Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-05 13:31 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.13% done; ETC: 13:33 (0:00:01 remaining)
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.00017s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
| temp: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2012-6095] ProFTPD before 1.3.5rc1, when using the UserOwner directive, allows local users to modify the ownership of arbitrary files via a race condition and a symlink attack on the (1) MKD or (2) XMKD commands.
| [CVE-2011-4130] Use-after-free vulnerability in the Response API in ProFTPD before 1.3.3g allows remote authenticated users to execute arbitrary code via vectors involving an error that occurs after an FTP data transfer.
| [CVE-2011-1137] Integer overflow in the mod_sftp (aka SFTP) module in ProFTPD 1.3.3d and earlier allows remote attackers to cause a denial of service (memory consumption leading to OOM kill) via a malformed SSH message.
| [CVE-2010-4652] Heap-based buffer overflow in the sql_prepare_where function (contrib/mod_sql.c) in ProFTPD before 1.3.3d, when mod_sql is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted username containing substitution tags, which are not properly handled during construction of an SQL query.
| [CVE-2010-4221] Multiple stack-based buffer overflows in the pr_netio_telnet_gets function in netio.c in ProFTPD before 1.3.3c allow remote attackers to execute arbitrary code via vectors involving a TELNET IAC escape character to a (1) FTP or (2) FTPS server.
| [CVE-2010-3867] Multiple directory traversal vulnerabilities in the mod_site_misc module in ProFTPD before 1.3.3c allow remote authenticated users to create directories, delete directories, create symlinks, and modify file timestamps via directory traversal sequences in a (1) SITE MKDIR, (2) SITE RMDIR, (3) SITE SYMLINK, or (4) SITE UTIME command.
| [CVE-2009-3639] The mod_tls module in ProFTPD before 1.3.2b, and 1.3.3 before 1.3.3rc2, when the dNSNameRequired TLS option is enabled, does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 client certificate, which allows remote attackers to bypass intended client-hostname restrictions via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
| [CVE-2009-0543] ProFTPD Server 1.3.1, with NLS support enabled, allows remote attackers to bypass SQL injection protection mechanisms via invalid, encoded multibyte characters, which are not properly handled in (1) mod_sql_mysql and (2) mod_sql_postgres.
| [CVE-2009-0542] SQL injection vulnerability in ProFTPD Server 1.3.1 through 1.3.2rc2 allows remote attackers to execute arbitrary SQL commands via a "%" (percent) character in the username, which introduces a "'" (single quote) character during variable substitution by mod_sql.
| [CVE-2008-7265] The pr_data_xfer function in ProFTPD before 1.3.2rc3 allows remote authenticated users to cause a denial of service (CPU consumption) via an ABOR command during a data transfer.
| [CVE-2008-4242] ProFTPD 1.3.1 interprets long commands from an FTP client as multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web browser.
| [CVE-2006-6563] Stack-based buffer overflow in the pr_ctrls_recv_request function in ctrls.c in the mod_ctrls module in ProFTPD before 1.3.1rc1 allows local users to execute arbitrary code via a large reqarglen length value.
| [CVE-2006-6171] ** DISPUTED ** ProFTPD 1.3.0a and earlier does not properly set the buffer size limit

when CommandBufferSize is specified in the configuration file, which leads to an off-by-two buffer underflow. NOTE: in November 2006, the role of CommandBufferSize was originally associated with CVE-2006-5815, but this was an error stemming from a vague initial disclosure. NOTE: ProFTPD developers dispute this issue, saying that the relevant memory location is overwritten by assignment before further use within the affected function, so this is not a vulnerability.
| [CVE-2006-6170] Buffer overflow in the tls_x509_name_oneline function in the mod_tls module, as used in ProFTPD 1.3.0a and earlier, and possibly other products, allows remote attackers to execute arbitrary code via a large data length argument, a different vulnerability than CVE-2006-5815.
| [CVE-2006-5815] Stack-based buffer overflow in the sreplace function in ProFTPD 1.3.0 and earlier allows remote attackers, probably authenticated, to cause a denial of service and execute arbitrary code, as demonstrated by vd_proftpd.pm, a "ProFTPD remote exploit."
| [CVE-2005-4816] Buffer overflow in mod_radius in ProFTPD before 1.3.0rc2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long password.
| [CVE-2005-2390] Multiple format string vulnerabilities in ProFTPD before 1.3.0rc2 allow attackers to cause a denial of service or obtain sensitive information via (1) certain inputs to the shutdown message from ftpshut, or (2) the SQLShowInfo mod_sql directive.
| [CVE-2004-0529] The modified suexec program in cPanel, when configured for mod_php and compiled for Apache 1.3.31 and earlier without mod_phpsuexec, allows local users to execute untrusted shared scripts and gain privileges, as demonstrated using untainted scripts such as (1) proftpdvhosts or (2) addalink.cgi, a different vulnerability than CVE-2004-0490.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [50631] ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [80980] ProFTPD FTP commands symlink
| [71226] ProFTPD pool code execution
| [65207] ProFTPD mod_sftp module denial of service
| [64495] ProFTPD sql_prepare_where() buffer overflow
| [63658] ProFTPD FTP server backdoor
| [63407] mod_sql module for ProFTPD buffer overflow
| [63155] ProFTPD pr_data_xfer denial of service
| [62909] ProFTPD mod_site_misc directory traversal
| [62908] ProFTPD pr_netio_telnet_gets() buffer overflow
| [53936] ProFTPD mod_tls SSL certificate security bypass
| [48951] ProFTPD mod_sql username percent SQL injection
| [48558] ProFTPD NLS support SQL injection protection bypass
| [45274] ProFTPD URL cross-site request forgery
| [33733] ProFTPD Auth API security bypass
| [31461] ProFTPD mod_radius buffer overflow
| [30906] ProFTPD Controls (mod_ctrls) module buffer overflow
| [30554] ProFTPD mod_tls module tls_x509_name_oneline() buffer overflow
| [30147] ProFTPD sreplace() buffer overflow
| [21530] ProFTPD mod_sql format string attack
| [21528] ProFTPD shutdown message format string attack
| [19410] GProFTPD file name format string attack
| [18453] ProFTPD SITE CHGRP command allows group ownership modification
| [17724] ProFTPD could allow an attacker to obtain valid accounts
| [16038] ProFTPD CIDR entry ACL bypass
| [15387] ProFTPD off-by-one _xlate_ascii_write function buffer overflow
| [12369] ProFTPD mod_sql SQL injection
| [12200] ProFTPD ASCII file newline buffer overflow
| [10932] ProFTPD long PASS command buffer overflow
| [8332] ProFTPD mod_sqlpw stores passwords in the wtmp log file
| [7818] ProFTPD ls &quot

| [7816] ProFTPD file globbing denial of service
| [7126] ProFTPD fails to resolve hostnames
| [6433] ProFTPD format string
| [6209] proFTPD /var symlink
| [6208] ProFTPD contains configuration error in postinst script when running as root
| [5801] proftpd memory leak when using SIZE or USER commands
| [5737] ProFTPD system using mod_sqlpw unauthorized access
|
| Exploit-DB - https://www.exploit-db.com:
| [20690] wu-ftpd 2.4/2.5/2.6,Trolltech ftpd 1.2,ProFTPD 1.2,BeroFTPD 1.3.4 FTP glob Expansion Vulnera
bility
| [16878] ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
| [16852] ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
| [16851] ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
| [15662] ProFTPD 1.3.3c compromised source remote root Trojan
| [10044] ProFTPd 1.3.0 mod_ctrls Local Stack Overflow (opensuse)
| [3730] ProFTPD 1.3.0/1.3.0a (mod_ctrls) Local Overflow Exploit (exec-shield)
| [3333] ProFTPD 1.3.0/1.3.0a (mod_ctrls support) Local Buffer Overflow Exploit 2
| [3330] ProFTPD 1.3.0/1.3.0a (mod_ctrls support) Local Buffer Overflow Exploit
| [2928] ProFTPD <= 1.3.0a (mod_ctrls support) Local Buffer Overflow PoC
| [2856] ProFTPD 1.3.0 (sreplace) Remote Stack Overflow Exploit (meta)
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [103331] ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability
| [63497] Debian Security Advisory DSA 1730-1 (proftpd-dfsg)
|
| SecurityTracker - https://www.securitytracker.com:
| [1028040] ProFTPD MKD/XMKD Race Condition Lets Local Users Gain Elevated Privileges
| [1026321] ProFTPD Use-After-Free Memory Error Lets Remote Authenticated Users Execute Arbitrary
Code
| [1020945] ProFTPD Request Processing Bug Permits Cross-Site Request Forgery Attacks
| [1017931] ProFTPD Auth API State Error May Let Remote Users Access the System in Certain Cases
| [1017167] ProFTPD sreplace() Off-by-one Bug Lets Remote Users Execute Arbitrary Code
| [1012488] ProFTPD SITE CHGRP Command Lets Remote Authenticated Users Modify File/Directory Gr
oup Ownership
| [1011687] ProFTPd Login Timing Differences Disclose Valid User Account Names to Remote Users
| [1009997] ProFTPD Access Control Bug With CIDR Addresses May Let Remote Authenticated Users Ac
cess Files
| [1009297] ProFTPD _xlate_ascii_write() Off-By-One Buffer Overflows Let Remote Users Execute Arbitra
ry Code With Root Privileges
| [1007794] ProFTPD ASCII Mode File Upload Buffer Overflow Lets Certain Remote Users Execute Arbitr
ary Code
| [1007020] ProFTPD Input Validation Flaw When Authenticating Against Postgresql Using ’mod_sql’ Lets
Remote Users Gain Access
| [1003019] ProFTPD FTP Server May Allow Local Users to Execute Code on the Server
| [1002354] ProFTPD Reverse DNS Feature Fails to Check Forward-to-Reverse DNS Mappings
| [1002148] ProFTPD Site and Quote Commands May Allow Remote Users to Execute Arbitrary Comman
ds on the Server
|
| OSVDB - http://www.osvdb.org:
| [89051] ProFTPD Multiple FTP Command Handling Symlink Arbitrary File Overwrite
| [77004] ProFTPD Use-After-Free Response Pool Allocation List Parsing Remote Memory Corruption
| [70868] ProFTPD mod_sftp Component SSH Payload DoS
| [70782] ProFTPD contrib/mod_sql.c sql_prepare_where Function Crafted Username Handling Remote
Overflow

