1046)

Amazon Linux 2 : kernel (ALAS-2018-1050)

Amazon Linux 2 : kernel (ALAS-2018-1051)

Amazon Linux 2 : kernel (ALAS-2018-1058) (Foreshadow)

Amazon Linux 2 : kernel (ALAS-2018-1086)

Amazon Linux 2 : kernel (ALAS-2018-1087)

Amazon Linux 2 : kernel (ALAS-2018-1100)

Amazon Linux 2 : kernel (ALAS-2018-1133)

Amazon Linux 2 : kernel (ALAS-2018-939) (Meltdown) (Spectre)

Amazon Linux 2 : kernel (ALAS-2018-956) (Dirty COW) (Spectre)

Amazon Linux 2 : kernel (ALAS-2018-971)

Amazon Linux 2 : kernel (ALAS-2018-994)

Amazon Linux 2 : kernel (ALAS-2019-1145)

Amazon Linux 2 : kernel (ALAS-2019-1149)

Amazon Linux 2 : kernel (ALAS-2019-1165)

Amazon Linux 2 : kernel (ALAS-2019-1167)

Amazon Linux 2 : kernel (ALAS-2019-1179)

Amazon Linux 2 : kernel (ALAS-2019-1201)

Amazon Linux 2 : kernel (ALAS-2019-1205) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Amazon Linux 2 : kernel (ALAS-2019-1212)

Amazon Linux 2 : kernel (ALAS-2019-1214)

Amazon Linux 2 : kernel (ALAS-2019-1222) (SACK Panic) (SACK Slowness)

Amazon Linux 2 : kernel (ALAS-2019-1232)

Amazon Linux 2 : kernel (ALAS-2019-1253)

Amazon Linux 2 : kernel (ALAS-2019-1278)

Amazon Linux 2 : kernel (ALAS-2019-1279)

Amazon Linux 2 : kernel (ALAS-2019-1280)

Amazon Linux 2 : kernel (ALAS-2019-1281)

Amazon Linux 2 : kernel (ALAS-2019-1293)

Amazon Linux 2 : kernel (ALAS-2019-1366)

Amazon Linux 2 : kernel (ALAS-2020-1392)

Amazon Linux 2 : kernel (ALAS-2020-1399)

Amazon Linux 2 : kernel (ALAS-2020-1405)

Amazon Linux 2 : keycloak-httpd-client-install (ALAS-2019-1324)

Amazon Linux 2 : krb5 (ALAS-2018-1010)

Amazon Linux 2 : krb5 (ALAS-2018-1129)

Amazon Linux 2 : libarchive (ALAS-2019-1325)

Amazon Linux 2 : libarchive (ALAS-2020-1391)

Amazon Linux 2 : libcdio (ALAS-2019-1151)

Amazon Linux 2 : libcgroup (ALAS-2019-1336)

Amazon Linux 2 : libevent (ALAS-2019-1359)

Amazon Linux 2 : libidn2 (ALAS-2019-1373)

Amazon Linux 2 : libjpeg-turbo (ALAS-2019-1198)

Amazon Linux 2 : libjpeg-turbo (ALAS-2019-1350)

Amazon Linux 2 : libmspack (ALAS-2019-1152)

Amazon Linux 2 : libmspack (ALAS-2019-1310)

Amazon Linux 2 : libqb (ALAS-2019-1210)

Amazon Linux 2 : librelp (ALAS-2018-998)

Amazon Linux 2 : libseccomp (ALAS-2019-1360)

Amazon Linux 2 : libsolv (ALAS-2019-1374)

Amazon Linux 2 : libssh2 (ALAS-2019-1199)

Amazon Linux 2 : libssh2 (ALAS-2019-1263)

Amazon Linux 2 : libssh2 (ALAS-2019-1303)

Amazon Linux 2 : libtiff (ALAS-2019-1327)

Amazon Linux 2 : libvirt (ALAS-2018-1033) (Spectre)

Amazon Linux 2 : libvirt (ALAS-2018-1049) (Spectre)

Amazon Linux 2 : libvirt (ALAS-2018-1134)

Amazon Linux 2 : libvirt (ALAS-2018-952) (Spectre)

Amazon Linux 2 : libvirt (ALAS-2019-1274) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Amazon Linux 2 : libvirt (ALAS-2019-1361)

Amazon Linux 2 : libvncserver (ALAS-2018-1012)

Amazon Linux 2 : libvncserver (ALAS-2019-1161)

Amazon Linux 2 : libvorbis (ALAS-2018-981)

Amazon Linux 2 : libvpx (ALAS-2018-1015)

Amazon Linux 2 : libwmf (ALAS-2019-1174)

Amazon Linux 2 : libwpd (ALAS-2019-1311)

Amazon Linux 2 : libX11 (ALAS-2019-1226)

Amazon Linux 2 : libXcursor (ALAS-2019-1173)

Amazon Linux 2 : libxml2 (ALAS-2019-1220)

Amazon Linux 2 : libxml2 (ALAS-2019-1301)

Amazon Linux 2 : linux-firmware (ALAS-2018-962) (Spectre)

Amazon Linux 2 : mailman (ALAS-2018-985)

Amazon Linux 2 : mariadb (ALAS-2018-1078)

Amazon Linux 2 : mariadb (ALAS-2019-1193)

Amazon Linux 2 : mariadb (ALAS-2019-1292)

Amazon Linux 2 : memcached (ALAS-2018-964)

Amazon Linux 2 : mercurial (ALAS-2019-1328)

Amazon Linux 2 : microcode\_ctl (ALAS-2018-953) (Spectre)

Amazon Linux 2 : microcode\_ctl / kernel (ALAS-2019-1364)

Amazon Linux 2 : mod\_auth\_mellon (ALAS-2019-1200)

Amazon Linux 2 : mod\_auth\_openidc (ALAS-2019-1329)

Amazon Linux 2 : mod\_http2 (ALAS-2018-1104)

Amazon Linux 2 : mod\_http2 (ALAS-2019-1197)

Amazon Linux 2 : mod\_http2 (ALAS-2019-1264)

Amazon Linux 2 : mod\_http2 (ALAS-2019-1342) (0-Length Headers Leak) (Data Dribble) (Internal Data Buffering)

Amazon Linux 2 : mod\_wsgi (ALAS-2018-987)

Amazon Linux 2 : mutt (ALAS-2018-1077)

Amazon Linux 2 : nautilus (ALAS-2018-960)

Amazon Linux 2 : ncurses (ALAS-2018-1053)

Amazon Linux 2 : ncurses (ALAS-2019-1302)

Amazon Linux 2 : NetworkManager (ALAS-2019-1144)

Amazon Linux 2 : nghttp2 (ALAS-2018-1020)

Amazon Linux 2 : nghttp2 (ALAS-2019-1298) (Data Dribble) (Resource Loop)

Amazon Linux 2 : nss (ALAS-2018-1095)

Amazon Linux 2 : nss (ALAS-2019-1305)

Amazon Linux 2 : nss (ALAS-2020-1384)

Amazon Linux 2 : nss-pem (ALAS-2019-1139)

Amazon Linux 2 : nss-softokn (ALAS-2020-1379)

Amazon Linux 2 : ntp (ALAS-2018-1009)

Amazon Linux 2 : ntp (ALAS-2019-1367)

Amazon Linux 2 : oniguruma (ALAS-2019-1288)

Amazon Linux 2 : oniguruma (ALAS-2020-1380)

Amazon Linux 2 : opensc (ALAS-2019-1312)

Amazon Linux 2 : openslp (ALAS-2018-1060)

Amazon Linux 2 : openslp (ALAS-2019-1378)

Amazon Linux 2 : openssh (ALAS-2018-1042)

Amazon Linux 2 : openssh (ALAS-2018-1075)

Amazon Linux 2 : openssh (ALAS-2019-1216)

Amazon Linux 2 : openssl (ALAS-2018-1004)

Amazon Linux 2 : openssl (ALAS-2018-1102)

Amazon Linux 2 : openssl (ALAS-2019-1153)

Amazon Linux 2 : openssl (ALAS-2019-1188)

Amazon Linux 2 : openssl (ALAS-2019-1362)

Amazon Linux 2 : openssl (ALAS-2020-1406)

Amazon Linux 2 : openwsman (ALAS-2019-1196)

Amazon Linux 2 : optipng (ALAS-2019-1313)

Amazon Linux 2 : pacemaker (ALAS-2019-1275)

Amazon Linux 2 : PackageKit (ALAS-2018-1006)

Amazon Linux 2 : patch (ALAS-2018-1008)

Amazon Linux 2 : patch (ALAS-2019-1317)

Amazon Linux 2 : pcs (ALAS-2018-1005)

Amazon Linux 2 : perl (ALAS-2019-1166)

Amazon Linux 2 : perl-Archive-Tar (ALAS-2019-1330)

Amazon Linux 2 : php (ALAS-2019-1344)

Amazon Linux 2 : php-pear (ALAS-2019-1159)

Amazon Linux 2 : plexus-archiver (ALAS-2018-1043)

Amazon Linux 2 : policycoreutils (ALAS-2018-1076)

Amazon Linux 2 : polkit (ALAS-2019-1171)

Amazon Linux 2 : polkit (ALAS-2019-1331)

Amazon Linux 2 : poppler (ALAS-2019-1217)

Amazon Linux 2 : poppler (ALAS-2019-1332)

Amazon Linux 2 : postgresql (ALAS-2018-1080)

Amazon Linux 2 : ppp (ALAS-2020-1400)

Amazon Linux 2 : procps-ng (ALAS-2018-1031)

Amazon Linux 2 : procps-ng (ALAS-2019-1333)

Amazon Linux 2 : python (ALAS-2019-1230)

Amazon Linux 2 : python (ALAS-2019-1258)

Amazon Linux 2 : python (ALAS-2019-1291)

Amazon Linux 2 : python / python3 (ALAS-2019-1368)

Amazon Linux 2 : python-jinja2 (ALAS-2019-1223)

Amazon Linux 2 : python-pip (ALAS-2020-1389)

Amazon Linux 2 : python-reportlab (ALAS-2020-1390)

Amazon Linux 2 : python-requests (ALAS-2019-1334)

Amazon Linux 2 : python-urllib3 (ALAS-2019-1211)

Amazon Linux 2 : python3 (ALAS-2018-1132)

Amazon Linux 2 : python3 (ALAS-2019-1169)

Amazon Linux 2 : python3 (ALAS-2019-1204)

Amazon Linux 2 : python3 (ALAS-2019-1247)

Amazon Linux 2 : python3 (ALAS-2019-1259)

Amazon Linux 2 : qemu (ALAS-2019-1248)

Amazon Linux 2 : qemu (ALAS-2020-1401)

Amazon Linux 2 : qemu (ALAS-2020-1407)

Amazon Linux 2 : qemu-kvm (ALAS-2018-1034) (Spectre)

Amazon Linux 2 : qemu-kvm (ALAS-2018-1073)

Amazon Linux 2 : qemu-kvm (ALAS-2018-942) (Spectre)

Amazon Linux 2 : qt5-qtbase (ALAS-2020-1397)

Amazon Linux 2 : rsyslog (ALAS-2019-1369)

Amazon Linux 2 : ruby (ALAS-2018-983)

Amazon Linux 2 : ruby (ALAS-2019-1143)

Amazon Linux 2 : ruby (ALAS-2019-1249)

Amazon Linux 2 : ruby (ALAS-2019-1276)

Amazon Linux 2 : samba (ALAS-2018-1126)

Amazon Linux 2 : samba (ALAS-2019-1351)

Amazon Linux 2 : SDL (ALAS-2019-1375)

Amazon Linux 2 : SDL2 (ALAS-2019-1318)

Amazon Linux 2 : setup (ALAS-2019-1158)

Amazon Linux 2 : slf4j (ALAS-2018-999)

Amazon Linux 2 : sox (ALAS-2019-1352)

Amazon Linux 2 : spamassassin (ALAS-2018-1103)

Amazon Linux 2 : spice (ALAS-2019-1184)

Amazon Linux 2 : spice-gtk (ALAS-2019-1363)

Amazon Linux 2 : sqlite (ALAS-2020-1394)

Amazon Linux 2 : sssd (ALAS-2018-1127)