| [69562] ProFTPD on ftp.proftpd.org Compromised Source Packages Trojaned Distribution
| [69200] ProFTPD pr_data_xfer Function ABOR Command Remote DoS
| [68988] ProFTPD mod_site_misc Module Multiple Command Traversal Arbitrary File Manipulation
| [68985] ProFTPD netio.c pr_netio_telnet_gets Function TELNET_IAC Escape Sequence Remote Overfl
ow
| [59292] ProFTPD mod_tls Module Certificate Authority (CA) subjectAltName Field Null Byte Handling SS
L MiTM Weakness
| [57311] ProFTPD contrib/mod_ratio.c Multiple Unspecified Buffer Handling Issues
| [57310] ProFTPD Multiple Unspecified Overflows
| [57309] ProFTPD src/support.c Unspecified Buffer Handling Issue
| [57308] ProFTPD modules/mod_core.c Multiple Unspecified Overflows
| [57307] ProFTPD Multiple Modules Unspecified Overflows
| [57306] ProFTPD contrib/mod_pam.c Multiple Unspecified Buffer Handling Issues
| [57305] ProFTPD src/main.c Unspecified Overflow
| [57304] ProFTPD src/log.c Logfile Handling Unspecified Race Condition
| [57303] ProFTPD modules/mod_auth.c Unspecified Issue
| [51954] ProFTPD Server NLS Support mod_sql_* Encoded Multibyte Character SQL Injection Protection
 Bypass
| [51953] ProFTPD Server mod_sql username % Character Handling SQL Injection
| [51849] ProFTPD Character Encoding SQL Injection
| [51720] ProFTPD NLST Command Argument Handling Remote Overflow
| [51719] ProFTPD MKDIR Command Directory Name Handling Remote Overflow
| [48411] ProFTPD FTP Command Truncation CSRF
| [34602] ProFTPD Auth API Multiple Auth Module Authentication Bypass
| [31509] ProFTPD mod_ctrls Module pr_ctrls_recv_request Function Local Overflow
| [30719] mod_tls Module for ProFTPD tls_x509_name_oneline Function Remote Overflow
| [30660] ProFTPD CommandBufferSize Option cmd_loop() Function DoS
| [30267] ProFTPD src/support.c sreplace() Function Remote Overflow
| [23063] ProFTPD mod_radius Password Overflow DoS
| [20212] ProFTPD Host Reverse Resolution Failure ACL Bypass
| [18271] ProFTPD mod_sql SQLShowInfo Directive Format String
| [18270] ProFTPD ftpshut Shutdown Message Format String
| [14012] GProftpd gprostats Utility Log Parser Remote Format String
| [10769] ProFTPD File Transfer Newline Character Overflow
| [10768] ProFTPD STAT Command Remote DoS
| [10758] ProFTPD Login Timing Account Name Enumeration
| [10173] ProFTPD mod_sqlpw wtmp Authentication Credential Disclosure
| [9507] PostgreSQL Authentication Module (mod_sql) for ProFTPD USER Name Parameter SQL Injectio
n
| [9163] ProFTPD MKDIR Directory Creation / Change Remote Overflow (palmetto)
| [7166] ProFTPD SIZE Command Memory Leak Remote DoS
| [7165] ProFTPD USER Command Memory Leak DoS
| [5744] ProFTPD CIDR IP Subnet ACL Bypass
| [5705] ProFTPD Malformed cwd Command Format String
| [5638] ProFTPD on Debian Linux postinst Installation Privilege Escalation
| [4134] ProFTPD in_xlate_ascii_write() Function RETR Command Remote Overflow
| [144] ProFTPD src/log.c log_xfer() Function Remote Overflow
|_
| vulners:
| cpe:/a:proftpd:proftpd:1.3.5:
| SAINT:FD1752E124A72FD3A26EEB9B315E8382 10.0 https://vulners.com/saint/SAINT:FD1752E12
4A72FD3A26EEB9B315E8382 *EXPLOIT*
| SAINT:950EB68D408A40399926A4CCAD3CC62E 10.0 https://vulners.com/saint/SAINT:950EB68D4
08A40399926A4CCAD3CC62E *EXPLOIT*
| SAINT:63FB77B9136D48259E4F0D4CDA35E957 10.0 https://vulners.com/saint/SAINT:63FB77B91

36D48259E4F0D4CDA35E957 *EXPLOIT*
| SAINT:1B08F4664C428B180EEC9617B41D9A2C 10.0 https://vulners.com/saint/SAINT:1B08F4664
C428B180EEC9617B41D9A2C *EXPLOIT*
| PROFTPD_MOD_COPY 10.0 https://vulners.com/canvas/PROFTPD_MOD_COPY *EXPLOIT*
| PRION:CVE-2015-3306 10.0 https://vulners.com/prion/PRION:CVE-2015-3306
| PACKETSTORM:162777 10.0 https://vulners.com/packetstorm/PACKETSTORM:162777 *EXPLOIT*
| PACKETSTORM:132218 10.0 https://vulners.com/packetstorm/PACKETSTORM:132218 *EXPLOIT*
| PACKETSTORM:131567 10.0 https://vulners.com/packetstorm/PACKETSTORM:131567 *EXPLOIT*
| PACKETSTORM:131555 10.0 https://vulners.com/packetstorm/PACKETSTORM:131555 *EXPLOIT*
| PACKETSTORM:131505 10.0 https://vulners.com/packetstorm/PACKETSTORM:131505 *EXPLOIT*
| EDB-ID:49908 10.0 https://vulners.com/exploitdb/EDB-ID:49908 *EXPLOIT*
| CVE-2015-3306 10.0 https://vulners.com/cve/CVE-2015-3306
| 1337DAY-ID-36298 10.0 https://vulners.com/zdt/1337DAY-ID-36298 *EXPLOIT*
| 1337DAY-ID-23720 10.0 https://vulners.com/zdt/1337DAY-ID-23720 *EXPLOIT*
| 1337DAY-ID-23544 10.0 https://vulners.com/zdt/1337DAY-ID-23544 *EXPLOIT*
| SSV:61050 5.0 https://vulners.com/seebug/SSV:61050 *EXPLOIT*
| PRION:CVE-2019-19272 5.0 https://vulners.com/prion/PRION:CVE-2019-19272
| PRION:CVE-2019-19271 5.0 https://vulners.com/prion/PRION:CVE-2019-19271
| PRION:CVE-2019-19270 5.0 https://vulners.com/prion/PRION:CVE-2019-19270
| PRION:CVE-2019-18217 5.0 https://vulners.com/prion/PRION:CVE-2019-18217
| PRION:CVE-2016-3125 5.0 https://vulners.com/prion/PRION:CVE-2016-3125
| CVE-2021-46854 5.0 https://vulners.com/cve/CVE-2021-46854
| CVE-2020-9272 5.0 https://vulners.com/cve/CVE-2020-9272
| CVE-2019-19272 5.0 https://vulners.com/cve/CVE-2019-19272
| CVE-2019-19271 5.0 https://vulners.com/cve/CVE-2019-19271
| CVE-2019-19270 5.0 https://vulners.com/cve/CVE-2019-19270
| CVE-2019-18217 5.0 https://vulners.com/cve/CVE-2019-18217
| CVE-2016-3125 5.0 https://vulners.com/cve/CVE-2016-3125
| CVE-2013-4359 5.0 https://vulners.com/cve/CVE-2013-4359
| PRION:CVE-2017-7418 2.1 https://vulners.com/prion/PRION:CVE-2017-7418
|_ CVE-2017-7418 2.1 https://vulners.com/cve/CVE-2017-7418
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:6.6.1p1:
| PRION:CVE-2015-5600 8.5 https://vulners.com/prion/PRION:CVE-2015-5600
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| PRION:CVE-2020-16088 7.5 https://vulners.com/prion/PRION:CVE-2020-16088
| PRION:CVE-2015-6564 6.9 https://vulners.com/prion/PRION:CVE-2015-6564
| CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564
| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919
| PRION:CVE-2015-5352 4.3 https://vulners.com/prion/PRION:CVE-2015-5352
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2015-5352 4.3 https://vulners.com/cve/CVE-2015-5352
| PRION:CVE-2015-6563 1.9 https://vulners.com/prion/PRION:CVE-2015-6563
|_ CVE-2015-6563 1.9 https://vulners.com/cve/CVE-2015-6563
| temp: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2012-5975] The SSH USERAUTH CHANGE REQUEST feature in SSH Tectia Server 6.0.4 throug
h 6.0.20, 6.1.0 through 6.1.12, 6.2.0 through 6.2.5, and 6.3.0 through 6.3.2 on UNIX and Linux, when old-
style password authentication is enabled, allows remote attackers to bypass authentication via a crafted s
ession involving entry of blank passwords, as demonstrated by a root login session from a modified Open
SSH client with an added input_userauth_passwd_changereq call in sshconnect2.c.
| [CVE-2012-5536] A certain Red Hat build of the pam_ssh_agent_auth module on Red Hat Enterprise Li

nux (RHEL) 6 and Fedora Rawhide calls the glibc error function instead of the error function in the OpenSSH codebase, which allows local users to obtain sensitive information from process memory or possibly gain privileges via crafted use of an application that relies on this module, as demonstrated by su and sudo.
| [CVE-2010-5107] The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.
| [CVE-2008-1483] OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.
| [CVE-2007-3102] Unspecified vulnerability in the linux_audit_record_event function in OpenSSH 4.3p2, as used on Fedora Core 6 and possibly other systems, allows remote attackers to write arbitrary characters to an audit log via a crafted username. NOTE: some of these details are obtained from third party information.
| [CVE-2004-2414] Novell NetWare 6.5 SP 1.1, when installing or upgrading using the Overlay CDs and performing a custom installation with OpenSSH, includes sensitive password information in the (1) NIOUTPUT.TXT and (2) NI.LOG log files, which might allow local users to obtain the passwords.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [102780] OpenSSH CVE-2016-10708 Multiple Denial of Service Vulnerabilities
| [101552] OpenSSH ’sftp-server.c’ Remote Security Bypass Vulnerability
| [94977] OpenSSH CVE-2016-10011 Local Information Disclosure Vulnerability
| [94975] OpenSSH CVE-2016-10012 Security Bypass Vulnerability
| [94972] OpenSSH CVE-2016-10010 Privilege Escalation Vulnerability
| [94968] OpenSSH CVE-2016-10009 Remote Code Execution Vulnerability
| [93776] OpenSSH ’ssh/kex.c’ Denial of Service Vulnerability
| [92212] OpenSSH CVE-2016-6515 Denial of Service Vulnerability
| [92210] OpenSSH CBC Padding Weak Encryption Security Weakness
| [92209] OpenSSH MAC Verification Security Bypass Vulnerability
| [91812] OpenSSH CVE-2016-6210 User Enumeration Vulnerability
| [90440] OpenSSH CVE-2004-1653 Remote Security Vulnerability
| [90340] OpenSSH CVE-2004-2760 Remote Security Vulnerability
| [89385] OpenSSH CVE-2005-2666 Local Security Vulnerability
| [88655] OpenSSH CVE-2001-1382 Remote Security Vulnerability
| [88513] OpenSSH CVE-2000-0999 Remote Security Vulnerability
| [88367] OpenSSH CVE-1999-1010 Local Security Vulnerability
| [87789] OpenSSH CVE-2003-0682 Remote Security Vulnerability
| [86187] OpenSSH ’session.c’ Local Security Bypass Vulnerability
| [86144] OpenSSH CVE-2007-2768 Remote Security Vulnerability
| [84427] OpenSSH CVE-2016-1908 Security Bypass Vulnerability
| [84314] OpenSSH CVE-2016-3115 Remote Command Injection Vulnerability
| [84185] OpenSSH CVE-2006-4925 Denial-Of-Service Vulnerability
| [81293] OpenSSH CVE-2016-1907 Denial of Service Vulnerability
| [80698] OpenSSH CVE-2016-0778 Heap Based Buffer Overflow Vulnerability
| [80695] OpenSSH CVE-2016-0777 Information Disclosure Vulnerability
| [76497] OpenSSH CVE-2015-6565 Local Security Bypass Vulnerability
| [76317] OpenSSH PAM Support Multiple Remote Code Execution Vulnerabilities
| [75990] OpenSSH Login Handling Security Bypass Weakness
| [75525] OpenSSH ’x11_open_helper()’ Function Security Bypass Vulnerability
| [71420] Portable OpenSSH ’gss-serv-krb5.c’ Security Bypass Vulnerability
| [68757] OpenSSH Multiple Remote Denial of Service Vulnerabilities
| [66459] OpenSSH Certificate Validation Security Bypass Vulnerability
| [66355] OpenSSH ’child_set_env()’ Function Security Bypass Vulnerability
| [65674] OpenSSH ’ssh-keysign.c’ Local Information Disclosure Vulnerability
| [65230] OpenSSH ’schnorr.c’ Remote Memory Corruption Vulnerability