Amazon Linux 2 : sssd (ALAS-2019-1343)

Amazon Linux 2 : stunnel / amazon-efs-utils (ALAS-2018-996)

Amazon Linux 2 : sudo (ALAS-2019-1315)

Amazon Linux 2 : sudo (ALAS-2020-1404)

Amazon Linux 2 : systemd (ALAS-2018-961)

Amazon Linux 2 : systemd (ALAS-2019-1141)

Amazon Linux 2 : systemd (ALAS-2019-1160)

Amazon Linux 2 : systemd (ALAS-2019-1164)

Amazon Linux 2 : systemd (ALAS-2020-1388)

Amazon Linux 2 : tcpdump (ALAS-2020-1385)

Amazon Linux 2 : thunderbird (ALAS-2018-1032)

Amazon Linux 2 : thunderbird (ALAS-2018-1061)

Amazon Linux 2 : thunderbird (ALAS-2019-1157)

Amazon Linux 2 : thunderbird (ALAS-2019-1168)

Amazon Linux 2 : thunderbird (ALAS-2019-1195)

Amazon Linux 2 : thunderbird (ALAS-2019-1229)

Amazon Linux 2 : thunderbird (ALAS-2019-1250)

Amazon Linux 2 : thunderbird (ALAS-2019-1267)

Amazon Linux 2 : thunderbird (ALAS-2019-1304)

Amazon Linux 2 : thunderbird (ALAS-2019-1376)

Amazon Linux 2 : thunderbird (ALAS-2020-1386)

Amazon Linux 2 : thunderbird (ALAS-2020-1393)

Amazon Linux 2 : thunderbird (ALAS-2020-1408)

Amazon Linux 2 : tomcat (ALAS-2018-1105)

Amazon Linux 2 : tomcat (ALAS-2019-1192)

Amazon Linux 2 : tomcat (ALAS-2020-1402)

Amazon Linux 2 : transfig (ALAS-2020-1398)

Amazon Linux 2 : udisks2 (ALAS-2019-1377)

Amazon Linux 2 : unixODBC (ALAS-2019-1354)

Amazon Linux 2 : unzip (ALAS-2019-1355)

Amazon Linux 2 : uriparser (ALAS-2019-1356)

Amazon Linux 2 : vim (ALAS-2019-1239)

Amazon Linux 2 : wget (ALAS-2018-1121)

Amazon Linux 2 : wget (ALAS-2019-1227)

Amazon Linux 2 : wpa\_supplicant (ALAS-2018-1122)

Amazon Linux 2 : xdg-user-dirs (ALAS-2018-1030)

Amazon Linux 2 : xerces-c (ALAS-2018-1124)

Amazon Linux 2 : xmlrpc (ALAS-2018-1041)

Amazon Linux 2 : yum-utils (ALAS-2018-1063)

Amazon Linux 2 : zsh (ALAS-2018-1013)

Amazon Linux 2 : zsh (ALAS-2018-1089)

Amazon Linux 2 : zsh (ALAS-2018-986)

Amazon Linux 2 : zziplib (ALAS-2019-1142)

Amazon Linux 2 : zziplib (ALAS-2019-1357)

Amazon Linux AMI : 389-ds-base (ALAS-2013-184)

Amazon Linux AMI : 389-ds-base (ALAS-2013-223)

Amazon Linux AMI : 389-ds-base (ALAS-2013-255)

Amazon Linux AMI : 389-ds-base (ALAS-2014-311)

Amazon Linux AMI : 389-ds-base (ALAS-2014-396)

Amazon Linux AMI : 389-ds-base (ALAS-2015-501)

Amazon Linux AMI : 389-ds-base (ALAS-2015-538)

Amazon Linux AMI : 389-ds-base (ALAS-2015-567)

Amazon Linux AMI : 389-ds-base (ALAS-2016-664)

Amazon Linux AMI : 389-ds-base (ALAS-2016-773)

Amazon Linux AMI : 389-ds-base (ALAS-2017-824)

Amazon Linux AMI : 389-ds-base (ALAS-2017-905)

Amazon Linux AMI : 389-ds-base (ALAS-2018-1036)

Amazon Linux AMI : 389-ds-base (ALAS-2018-1094)

Amazon Linux AMI : 389-ds-base (ALAS-2018-1106)

Amazon Linux AMI : 389-ds-base (ALAS-2018-955)

Amazon Linux AMI : 389-ds-base (ALAS-2018-980)

Amazon Linux AMI : 389-ds-base (ALAS-2019-1261)

Amazon Linux AMI : 389-ds-base (ALAS-2020-1334)

Amazon Linux AMI : ant (ALAS-2018-1047)

Amazon Linux AMI : apache-commons-collections (ALAS-2015-618)

Amazon Linux AMI : apache-commons-collections (ALAS-2016-692)

Amazon Linux AMI : apr (ALAS-2017-928)

Amazon Linux AMI : apr-util (ALAS-2017-929)

Amazon Linux AMI : augeas (ALAS-2013-250)

Amazon Linux AMI : augeas (ALAS-2014-286)

Amazon Linux AMI : authconfig (ALAS-2017-875)

Amazon Linux AMI : autofs (ALAS-2015-626)

Amazon Linux AMI : automake19 (ALAS-2014-401)

Amazon Linux AMI : aws-cfn-bootstrap (ALAS-2017-861)

Amazon Linux AMI : aws-cfn-bootstrap (ALAS-2017-866)

Amazon Linux AMI : aws-cfn-bootstrap (ALAS-2017-886)

Amazon Linux AMI : aws-cfn-bootstrap (ALAS-2017-895)

Amazon Linux AMI : axis (ALAS-2013-164)

Amazon Linux AMI : axis (ALAS-2014-412)

Amazon Linux AMI : bash (ALAS-2014-418) (Shellshock)

Amazon Linux AMI : bash (ALAS-2014-419)

Amazon Linux AMI : bash (ALAS-2017-878)

Amazon Linux AMI : bind (ALAS-2011-24)

Amazon Linux AMI : bind (ALAS-2012-113)

Amazon Linux AMI : bind (ALAS-2012-124)

Amazon Linux AMI : bind (ALAS-2012-138)

Amazon Linux AMI : bind (ALAS-2012-146)

Amazon Linux AMI : bind (ALAS-2012-84)

Amazon Linux AMI : bind (ALAS-2013-158)

Amazon Linux AMI : bind (ALAS-2013-176)

Amazon Linux AMI : bind (ALAS-2013-214)

Amazon Linux AMI : bind (ALAS-2014-287)

Amazon Linux AMI : bind (ALAS-2015-465)

Amazon Linux AMI : bind (ALAS-2015-490)

Amazon Linux AMI : bind (ALAS-2015-566)

Amazon Linux AMI : bind (ALAS-2015-573)

Amazon Linux AMI : bind (ALAS-2015-594)

Amazon Linux AMI : bind (ALAS-2015-631)

Amazon Linux AMI : bind (ALAS-2016-641)

Amazon Linux AMI : bind (ALAS-2016-665)

Amazon Linux AMI : bind (ALAS-2016-745)

Amazon Linux AMI : bind (ALAS-2016-751)

Amazon Linux AMI : bind (ALAS-2016-758)

Amazon Linux AMI : bind (ALAS-2016-768)

Amazon Linux AMI : bind (ALAS-2017-798)

Amazon Linux AMI : bind (ALAS-2017-826)

Amazon Linux AMI : bind (ALAS-2017-833)

Amazon Linux AMI : bind (ALAS-2017-858)

Amazon Linux AMI : bind (ALAS-2018-1082)

Amazon Linux AMI : bind (ALAS-2018-954)

Amazon Linux AMI : bind (ALAS-2019-1187)

Amazon Linux AMI : bind (ALAS-2019-1244)

Amazon Linux AMI : binutils (ALAS-2015-620)

Amazon Linux AMI : blktrace (ALAS-2019-1319)

Amazon Linux AMI : busybox (ALAS-2012-103)

Amazon Linux AMI : c-ares (ALAS-2017-859)

Amazon Linux AMI : ca-certificates (ALAS-2011-03)

Amazon Linux AMI : ca-certificates (ALAS-2011-3)

Amazon Linux AMI : ca-certificates (ALAS-2014-281)

Amazon Linux AMI : cacti (ALAS-2011-23)

Amazon Linux AMI : cacti (ALAS-2012-32)

Amazon Linux AMI : cacti (ALAS-2013-222)

Amazon Linux AMI : cacti (ALAS-2014-347)

Amazon Linux AMI : cacti (ALAS-2014-381)

Amazon Linux AMI : cacti (ALAS-2016-673)

Amazon Linux AMI : cacti (ALAS-2016-711)

Amazon Linux AMI : cacti (ALAS-2017-817)

Amazon Linux AMI : cacti (ALAS-2017-874)

Amazon Linux AMI : cacti (ALAS-2017-904)

Amazon Linux AMI : cacti (ALAS-2017-923)

Amazon Linux AMI : chkrootkit (ALAS-2014-370)

Amazon Linux AMI : chrony (ALAS-2014-366)

Amazon Linux AMI : chrony (ALAS-2015-539)

Amazon Linux AMI : clamav (ALAS-2014-457)

Amazon Linux AMI : clamav (ALAS-2015-486)

Amazon Linux AMI : clamav (ALAS-2015-537)

Amazon Linux AMI : clamav (ALAS-2018-958)

Amazon Linux AMI : clamav (ALAS-2018-976)

Amazon Linux AMI : clamav (ALAS-2019-1146)

Amazon Linux AMI : clamav (ALAS-2019-1213)

Amazon Linux AMI : clamav (ALAS-2020-1335)

Amazon Linux AMI : cloud-init (ALAS-2016-763)

Amazon Linux AMI : collectd (ALAS-2016-739)

Amazon Linux AMI : collectd (ALAS-2017-829)

Amazon Linux AMI : collectd (ALAS-2018-940)

Amazon Linux AMI : compat-libtiff3 (ALAS-2016-734)

Amazon Linux AMI : coreutils (ALAS-2013-261)

Amazon Linux AMI : cups (ALAS-2013-170)

Amazon Linux AMI : cups (ALAS-2014-438)

Amazon Linux AMI : cups (ALAS-2015-559)

Amazon Linux AMI : curl (ALAS-2013-210)

Amazon Linux AMI : curl (ALAS-2014-295)

Amazon Linux AMI : curl (ALAS-2014-322)

Amazon Linux AMI : curl (ALAS-2014-407)

Amazon Linux AMI : curl (ALAS-2015-477)

Amazon Linux AMI : curl (ALAS-2015-514)

Amazon Linux AMI : curl (ALAS-2015-551)

Amazon Linux AMI : curl (ALAS-2016-652)

Amazon Linux AMI : curl (ALAS-2016-730)

Amazon Linux AMI : curl (ALAS-2016-742)

Amazon Linux AMI : curl (ALAS-2016-766)

Amazon Linux AMI : curl (ALAS-2017-806)

Amazon Linux AMI : curl (ALAS-2017-850)

Amazon Linux AMI : curl (ALAS-2017-889)

Amazon Linux AMI : curl (ALAS-2017-919)

Amazon Linux AMI : curl (ALAS-2017-922)

Amazon Linux AMI : curl (ALAS-2018-1112)

Amazon Linux AMI : curl (ALAS-2018-938)

Amazon Linux AMI : curl (ALAS-2018-951)

Amazon Linux AMI : curl (ALAS-2018-995)

Amazon Linux AMI : curl (ALAS-2019-1148)

Amazon Linux AMI : curl (ALAS-2019-1151)

Amazon Linux AMI : curl (ALAS-2019-1233)

Amazon Linux AMI : curl (ALAS-2019-1294)

Amazon Linux AMI : cvs (ALAS-2012-51)

Amazon Linux AMI : cyrus-imapd (ALAS-2011-2)

Amazon Linux AMI : cyrus-imapd (ALAS-2011-27)

Amazon Linux AMI : cyrus-impad (ALAS-2011-02)

Amazon Linux AMI : cyrus-sasl (ALAS-2014-338)

Amazon Linux AMI : dbus (ALAS-2012-128)

Amazon Linux AMI : dbus (ALAS-2019-1246)

Amazon Linux AMI : dhcp (ALAS-2012-115)

Amazon Linux AMI : dhcp (ALAS-2012-31)

Amazon Linux AMI : dhcp (ALAS-2013-157)

Amazon Linux AMI : dhcp (ALAS-2016-637)

Amazon Linux AMI : dhcp (ALAS-2018-1024)

Amazon Linux AMI : dhcp (ALAS-2018-984)

Amazon Linux AMI : dnsmasq (ALAS-2013-161)

Amazon Linux AMI : dnsmasq (ALAS-2017-907)

Amazon Linux AMI : docker (ALAS-2014-454)

Amazon Linux AMI : docker (ALAS-2014-461)

Amazon Linux AMI : docker (ALAS-2015-522)

Amazon Linux AMI : docker (ALAS-2017-783)

Amazon Linux AMI : docker (ALAS-2018-1071)

Amazon Linux AMI : docker (ALAS-2018-941)

Amazon Linux AMI : docker (ALAS-2019-1156)

Amazon Linux AMI : docker (ALAS-2019-1245)

Amazon Linux AMI : docker (ALAS-2019-1316)

Amazon Linux AMI : dovecot (ALAS-2014-386)

Amazon Linux AMI : dracut (ALAS-2013-257)

Amazon Linux AMI : e2fsprogs (ALAS-2015-478)

Amazon Linux AMI : e2fsprogs (ALAS-2015-542)

Amazon Linux AMI : elfutils (ALAS-2014-345)

Amazon Linux AMI : emacs (ALAS-2017-912)

Amazon Linux AMI : exim (ALAS-2014-395)

Amazon Linux AMI : exim (ALAS-2017-804)

Amazon Linux AMI : exim (ALAS-2017-932)

Amazon Linux AMI : exim (ALAS-2018-970)

Amazon Linux AMI : exim (ALAS-2018-997)

Amazon Linux AMI : exim (ALAS-2019-1221)

Amazon Linux AMI : exim (ALAS-2019-1252)

Amazon Linux AMI : exim (ALAS-2019-1277)

Amazon Linux AMI : exim (ALAS-2019-1310)

Amazon Linux AMI : expat (ALAS-2012-89)

Amazon Linux AMI : expat (ALAS-2016-775)

Amazon Linux AMI : facter (ALAS-2014-456)

Amazon Linux AMI : fail2ban (ALAS-2013-209)

Amazon Linux AMI : fetchmail (ALAS-2012-132)

Amazon Linux AMI : file (ALAS-2014-304)

Amazon Linux AMI : file (ALAS-2014-323)

Amazon Linux AMI : file (ALAS-2014-382)

Amazon Linux AMI : file (ALAS-2014-398)

Amazon Linux AMI : file (ALAS-2014-453)

Amazon Linux AMI : file (ALAS-2015-497)

Amazon Linux AMI : file (ALAS-2017-900)

Amazon Linux AMI : file (ALAS-2019-1186)

Amazon Linux AMI : file (ALAS-2019-1326)

Amazon Linux AMI : flac (ALAS-2015-505)

Amazon Linux AMI : foomatic (ALAS-2016-690)

Amazon Linux AMI : freeradius (ALAS-2012-131)

Amazon Linux AMI : freeradius (ALAS-2015-581)

Amazon Linux AMI : freeradius (ALAS-2017-865)

Amazon Linux AMI : freetype (ALAS-2011-08)

Amazon Linux AMI : freetype (ALAS-2011-20)

Amazon Linux AMI : freetype (ALAS-2011-8)

Amazon Linux AMI : freetype (ALAS-2012-66)

Amazon Linux AMI : freetype (ALAS-2013-150)

Amazon Linux AMI : freetype (ALAS-2015-502)

Amazon Linux AMI : freetype (ALAS-2020-1348)

Amazon Linux AMI : fuse (ALAS-2015-558)

Amazon Linux AMI : fuse (ALAS-2018-1123)

Amazon Linux AMI : fwsnort (ALAS-2014-409)

Amazon Linux AMI : ganglia (ALAS-2013-268)

Amazon Linux AMI : ganglia (ALAS-2015-612)

Amazon Linux AMI : gc (ALAS-2013-245)

Amazon Linux AMI : gdb (ALAS-2013-159)

Amazon Linux AMI : ghostscript (ALAS-2012-127)

Amazon Linux AMI : ghostscript (ALAS-2012-42)

Amazon Linux AMI : ghostscript (ALAS-2017-784)

Amazon Linux AMI : ghostscript (ALAS-2017-837)

Amazon Linux AMI : ghostscript (ALAS-2018-1137)

Amazon Linux AMI : git (ALAS-2015-613)

Amazon Linux AMI : git (ALAS-2016-672)

Amazon Linux AMI : git (ALAS-2017-842)

Amazon Linux AMI : git (ALAS-2017-882)

Amazon Linux AMI : git (ALAS-2017-910)

Amazon Linux AMI : git (ALAS-2018-1035)

Amazon Linux AMI : git (ALAS-2018-1093)

Amazon Linux AMI : git (ALAS-2018-1136)

Amazon Linux AMI : git (ALAS-2018-948)

Amazon Linux AMI : git (ALAS-2019-1325)

Amazon Linux AMI : git (ALAS-2020-1357)

Amazon Linux AMI : gitolite3 (ALAS-2018-1092)

Amazon Linux AMI : glib2 (ALAS-2019-1256)

Amazon Linux AMI : glibc (ALAS-2012-109)

Amazon Linux AMI : glibc (ALAS-2012-120)

Amazon Linux AMI : glibc (ALAS-2012-39)

Amazon Linux AMI : glibc (ALAS-2012-57)

Amazon Linux AMI : glibc (ALAS-2013-270)

Amazon Linux AMI : glibc (ALAS-2014-355)

Amazon Linux AMI : glibc (ALAS-2014-399)

Amazon Linux AMI : glibc (ALAS-2014-400)

Amazon Linux AMI : glibc (ALAS-2015-468)

Amazon Linux AMI : glibc (ALAS-2015-473)

Amazon Linux AMI : glibc (ALAS-2015-495)

Amazon Linux AMI : glibc (ALAS-2015-513)

Amazon Linux AMI : glibc (ALAS-2015-617)

Amazon Linux AMI : glibc (ALAS-2016-653)

Amazon Linux AMI : glibc (ALAS-2016-660)

Amazon Linux AMI : glibc (ALAS-2017-792)

Amazon Linux AMI : glibc (ALAS-2017-844) (Stack Clash)

Amazon Linux AMI : glibc (ALAS-2017-877)

Amazon Linux AMI : glibc (ALAS-2018-1017)

Amazon Linux AMI : glibc (ALAS-2018-1109)

Amazon Linux AMI : glibc (ALAS-2019-1320)

Amazon Linux AMI : gnupg (ALAS-2013-225)

Amazon Linux AMI : gnupg (ALAS-2013-236)

Amazon Linux AMI : gnupg (ALAS-2014-278)

Amazon Linux AMI : gnupg (ALAS-2014-378)

Amazon Linux AMI : gnupg / gnupg2 (ALAS-2018-1045)

Amazon Linux AMI : gnupg2 (ALAS-2013-237)

Amazon Linux AMI : gnupg2 (ALAS-2014-379)

Amazon Linux AMI : gnupg2 (ALAS-2015-574)

Amazon Linux AMI : gnupg2 (ALAS-2018-1025)

Amazon Linux AMI : gnutls (ALAS-2012-59)

Amazon Linux AMI : gnutls (ALAS-2013-172)

Amazon Linux AMI : gnutls (ALAS-2013-197)

Amazon Linux AMI : gnutls (ALAS-2014-301)

Amazon Linux AMI : gnutls (ALAS-2014-352)

Amazon Linux AMI : gnutls (ALAS-2015-575)

Amazon Linux AMI : gnutls (ALAS-2016-651) (SLOTH)

Amazon Linux AMI : gnutls (ALAS-2017-815)

Amazon Linux AMI : golang (ALAS-2014-437)

Amazon Linux AMI : golang (ALAS-2016-687)

Amazon Linux AMI : golang (ALAS-2016-731) (httpoxy)

Amazon Linux AMI : golang (ALAS-2017-857)

Amazon Linux AMI : golang (ALAS-2017-918)

Amazon Linux AMI : golang (ALAS-2018-1130)

Amazon Linux AMI : golang (ALAS-2018-975)

Amazon Linux AMI : golang (ALAS-2019-1172)

Amazon Linux AMI : golang (ALAS-2019-1238)

Amazon Linux AMI : golang (ALAS-2019-1270) (Ping Flood) (Reset Flood)

Amazon Linux AMI : golang (ALAS-2019-1321)

Amazon Linux AMI : golang (ALAS-2020-1336)

Amazon Linux AMI : golang / docker (ALAS-2015-588)

Amazon Linux AMI : gpgme (ALAS-2015-500)

Amazon Linux AMI : GraphicsMagick (ALAS-2014-420)

Amazon Linux AMI : GraphicsMagick (ALAS-2016-678)

Amazon Linux AMI : GraphicsMagick (ALAS-2016-717)

Amazon Linux AMI : GraphicsMagick (ALAS-2016-752)

Amazon Linux AMI : GraphicsMagick (ALAS-2017-820)

Amazon Linux AMI : GraphicsMagick (ALAS-2017-891)

Amazon Linux AMI : GraphicsMagick (ALAS-2018-966)

Amazon Linux AMI : GraphicsMagick (ALAS-2019-1257)

Amazon Linux AMI : graphite2 (ALAS-2016-696)

Amazon Linux AMI : graphite2 (ALAS-2017-872)

Amazon Linux AMI : graphviz (ALAS-2014-284)

Amazon Linux AMI : graphviz (ALAS-2014-296)

Amazon Linux AMI : graphviz (ALAS-2015-487)

Amazon Linux AMI : graphviz (ALAS-2019-1207)

Amazon Linux AMI : graphviz-php (ALAS-2014-285)

Amazon Linux AMI : graphviz-php (ALAS-2014-297)

Amazon Linux AMI : graphviz-php (ALAS-2015-488)

Amazon Linux AMI : grep (ALAS-2015-598)

Amazon Linux AMI : grep (ALAS-2016-639)

Amazon Linux AMI : haproxy (ALAS-2013-215)

Amazon Linux AMI : httpd (ALAS-2011-01)

Amazon Linux AMI : httpd (ALAS-2011-09)

Amazon Linux AMI : httpd (ALAS-2011-1)

Amazon Linux AMI : httpd (ALAS-2011-9)

Amazon Linux AMI : httpd (ALAS-2012-46)

Amazon Linux AMI : httpd (ALAS-2013-174)

Amazon Linux AMI : httpd (ALAS-2013-193)

Amazon Linux AMI : httpd (ALAS-2014-331)

Amazon Linux AMI : httpd (ALAS-2014-388)

Amazon Linux AMI : httpd (ALAS-2014-414)

Amazon Linux AMI : httpd (ALAS-2015-578)

Amazon Linux AMI : httpd (ALAS-2017-851)

Amazon Linux AMI : httpd (ALAS-2017-892)

Amazon Linux AMI : httpd (ALAS-2017-921)

Amazon Linux AMI : httpd24 (ALAS-2013-175)

Amazon Linux AMI : httpd24 (ALAS-2013-194)

Amazon Linux AMI : httpd24 (ALAS-2014-309)

Amazon Linux AMI : httpd24 (ALAS-2014-389)

Amazon Linux AMI : httpd24 (ALAS-2015-483)

Amazon Linux AMI : httpd24 (ALAS-2015-579)

Amazon Linux AMI : httpd24 (ALAS-2017-785)

Amazon Linux AMI : httpd24 (ALAS-2017-863)

Amazon Linux AMI : httpd24 (ALAS-2018-1004)

Amazon Linux AMI : httpd24 (ALAS-2018-1062)

Amazon Linux AMI : httpd24 (ALAS-2018-1104)

Amazon Linux AMI : httpd24 (ALAS-2019-1166)

Amazon Linux AMI : httpd24 (ALAS-2019-1189)

Amazon Linux AMI : httpd24 (ALAS-2019-1311) (Internal Data Buffering)

Amazon Linux AMI : httpd24 / httpd (ALAS-2016-725) (httpoxy)