| [63605] OpenSSH 'sshd' Process Remote Memory Corruption Vulnerability
| [61286] OpenSSH Remote Denial of Service Vulnerability
| [58894] GSI-OpenSSH PAM_USER Security Bypass Vulnerability
| [58162] OpenSSH CVE-2010-5107 Denial of Service Vulnerability
| [54114] OpenSSH 'ssh_gssapi_parse_ename()' Function Denial of Service Vulnerability
| [51702] Debian openssh-server Forced Command Handling Information Disclosure Vulnerability
| [50416] Linux Kernel 'kdump' and 'mkdumprd' OpenSSH Integration Remote Information Disclosure Vul
nerability
| [49473] OpenSSH Ciphersuite Specification Information Disclosure Weakness
| [48507] OpenSSH 'pam_thread()' Remote Buffer Overflow Vulnerability
| [47691] Portable OpenSSH 'ssh-keysign' Local Unauthorized Access Vulnerability
| [46155] OpenSSH Legacy Certificate Signing Information Disclosure Vulnerability
| [45304] OpenSSH J-PAKE Security Bypass Vulnerability
| [36552] Red Hat Enterprise Linux OpenSSH 'ChrootDirectory' Option Local Privilege Escalation Vulnera
bility
| [32319] OpenSSH CBC Mode Information Disclosure Vulnerability
| [30794] Red Hat OpenSSH Backdoor Vulnerability
| [30339] OpenSSH 'X11UseLocalhost' X11 Forwarding Session Hijacking Vulnerability
| [30276] Debian OpenSSH SELinux Privilege Escalation Vulnerability
| [28531] OpenSSH ForceCommand Command Execution Weakness
| [28444] OpenSSH X Connections Session Hijacking Vulnerability
| [26097] OpenSSH LINUX_AUDIT_RECORD_EVENT Remote Log Injection Weakness
| [25628] OpenSSH X11 Cookie Local Authentication Bypass Vulnerability
| [23601] OpenSSH S/Key Remote Information Disclosure Vulnerability
| [20956] OpenSSH Privilege Separation Key Signature Weakness
| [20418] OpenSSH-Portable Existing Password Remote Information Disclosure Weakness
| [20245] OpenSSH-Portable GSSAPI Authentication Abort Information Disclosure Weakness
| [20241] Portable OpenSSH GSSAPI Remote Code Execution Vulnerability
| [20216] OpenSSH Duplicated Block Remote Denial of Service Vulnerability
| [16892] OpenSSH Remote PAM Denial Of Service Vulnerability
| [14963] OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability
| [14729] OpenSSH GSSAPI Credential Disclosure Vulnerability
| [14727] OpenSSH DynamicForward Inadvertent GatewayPorts Activation Vulnerability
| [11781] OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability
| [9986] RCP, OpenSSH SCP Client File Corruption Vulnerability
| [9040] OpenSSH PAM Conversation Memory Scrubbing Weakness
| [8677] Multiple Portable OpenSSH PAM Vulnerabilities
| [8628] OpenSSH Buffer Mismanagement Vulnerabilities
| [7831] OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability
| [7482] OpenSSH Remote Root Authentication Timing Side-Channel Weakness
| [7467] OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability
| [7343] OpenSSH Authentication Execution Path Timing Information Leakage Weakness
| [6168] OpenSSH Visible Password Vulnerability
| [5374] OpenSSH Trojan Horse Vulnerability
| [5093] OpenSSH Challenge-Response Buffer Overflow Vulnerabilities
| [4560] OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow Vulnerability
| [4241] OpenSSH Channel Code Off-By-One Vulnerability
| [3614] OpenSSH UseLogin Environment Variable Passing Vulnerability
| [3560] OpenSSH Kerberos Arbitrary Privilege Elevation Vulnerability
| [3369] OpenSSH Key Based Source IP Access Control Bypass Vulnerability
| [3345] OpenSSH SFTP Command Restriction Bypassing Vulnerability
| [2917] OpenSSH PAM Session Evasion Vulnerability
| [2825] OpenSSH Client X11 Forwarding Cookie Removal File Symbolic Link Vulnerability
| [2356] OpenSSH Private Key Authentication Check Vulnerability
| [1949] OpenSSH Client Unauthorized Remote Forwarding Vulnerability

| [1334] OpenSSH UseLogin Vulnerability
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [83258] GSI-OpenSSH auth-pam.c security bypass
| [82781] OpenSSH time limit denial of service
| [82231] OpenSSH pam_ssh_agent_auth PAM code execution
| [74809] OpenSSH ssh_gssapi_parse_ename denial of service
| [72756] Debian openssh-server commands information disclosure
| [68339] OpenSSH pam_thread buffer overflow
| [67264] OpenSSH ssh-keysign unauthorized access
| [65910] OpenSSH remote_glob function denial of service
| [65163] OpenSSH certificate information disclosure
| [64387] OpenSSH J-PAKE security bypass
| [63337] Cisco Unified Videoconferencing OpenSSH weak security
| [46620] OpenSSH and multiple SSH Tectia products CBC mode information disclosure
| [45202] OpenSSH signal handler denial of service
| [44747] RHEL OpenSSH backdoor
| [44280] OpenSSH PermitRootLogin information disclosure
| [44279] OpenSSH sshd weak security
| [44037] OpenSSH sshd SELinux role unauthorized access
| [43940] OpenSSH X11 forwarding information disclosure
| [41549] OpenSSH ForceCommand directive security bypass
| [41438] OpenSSH sshd session hijacking
| [40897] OpenSSH known_hosts weak security
| [40587] OpenSSH username weak security
| [37371] OpenSSH username data manipulation
| [37118] RHSA update for OpenSSH privilege separation monitor authentication verification weakness no
t installed
| [37112] RHSA update for OpenSSH signal handler race condition not installed
| [37107] RHSA update for OpenSSH identical block denial of service not installed
| [36637] OpenSSH X11 cookie privilege escalation
| [35167] OpenSSH packet.c newkeys[mode] denial of service
| [34490] OpenSSH OPIE information disclosure
| [33794] OpenSSH ChallengeResponseAuthentication information disclosure
| [32975] Apple Mac OS X OpenSSH denial of service
| [32387] RHSA-2006:0738 updates for openssh not installed
| [32359] RHSA-2006:0697 updates for openssh not installed
| [32230] RHSA-2006:0298 updates for openssh not installed
| [32132] RHSA-2006:0044 updates for openssh not installed
| [30120] OpenSSH privilege separation monitor authentication verification weakness
| [29255] OpenSSH GSSAPI user enumeration
| [29254] OpenSSH signal handler race condition
| [29158] OpenSSH identical block denial of service
| [28147] Apple Mac OS X OpenSSH nonexistent user login denial of service
| [25116] OpenSSH OpenPAM denial of service
| [24305] OpenSSH SCP shell expansion command execution
| [22665] RHSA-2005:106 updates for openssh not installed
| [22117] OpenSSH GSSAPI allows elevated privileges
| [22115] OpenSSH GatewayPorts security bypass
| [20930] OpenSSH sshd.c LoginGraceTime denial of service
| [19441] Sun Solaris OpenSSH LDAP (1) client authentication denial of service
| [17213] OpenSSH allows port bouncing attacks
| [16323] OpenSSH scp file overwrite
| [13797] OpenSSH PAM information leak
| [13271] OpenSSH could allow an attacker to corrupt the PAM conversion stack

| [13264] OpenSSH PAM code could allow an attacker to gain access
| [13215] OpenSSH buffer management errors could allow an attacker to execute code
| [13214] OpenSSH memory vulnerabilities
| [13191] OpenSSH large packet buffer overflow
| [12196] OpenSSH could allow an attacker to bypass login restrictions
| [11970] OpenSSH could allow an attacker to obtain valid administrative account
| [11902] OpenSSH PAM support enabled information leak
| [9803] OpenSSH &quot
| [9763] OpenSSH downloaded from the OpenBSD FTP site or OpenBSD FTP mirror sites could contain a Trojan Horse
| [9307] OpenSSH is running on the system
| [9169] OpenSSH &quot
| [8896] OpenSSH Kerberos 4 TGT/AFS buffer overflow
| [8697] FreeBSD libutil in OpenSSH fails to drop privileges prior to using the login class capability database
| [8383] OpenSSH off-by-one error in channel code
| [7647] OpenSSH UseLogin option arbitrary code execution
| [7634] OpenSSH using sftp and restricted keypairs could allow an attacker to bypass restrictions
| [7598] OpenSSH with Kerberos allows attacker to gain elevated privileges
| [7179] OpenSSH source IP access control bypass
| [6757] OpenSSH &quot
| [6676] OpenSSH X11 forwarding symlink attack could allow deletion of arbitrary files
| [6084] OpenSSH 2.3.1 allows remote users to bypass authentication
| [5517] OpenSSH allows unauthorized access to resources
| [4646] OpenSSH UseLogin option allows remote users to execute commands as root
|
| Exploit-DB - https://www.exploit-db.com:
| [14866] Novell Netware 6.5 - OpenSSH Remote Stack Overflow
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [902488] OpenSSH 'sshd' GSSAPI Credential Disclosure Vulnerability
| [900179] OpenSSH CBC Mode Information Disclosure Vulnerability
| [881183] CentOS Update for openssh CESA-2012:0884 centos6
| [880802] CentOS Update for openssh CESA-2009:1287 centos5 i386
| [880746] CentOS Update for openssh CESA-2009:1470 centos5 i386
| [870763] RedHat Update for openssh RHSA-2012:0884-04
| [870129] RedHat Update for openssh RHSA-2008:0855-01
| [861813] Fedora Update for openssh FEDORA-2010-5429
| [861319] Fedora Update for openssh FEDORA-2007-395
| [861170] Fedora Update for openssh FEDORA-2007-394
| [861012] Fedora Update for openssh FEDORA-2007-715
| [840345] Ubuntu Update for openssh vulnerability USN-597-1
| [840300] Ubuntu Update for openssh update USN-612-5
| [840271] Ubuntu Update for openssh vulnerability USN-612-2
| [840268] Ubuntu Update for openssh update USN-612-7
| [840259] Ubuntu Update for openssh vulnerabilities USN-649-1
| [840214] Ubuntu Update for openssh vulnerability USN-566-1
| [831074] Mandriva Update for openssh MDVA-2010:162 (openssh)
| [830929] Mandriva Update for openssh MDVA-2010:090 (openssh)
| [830807] Mandriva Update for openssh MDVA-2010:026 (openssh)
| [830603] Mandriva Update for openssh MDVSA-2008:098 (openssh)
| [830523] Mandriva Update for openssh MDVSA-2008:078 (openssh)
| [830317] Mandriva Update for openssh-askpass-qt MDKA-2007:127 (openssh-askpass-qt)
| [830191] Mandriva Update for openssh MDKSA-2007:236 (openssh)
| [802407] OpenSSH 'sshd' Challenge Response Authentication Buffer Overflow Vulnerability