Amazon Linux AMI : httpd24 / httpd (ALAS-2017-896) (Optionsbleed)

Amazon Linux AMI : icu (ALAS-2012-33)

Amazon Linux AMI : ImageMagick (ALAS-2012-76)

Amazon Linux AMI : ImageMagick (ALAS-2014-336)

Amazon Linux AMI : ImageMagick (ALAS-2016-699) (ImageTragick)

Amazon Linux AMI : ImageMagick (ALAS-2016-716)

Amazon Linux AMI : iproute (ALAS-2012-64)

Amazon Linux AMI : jakarta-commons-httpclient (ALAS-2013-169)

Amazon Linux AMI : jakarta-commons-httpclient (ALAS-2014-410)

Amazon Linux AMI : jakarta-taglibs-standard (ALAS-2015-595)

Amazon Linux AMI : jasper (ALAS-2011-29)

Amazon Linux AMI : jasper (ALAS-2015-466)

Amazon Linux AMI : jasper (ALAS-2015-479)

Amazon Linux AMI : jasper (ALAS-2017-836)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2011-10) (BEAST)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2012-119)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2012-136) (ROBOT)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2012-43)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2012-88)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2013-155)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2013-163)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2013-167)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2013-185)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2013-207)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2013-246)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2014-283)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2014-326)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2014-387)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2014-430)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2015-480) (POODLE)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2015-515)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2015-586) (Bar Mitzvah) (Logjam)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2015-616)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2016-654)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2016-700)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2016-748)

Amazon Linux AMI : java-1.6.0-openjdk (ALAS-2017-795)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2012-137) (ROBOT)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2013-151)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2013-156)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2013-162)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2013-168)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2013-183)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2013-204)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2013-235)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2014-280)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2014-327)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2014-383)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2014-431)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2015-471) (POODLE)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2015-516)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2015-570) (Bar Mitzvah) (Logjam)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2015-605)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2016-643) (SLOTH)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2016-693)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2016-729)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2016-771)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2017-797)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2017-835)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2017-869)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2017-936)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2018-1007)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2018-1037) (Spectre)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2018-1064)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2018-1111)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2018-974)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2019-1177)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2019-1268)

Amazon Linux AMI : java-1.7.0-openjdk (ALAS-2020-1354)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2014-432)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2015-472) (POODLE)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2015-517)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2015-571) (Bar Mitzvah) (Logjam)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2015-606)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2016-647) (SLOTH)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2016-688)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2016-723)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2016-759)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2017-791)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2017-827)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2017-860)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2017-917)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2018-1002)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2018-1039) (Spectre)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2018-1054)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2018-1097)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2018-949)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2019-1266)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2019-1269)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2020-1330)

Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2020-1345)

Amazon Linux AMI : java-1.8.0-openjdk / java-1.7.0-openjdk (ALAS-2016-677)

Amazon Linux AMI : jbigkit (ALAS-2014-337)

Amazon Linux AMI : jq (ALAS-2016-705)

Amazon Linux AMI : json-c (ALAS-2014-416)

Amazon Linux AMI : kernel (ALAS-2011-16)

Amazon Linux AMI : kernel (ALAS-2011-22)

Amazon Linux AMI : kernel (ALAS-2011-26)

Amazon Linux AMI : kernel (ALAS-2012-100)

Amazon Linux AMI : kernel (ALAS-2012-118)

Amazon Linux AMI : kernel (ALAS-2012-122)

Amazon Linux AMI : kernel (ALAS-2012-133)

Amazon Linux AMI : kernel (ALAS-2012-142)

Amazon Linux AMI : kernel (ALAS-2012-34)

Amazon Linux AMI : kernel (ALAS-2012-45)

Amazon Linux AMI : kernel (ALAS-2012-55)

Amazon Linux AMI : kernel (ALAS-2012-58)

Amazon Linux AMI : kernel (ALAS-2012-78)

Amazon Linux AMI : kernel (ALAS-2012-83)

Amazon Linux AMI : kernel (ALAS-2013-166)

Amazon Linux AMI : kernel (ALAS-2013-200)

Amazon Linux AMI : kernel (ALAS-2013-218)

Amazon Linux AMI : kernel (ALAS-2013-228)

Amazon Linux AMI : kernel (ALAS-2013-233)

Amazon Linux AMI : kernel (ALAS-2013-252)

Amazon Linux AMI : kernel (ALAS-2013-258)

Amazon Linux AMI : kernel (ALAS-2014-289)

Amazon Linux AMI : kernel (ALAS-2014-317)

Amazon Linux AMI : kernel (ALAS-2014-328)

Amazon Linux AMI : kernel (ALAS-2014-339)

Amazon Linux AMI : kernel (ALAS-2014-363)

Amazon Linux AMI : kernel (ALAS-2014-368)

Amazon Linux AMI : kernel (ALAS-2014-392)

Amazon Linux AMI : kernel (ALAS-2014-417)

Amazon Linux AMI : kernel (ALAS-2014-455)

Amazon Linux AMI : kernel (ALAS-2015-476)

Amazon Linux AMI : kernel (ALAS-2015-489)

Amazon Linux AMI : kernel (ALAS-2015-491)

Amazon Linux AMI : kernel (ALAS-2015-523)

Amazon Linux AMI : kernel (ALAS-2015-544)

Amazon Linux AMI : kernel (ALAS-2015-565)

Amazon Linux AMI : kernel (ALAS-2015-603)

Amazon Linux AMI : kernel (ALAS-2015-610)

Amazon Linux AMI : kernel (ALAS-2016-642)

Amazon Linux AMI : kernel (ALAS-2016-648)

Amazon Linux AMI : kernel (ALAS-2016-669)

Amazon Linux AMI : kernel (ALAS-2016-694)

Amazon Linux AMI : kernel (ALAS-2016-703)

Amazon Linux AMI : kernel (ALAS-2016-704)

Amazon Linux AMI : kernel (ALAS-2016-718)

Amazon Linux AMI : kernel (ALAS-2016-726)

Amazon Linux AMI : kernel (ALAS-2016-740)

Amazon Linux AMI : kernel (ALAS-2016-757) (Dirty COW)

Amazon Linux AMI : kernel (ALAS-2016-762)

Amazon Linux AMI : kernel (ALAS-2016-772)

Amazon Linux AMI : kernel (ALAS-2017-782)

Amazon Linux AMI : kernel (ALAS-2017-786)

Amazon Linux AMI : kernel (ALAS-2017-805)

Amazon Linux AMI : kernel (ALAS-2017-811)

Amazon Linux AMI : kernel (ALAS-2017-814)

Amazon Linux AMI : kernel (ALAS-2017-828)

Amazon Linux AMI : kernel (ALAS-2017-832)

Amazon Linux AMI : kernel (ALAS-2017-845) (Stack Clash)

Amazon Linux AMI : kernel (ALAS-2017-846)

Amazon Linux AMI : kernel (ALAS-2017-868)

Amazon Linux AMI : kernel (ALAS-2017-870)

Amazon Linux AMI : kernel (ALAS-2017-897)

Amazon Linux AMI : kernel (ALAS-2017-901)

Amazon Linux AMI : kernel (ALAS-2017-914) (BlueBorne)

Amazon Linux AMI : kernel (ALAS-2017-925)

Amazon Linux AMI : kernel (ALAS-2017-937) (Dirty COW)

Amazon Linux AMI : kernel (ALAS-2018-1023)

Amazon Linux AMI : kernel (ALAS-2018-1038) (Spectre)

Amazon Linux AMI : kernel (ALAS-2018-1044)

Amazon Linux AMI : kernel (ALAS-2018-1046)

Amazon Linux AMI : kernel (ALAS-2018-1048)

Amazon Linux AMI : kernel (ALAS-2018-1049)

Amazon Linux AMI : kernel (ALAS-2018-1058) (Foreshadow)

Amazon Linux AMI : kernel (ALAS-2018-1086)

Amazon Linux AMI : kernel (ALAS-2018-1087)

Amazon Linux AMI : kernel (ALAS-2018-1100)

Amazon Linux AMI : kernel (ALAS-2018-1133)

Amazon Linux AMI : kernel (ALAS-2018-939) (Meltdown) (Spectre)

Amazon Linux AMI : kernel (ALAS-2018-944)

Amazon Linux AMI : kernel (ALAS-2018-956) (Dirty COW) (Spectre)

Amazon Linux AMI : kernel (ALAS-2018-971)

Amazon Linux AMI : kernel (ALAS-2018-993)

Amazon Linux AMI : kernel (ALAS-2019-1145)

Amazon Linux AMI : kernel (ALAS-2019-1149)

Amazon Linux AMI : kernel (ALAS-2019-1165)

Amazon Linux AMI : kernel (ALAS-2019-1167)

Amazon Linux AMI : kernel (ALAS-2019-1179)

Amazon Linux AMI : kernel (ALAS-2019-1201)

Amazon Linux AMI : kernel (ALAS-2019-1205) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Amazon Linux AMI : kernel (ALAS-2019-1212)

Amazon Linux AMI : kernel (ALAS-2019-1214)

Amazon Linux AMI : kernel (ALAS-2019-1222) (SACK Panic) (SACK Slowness)

Amazon Linux AMI : kernel (ALAS-2019-1232)

Amazon Linux AMI : kernel (ALAS-2019-1253)

Amazon Linux AMI : kernel (ALAS-2019-1278)

Amazon Linux AMI : kernel (ALAS-2019-1279)

Amazon Linux AMI : kernel (ALAS-2019-1280)

Amazon Linux AMI : kernel (ALAS-2019-1281)

Amazon Linux AMI : kernel (ALAS-2019-1293)

Amazon Linux AMI : kernel (ALAS-2019-1322)

Amazon Linux AMI : kernel (ALAS-2020-1338)

Amazon Linux AMI : kernel (ALAS-2020-1349)

Amazon Linux AMI : kernel / nvidia (ALAS-2013-148)

Amazon Linux AMI : kernel / nvidia (ALAS-2013-154)

Amazon Linux AMI : kernel Privilege Escalation (ALAS-2013-190)

Amazon Linux AMI : krb5 (ALAS-2011-15)

Amazon Linux AMI : krb5 (ALAS-2011-28)

Amazon Linux AMI : krb5 (ALAS-2012-114)

Amazon Linux AMI : krb5 (ALAS-2013-182)

Amazon Linux AMI : krb5 (ALAS-2013-208)

Amazon Linux AMI : krb5 (ALAS-2014-443)

Amazon Linux AMI : krb5 (ALAS-2015-518)

Amazon Linux AMI : krb5 (ALAS-2015-624)

Amazon Linux AMI : krb5 (ALAS-2016-691)

Amazon Linux AMI : krb5 (ALAS-2017-793)

Amazon Linux AMI : krb5 (ALAS-2018-1010)

Amazon Linux AMI : krb5 (ALAS-2018-1129)

Amazon Linux AMI : libapreq2 (ALAS-2019-1323)

Amazon Linux AMI : libarchive (ALAS-2016-743)

Amazon Linux AMI : libarchive (ALAS-2019-1308)

Amazon Linux AMI : libarchive (ALAS-2020-1343)

Amazon Linux AMI : libcap-ng (ALAS-2015-543)

Amazon Linux AMI : libexif (ALAS-2012-126)

Amazon Linux AMI : libgcrypt (ALAS-2013-226)

Amazon Linux AMI : libgcrypt (ALAS-2015-577)

Amazon Linux AMI : libgcrypt / gnupg (ALAS-2016-744)

Amazon Linux AMI : libidn2 (ALAS-2019-1327)

Amazon Linux AMI : libjpeg-turbo (ALAS-2013-267)

Amazon Linux AMI : libjpeg-turbo (ALAS-2015-540)

Amazon Linux AMI : libjpeg-turbo (ALAS-2019-1286)

Amazon Linux AMI : libksba (ALAS-2016-712)

Amazon Linux AMI : libldb (ALAS-2016-633)

Amazon Linux AMI : libmicrohttpd (ALAS-2014-353)

Amazon Linux AMI : libnl3 (ALAS-2017-876)

Amazon Linux AMI : libpng (ALAS-2012-49)

Amazon Linux AMI : libpng (ALAS-2012-56)

Amazon Linux AMI : libpng (ALAS-2012-68)

Amazon Linux AMI : libpng (ALAS-2015-611)

Amazon Linux AMI : libpng (ALAS-2015-615)

Amazon Linux AMI : libproxy (ALAS-2012-140)

Amazon Linux AMI : libserf (ALAS-2014-397)

Amazon Linux AMI : libssh2 (ALAS-2016-683)

Amazon Linux AMI : libssh2 (ALAS-2019-1254)

Amazon Linux AMI : libtasn1 (ALAS-2012-60)

Amazon Linux AMI : libtasn1 (ALAS-2014-359)

Amazon Linux AMI : libtiff (ALAS-2012-106)

Amazon Linux AMI : libtiff (ALAS-2012-147)

Amazon Linux AMI : libtiff (ALAS-2012-65)

Amazon Linux AMI : libtiff (ALAS-2014-307)

Amazon Linux AMI : libtiff (ALAS-2014-365)

Amazon Linux AMI : libtiff (ALAS-2015-553)

Amazon Linux AMI : libtiff (ALAS-2016-733)

Amazon Linux AMI : libtiff (ALAS-2019-1306)

Amazon Linux AMI : libtiff / compat-libtiff3 (ALAS-2017-802)

Amazon Linux AMI : libtirpc (ALAS-2013-199)

Amazon Linux AMI : libtirpc (ALAS-2017-840)

Amazon Linux AMI : libtommath / libtomcrypt (ALAS-2017-864)

Amazon Linux AMI : libunwind (ALAS-2015-600)

Amazon Linux AMI : libvorbis (ALAS-2012-47)

Amazon Linux AMI : libvorbis (ALAS-2018-981)

Amazon Linux AMI : libvpx (ALAS-2018-967)

Amazon Linux AMI : libwmf (ALAS-2015-604)

Amazon Linux AMI : libwmf (ALAS-2019-1174)

Amazon Linux AMI : libX11 / libXcursor,libXfixes,libXi,libXrandr,libXrender,libXres,libXt,libXv,libXvMC,libXxf86dga,libXxf86vm,libdmx,xorg-x11-proto-devel (ALAS-2014-452)

Amazon Linux AMI : libxcb (ALAS-2014-405)

Amazon Linux AMI : libXcursor (ALAS-2019-1150)

Amazon Linux AMI : libXext (ALAS-2014-403)

Amazon Linux AMI : libXfont (ALAS-2014-282)

Amazon Linux AMI : libXfont (ALAS-2014-404)

Amazon Linux AMI : libXfont (ALAS-2015-597)

Amazon Linux AMI : libxml2 (ALAS-2012-134)

Amazon Linux AMI : libxml2 (ALAS-2012-143)

Amazon Linux AMI : libxml2 (ALAS-2012-36)

Amazon Linux AMI : libxml2 (ALAS-2012-52)

Amazon Linux AMI : libxml2 (ALAS-2013-188)

Amazon Linux AMI : libxml2 (ALAS-2014-340)

Amazon Linux AMI : libxml2 (ALAS-2014-341)

Amazon Linux AMI : libxml2 (ALAS-2014-444)

Amazon Linux AMI : libxml2 (ALAS-2015-628)

Amazon Linux AMI : libxml2 (ALAS-2016-719)

Amazon Linux AMI : libxml2 (ALAS-2018-1072)

Amazon Linux AMI : libxslt (ALAS-2012-123)

Amazon Linux AMI : libxslt (ALAS-2019-1241)

Amazon Linux AMI : libXtst (ALAS-2014-406)

Amazon Linux AMI : libyaml (ALAS-2014-291)

Amazon Linux AMI : libyaml (ALAS-2014-321)

Amazon Linux AMI : libyaml (ALAS-2015-481)

Amazon Linux AMI : lighttpd (ALAS-2012-107)

Amazon Linux AMI : lighttpd (ALAS-2013-179)

Amazon Linux AMI : lighttpd (ALAS-2014-299)

Amazon Linux AMI : lighttpd (ALAS-2014-346)

Amazon Linux AMI : lighttpd (ALAS-2016-746)

Amazon Linux AMI : lighttpd (ALAS-2019-1265)

Amazon Linux AMI : lua (ALAS-2014-402)

Amazon Linux AMI : lynis (ALAS-2017-847)

Amazon Linux AMI : lzo (ALAS-2014-373)

Amazon Linux AMI : mailman (ALAS-2015-582)

Amazon Linux AMI : mailman (ALAS-2018-985)

Amazon Linux AMI : mailx (ALAS-2015-467)

Amazon Linux AMI : memcached (ALAS-2016-761)

Amazon Linux AMI : memcached (ALAS-2018-964)

Amazon Linux AMI : mercurial (ALAS-2016-697)

Amazon Linux AMI : mercurial (ALAS-2017-856)

Amazon Linux AMI : mercurial (ALAS-2017-893)

Amazon Linux AMI : mesa (ALAS-2013-198)

Amazon Linux AMI : microcode\_ctl / kernel (ALAS-2019-1318)

Amazon Linux AMI : mod24\_auth\_mellon (ALAS-2019-1200)

Amazon Linux AMI : mod24\_auth\_openidc (ALAS-2019-1300)

Amazon Linux AMI : mod24\_fcgid (ALAS-2013-239)

Amazon Linux AMI : mod24\_nss (ALAS-2013-254)

Amazon Linux AMI : mod24\_nss (ALAS-2016-650)

Amazon Linux AMI : mod24\_nss (ALAS-2016-714)

Amazon Linux AMI : mod24\_security (ALAS-2014-334)

Amazon Linux AMI : mod24\_wsgi (ALAS-2014-375)

Amazon Linux AMI : mod24\_wsgi (ALAS-2018-987)

Amazon Linux AMI : mod\_auth\_mellon / mod24\_auth\_mellon (ALAS-2018-968)

Amazon Linux AMI : mod\_auth\_mellon / mod24\_auth\_mellon (ALAS-2020-1331)

Amazon Linux AMI : mod\_dav\_svn (ALAS-2016-710)

Amazon Linux AMI : mod\_dav\_svn / subversion (ALAS-2015-555)

Amazon Linux AMI : mod\_dav\_svn / subversion (ALAS-2016-676)

Amazon Linux AMI : mod\_fcgid (ALAS-2013-238)

Amazon Linux AMI : mod\_nss (ALAS-2013-253)

Amazon Linux AMI : mod\_perl / mod24\_perl (ALAS-2018-1085)

Amazon Linux AMI : mod\_security (ALAS-2014-335)

Amazon Linux AMI : mod\_wsgi (ALAS-2014-376)

Amazon Linux AMI : munin (ALAS-2012-130)

Amazon Linux AMI : munin (ALAS-2014-275)

Amazon Linux AMI : munin (ALAS-2014-348)

Amazon Linux AMI : munin (ALAS-2017-818)

Amazon Linux AMI : mutt (ALAS-2014-310)

Amazon Linux AMI : mysql (ALAS-2012-44)

Amazon Linux AMI : mysql51 (ALAS-2012-141)

Amazon Linux AMI : mysql51 (ALAS-2012-145)

Amazon Linux AMI : mysql51 (ALAS-2012-92)

Amazon Linux AMI : mysql51 (ALAS-2013-152)

Amazon Linux AMI : mysql51 (ALAS-2013-186)

Amazon Linux AMI : mysql51 (ALAS-2013-240)

Amazon Linux AMI : mysql51 (ALAS-2014-298)

Amazon Linux AMI : mysql51 (ALAS-2017-800)

Amazon Linux AMI : mysql55 (ALAS-2012-144)

Amazon Linux AMI : mysql55 (ALAS-2012-93)

Amazon Linux AMI : mysql55 (ALAS-2013-187)

Amazon Linux AMI : mysql55 (ALAS-2014-329)

Amazon Linux AMI : mysql55 (ALAS-2014-428)

Amazon Linux AMI : mysql55 (ALAS-2016-738)

Amazon Linux AMI : mysql55 (ALAS-2017-789)

Amazon Linux AMI : mysql55 (ALAS-2017-831)

Amazon Linux AMI : mysql55 (ALAS-2017-887)

Amazon Linux AMI : mysql55 (ALAS-2017-927)

Amazon Linux AMI : mysql55 (ALAS-2018-1028)

Amazon Linux AMI : mysql55 (ALAS-2018-1068)

Amazon Linux AMI : mysql55 (ALAS-2018-1116)

Amazon Linux AMI : mysql55 / mysql56 (ALAS-2016-756)

Amazon Linux AMI : mysql55 / mysql56,mysql57 (ALAS-2018-969)

Amazon Linux AMI : mysql56 (ALAS-2016-684)

Amazon Linux AMI : mysql56 (ALAS-2016-701)

Amazon Linux AMI : mysql56 (ALAS-2016-737)

Amazon Linux AMI : mysql56 (ALAS-2017-790)

Amazon Linux AMI : mysql56 (ALAS-2017-830)

Amazon Linux AMI : mysql56 (ALAS-2017-888)

Amazon Linux AMI : mysql56 (ALAS-2018-1027)

Amazon Linux AMI : mysql56 (ALAS-2018-1069)

Amazon Linux AMI : mysql56 (ALAS-2018-1115)

Amazon Linux AMI : mysql56 (ALAS-2019-1178)

Amazon Linux AMI : mysql56 (ALAS-2019-1296)

Amazon Linux AMI : mysql56 (ALAS-2020-1332)

Amazon Linux AMI : mysql56 / mysql57 (ALAS-2017-926)

Amazon Linux AMI : mysql57 (ALAS-2018-1026)

Amazon Linux AMI : mysql57 (ALAS-2018-1070)

Amazon Linux AMI : mysql57 (ALAS-2018-1114)

Amazon Linux AMI : mysql57 (ALAS-2019-1181)

Amazon Linux AMI : mysql57 (ALAS-2019-1297)

Amazon Linux AMI : mysql57 (ALAS-2020-1333)

Amazon Linux AMI : nagios (ALAS-2012-50)

Amazon Linux AMI : nagios (ALAS-2013-227)

Amazon Linux AMI : nagios (ALAS-2017-899)

Amazon Linux AMI : net-snmp (ALAS-2012-97)

Amazon Linux AMI : net-snmp (ALAS-2014-316)

Amazon Linux AMI : net-snmp (ALAS-2015-590)

Amazon Linux AMI : nghttp2 (ALAS-2019-1298) (Data Dribble) (Resource Loop)

Amazon Linux AMI : nginx (ALAS-2011-30)

Amazon Linux AMI : nginx (ALAS-2012-63)

Amazon Linux AMI : nginx (ALAS-2012-74)

Amazon Linux AMI : nginx (ALAS-2013-189)

Amazon Linux AMI : nginx (ALAS-2013-249)

Amazon Linux AMI : nginx (ALAS-2014-308)

Amazon Linux AMI : nginx (ALAS-2014-421)

Amazon Linux AMI : nginx (ALAS-2016-655)

Amazon Linux AMI : nginx (ALAS-2016-715)

Amazon Linux AMI : nginx (ALAS-2017-894)

Amazon Linux AMI : nginx (ALAS-2018-1125)

Amazon Linux AMI : nginx (ALAS-2019-1299) (0-Length Headers Leak) (Data Dribble) (Resource Loop)

Amazon Linux AMI : nmap (ALAS-2016-671)

Amazon Linux AMI : nrpe (ALAS-2013-203)

Amazon Linux AMI : nrpe (ALAS-2014-364)

Amazon Linux AMI : nspr (ALAS-2013-216)

Amazon Linux AMI : nspr (ALAS-2013-266)

Amazon Linux AMI : nspr (ALAS-2014-384)

Amazon Linux AMI : nspr / nss-util,nss,jss (ALAS-2015-608)

Amazon Linux AMI : nspr / nss-util,nss,nss-softokn (ALAS-2016-702)

Amazon Linux AMI : nss (ALAS-2011-21)

Amazon Linux AMI : nss (ALAS-2012-102)

Amazon Linux AMI : nss (ALAS-2012-108)

Amazon Linux AMI : nss (ALAS-2013-149)

Amazon Linux AMI : nss (ALAS-2013-217)