| [103503] openssh-server Forced Command Handling Information Disclosure Vulnerability
| [103247] OpenSSH Ciphersuite Specification Information Disclosure Weakness
| [103064] OpenSSH Legacy Certificate Signing Information Disclosure Vulnerability
| [100584] OpenSSH X Connections Session Hijacking Vulnerability
| [100153] OpenSSH CBC Mode Information Disclosure Vulnerability
| [66170] CentOS Security Advisory CESA-2009:1470 (openssh)
| [65987] SLES10: Security update for OpenSSH
| [65819] SLES10: Security update for OpenSSH
| [65514] SLES9: Security update for OpenSSH
| [65513] SLES9: Security update for OpenSSH
| [65334] SLES9: Security update for OpenSSH
| [65248] SLES9: Security update for OpenSSH
| [65218] SLES9: Security update for OpenSSH
| [65169] SLES9: Security update for openssh,openssh-askpass
| [65126] SLES9: Security update for OpenSSH
| [65019] SLES9: Security update for OpenSSH
| [65015] SLES9: Security update for OpenSSH
| [64931] CentOS Security Advisory CESA-2009:1287 (openssh)
| [61639] Debian Security Advisory DSA 1638-1 (openssh)
| [61030] Debian Security Advisory DSA 1576-2 (openssh)
| [61029] Debian Security Advisory DSA 1576-1 (openssh)
| [60840] FreeBSD Security Advisory (FreeBSD-SA-08:05.openssh.asc)
| [60803] Gentoo Security Advisory GLSA 200804-03 (openssh)
| [60667] Slackware Advisory SSA:2008-095-01 openssh
| [59014] Slackware Advisory SSA:2007-255-01 openssh
| [58741] Gentoo Security Advisory GLSA 200711-02 (openssh)
| [57919] Gentoo Security Advisory GLSA 200611-06 (openssh)
| [57895] Gentoo Security Advisory GLSA 200609-17 (openssh)
| [57585] Debian Security Advisory DSA 1212-1 (openssh (1:3.8.1p1-8.sarge.6))
| [57492] Slackware Advisory SSA:2006-272-02 openssh
| [57483] Debian Security Advisory DSA 1189-1 (openssh-krb5)
| [57476] FreeBSD Security Advisory (FreeBSD-SA-06:22.openssh.asc)
| [57470] FreeBSD Ports: openssh
| [56352] FreeBSD Security Advisory (FreeBSD-SA-06:09.openssh.asc)
| [56330] Gentoo Security Advisory GLSA 200602-11 (OpenSSH)
| [56294] Slackware Advisory SSA:2006-045-06 openssh
| [53964] Slackware Advisory SSA:2003-266-01 New OpenSSH packages
| [53885] Slackware Advisory SSA:2003-259-01 OpenSSH Security Advisory
| [53884] Slackware Advisory SSA:2003-260-01 OpenSSH updated again
| [53788] Debian Security Advisory DSA 025-1 (openssh)
| [52638] FreeBSD Security Advisory (FreeBSD-SA-03:15.openssh.asc)
| [52635] FreeBSD Security Advisory (FreeBSD-SA-03:12.openssh.asc)
| [11343] OpenSSH Client Unauthorized Remote Forwarding
| [10954] OpenSSH AFS/Kerberos ticket/token passing
| [10883] OpenSSH Channel Code Off by 1
| [10823] OpenSSH UseLogin Environment Variables
|
| SecurityTracker - https://www.securitytracker.com:
| [1028187] OpenSSH pam_ssh_agent_auth Module on Red Hat Enterprise Linux Lets Remote Users Ex
ecute Arbitrary Code
| [1026593] OpenSSH Lets Remote Authenticated Users Obtain Potentially Sensitive Information
| [1025739] OpenSSH on FreeBSD Has Buffer Overflow in pam_thread() That Lets Remote Users Execut
e Arbitrary Code
| [1025482] OpenSSH ssh-keysign Utility Lets Local Users Gain Elevated Privileges
| [1025028] OpenSSH Legacy Certificates May Disclose Stack Contents to Remote Users

| [1022967] OpenSSH on Red Hat Enterprise Linux Lets Remote Authenticated Users Gain Elevated Privil
eges
| [1021235] OpenSSH CBC Mode Error Handling May Let Certain Remote Users Obtain Plain Text in Cert
ain Cases
| [1020891] OpenSSH on Debian Lets Remote Users Prevent Logins
| [1020730] OpenSSH for Red Hat Enterprise Linux Packages May Have Been Compromised
| [1020537] OpenSSH on HP-UX Lets Local Users Hijack X11 Sessions
| [1019733] OpenSSH Unsafe Default Configuration May Let Local Users Execute Arbitrary Commands
| [1019707] OpenSSH Lets Local Users Hijack Forwarded X Sessions in Certain Cases
| [1017756] Apple OpenSSH Key Generation Process Lets Remote Users Deny Service
| [1017183] OpenSSH Privilege Separation Monitor Validation Error May Cause the Monitor to Fail to Pro
perly Control the Unprivileged Process
| [1016940] OpenSSH Race Condition in Signal Handler Lets Remote Users Deny Service and May Poten
tially Permit Code Execution
| [1016939] OpenSSH GSSAPI Authentication Abort Error Lets Remote Users Determine Valid Username
s
| [1016931] OpenSSH SSH v1 CRC Attack Detection Implementation Lets Remote Users Deny Service
| [1016672] OpenSSH on Mac OS X Lets Remote Users Deny Service
| [1015706] OpenSSH Interaction With OpenPAM Lets Remote Users Deny Service
| [1015540] OpenSSH scp Double Shell Character Expansion During Local-to-Local Copying May Let Loc
al Users Gain Elevated Privileges in Certain Cases
| [1014845] OpenSSH May Unexpectedly Activate GatewayPorts and Also May Disclose GSSAPI Creden
tials in Certain Cases
| [1011193] OpenSSH scp Directory Traversal Flaw Lets Remote SSH Servers Overwrite Files in Certain
Cases
| [1011143] OpenSSH Default Configuration May Be Unsafe When Used With Anonymous SSH Services
| [1007791] Portable OpenSSH PAM free() Bug May Let Remote Users Execute Root Code
| [1007716] OpenSSH buffer_append_space() and Other Buffer Management Errors May Let Remote Us
ers Execute Arbitrary Code
| [1006926] OpenSSH Host Access Restrictions Can Be Bypassed By Remote Users
| [1006688] OpenSSH Timing Flaw With Pluggable Authentication Modules Can Disclose Valid User Acco
unt Names to Remote Users
| [1004818] OpenSSH’s Secure Shell (SSH) Implementation Weakness May Disclose User Passwords to
Remote Users During Man-in-the-Middle Attacks
| [1004616] OpenSSH Integer Overflow and Buffer Overflow May Allow Remote Users to Gain Root Acce
ss to the System
| [1004391] OpenSSH ’BSD_AUTH’ Access Control Bug May Allow Unauthorized Remote Users to Authe
nticated to the System
| [1004115] OpenSSH Buffer Overflow in Kerberos Ticket and AFS Token Processing Lets Local Users E
xecute Arbitrary Code With Root Level Permissions
| [1003758] OpenSSH Off-by-one ’Channels’ Bug May Let Authorized Remote Users Execute Arbitrary Co
de with Root Privileges
| [1002895] OpenSSH UseLogin Environment Variable Bug Lets Local Users Execute Commands and Ga
in Root Access
| [1002748] OpenSSH 3.0 Denial of Service Condition May Allow Remote Users to Crash the sshd Daem
on and KerberosV Configuration Error May Allow Remote Users to Partially Authenticate When Authentic
ation Should Not Be Permitted
| [1002734] OpenSSH’s S/Key Implementation Information Disclosure Flaw Provides Remote Users With I
nformation About Valid User Accounts
| [1002455] OpenSSH May Fail to Properly Restrict IP Addresses in Certain Configurations
| [1002432] OpenSSH’s Sftp-server Subsystem Lets Authorized Remote Users with Restricted Keypairs O
btain Additional Access on the Server
| [1001683] OpenSSH Allows Authorized Users to Delete Other User Files Named Cookies
|
| OSVDB - http://www.osvdb.org:

| [92034] GSI-OpenSSH auth-pam.c Memory Management Authentication Bypass
| [90474] Red Hat / Fedora PAM Module for OpenSSH Incorrect error() Function Calling Local Privilege E
scalation
| [90007] OpenSSH logingracetime / maxstartup Threshold Connection Saturation Remote DoS
| [81500] OpenSSH gss-serv.c ssh_gssapi_parse_ename Function Field Length Value Parsing Remote D
oS
| [78706] OpenSSH auth-options.c sshd auth_parse_options Function authorized_keys Command Option
Debug Message Information Disclosure
| [75753] OpenSSH PAM Module Aborted Conversation Local Information Disclosure
| [75249] OpenSSH sftp-glob.c remote_glob Function Glob Expression Parsing Remote DoS
| [75248] OpenSSH sftp.c process_put Function Glob Expression Parsing Remote DoS
| [72183] Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Di
sclosure
| [70873] OpenSSH Legacy Certificates Stack Memory Disclosure
| [69658] OpenSSH J-PAKE Public Parameter Validation Shared Secret Authentication Bypass
| [67743] Novell NetWare OpenSSH SSHD.NLM Absolute Path Handling Remote Overflow
| [59353] OpenSSH sshd Local TCP Redirection Connection Masking Weakness
| [58495] OpenSSH sshd ChrootDirectory Feature SetUID Hard Link Local Privilege Escalation
| [56921] OpenSSH Unspecified Remote Compromise
| [53021] OpenSSH on ftp.openbsd.org Trojaned Distribution
| [50036] OpenSSH CBC Mode Chosen Ciphertext 32-bit Chunk Plaintext Context Disclosure
| [49386] OpenSSH sshd TCP Connection State Remote Account Enumeration
| [48791] OpenSSH on Debian sshd Crafted Username Arbitrary Remote SELinux Role Access
| [47635] OpenSSH Packages on Red Hat Enterprise Linux Compromised Distribution
| [47227] OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
| [45873] Cisco WebNS SSHield w/ OpenSSH Crafted Large Packet Remote DoS
| [43911] OpenSSH ~/.ssh/rc ForceCommand Bypass Arbitrary Command Execution
| [43745] OpenSSH X11 Forwarding Local Session Hijacking
| [43371] OpenSSH Trusted X11 Cookie Connection Policy Bypass
| [39214] OpenSSH linux_audit_record_event Crafted Username Audit Log Injection
| [37315] pam_usb OpenSSH Authentication Unspecified Issue
| [34850] OpenSSH on Mac OS X Key Generation Remote Connection DoS
| [34601] OPIE w/ OpenSSH Account Enumeration
| [34600] OpenSSH S/KEY Authentication Account Enumeration
| [32721] OpenSSH Username Password Complexity Account Enumeration
| [30232] OpenSSH Privilege Separation Monitor Weakness
| [29494] OpenSSH packet.c Invalid Protocol Sequence Remote DoS
| [29266] OpenSSH GSSAPI Authentication Abort Username Enumeration
| [29264] OpenSSH Signal Handler Pre-authentication Race Condition Code Execution
| [29152] OpenSSH Identical Block Packet DoS
| [27745] Apple Mac OS X OpenSSH Nonexistent Account Login Enumeration DoS
| [23797] OpenSSH with OpenPAM Connection Saturation Forked Process Saturation DoS
| [22692] OpenSSH scp Command Line Filename Processing Command Injection
| [20216] OpenSSH with KerberosV Remote Authentication Bypass
| [19142] OpenSSH Multiple X11 Channel Forwarding Leaks
| [19141] OpenSSH GSSAPIAuthentication Credential Escalation
| [18236] OpenSSH no pty Command Execution Local PAM Restriction Bypass
| [16567] OpenSSH Privilege Separation LoginGraceTime DoS
| [16039] Solaris 108994 Series Patch OpenSSH LDAP Client Authentication DoS
| [9562] OpenSSH Default Configuration Anon SSH Service Port Bounce Weakness
| [9550] OpenSSH scp Traversal Arbitrary File Overwrite
| [6601] OpenSSH *realloc() Unspecified Memory Errors
| [6245] OpenSSH SKEY/BSD_AUTH Challenge-Response Remote Overflow
| [6073] OpenSSH on FreeBSD libutil Arbitrary File Read
| [6072] OpenSSH PAM Conversation Function Stack Modification