Amazon Linux AMI : nss (ALAS-2013-265)

Amazon Linux AMI : nss (ALAS-2014-274)

Amazon Linux AMI : nss (ALAS-2014-385)

Amazon Linux AMI : nss (ALAS-2014-424)

Amazon Linux AMI : nss (ALAS-2014-429) (POODLE)

Amazon Linux AMI : nss (ALAS-2016-645) (SLOTH)

Amazon Linux AMI : nss (ALAS-2017-848)

Amazon Linux AMI : nss (ALAS-2017-911)

Amazon Linux AMI : nss (ALAS-2018-1095)

Amazon Linux AMI : nss / nss-softokn,nss-util,nspr (ALAS-2020-1355)

Amazon Linux AMI : nss / nss-util (ALAS-2015-569) (Logjam)

Amazon Linux AMI : nss / nss-util (ALAS-2017-825)

Amazon Linux AMI : nss-softokn (ALAS-2014-423)

Amazon Linux AMI : nss-softokn (ALAS-2015-596)

Amazon Linux AMI : nss-util (ALAS-2014-422)

Amazon Linux AMI : nss-util (ALAS-2016-667)

Amazon Linux AMI : nss-util / nss,nss-softokn (ALAS-2016-774)

Amazon Linux AMI : ntp (ALAS-2014-462)

Amazon Linux AMI : ntp (ALAS-2015-496)

Amazon Linux AMI : ntp (ALAS-2015-520)

Amazon Linux AMI : ntp (ALAS-2015-593)

Amazon Linux AMI : ntp (ALAS-2015-607)

Amazon Linux AMI : ntp (ALAS-2016-649)

Amazon Linux AMI : ntp (ALAS-2016-708)

Amazon Linux AMI : ntp (ALAS-2016-727)

Amazon Linux AMI : ntp (ALAS-2017-781)

Amazon Linux AMI : ntp (ALAS-2017-816)

Amazon Linux AMI : ntp (ALAS-2018-1009)

Amazon Linux AMI : ntp (ALAS-2018-1083)

Amazon Linux AMI : ntp (ALAS-2019-1206)

Amazon Linux AMI : numpy (ALAS-2014-302)

Amazon Linux AMI : nvidia (ALAS-2012-67)

Amazon Linux AMI : nvidia (ALAS-2018-991)

Amazon Linux AMI : nvidia (ALAS-2019-1182)

Amazon Linux AMI : oniguruma (ALAS-2019-1295)

Amazon Linux AMI : openjpeg (ALAS-2012-111)

Amazon Linux AMI : openjpeg (ALAS-2012-125)

Amazon Linux AMI : openjpeg (ALAS-2014-271)

Amazon Linux AMI : openjpeg (ALAS-2017-807)

Amazon Linux AMI : openldap (ALAS-2012-101)

Amazon Linux AMI : openldap (ALAS-2012-117)

Amazon Linux AMI : openldap (ALAS-2014-294)

Amazon Linux AMI : openldap (ALAS-2017-799)

Amazon Linux AMI : openldap / compat-openldap (ALAS-2015-599)

Amazon Linux AMI : openmpi (ALAS-2013-256)

Amazon Linux AMI : openssh (ALAS-2012-99)

Amazon Linux AMI : openssh (ALAS-2013-165)

Amazon Linux AMI : openssh (ALAS-2014-369)

Amazon Linux AMI : openssh (ALAS-2015-568)

Amazon Linux AMI : openssh (ALAS-2015-592)

Amazon Linux AMI : openssh (ALAS-2015-625)

Amazon Linux AMI : openssh (ALAS-2016-638)

Amazon Linux AMI : openssh (ALAS-2016-668)

Amazon Linux AMI : openssh (ALAS-2016-675)

Amazon Linux AMI : openssh (ALAS-2016-770)

Amazon Linux AMI : openssh (ALAS-2017-898)

Amazon Linux AMI : openssh (ALAS-2018-1018)

Amazon Linux AMI : openssh (ALAS-2018-1075)

Amazon Linux AMI : openssh (ALAS-2019-1313)

Amazon Linux AMI : openssl (ALAS-2011-04)

Amazon Linux AMI : openssl (ALAS-2011-4)

Amazon Linux AMI : openssl (ALAS-2012-38)

Amazon Linux AMI : openssl (ALAS-2012-62)

Amazon Linux AMI : openssl (ALAS-2012-72)

Amazon Linux AMI : openssl (ALAS-2012-85)

Amazon Linux AMI : openssl (ALAS-2013-171)

Amazon Linux AMI : openssl (ALAS-2014-273)

Amazon Linux AMI : openssl (ALAS-2014-349)

Amazon Linux AMI : openssl (ALAS-2014-391)

Amazon Linux AMI : openssl (ALAS-2014-426) (POODLE)

Amazon Linux AMI : openssl (ALAS-2014-427)

Amazon Linux AMI : openssl (ALAS-2015-469) (FREAK)

Amazon Linux AMI : openssl (ALAS-2015-498)

Amazon Linux AMI : openssl (ALAS-2015-550) (Logjam)

Amazon Linux AMI : openssl (ALAS-2015-564)

Amazon Linux AMI : openssl (ALAS-2015-614)

Amazon Linux AMI : openssl (ALAS-2016-661) (DROWN) (SLOTH)

Amazon Linux AMI : openssl (ALAS-2016-695)

Amazon Linux AMI : openssl (ALAS-2016-749)

Amazon Linux AMI : openssl (ALAS-2016-755)

Amazon Linux AMI : openssl (ALAS-2017-803)

Amazon Linux AMI : openssl (ALAS-2018-1000)

Amazon Linux AMI : openssl (ALAS-2018-1016)

Amazon Linux AMI : openssl (ALAS-2018-1065)

Amazon Linux AMI : openssl (ALAS-2018-1098)

Amazon Linux AMI : openssl (ALAS-2018-1102)

Amazon Linux AMI : openssl (ALAS-2019-1153)

Amazon Linux AMI : openssl (ALAS-2019-1188)

Amazon Linux AMI : openssl (ALAS-2020-1344)

Amazon Linux AMI : openssl Information Disclosure Vulnerability (ALAS-2014-320)

Amazon Linux AMI : openssl097a (ALAS-2014-351)

Amazon Linux AMI : openssl098e (ALAS-2012-73)

Amazon Linux AMI : openssl098e (ALAS-2014-350)

Amazon Linux AMI : openssl098e (ALAS-2016-682) (DROWN)

Amazon Linux AMI : openswan (ALAS-2011-06)

Amazon Linux AMI : openswan (ALAS-2011-18)

Amazon Linux AMI : openswan (ALAS-2011-6)

Amazon Linux AMI : openswan (ALAS-2013-192)

Amazon Linux AMI : openswan (ALAS-2014-303)

Amazon Linux AMI : openvpn (ALAS-2013-201)

Amazon Linux AMI : openvpn (ALAS-2014-459)

Amazon Linux AMI : openvpn (ALAS-2016-750) (SWEET32)

Amazon Linux AMI : openvpn (ALAS-2017-852)

Amazon Linux AMI : openvpn (ALAS-2017-920)

Amazon Linux AMI : pam (ALAS-2013-160)

Amazon Linux AMI : pam (ALAS-2014-354)

Amazon Linux AMI : pam (ALAS-2015-589)

Amazon Linux AMI : patch (ALAS-2018-1008)

Amazon Linux AMI : patch (ALAS-2019-1312)

Amazon Linux AMI : pcre (ALAS-2015-528)

Amazon Linux AMI : pcre (ALAS-2018-1076)

Amazon Linux AMI : perl (ALAS-2011-19)

Amazon Linux AMI : perl (ALAS-2013-177)

Amazon Linux AMI : perl (ALAS-2019-1180)

Amazon Linux AMI : perl-Archive-Tar (ALAS-2019-1287)

Amazon Linux AMI : perl-Capture-Tiny (ALAS-2014-358)

Amazon Linux AMI : perl-DBD-Pg (ALAS-2012-112)

Amazon Linux AMI : perl-FCGI (ALAS-2011-05)

Amazon Linux AMI : perl-FCGI (ALAS-2011-5)

Amazon Linux AMI : perl-HTML-Scrubber (ALAS-2015-629)

Amazon Linux AMI : perl-IPTables-Parse (ALAS-2015-627)

Amazon Linux AMI : perl-libwww-perl (ALAS-2011-17)

Amazon Linux AMI : perl-YAML-LibYAML (ALAS-2012-69)

Amazon Linux AMI : perl-YAML-LibYAML (ALAS-2014-324)

Amazon Linux AMI : perl-YAML-LibYAML (ALAS-2015-482)

Amazon Linux AMI : perltidy (ALAS-2014-356)

Amazon Linux AMI : php (ALAS-2011-07)

Amazon Linux AMI : php (ALAS-2011-7)

Amazon Linux AMI : php (ALAS-2012-116)

Amazon Linux AMI : php (ALAS-2012-37)

Amazon Linux AMI : php (ALAS-2012-41)

Amazon Linux AMI : php (ALAS-2012-77)

Amazon Linux AMI : php (ALAS-2012-95)

Amazon Linux AMI : php (ALAS-2013-205)

Amazon Linux AMI : php (ALAS-2013-211)

Amazon Linux AMI : php (ALAS-2013-262)

Amazon Linux AMI : php (ALAS-2014-393)

Amazon Linux AMI : php (ALAS-2015-524)

Amazon Linux AMI : php-pecl-apc (ALAS-2012-96)

Amazon Linux AMI : php-ZendFramework (ALAS-2013-153)

Amazon Linux AMI : php-ZendFramework (ALAS-2014-377)

Amazon Linux AMI : php-ZendFramework (ALAS-2014-394)

Amazon Linux AMI : php-ZendFramework (ALAS-2014-460)

Amazon Linux AMI : php-ZendFramework (ALAS-2015-560)

Amazon Linux AMI : php-ZendFramework (ALAS-2016-767)

Amazon Linux AMI : php54 (ALAS-2013-206)

Amazon Linux AMI : php54 (ALAS-2013-212)

Amazon Linux AMI : php54 (ALAS-2013-224)

Amazon Linux AMI : php54 (ALAS-2013-263)

Amazon Linux AMI : php54 (ALAS-2014-313)

Amazon Linux AMI : php54 (ALAS-2014-333)

Amazon Linux AMI : php54 (ALAS-2014-343)

Amazon Linux AMI : php54 (ALAS-2014-361)

Amazon Linux AMI : php54 (ALAS-2014-367)

Amazon Linux AMI : php54 (ALAS-2014-434)

Amazon Linux AMI : php54 (ALAS-2014-450)

Amazon Linux AMI : php54 (ALAS-2015-463)

Amazon Linux AMI : php54 (ALAS-2015-475)

Amazon Linux AMI : php54 (ALAS-2015-493) (GHOST)

Amazon Linux AMI : php54 (ALAS-2015-506)

Amazon Linux AMI : php54 (ALAS-2015-509)

Amazon Linux AMI : php54 (ALAS-2015-534)

Amazon Linux AMI : php54 (ALAS-2015-561)

Amazon Linux AMI : php54 (ALAS-2015-583) (BACKRONYM)

Amazon Linux AMI : php54 (ALAS-2016-670)

Amazon Linux AMI : php54-pecl-imagick / php55-pecl-imagick,php56-pecl-imagick,php70-pecl-imagick,php71-pecl-imagick,php72-pecl-imagick (ALAS-2019-1237)

Amazon Linux AMI : php55 (ALAS-2013-264)

Amazon Linux AMI : php55 (ALAS-2014-314)

Amazon Linux AMI : php55 (ALAS-2014-332)

Amazon Linux AMI : php55 (ALAS-2014-342)

Amazon Linux AMI : php55 (ALAS-2014-362)

Amazon Linux AMI : php55 (ALAS-2014-372)

Amazon Linux AMI : php55 (ALAS-2014-415)

Amazon Linux AMI : php55 (ALAS-2014-435)

Amazon Linux AMI : php55 (ALAS-2014-451)

Amazon Linux AMI : php55 (ALAS-2015-464)

Amazon Linux AMI : php55 (ALAS-2015-474)

Amazon Linux AMI : php55 (ALAS-2015-494) (GHOST)

Amazon Linux AMI : php55 (ALAS-2015-507)

Amazon Linux AMI : php55 (ALAS-2015-510)

Amazon Linux AMI : php55 (ALAS-2015-535)

Amazon Linux AMI : php55 (ALAS-2015-562)

Amazon Linux AMI : php55 (ALAS-2015-584) (BACKRONYM)

Amazon Linux AMI : php55 (ALAS-2015-602)

Amazon Linux AMI : php55 (ALAS-2016-707)

Amazon Linux AMI : php55 / php56 (ALAS-2016-728) (httpoxy)

Amazon Linux AMI : php56 (ALAS-2015-508)

Amazon Linux AMI : php56 (ALAS-2015-511)

Amazon Linux AMI : php56 (ALAS-2015-536)

Amazon Linux AMI : php56 (ALAS-2015-563)

Amazon Linux AMI : php56 (ALAS-2015-585) (BACKRONYM)

Amazon Linux AMI : php56 (ALAS-2015-601)

Amazon Linux AMI : php56 (ALAS-2016-706)

Amazon Linux AMI : php56 (ALAS-2016-753)

Amazon Linux AMI : php56 (ALAS-2017-787)

Amazon Linux AMI : php56 (ALAS-2017-808)

Amazon Linux AMI : php56 (ALAS-2017-871)

Amazon Linux AMI : php56 / php55 (ALAS-2016-640)

Amazon Linux AMI : php56 / php55 (ALAS-2016-685)

Amazon Linux AMI : php56 / php55 (ALAS-2016-698)

Amazon Linux AMI : php56 / php70,php71 (ALAS-2017-924)

Amazon Linux AMI : php56 / php70,php71 (ALAS-2018-1019)

Amazon Linux AMI : php56 / php70,php71 (ALAS-2018-1066)

Amazon Linux AMI : php56 / php70,php71 (ALAS-2018-946)

Amazon Linux AMI : php56 / php70,php71,php72 (ALAS-2018-1090)

Amazon Linux AMI : php56 / php70,php71,php72 (ALAS-2019-1147)

Amazon Linux AMI : php70 (ALAS-2016-754)

Amazon Linux AMI : php70 (ALAS-2017-788)

Amazon Linux AMI : php70 (ALAS-2017-812)

Amazon Linux AMI : php70 (ALAS-2017-867)

Amazon Linux AMI : php70 / php56 (ALAS-2018-988)

Amazon Linux AMI : php71 (ALAS-2018-982)

Amazon Linux AMI : php71 / php72,php73 (ALAS-2019-1225)

Amazon Linux AMI : php71 / php72,php73 (ALAS-2019-1240)

Amazon Linux AMI : php71 / php72,php73 (ALAS-2019-1282)

Amazon Linux AMI : php71 / php72,php73,php56 (ALAS-2019-1315)

Amazon Linux AMI : php71 / php73 (ALAS-2019-1283)

Amazon Linux AMI : php72 (ALAS-2018-1067)

Amazon Linux AMI : php72 (ALAS-2019-1284)

Amazon Linux AMI : php72 (ALAS-2020-1346)

Amazon Linux AMI : php72 (ALAS-2020-1350)

Amazon Linux AMI : php72 / php73 (ALAS-2020-1339)

Amazon Linux AMI : php73 (ALAS-2020-1347)

Amazon Linux AMI : php73 (ALAS-2020-1351)

Amazon Linux AMI : pigz (ALAS-2015-499)

Amazon Linux AMI : pixman (ALAS-2014-272)

Amazon Linux AMI : pngcrush (ALAS-2016-646)

Amazon Linux AMI : policycoreutils (ALAS-2016-765)

Amazon Linux AMI : poppler (ALAS-2016-769)

Amazon Linux AMI : poppler (ALAS-2017-902)

Amazon Linux AMI : poppler (ALAS-2018-1110)

Amazon Linux AMI : poppler (ALAS-2019-1271)

Amazon Linux AMI : postgresql (ALAS-2011-12)

Amazon Linux AMI : postgresql8 (ALAS-2012-129)

Amazon Linux AMI : postgresql8 (ALAS-2012-82)

Amazon Linux AMI : postgresql8 (ALAS-2012-94)

Amazon Linux AMI : postgresql8 (ALAS-2013-244)

Amazon Linux AMI : postgresql8 (ALAS-2014-305)

Amazon Linux AMI : postgresql8 (ALAS-2015-503)

Amazon Linux AMI : postgresql8 (ALAS-2015-556)

Amazon Linux AMI : postgresql8 (ALAS-2015-619)

Amazon Linux AMI : postgresql8 (ALAS-2016-689)

Amazon Linux AMI : postgresql9 (ALAS-2012-121)

Amazon Linux AMI : postgresql9 (ALAS-2012-91)

Amazon Linux AMI : postgresql9 (ALAS-2013-178)

Amazon Linux AMI : postgresql9 (ALAS-2014-306)

Amazon Linux AMI : postgresql92 (ALAS-2015-492)

Amazon Linux AMI : postgresql92 (ALAS-2015-545)

Amazon Linux AMI : postgresql92 (ALAS-2017-838)

Amazon Linux AMI : postgresql92 (ALAS-2018-1080)

Amazon Linux AMI : postgresql92 / postgresql93,postgresql94 (ALAS-2015-609)

Amazon Linux AMI : postgresql92 / postgresql93,postgresql94 (ALAS-2016-747)

Amazon Linux AMI : postgresql92 / postgresql93,postgresql94 (ALAS-2017-931)

Amazon Linux AMI : postgresql93 (ALAS-2015-485)

Amazon Linux AMI : postgresql93 (ALAS-2015-546)

Amazon Linux AMI : postgresql93 / postgresql92 (ALAS-2017-884)

Amazon Linux AMI : postgresql93 / postgresql94 (ALAS-2018-1117)

Amazon Linux AMI : postgresql93 / postgresql94,postgresql95 (ALAS-2017-839)

Amazon Linux AMI : postgresql93 / postgresql94,postgresql95 (ALAS-2018-1079)

Amazon Linux AMI : postgresql93 / postgresql94,postgresql95,postgresql96 (ALAS-2018-990)

Amazon Linux AMI : postgresql94 / postgresql93,postgresql92 (ALAS-2016-662)

Amazon Linux AMI : postgresql94 / postgresql95 (ALAS-2017-885)

Amazon Linux AMI : postgresql95 (ALAS-2018-1118)

Amazon Linux AMI : postgresql95 / postgresql96 (ALAS-2017-930)

Amazon Linux AMI : postgresql96 (ALAS-2017-908)

Amazon Linux AMI : postgresql96 (ALAS-2018-1074)

Amazon Linux AMI : postgresql96 (ALAS-2018-1119)

Amazon Linux AMI : privoxy (ALAS-2016-663)

Amazon Linux AMI : procmail (ALAS-2014-408)

Amazon Linux AMI : procmail (ALAS-2018-1084)

Amazon Linux AMI : puppet (ALAS-2011-11)

Amazon Linux AMI : puppet (ALAS-2012-135)

Amazon Linux AMI : puppet (ALAS-2012-53)

Amazon Linux AMI : puppet (ALAS-2012-75)

Amazon Linux AMI : puppet (ALAS-2013-181)

Amazon Linux AMI : puppet (ALAS-2013-213)

Amazon Linux AMI : puppet (ALAS-2013-219)

Amazon Linux AMI : puppet (ALAS-2014-288)

Amazon Linux AMI : puppet (ALAS-2015-484)

Amazon Linux AMI : puppet3 (ALAS-2017-849)

Amazon Linux AMI : python-botocore (ALAS-2015-512)

Amazon Linux AMI : python-crypto (ALAS-2012-86)

Amazon Linux AMI : python-crypto (ALAS-2013-243)

Amazon Linux AMI : python-crypto (ALAS-2017-801)

Amazon Linux AMI : python-crypto (ALAS-2018-977)

Amazon Linux AMI : python-jinja2 (ALAS-2014-371)

Amazon Linux AMI : python-jinja2 (ALAS-2019-1223)

Amazon Linux AMI : python-oauth2 (ALAS-2014-425)

Amazon Linux AMI : python-paramiko (ALAS-2018-1096)

Amazon Linux AMI : python-paramiko (ALAS-2018-989)

Amazon Linux AMI : python-pip (ALAS-2015-541)

Amazon Linux AMI : python-pip (ALAS-2020-1340)

Amazon Linux AMI : python-pygments (ALAS-2015-630)

Amazon Linux AMI : python-rsa (ALAS-2016-644)

Amazon Linux AMI : python-simplejson (ALAS-2014-374)

Amazon Linux AMI : python-tornado (ALAS-2015-521)

Amazon Linux AMI : python-twisted-web (ALAS-2016-760)

Amazon Linux AMI : python-urllib3 (ALAS-2019-1224)

Amazon Linux AMI : python-urllib3 (ALAS-2019-1236)

Amazon Linux AMI : python26 (ALAS-2012-80)

Amazon Linux AMI : python26 (ALAS-2012-98)

Amazon Linux AMI : python26 (ALAS-2013-241)

Amazon Linux AMI : python26 (ALAS-2014-292)

Amazon Linux AMI : python26 (ALAS-2015-621)

Amazon Linux AMI : python26 / python27,python34 (ALAS-2016-724)

Amazon Linux AMI : python27 (ALAS-2012-81)

Amazon Linux AMI : python27 (ALAS-2013-220)

Amazon Linux AMI : python27 (ALAS-2014-293)

Amazon Linux AMI : python27 (ALAS-2014-380)

Amazon Linux AMI : python27 (ALAS-2014-440)

Amazon Linux AMI : python27 (ALAS-2015-552)

Amazon Linux AMI : python27 (ALAS-2018-1108)

Amazon Linux AMI : python27 (ALAS-2018-945)

Amazon Linux AMI : python27 (ALAS-2019-1230)

Amazon Linux AMI : python27 (ALAS-2019-1258)

Amazon Linux AMI : python27 / python34,python35,python36 (ALAS-2019-1169)

Amazon Linux AMI : python27 / python34,python35,python36 (ALAS-2019-1314)

Amazon Linux AMI : python27 / python35,python36 (ALAS-2020-1342)

Amazon Linux AMI : python34 (ALAS-2019-1202)

Amazon Linux AMI : python34 (ALAS-2019-1242)

Amazon Linux AMI : python34 (ALAS-2019-1324)

Amazon Linux AMI : python34 / python27,python26 (ALAS-2016-741) (httpoxy)

Amazon Linux AMI : python34 / python35,python36 (ALAS-2019-1259)

Amazon Linux AMI : python34 / python35,python36,python27 (ALAS-2018-1003)

Amazon Linux AMI : python34 / python36 (ALAS-2018-1132)

Amazon Linux AMI : python35 (ALAS-2018-1101)

Amazon Linux AMI : python35 (ALAS-2019-1243)

Amazon Linux AMI : python35 / python34 (ALAS-2018-943)

Amazon Linux AMI : python36 (ALAS-2019-1204)

Amazon Linux AMI : qemu-kvm (ALAS-2017-934)

Amazon Linux AMI : qemu-kvm (ALAS-2018-1034) (Spectre)

Amazon Linux AMI : qemu-kvm (ALAS-2018-1073)

Amazon Linux AMI : qemu-kvm (ALAS-2018-942) (Spectre)

Amazon Linux AMI : qemu-kvm (ALAS-2019-1260) (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)

Amazon Linux AMI : quagga (ALAS-2012-70)

Amazon Linux AMI : quagga (ALAS-2012-90)

Amazon Linux AMI : quagga (ALAS-2014-279)

Amazon Linux AMI : quagga (ALAS-2018-957)

Amazon Linux AMI : R (ALAS-2017-819)

Amazon Linux AMI : readline (ALAS-2014-357)

Amazon Linux AMI : realmd (ALAS-2016-636)

Amazon Linux AMI : rpcbind (ALAS-2016-659)

Amazon Linux AMI : rpcbind (ALAS-2017-841)

Amazon Linux AMI : rpm (ALAS-2011-14)

Amazon Linux AMI : rpm (ALAS-2012-61)

Amazon Linux AMI : rpm (ALAS-2014-458)

Amazon Linux AMI : rssh (ALAS-2019-1328)