| [6071] OpenSSH SSHv1 PAM Challenge-Response Authentication Privilege Escalation
| [5536] OpenSSH sftp-server Restricted Keypair Restriction Bypass
| [5408] OpenSSH echo simulation Information Disclosure
| [5113] OpenSSH NIS YP Netgroups Authentication Bypass
| [4536] OpenSSH Portable AIX linker Privilege Escalation
| [3938] OpenSSL and OpenSSH /dev/random Check Failure
| [3456] OpenSSH buffer_append_space() Heap Corruption
| [2557] OpenSSH Multiple Buffer Management Multiple Overflows
| [2140] OpenSSH w/ PAM Username Validity Timing Attack
| [2112] OpenSSH Reverse DNS Lookup Bypass
| [2109] OpenSSH sshd Root Login Timing Side-Channel Weakness
| [1853] OpenSSH Symbolic Link 'cookies' File Removal
| [839] OpenSSH PAMAuthenticationViaKbdInt Challenge-Response Remote Overflow
| [781] OpenSSH Kerberos TGT/AFS Token Passing Remote Overflow
| [730] OpenSSH Channel Code Off by One Remote Privilege Escalation
| [688] OpenSSH UseLogin Environment Variable Local Command Execution
| [642] OpenSSH Multiple Key Type ACL Bypass
| [504] OpenSSH SSHv2 Public Key Authentication Bypass
| [341] OpenSSH UseLogin Local Privilege Escalation
|_
80/tcp open http Apache httpd 2.4.7
| temp: VulDB - https://vuldb.com:
| [160579] Apache Cassandra up to 2.1.21/2.2.17/3.0.21/3.11.7/4.0-beta1 RMI Registry exposure of resou
rce
| [121358] Apache Spark up to 2.1.2/2.2.1/2.3.0 PySpark/SparkR information disclosure
| [113146] Apache CouchDB 2.0.0 Windows Installer nssm.exe access control
| [99052] Apache Ambari up to 2.3.x kadmin information disclosure
| [87539] Apache Ambari up to 2.1.1 Agent data access control
| [79073] Apache Ambari up to 2.0 Config File Password information disclosure
| [79072] Apache Ambari up to 2.0 Config Screen Password information disclosure
| [60632] Debian apache2 2.2.16-6/2.2.22-1/2.22-3 mod_php cross site scripting
| [55501] Apache Mod Fcgid up to 2.3.2 mod_fcgid fcgid_bucket.c fcgid_header_bucket_read numeric err
or
| [23524] Apache James 2.2.0 Foundation retrieve memory leak
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2012-2378] Apache CXF 2.4.5 through 2.4.7, 2.5.1 through 2.5.3, and 2.6.x before 2.6.1, does not
properly enforce child policies of a WS-SecurityPolicy 1.1 SupportingToken policy on the client side, whic
h allows remote attackers to bypass the (1) AlgorithmSuite, (2) SignedParts, (3) SignedElements, (4) Encr
yptedParts, and (5) EncryptedElements policies.
| [CVE-2013-2249] mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server bef
ore 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requireme
nt for a new session ID, which has unspecified impact and remote attack vectors.
| [CVE-2012-4558] Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in th
e manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP S
erver 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or
HTML via a crafted string.
| [CVE-2012-3502] The proxy functionality in (1) mod_proxy_ajp.c in the mod_proxy_ajp module and (2)
mod_proxy_http.c in the mod_proxy_http module in the Apache HTTP Server 2.4.x before 2.4.3 does not
properly determine the situations that require closing a back-end connection, which allows remote attacke
rs to obtain sensitive information in opportunistic circumstances by reading a response that was intended
for a different client.
| [CVE-2012-3499] Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x bef
ore 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vec
tors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy

_ftp, and (5) mod_status modules.
| [CVE-2012-3451] Apache CXF before 2.4.9, 2.5.x before 2.5.5, and 2.6.x before 2.6.2 allows remote attackers to execute unintended web-service operations by sending a header with a SOAP Action String that is inconsistent with the message body.
| [CVE-2012-2687] Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.
| [CVE-2012-2379] Apache CXF 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1, when a Supporting Token specifies a child WS-SecurityPolicy 1.1 or 1.2 policy, does not properly ensure that an XML element is signed or encrypted, which has unspecified impact and attack vectors.
| [CVE-2012-0883] envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
| [CVE-2011-2516] Off-by-one error in the XML signature feature in Apache XML Security for C++ 1.6.0, as used in Shibboleth before 2.4.3 and possibly other products, allows remote attackers to cause a denial of service (crash) via a signature using a large RSA key, which triggers a buffer overflow.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [42102] Apache 'mod_proxy_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability
| [27237] Apache HTTP Server 2.2.6, 2.0.61 and 1.3.39 'mod_status' Cross-Site Scripting Vulnerability
| [15413] PHP Apache 2 Virtual() Safe_Mode and Open_Basedir Restriction Bypass Vulnerability
| [15177] PHP Apache 2 Local Denial of Service Vulnerability
| [6065] Apache 2 WebDAV CGI POST Request Information Disclosure Vulnerability
| [5816] Apache 2 mod_dav Denial Of Service Vulnerability
| [5486] Apache 2.0 CGI Path Disclosure Vulnerability
| [5485] Apache 2.0 Path Disclosure Vulnerability
| [5434] Apache 2.0 Encoded Backslash Directory Traversal Vulnerability
| [5256] Apache httpd 2.0 CGI Error Path Disclosure Vulnerability
| [4057] Apache 2 for Windows OPTIONS request Path Disclosure Vulnerability
| [4056] Apache 2 for Windows php.exe Path Disclosure Vulnerability
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [75211] Debian GNU/Linux apache 2 cross-site scripting
|
| Exploit-DB - https://www.exploit-db.com:
| [31052] Apache <= 2.2.6 'mod_negotiation' HTML Injection and HTTP Response Splitting Vulnerability
| [30901] Apache HTTP Server 2.2.6 Windows Share PHP File Extension Mapping Information Disclosure Vulnerability
| [30835] Apache HTTP Server <= 2.2.4 413 Error HTTP Request Method Cross-Site Scripting Weakness
| [28424] Apache 2.x HTTP Server Arbitrary HTTP Request Headers Security Weakness
| [28365] Apache 2.2.2 CGI Script Source Code Information Disclosure Vulnerability
| [27915] Apache James 2.2 SMTP Denial of Service Vulnerability
| [27135] Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
| [26710] Apache CXF prior to 2.5.10, 2.6.7 and 2.7.4 - Denial of Service
| [24590] Apache 2.0.x mod_ssl Remote Denial of Service Vulnerability
| [23581] Apache 2.0.4x mod_perl Module File Descriptor Leakage Vulnerability
| [23482] Apache 2.0.4x mod_php Module File Descriptor Leakage Vulnerability (2)
| [23481] Apache 2.0.4x mod_php Module File Descriptor Leakage Vulnerability (1)
| [23296] Red Hat Apache 2.0.40 Directory Index Default Configuration Error
| [23282] apache cocoon 2.14/2.2 - Directory Traversal vulnerability
| [22191] Apache Web Server 2.0.x MS-DOS Device Name Denial of Service Vulnerability
| [21854] Apache 2.0.39/40 Oversized STDERR Buffer Denial of Service Vulnerability
| [21719] Apache 2.0 Path Disclosure Vulnerability
| [21697] Apache 2.0 Encoded Backslash Directory Traversal Vulnerability

| [20272] Apache 1.2.5/1.3.1,UnityMail 2.0 MIME Header DoS Vulnerability
| [19828] Cobalt RaQ 2.0/3.0 Apache .htaccess Disclosure Vulnerability
| [18984] Apache Struts <= 2.2.1.1 - Remote Command Execution
| [18329] Apache Struts2 <= 2.3.1 - Multiple Vulnerabilities
| [17691] Apache Struts < 2.2.0 - Remote Command Execution
| [15319] Apache 2.2 (Windows) Local Denial of Service
| [14617] Apache JackRabbit 2.0.0 webapp XPath Injection
| [11650] Apache 2.2.14 mod_isapi Dangling Pointer Remote SYSTEM Exploit
| [8458] Apache Geronimo <= 2.1.3 - Multiple Directory Traversal Vulnerabilities
| [5330] Apache 2.0 mod_jk2 2.0.2 - Remote Buffer Overflow Exploit (win32)
| [3996] Apache 2.0.58 mod_rewrite Remote Overflow Exploit (win2k3)
| [2237] Apache < 1.3.37, 2.0.59, 2.2.3 (mod_rewrite) Remote Overflow PoC
| [1056] Apache <= 2.0.49 Arbitrary Long HTTP Headers Denial of Service
| [855] Apache <= 2.0.52 HTTP GET request Denial of Service Exploit
| [132] Apache 1.3.x - 2.0.48 - mod_userdir Remote Users Disclosure Exploit
| [38] Apache <= 2.0.45 APR Remote Exploit -Apache-Knacker.pl
| [34] Webfroot Shoutbox < 2.32 (Apache) Remote Exploit
| [11] Apache <= 2.0.44 Linux Remote Denial of Service Exploit
| [9] Apache HTTP Server 2.x Memory Leak Exploit
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [855524] Solaris Update for Apache 2 120544-14
| [855077] Solaris Update for Apache 2 120543-14
| [100858] Apache 'mod_proxy_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability
| [72626] Debian Security Advisory DSA 2579-1 (apache2)
| [71551] Gentoo Security Advisory GLSA 201206-25 (apache)
| [71550] Gentoo Security Advisory GLSA 201206-24 (apache tomcat)
| [71485] Debian Security Advisory DSA 2506-1 (libapache-mod-security)
| [71256] Debian Security Advisory DSA 2452-1 (apache2)
| [71238] Debian Security Advisory DSA 2436-1 (libapache2-mod-fcgid)
| [70724] Debian Security Advisory DSA 2405-1 (apache2)
| [70235] Debian Security Advisory DSA 2298-2 (apache2)
| [70233] Debian Security Advisory DSA 2298-1 (apache2)
| [69988] Debian Security Advisory DSA 2279-1 (libapache2-mod-authnz-external)
| [69338] Debian Security Advisory DSA 2202-1 (apache2)
| [65131] SLES9: Security update for Apache 2 oes/CORE
| [64426] Gentoo Security Advisory GLSA 200907-04 (apache)
| [61381] Gentoo Security Advisory GLSA 200807-06 (apache)
| [60582] Gentoo Security Advisory GLSA 200803-19 (apache)
| [58745] Gentoo Security Advisory GLSA 200711-06 (apache)
| [57851] Gentoo Security Advisory GLSA 200608-01 (apache)
| [56246] Gentoo Security Advisory GLSA 200602-03 (Apache)
| [55392] Gentoo Security Advisory GLSA 200509-12 (Apache)
| [55129] Gentoo Security Advisory GLSA 200508-15 (apache)
| [54739] Gentoo Security Advisory GLSA 200411-18 (apache)
| [54724] Gentoo Security Advisory GLSA 200411-03 (apache)
| [54712] Gentoo Security Advisory GLSA 200410-21 (apache)
| [54689] Gentoo Security Advisory GLSA 200409-33 (net=www/apache)
| [54677] Gentoo Security Advisory GLSA 200409-21 (apache)
| [54610] Gentoo Security Advisory GLSA 200407-03 (Apache)
| [54601] Gentoo Security Advisory GLSA 200406-16 (Apache)
| [54590] Gentoo Security Advisory GLSA 200406-05 (Apache)
| [54582] Gentoo Security Advisory GLSA 200405-22 (Apache)
| [54529] Gentoo Security Advisory GLSA 200403-04 (Apache)
| [54499] Gentoo Security Advisory GLSA 200310-04 (Apache)