Amazon Linux AMI : rsyslog (ALAS-2012-105)

Amazon Linux AMI : rsyslog (ALAS-2014-445)

Amazon Linux AMI : ruby (ALAS-2012-139)

Amazon Linux AMI : ruby (ALAS-2012-35)

Amazon Linux AMI : ruby (ALAS-2013-173)

Amazon Linux AMI : ruby (ALAS-2013-248)

Amazon Linux AMI : ruby18 (ALAS-2015-529)

Amazon Linux AMI : ruby19 (ALAS-2013-195)

Amazon Linux AMI : ruby19 (ALAS-2013-229)

Amazon Linux AMI : ruby19 (ALAS-2013-247)

Amazon Linux AMI : ruby19 (ALAS-2014-290)

Amazon Linux AMI : ruby19 (ALAS-2014-447)

Amazon Linux AMI : ruby19 (ALAS-2015-530)

Amazon Linux AMI : ruby19 / ruby20,ruby21,ruby22 (ALAS-2016-632)

Amazon Linux AMI : ruby20 (ALAS-2014-441)

Amazon Linux AMI : ruby20 (ALAS-2014-448)

Amazon Linux AMI : ruby20 (ALAS-2015-531)

Amazon Linux AMI : ruby20 (ALAS-2015-547)

Amazon Linux AMI : ruby20 / ruby21,ruby24 (ALAS-2019-1255)

Amazon Linux AMI : ruby20 / ruby22,ruby23,ruby24 (ALAS-2018-983)

Amazon Linux AMI : ruby21 (ALAS-2014-439)

Amazon Linux AMI : ruby21 (ALAS-2014-449)

Amazon Linux AMI : ruby21 (ALAS-2015-532)

Amazon Linux AMI : ruby21 (ALAS-2015-548)

Amazon Linux AMI : ruby22 (ALAS-2015-533)

Amazon Linux AMI : ruby22 (ALAS-2015-549)

Amazon Linux AMI : ruby22 / ruby23 (ALAS-2017-906)

Amazon Linux AMI : ruby23 (ALAS-2017-880)

Amazon Linux AMI : ruby23 / ruby24 (ALAS-2018-1113)

Amazon Linux AMI : ruby24 (ALAS-2017-915)

Amazon Linux AMI : ruby24 / ruby22,ruby23 (ALAS-2018-978)

Amazon Linux AMI : rubygems (ALAS-2012-79)

Amazon Linux AMI : rubygems (ALAS-2013-230)

Amazon Linux AMI : rubygems (ALAS-2013-231)

Amazon Linux AMI : samba (ALAS-2016-634)

Amazon Linux AMI : samba (ALAS-2016-674)

Amazon Linux AMI : samba (ALAS-2016-686) (Badlock)

Amazon Linux AMI : samba (ALAS-2016-732)

Amazon Linux AMI : samba (ALAS-2017-834) (SambaCry)

Amazon Linux AMI : samba (ALAS-2017-909)

Amazon Linux AMI : samba (ALAS-2017-933)

Amazon Linux AMI : samba (ALAS-2018-1126)

Amazon Linux AMI : samba (ALAS-2019-1329)

Amazon Linux AMI : scipy (ALAS-2013-242)

Amazon Linux AMI : socat (ALAS-2012-87)

Amazon Linux AMI : socat (ALAS-2013-202)

Amazon Linux AMI : socat (ALAS-2014-300)

Amazon Linux AMI : sos (ALAS-2016-666)

Amazon Linux AMI : spamassassin (ALAS-2018-1091)

Amazon Linux AMI : spamassassin (ALAS-2020-1341)

Amazon Linux AMI : sqlite (ALAS-2015-591)

Amazon Linux AMI : squid (ALAS-2014-360)

Amazon Linux AMI : squid (ALAS-2014-411)

Amazon Linux AMI : squid (ALAS-2014-433)

Amazon Linux AMI : squid (ALAS-2016-713)

Amazon Linux AMI : squid (ALAS-2016-735)

Amazon Linux AMI : squid (ALAS-2018-1081)

Amazon Linux AMI : squid (ALAS-2019-1176)

Amazon Linux AMI : sssd (ALAS-2016-635)

Amazon Linux AMI : sssd (ALAS-2017-935)

Amazon Linux AMI : sssd (ALAS-2018-1127)

Amazon Linux AMI : sssd (ALAS-2019-1307)

Amazon Linux AMI : stunnel / amazon-efs-utils (ALAS-2018-996)

Amazon Linux AMI : subversion (ALAS-2013-180)

Amazon Linux AMI : subversion (ALAS-2013-221)

Amazon Linux AMI : subversion (ALAS-2013-269)

Amazon Linux AMI : subversion (ALAS-2014-318)

Amazon Linux AMI : subversion (ALAS-2014-413)

Amazon Linux AMI : subversion (ALAS-2016-709)

Amazon Linux AMI : subversion (ALAS-2019-1317)

Amazon Linux AMI : subversion / mod\_dav\_svn (ALAS-2015-587)

Amazon Linux AMI : subversion / mod\_dav\_svn (ALAS-2017-794)

Amazon Linux AMI : subversion / mod\_dav\_svn (ALAS-2017-883)

Amazon Linux AMI : sudo (ALAS-2012-110)

Amazon Linux AMI : sudo (ALAS-2013-259)

Amazon Linux AMI : sudo (ALAS-2017-780)

Amazon Linux AMI : sudo (ALAS-2017-843)

Amazon Linux AMI : sudo (ALAS-2017-855)

Amazon Linux AMI : sudo (ALAS-2019-1309)

Amazon Linux AMI : sudo (ALAS-2020-1356)

Amazon Linux AMI : systemtap (ALAS-2012-54)

Amazon Linux AMI : t1lib (ALAS-2012-40)

Amazon Linux AMI : t1utils (ALAS-2015-554)

Amazon Linux AMI : tcpdump (ALAS-2015-557)

Amazon Linux AMI : texlive (ALAS-2012-48)

Amazon Linux AMI : tigervnc (ALAS-2015-576)

Amazon Linux AMI : tigervnc (ALAS-2015-623)

Amazon Linux AMI : tigervnc (ALAS-2017-879)

Amazon Linux AMI : tomcat-native (ALAS-2018-965)

Amazon Linux AMI : tomcat6 (ALAS-2011-25)

Amazon Linux AMI : tomcat6 (ALAS-2013-196)

Amazon Linux AMI : tomcat6 (ALAS-2014-344)

Amazon Linux AMI : tomcat6 (ALAS-2015-525)

Amazon Linux AMI : tomcat6 (ALAS-2016-656)

Amazon Linux AMI : tomcat6 (ALAS-2016-681)

Amazon Linux AMI : tomcat6 (ALAS-2016-776)

Amazon Linux AMI : tomcat6 (ALAS-2017-810)

Amazon Linux AMI : tomcat6 (ALAS-2017-821)

Amazon Linux AMI : tomcat6 / tomcat7,tomcat8 (ALAS-2016-722) (httpoxy)

Amazon Linux AMI : tomcat6 / tomcat7,tomcat8 (ALAS-2016-764)

Amazon Linux AMI : tomcat7 (ALAS-2013-191)

Amazon Linux AMI : tomcat7 (ALAS-2014-312)

Amazon Linux AMI : tomcat7 (ALAS-2015-526)

Amazon Linux AMI : tomcat7 (ALAS-2016-657)

Amazon Linux AMI : tomcat7 (ALAS-2016-680)

Amazon Linux AMI : tomcat7 (ALAS-2016-777)

Amazon Linux AMI : tomcat7 (ALAS-2017-853)

Amazon Linux AMI : tomcat7 (ALAS-2017-873)

Amazon Linux AMI : tomcat7 (ALAS-2018-1099)

Amazon Linux AMI : tomcat7 (ALAS-2018-947)

Amazon Linux AMI : tomcat7 (ALAS-2019-1235)

Amazon Linux AMI : tomcat7 (ALAS-2020-1352)

Amazon Linux AMI : tomcat7 / tomcat8 (ALAS-2016-736)

Amazon Linux AMI : tomcat7 / tomcat8 (ALAS-2017-796)

Amazon Linux AMI : tomcat7 / tomcat8 (ALAS-2017-822)

Amazon Linux AMI : tomcat7 / tomcat8 (ALAS-2017-903)

Amazon Linux AMI : tomcat7 / tomcat8 (ALAS-2018-972)

Amazon Linux AMI : tomcat7 / tomcat80 (ALAS-2018-1055)

Amazon Linux AMI : tomcat8 (ALAS-2015-527)

Amazon Linux AMI : tomcat8 (ALAS-2016-658)

Amazon Linux AMI : tomcat8 (ALAS-2016-679)

Amazon Linux AMI : tomcat8 (ALAS-2016-778)

Amazon Linux AMI : tomcat8 (ALAS-2017-854)

Amazon Linux AMI : tomcat8 (ALAS-2017-862)

Amazon Linux AMI : tomcat8 (ALAS-2018-1056)

Amazon Linux AMI : tomcat8 (ALAS-2018-959)

Amazon Linux AMI : tomcat8 (ALAS-2019-1208)

Amazon Linux AMI : tomcat8 (ALAS-2019-1234)

Amazon Linux AMI : tomcat8 (ALAS-2020-1337)

Amazon Linux AMI : tomcat8 (ALAS-2020-1353)

Amazon Linux AMI : tomcat8 / tomcat80,tomcat7 (ALAS-2017-913)

Amazon Linux AMI : tomcat80 (ALAS-2018-973)

Amazon Linux AMI : transmission (ALAS-2014-390)

Amazon Linux AMI : transmission (ALAS-2018-950)

Amazon Linux AMI : unzip (ALAS-2015-504)

Amazon Linux AMI : usermode / libuser (ALAS-2015-572)

Amazon Linux AMI : util-linux (ALAS-2017-823)

Amazon Linux AMI : varnish (ALAS-2014-276)

Amazon Linux AMI : varnish (ALAS-2016-721)

Amazon Linux AMI : vim (ALAS-2016-779)

Amazon Linux AMI : vim (ALAS-2017-809)

Amazon Linux AMI : vim (ALAS-2019-1239)

Amazon Linux AMI : wget (ALAS-2014-442)

Amazon Linux AMI : wget (ALAS-2016-720)

Amazon Linux AMI : wget (ALAS-2017-881)

Amazon Linux AMI : wget (ALAS-2017-916)

Amazon Linux AMI : wget (ALAS-2018-1040)

Amazon Linux AMI : wget (ALAS-2019-1194)

Amazon Linux AMI : wireshark (ALAS-2012-71)

Amazon Linux AMI : wireshark (ALAS-2013-251)

Amazon Linux AMI : wireshark (ALAS-2014-330)

Amazon Linux AMI : wireshark (ALAS-2014-446)

Amazon Linux AMI : wireshark (ALAS-2015-580)

Amazon Linux AMI : wireshark (ALAS-2017-813)

Amazon Linux AMI : xalan-j2 (ALAS-2014-325)

Amazon Linux AMI : xerces-j2 (ALAS-2014-436)

Amazon Linux AMI : xfsprogs (ALAS-2015-622)

Amazon Linux AMI : xinetd (ALAS-2013-232)

Amazon Linux AMI : xmlsec1 (ALAS-2017-890)

Amazon Linux AMI : xorg-x11-server (ALAS-2011-13)

Amazon Linux AMI : xorg-x11-server (ALAS-2012-104)

Amazon Linux AMI : xorg-x11-server (ALAS-2013-234)

Amazon Linux AMI : xorg-x11-server (ALAS-2013-260)

Amazon Linux AMI : xorg-x11-server (ALAS-2014-277)

Amazon Linux AMI : xorg-x11-server (ALAS-2015-470)

Amazon Linux AMI : xorg-x11-server (ALAS-2015-519)

Amazon Linux AMI : yum (ALAS-2014-315)

Amazon Linux AMI : yum-utils (ALAS-2018-1057)

Amazon Linux AMI : zsh (ALAS-2018-1107)

Amazon Linux AMI : zsh (ALAS-2019-1285)

Amazon Linux AMI Update: kernel / openssh Denial of Service (ALAS-2014-319)

# AIX Local Security Checks