| [54498] Gentoo Security Advisory GLSA 200310-03 (Apache)
| [11092] Apache 2.0.39 Win32 directory traversal
| [66081] SLES11: Security update for Apache 2
| [66074] SLES10: Security update for Apache 2
| [66070] SLES9: Security update for Apache 2
| [65893] SLES10: Security update for Apache 2
| [65888] SLES10: Security update for Apache 2
| [65510] SLES9: Security update for Apache 2
| [65249] SLES9: Security update for Apache 2
| [65230] SLES9: Security update for Apache 2
| [65228] SLES9: Security update for Apache 2
| [65207] SLES9: Security update for Apache 2
| [65136] SLES9: Security update for Apache 2
| [65017] SLES9: Security update for Apache 2
|
| SecurityTracker - https://www.securitytracker.com:
| [1008196] Apache 2.x on Windows May Return Unexpected Files For URLs Ending With Certain Charac
ters
| [1007143] Apache 2.0 Web Server May Use a Weaker Encryption Implementation Than Specified in So
me Cases
| [1006444] Apache 2.0 Web Server Line Feed Buffer Allocation Flaw Lets Remote Users Deny Service
| [1005963] Apache Web Server 2.x Windows Device Access Flaw Lets Remote Users Crash the Server
or Possibly Execute Arbitrary Code
| [1004770] Apache 2.x Web Server ap_log_rerror() Function May Disclose Full Installation Path to Remot
e Users
|
| OSVDB - http://www.osvdb.org:
| [20897] PHP w/ Apache 2 SAPI virtual() Function Unspecified INI Setting Disclosure
|_
| vulners:
| cpe:/a:apache:http_server:2.4.7:
| PACKETSTORM:171631 7.5 https://vulners.com/packetstorm/PACKETSTORM:171631 *EXPLOIT*
| EDB-ID:51193 7.5 https://vulners.com/exploitdb/EDB-ID:51193 *EXPLOIT*
| CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
| CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
| CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
| CVE-2021-44790 7.5 https://vulners.com/cve/CVE-2021-44790
| CVE-2021-39275 7.5 https://vulners.com/cve/CVE-2021-39275
| CVE-2021-26691 7.5 https://vulners.com/cve/CVE-2021-26691
| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679
| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167
| CNVD-2022-73123 7.5 https://vulners.com/cnvd/CNVD-2022-73123
| CNVD-2022-03225 7.5 https://vulners.com/cnvd/CNVD-2022-03225
| CNVD-2021-102386 7.5 https://vulners.com/cnvd/CNVD-2021-102386
| 1337DAY-ID-38427 7.5 https://vulners.com/zdt/1337DAY-ID-38427 *EXPLOIT*
| PACKETSTORM:127546 6.8 https://vulners.com/packetstorm/PACKETSTORM:127546 *EXPLOIT*
| FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 https://vulners.com/githubexploit/FDF3DFA1-ED
74-5EE2-BF5C-BA752CA34AE8 *EXPLOIT*
| CVE-2021-40438 6.8 https://vulners.com/cve/CVE-2021-40438
| CVE-2020-35452 6.8 https://vulners.com/cve/CVE-2020-35452
| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312
| CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715
| CVE-2016-5387 6.8 https://vulners.com/cve/CVE-2016-5387
| CVE-2014-0226 6.8 https://vulners.com/cve/CVE-2014-0226
| CNVD-2022-03224 6.8 https://vulners.com/cnvd/CNVD-2022-03224

| AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C 6.8 https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C *EXPLOIT*
| 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 *EXPLOIT*
| 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 *EXPLOIT*
| 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B *EXPLOIT*
| 36618CA8-9316-59CA-B748-82F15F407C4F 6.8 https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F *EXPLOIT*
| 1337DAY-ID-22451 6.8 https://vulners.com/zdt/1337DAY-ID-22451 *EXPLOIT*
| 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE *EXPLOIT*
| OSV:BIT-2023-31122 6.4 https://vulners.com/osv/OSV:BIT-2023-31122
| CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
| CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
| CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788
| CVE-2019-0217 6.0 https://vulners.com/cve/CVE-2019-0217
| CVE-2022-22721 5.8 https://vulners.com/cve/CVE-2022-22721
| CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927
| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098
| 1337DAY-ID-33577 5.8 https://vulners.com/zdt/1337DAY-ID-33577 *EXPLOIT*
| CVE-2022-36760 5.1 https://vulners.com/cve/CVE-2022-36760
| SSV:96537 5.0 https://vulners.com/seebug/SSV:96537 *EXPLOIT*
| SSV:62058 5.0 https://vulners.com/seebug/SSV:62058 *EXPLOIT*
| SSV:61874 5.0 https://vulners.com/seebug/SSV:61874 *EXPLOIT*
| OSV:BIT-2023-45802 5.0 https://vulners.com/osv/OSV:BIT-2023-45802
| OSV:BIT-2023-43622 5.0 https://vulners.com/osv/OSV:BIT-2023-43622
| F7F6E599-CEF4-5E03-8E10-FE18C4101E38 5.0 https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38 *EXPLOIT*
| EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 5.0 https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7 *EXPLOIT*
| EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D *EXPLOIT*
| EDB-ID:42745 5.0 https://vulners.com/exploitdb/EDB-ID:42745 *EXPLOIT*
| EDB-ID:40961 5.0 https://vulners.com/exploitdb/EDB-ID:40961 *EXPLOIT*
| E5C174E5-D6E8-56E0-8403-D287DE52EB3F 5.0 https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F *EXPLOIT*
| DB6E1BBD-08B1-574D-A351-7D6BB9898A4A 5.0 https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A *EXPLOIT*
| CVE-2022-37436 5.0 https://vulners.com/cve/CVE-2022-37436
| CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
| CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
| CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
| CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
| CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
| CVE-2021-34798 5.0 https://vulners.com/cve/CVE-2021-34798
| CVE-2021-26690 5.0 https://vulners.com/cve/CVE-2021-26690
| CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934
| CVE-2019-17567 5.0 https://vulners.com/cve/CVE-2019-17567
| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220
| CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199
| CVE-2018-1303 5.0 https://vulners.com/cve/CVE-2018-1303
| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798
| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710

| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743
| CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161
| CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736
| CVE-2015-3183 5.0 https://vulners.com/cve/CVE-2015-3183
| CVE-2015-0228 5.0 https://vulners.com/cve/CVE-2015-0228
| CVE-2014-3581 5.0 https://vulners.com/cve/CVE-2014-3581
| CVE-2014-0231 5.0 https://vulners.com/cve/CVE-2014-0231
| CVE-2014-0098 5.0 https://vulners.com/cve/CVE-2014-0098
| CVE-2013-6438 5.0 https://vulners.com/cve/CVE-2013-6438
| CVE-2013-5704 5.0 https://vulners.com/cve/CVE-2013-5704
| CVE-2006-20001 5.0 https://vulners.com/cve/CVE-2006-20001
| CNVD-2023-93320 5.0 https://vulners.com/cnvd/CNVD-2023-93320
| CNVD-2023-80558 5.0 https://vulners.com/cnvd/CNVD-2023-80558
| CNVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
| CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
| CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
| CNVD-2022-03223 5.0 https://vulners.com/cnvd/CNVD-2022-03223
| C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B 5.0 https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B *EXPLOIT*
| BD3652A9-D066-57BA-9943-4E34970463B9 5.0 https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9 *EXPLOIT*
| B0208442-6E17-5772-B12D-B5BE30FA5540 5.0 https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540 *EXPLOIT*
| A820A056-9F91-5059-B0BC-8D92C7A31A52 5.0 https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52 *EXPLOIT*
| 9814661A-35A4-5DB7-BB25-A1040F365C81 5.0 https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81 *EXPLOIT*
| 5A864BCC-B490-5532-83AB-2E4109BB3C31 5.0 https://vulners.com/githubexploit/5A864BCC-B490-5532-83AB-2E4109BB3C31 *EXPLOIT*
| 17C6AD2A-8469-56C8-BBBE-1764D0DF1680 5.0 https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680 *EXPLOIT*
| 1337DAY-ID-28573 5.0 https://vulners.com/zdt/1337DAY-ID-28573 *EXPLOIT*
| 1337DAY-ID-26574 5.0 https://vulners.com/zdt/1337DAY-ID-26574 *EXPLOIT*
| SSV:87152 4.3 https://vulners.com/seebug/SSV:87152 *EXPLOIT*
| PACKETSTORM:127563 4.3 https://vulners.com/packetstorm/PACKETSTORM:127563 *EXPLOIT*
| CVE-2020-11985 4.3 https://vulners.com/cve/CVE-2020-11985
| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092
| CVE-2018-1302 4.3 https://vulners.com/cve/CVE-2018-1302
| CVE-2018-1301 4.3 https://vulners.com/cve/CVE-2018-1301
| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975
| CVE-2015-3185 4.3 https://vulners.com/cve/CVE-2015-3185
| CVE-2014-8109 4.3 https://vulners.com/cve/CVE-2014-8109
| CVE-2014-0118 4.3 https://vulners.com/cve/CVE-2014-0118
| CVE-2014-0117 4.3 https://vulners.com/cve/CVE-2014-0117
| 4013EC74-B3C1-5D95-938A-54197A58586D 4.3 https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D *EXPLOIT*
| 1337DAY-ID-33575 4.3 https://vulners.com/zdt/1337DAY-ID-33575 *EXPLOIT*
| CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283
| CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612
|_ PACKETSTORM:140265 0.0 https://vulners.com/packetstorm/PACKETSTORM:140265 *EXPLOIT*
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.15
| Found the following possible CSRF vulnerabilities:
|
| Path: http://10.0.2.15:80/chat/

| Form id: name
| Form action: index.php
|
| Path: http://10.0.2.15:80/drupal/
| Form id: user-login-form
| Form action: /drupal/?q=node&destination=node
|
| Path: http://10.0.2.15:80/payroll_app.php
| Form id:
| Form action:
|
| Path: http://10.0.2.15:80/chat/index.php
| Form id: name
|_   Form action: index.php
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
| Possible sqli for queries:
| http://10.0.2.15:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=S%3BO%3DD%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=M%3BO%3DD%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=D%3BO%3DD%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://10.0.2.15:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|_   http://10.0.2.15:80/?C=N%3BO%3DA%27%20OR%20sqlspider
| http-enum:
| /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
| /phpmyadmin/: phpMyAdmin
|_ /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-dombased-xss: Couldn't find any DOM based XSS.
445/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| temp: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2013-4124] Integer overflow in the read_nttrans_ea_list function in nttrans.c in smbd in Samba 3.x before 3.5.22, 3.6.x before 3.6.17, and 4.x before 4.0.8 allows remote attackers to cause a denial of service (memory consumption) via a malformed packet.
| [CVE-2011-0719] Samba 3.x before 3.3.15, 3.4.x before 3.4.12, and 3.5.x before 3.5.7 does not perform range checks for file descriptors before use of the FD_SET macro, which allows remote attackers to cause a denial of service (stack memory corruption, and infinite loop or daemon crash) by opening a large number of files, related to (1) Winbind or (2) smbd.

| [CVE-2013-0214] Cross-site request forgery (CSRF) vulnerability in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x before 3.6.12, and 4.x before 4.0.2 allows remote attackers to hijack the authentication of arbitrary users by leveraging knowledge of a password and composing reques ts that perform SWAT actions.
| [CVE-2013-0213] The Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x before 3.6.12, and 4.x before 4.0.2 allows remote attackers to conduct clickjacking attacks via a (1) FRAME or (2) IFRAME element.
| [CVE-2012-1182] The RPC code generator in Samba 3.x before 3.4.16, 3.5.x before 3.5.14, and 3.6.x b efore 3.6.4 does not implement validation of an array length in a manner consistent with validation of arra y memory allocation, which allows remote attackers to execute arbitrary code via a crafted RPC call.
| [CVE-2011-2694] Cross-site scripting (XSS) vulnerability in the chg_passwd function in web/swat.c in th e Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.10 allows remote authenticated admi nistrators to inject arbitrary web script or HTML via the username parameter to the passwd program (aka t he user field to the Change Password page).
| [CVE-2011-2522] Multiple cross-site request forgery (CSRF) vulnerabilities in the Samba Web Administr ation Tool (SWAT) in Samba 3.x before 3.5.10 allow remote attackers to hijack the authentication of admi nistrators for requests that (1) shut down daemons, (2) start daemons, (3) add shares, (4) remove shares, (5) add printers, (6) remove printers, (7) add user accounts, or (8) remove user accounts, as demonstrate d by certain start, stop, and restart parameters to the status program.
| [CVE-2004-0186] smbmnt in Samba 2.x and 3.x on Linux 2.6, when installed setuid, allows local users to gain root privileges by mounting a Samba share that contains a setuid root program, whose setuid attribu tes are not cleared when the share is mounted.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [36250] Samba 3.x Multiple Unspecified Remote Vulnerabilities
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [46975] Samba smbd information disclosure
| [37092] RHSA update for Samba smbd share connection request denial of service not installed
| [32301] Samba smbd file rename denial of service
| [27648] Samba smbd share connection request denial of service
| [17325] Samba ASN.1 smbd denial of service
| [86185] Samba read_nttrans_ea_list denial of service
| [82955] Samba Active Directory Domain Controller unauthorized access
| [81694] Samba SWAT clickjacking
| [81693] Samba Samba Web Administration Tool cross-site request forgery
| [81326] Samba objectClass based LDAP security bypass
| [78811] Samba unspecified code execution
| [75277] Samba LSA security bypass
| [74721] Samba RPC code execution
| [74438] Samba mount.cifs information disclosure
| [73361] BlackBerry PlayBook Samba code execution
| [72775] Samba connection request denial of service
| [70317] Samba mtab denial of service
| [69662] Samba check_mtab denial of service
| [68844] Samba user cross-site scripting
| [68843] Samba SWAT cross-site request forgery
| [66702] Samba smbfs security bypass
| [65724] Samba FD_SET denial of service
| [61773] Samba sid_parse() buffer overflow
| [59481] Samba SMB1 packet code execution
| [58565] Samba Negotiate Protocol Request denial of service
| [58564] Samba Session Setup AndX denial of service
| [58393] Samba mount.cifs symlink
| [56758] Samba CAP_DAC_OVERRIDE flag security bypass

| [56123] Samba mount.cifs.c denial of service
| [56111] Samba symlink directory traversal
| [55944] samba-client mount.cifs utility symlink
| [53575] Samba SMB denial of service
| [53574] Samba mount.cifs information disclosure
| [51328] Samba smbclient format string
| [51327] Samba ACL security bypass
| [50439] Samba winbind daemon denial of service
| [47733] Samba file system security bypass
| [45251] Xerox ESS/Network Controller Samba code execution
| [44678] Samba group_mapping.tdb security bypass
| [42664] Samba receive_smb_raw() buffer overflow
| [38965] Samba send_mailslot function buffer overflow
| [38502] Samba reply_netbios_packet() buffer overflow
| [38501] Samba nmbd buffer overflow
| [38123] GoSamba include_path file include
| [36893] SmbFTPD SMBDirList format string
| [36560] Samba smb.conf privilege escalation
| [35738] Apple Mac OS X Samba file system security bypass
| [35401] GSAMBAD populate_conns function symlink
| [34506] Samba version detected
| [34316] Samba lsa_io_trans_names buffer overflow
| [34315] Samba SID name translation privilege escalation
| [34314] Samba sec_io_acl buffer overflow
| [34312] Samba smb_io_notify_option_type_data buffer overflow
| [34311] Samba netdfs_io_dfs_EnumInfo_d buffer overflow
| [34309] Samba lsa_io_privilege_set buffer overflow
| [34307] Samba smb.conf shell command execution
| [32979] Apple Mac OS X Samba module (SMB File Server) buffer overflow
| [32304] Samba afsacl.so VFS plugin format string
| [32231] Samba nss_winbind.so.1 library gethostbyname and getipnodebyname buffer overflow
| [32151] Samba multiple unspecified buffer overflows
| [30920] Sambar FTP Server SIZE denial of service
| [29169] HP-UX CIFS Samba privilege escalation
| [25575] Samba clear text machine trust account credentials
| [22943] Sambar Server proxy.asp allows cross-site scripting
| [20710] Sambar Server search/results.stm and session/logout scripts cross-site scripting
| [18519] Samba MS-RPC request heap corruption
| [18070] Samba QFILEPATHINFO buffer overflow
| [17987] Samba ms_fnmatch denial of service
| [17556] Samba allows file access outside of the share‘s defined path
| [17454] Samba samba-vscan denial of service
| [17326] Samba nmbd mailslot denial of service
| [17139] Samba memory leak information disclosure
| [17138] Samba FindNextPrintChangeNotify request denial of service
| [16786] Samba mangling method buffer overflow
| [16785] Samba SWAT invalid base64 character causes buffer overflow
| [16287] Sambar showlog.asp and showini.asp scripts directory traversal
| [16286] Sambar show.asp and showperf.asp scripts cross-site scripting
| [16059] Sambar Server HTTP POST code execution
| [16056] Sambar Server multiple script cross-site scripting
| [16054] Sambar Server HTTP keep-alive allows unauthorized access
| [15545] Samba smbprint.log symlink attack
| [15132] Samba mksmbpasswd.sh could allow an attacker to gain access to user‘s account
| [15131] Samba smbmnt allows elevated privileges

| [15071] Sambar Server HTTP POST request buffer overflow
| [13305] Sambar Server multiple vulnerabilities
| [12749] Samba reply_nttrans function buffer overflow
| [12402] Sambar Server search.pl denial of service
| [11845] Sambar Server Pro Server WebMail interface transmits password and username in plain text
| [11726] Samba and Samba-TNG call_trans2open() function buffer overflow
| [11634] Sambar Server remote file cross-site scripting
| [11633] Sambar Server dot dot directory traversal
| [11631] Sambar Server multiple scripts cross-site scripting
| [11630] Sambar Server textcgi.exe and environ.pl path disclosure
| [11616] Samba-TNG security context management code could allow root access
| [11551] Samba .reg file code race condition
| [11550] Samba SMB/CIFS packet fragment re-assembly code buffer overflow
| [11128] Sambar Server search request cross-site scripting
| [10683] Samba encrypted password change request buffer overflow
| [10010] Samba enum_csc_policy memory structure buffer overflow
| [8876] Sambar Server Perl script source disclosure
| [8710] Sambar Server Pbcgi.exe denial of service
| [8709] Sambar Server testcgi.exe denial of service
| [8707] Sambar Server long HTTP header field denial of service
| [8705] Sambar Server MSVCRT.dll long username and password buffer overflow
| [7894] Sambar Server cgitest.exe example script denial of service
| [6973] Sambar Server Telnet proxy long password buffer overflow
| [6972] Sambar Server Telnet proxy continuous connections denial of service
| [6916] Sambar Server &quot
| [6909] Sambar Server insecure password protection
| [6731] samba NetBIOS name allows remote attackers to create symlink to SMB log file
| [6396] Samba tmpfile symlink attack could allow elevated privileges
| [5445] Samba swat logfile information retrieval
| [5444] Samba swat URL filename denial of service
| [5443] Samba swat logging symbolic link
| [5442] Samba swat brute force attack
| [5247] Sambar search.dll allows attacker to view folders on the system
| [4592] Sambar Server 4.3 buffer overflow
| [3999] Sambar Server hello.bat and echo.bat CGI scripts
| [3227] Samba smbmnt utility could allow mounting to arbitrary mount points
| [3225] Samba message service potential buffer overflow
| [3224] Samba nmbd daemon can be remotely crashed or caused to enter an infinite loop
| [3223] Sambar server allows remote viewing of environment information
| [1672] Sambar Server logging code buffer overflow
| [1671] Sambar mailit client allows script execution
| [1669] Sambar Server ships with default accounts
| [1406] Samba wsmbconf binary allows users access to the group root
| [1311] Samba open share
| [1237] Samba .. Bug
| [337] Samba SMB password buffer overflow
| [9] Samba .. bug
|
| Exploit-DB - https://www.exploit-db.com:
| [20223] Sambar Server 4.3/4.4 beta 3 Search CGI Vulnerability
| [10095] Samba 3.0.10 - 3.3.5 Format String And Security Bypass Vulnerabilities
| [9950] Samba 3.0.21-3.0.24 LSA trans names Heap Overflow
| [7701] Samba < 3.0.20 - Remote Heap Overflow Exploit
| [4732] Samba 3.0.27a send_mailslot() Remote Buffer Overflow PoC
| [364] Samba <= 3.0.4 SWAT Authorization Buffer Overflow Exploit

|
| OpenVAS (Nessus) - http://www.openvas.org:
| [90028] Samba 3.0.0 > 3.0.29 vulnerability
|
| SecurityTracker - https://www.securitytracker.com:
| [1028882] Samba smbd CPU Processing Loop Lets Remote Users Deny Service
| [1026595] Samba smbd Memory Leak Lets Remote Users Deny Service
| [1022976] Samba smbd Processing Flaw Lets Remote Authenticated Users Deny Service
| [1022442] Samba smbd Access Control Bug Lets Remote Authenticated Users Bypass Certain Access Controls
| [1017587] Samba smbd Deferred File Open Processing Bug Lets Remote Users Deny Service
| [1016459] Samba smbd Memory Limit Error in make_connection() Lets Remote Users Deny Service
| [1012587] Samba smbd Integer Overflow in Allocating Security Descriptors May Let Remote Users Execute Arbitrary Code
| [1011223] Samba smbd Infinite Loop Lets Remote Users Consume All Available Memory
| [1011097] Samba FindNextPrintChangeNotify() Error Lets Remote Authenticated Users Crash smbd
| [1006290] Samba 'smbd' Buffer Overflow May Let Remote Users Gain Root Access
| [1028389] Samba Bug Lets Remote Authenticated Users Modify Files
| [1028365] IBM Storwize V7000 Unified Samba Bug Lets Remote Authenticated Users Modify Files
| [1028312] Samba Active Directory Domain Controller File Permission Flaw Lets Remote Authenticated Users Access Files
| [1028006] Samba Active Directory Domain Controller Access Control Flaw Lets Remote Authenticated Gain Write Access to Certain Objects
| [1026988] Samba Local Security Authority Bug Lets Remote Authenticated Users Gain Elevated Privileges
| [1026913] Samba Buffer Overflow in NDR Marshalling Code Lets Remote Users Execute Arbitrary Code
| [1026739] Samba Bug in chain_reply()/construct_reply() Lets Remote Users Execute Arbitrary Code
| [1026727] Blackberry PlayBook Samba File Sharing Lets Remote Users Execute Arbitrary Code
| [1025984] Samba 'mount.cifs' check_newline() Error Lets Local Users Deny Service
| [1025852] Samba Web Administration Tool (SWAT) Input Validation Flaws Permit Cross-Site Request Forgery and Cross-Site Scripting Attacks
| [1025132] Samba FD_SET Stack Corruption Flaw Lets Remote and Local Users Deny Service
| [1024434] Samba Buffer Overflow in sid_parse() Lets Remote Users Execute Arbitrary Code
| [1024107] Samba SMB1 Packet Chaining Memory Corruption Error Lets Remote Users Execute Arbitrary Code
| [1023700] Samba Access Control Flaw Lets Remote Authenticated Users Gain Elevated Privileges
| [1023547] Samba 'mount.cifs' Race Condition Lets Local Users Gain Elevated Privileges
| [1023546] Samba Symlink Configuration Error Lets Remote Users Access Arbitrary Files
| [1022975] Samba 'mount.cifs' Lets Local Users View Portions of Files on the Target System
| [1022441] Samba smbclient Format String Bug May Let Users Execute Arbitrary Code
| [1021513] Samba Grants Remote Authenticated Users Access to the Root Filesystem in Certain Cases
| [1021287] Samba 'trans', 'trans2', and 'nttrans' Requests Let Remote Users Obtain Memory Contents
| [1020770] Samba 'group_mapping.ldb' Has Unsafe Permissions That Let Local Users Gain Elevated Privileges
| [1020123] Samba Buffer Overflow in receive_smb_raw() Lets Remote Users Execute Arbitrary Code
| [1019065] Samba Buffer Overflow in nmbd send_mailslot() Lets Remote Users Execute Arbitrary Code
| [1018954] Samba nmbd Buffer Overflow in Processing GETDC mailslot Requests Lets Remote Users Execute Arbitrary Code
| [1018953] Samba nmbd Buffer Overflow in reply_netbios_packet() Lets Remote Users Execute Arbitrary Code
| [1018681] Samba Winbind SFU/RFC2307 GID Error Lets Local Users Gain Elevated Privileges
| [1018051] Samba 'smb.conf' Scripts Input Validation Flaw Lets Remote Users Inject Arbitrary Commands
| [1018050] Samba Heap Overflows in Parsing NDR Data Let Remote Users Execute Arbitrary Code
| [1018049] Samba SID/Name Translation Bug Lets Local Users Gain Root Privileges

| [1017589] Samba Solaris winbindd Daemon Name Resolution Query Buffer Overflows May Let Remtoe Users Execute Arbitrary Code
| [1017588] Samba Format String Bug in 'afsacl.so' VFS Plugin May Let Remote Users Execute Arbitrary Code
| [1017393] Sambar Server FTP SIZE Command Lets Remote Authenticated Users Deny Service
| [1015850] Samba winbindd Daemon Discloses Server Password to Local Users
| [1012235] Samba QFILEPATHINFO Buffer Overflow Lets Remote Authenticated Users Execute Arbitrary Code
| [1012133] Samba Input Validation Error in ms_fnmatch() Lets Remote Authenticated Users Deny Service
| [1011949] Samba pppd Callback Control Protocol Pointer Dereference May Let Remote Users Deny Service
| [1011469] Samba DOS Path Conversion Flaw Discloses Files to Remote Users
| [1011222] Samba Input Validation Error in nmbd process_logon_packet() Lets Remote Users Crash the nmbd Service
| [1010753] Samba Buffer Overflows in Web Administration Tool and in 'hash' Mangling Method May Let Remote Users Execute Arbitrary Code
| [1010353] Sambar Server 'showini.asp' and 'showlog.asp' Disclose Files to Remote Authenticated Administrators
| [1009503] Samba 'smbprint' Unsafe Temporary File May Let Local Users Gain Elevated Privileges
| [1009000] Samba 'smbmnt' Permissions May Let Local Users Gain Root Privileges
| [1008990] Samba May Let Remote Users Access SMB Accounts That Have Invalid Passwords
| [1008979] Sambar Server 'results.stm' POST Request Buffer Overflow May Permit Remote Code Execution
| [1007819] Sambar Server Contains Multiple Unspecified Vulnerabilities
| [1007016] Sambar Server Buffer Overflow in 'search.pl' Lets Remote Users Crash the Service
| [1006934] Sambar Server Discloses Files on the System to Remote Users
| [1006637] Sambar Server WebMail Discloses User Passwords Transmitted Via the Network
| [1006498] Samba-TNG Buffer Overflow in call_trans2open() Function Lets Remote Users Execute Arbitrary Code With Root Privileges
| [1006497] Samba Buffer Overflow in call_trans2open() Function Lets Remote Users Execute Arbitrary Code With Root Privileges
| [1006390] Sambar Server Input Validation Flaws Disclose Files on the System to Remote Users and Permit Cross-Site Scripting Attacks
| [1005946] Sambar Server Input Validation Hole in Query Feature Lets Remote Users Conduct Cross-Site Scripting Attacks
| [1005677] Samba Buffer Overflow in User Input Routine May Let Remote Users Execute Arbitrary Code with Root Privileges
| [1004624] HP-UX Samba Common Internet File System (CIFS) Client Buffer Overflow May Let Local Users Obtain Elevated Privileges on the System
| [1004084] Sambar Server Discloses Script Source Code to Remote Users and Can Be Crashed By Remote Users via Malformed URLs
| [1003941] Sambar Server Buffer Overflow Holes Let Remote Users Crash the Service or Execute Arbitrary Code on the System
| [1003246] Sambar Web Server Sample CGI Allows Remote Users to Crash the Web Server
| [1002302] HP CIFS/9000 (Samba) Server Lets Authenticated Remote Users Change Another User's Password
| [1002187] Sambar Telnet Proxy/Server Password Buffer Overflow May Allow Remote Users to Execute Arbitrary Code on the Server
| [1002082] Sambar Web Server Lets Remote Users Modify Files on the Server
| [1002079] Sambar Server Password File Can Be Decrypted By Local Users
| [1002038] Sambar Server's Web Server Lets Local Users Disclose Files Outside of the Documents Directory
| [1002037] Sambar Server's SMTP Mail Server May Allow Remote Users to Relay Mail Through the Server

| [1001826] Samba Common Internet File System (CIFS) Lets Remote Users Obtain Root Level Access
| [1001339] Samba SMB Networking Software Allows Local Users to Destroy Data on Local Devices
|
| OSVDB - http://www.osvdb.org:
| [95969] Samba smbd nttrans.c read_nttrans_ea_list Function Malformed Packet Handling Remote DoS
| [78651] Samba smbd Connection Request Parsing Remote DoS
| [65518] Samba smbd process.c chain_reply Function SMB1 Packet Chaining Memory Corruption
| [65436] Samba smbd sesssetup.c Session Setup AndX Security Blob Length Value Uninitialized Variabl
e Out-of-bounds DoS
| [65435] Samba smbd process.c chain_reply Function Session Setup AndX Request NULL Dereference
Remote DoS
| [58519] Samba smbd Crafted SMB Request Remote CPU Consumption DoS
| [57651] Samba smbd Unspecified Heap Overflow
| [55411] Samba smbd/posix_acls.c acl_group_override Function Remote Access Control List Modificatio
n
| [50230] Samba smbd *trans* Request Arbitrary Remote Memory Disclosure
| [33100] Samba smbd Deferred Open Code Infinite Loop DoS
| [12422] Samba smbd Security Descriptor Parsing Remote Overflow
| [9362] Samba smbd FindNextPrintChangeNotify() Request Remote DoS
| [6323] Samba smbd SMB/CIFS Packet Fragment Reassembly Remote Overflow
| [93189] HP MPE/iX with Samba/iX Unspecified Remote Issue
| [92247] Red Hat Storage Management Console GlusterFS extras/hook-scripts/S30samba-stop.sh Symli
nk Arbitrary File Overwrite
| [91889] Samba SMB2 Implementation CIFS Share Attribute Enforcement Weakness
| [91503] Samba Active Directory Domain Controller CIFS Shares World-writeable Files Creation Weakne
ss
| [91255] ASUS RT-N66U Router root$ Samba Share Export Remote Information Disclosure
| [89627] Samba Web Administration Tool (SWAT) Manipulation CSRF
| [89626] Samba Web Administration Tool (SWAT) Clickjacking Weakness
| [89180] Samba AD DC LDAP Directory Objects Erroneous Write Access Permissions
| [83446] Samba smbmount Multiple Variable Username Handling Local Overflow
| [81648] Samba Multiple Remote Procedural Calls (RPC) Local Security Authority (LSA) Arbitrary File Ma
nipulation
| [81490] Samba mount.cifs chdir() Call File Enumeration
| [81303] Samba RPC Code Generator Network Data Representation (NDR) Multiple Request Parsing Re
mote Overflow
| [79443] Samba process.c Any Batched (AndX) Request Packet Parsing Remote Overflow
| [79041] Webmin Samba Windows File Sharing Module /tmp/.webmin Local Password Disclosure
| [76058] Samba mtab Lock File Handling Local DoS
| [74872] Samba smbfs mount.cifs / umount.cifs RLIMIT_FSIZE Value Handling mtab Local Corruption Do
S
| [74871] Samba mount.cifs Tool Share / Directory Name Newline Injection mtab Corruption Local DoS
| [74072] Samba Web Administration Tool (SWAT) Change Password Page user Field XSS
| [74071] Samba Web Administration Tool (SWAT) Multiple Function CSRF
| [71268] Samba FD_SET Macro Memory Corruption
| [69288] VLC Media Player Samba Network Share Module Incorrect Calling Convention Stack Corruption
| [67994] Samba sid_parse() Function SID Parsing Remote Overflow
| [62803] Samba CAP_DAC_OVERRIDE Capability Flag File Permission Restriction Bypass
| [62187] Samba sid_parse Stack Overflow
| [62186] Samba mount.cifs Symlink Arbitrary File Access
| [62155] Samba smbfs mount.cifs client/mount.cifs.c Crafted String mtab Corruption Local DoS
| [62145] Samba Guest Account Symlink Traversal Arbitrary File Access
| [60587] Windows File Sharing Samba Client Resource Exhaustion DoS
| [59810] Samba reply_nttrans Function Remote Overflow
| [59511] HP-UX CIFS/9000 Server (SAMBA) Unspecified Resource Modification Arbitrary File Overwrite

| [59350] Samba Web Administration Tool (SWAT) Malformed HTTP Request Saturation Remote DoS
| [58520] Samba SUID mount.cifs --verbose Argument Arbitrary File Portion Disclosure
| [57955] Samba Unconfigured Home Directory Windows File Share Directory Access Restriction Bypass
| [57653] Samba Unspecified Heap Overflow
| [57652] Samba --enable-developer Functionality Unspecified Heap Overflow
| [57172] Samba-TNG Unspecified Remote Privilege Escalation
| [55412] Samba smbclient client/client.c Filename Specifiers Multiple Format Strings
| [55370] Sambar Server Pbcgi.exe Remote Overflow
| [55369] Sambar Server testcgi.exe Remote Overflow
| [54378] Samba winbind Daemon Unresponsive Child Process Race Condition DoS
| [53074] Sambar Server /session/sendmail Arbitrary Mail Relay
| [51152] Samba Crafted Connection Request Remote Root File System Access
| [48699] CUPS cupsaddsmb Temporary File Cleartext Samba Credential Disclosure
| [47786] Samba group_mapping.tdb Permission Weakness Privilege Escalation
| [45657] Samba lib/util_sock.c receive_smb_raw() Function Crafted Packet Handling Overflow
| [42884] Sambar Server with IndigoPerl /cgi-bin/com1.pl Arbitrary Command Execution
| [42305] Samba Unspecified Remote Issue
| [42251] Sambar Server Unspecified Remote Command Execution
| [41385] SmbFTPD SMBDirList() Function Directory Name Remote Format String
| [40714] GoSamba main.php include_path Parameter Remote File Inclusion
| [40713] GoSamba inc_user.php include_path Parameter Remote File Inclusion
| [40712] GoSamba inc_smb_conf.php include_path Parameter Remote File Inclusion
| [40711] GoSamba inc_newgroup.php include_path Parameter Remote File Inclusion
| [40710] GoSamba inc_manager.php include_path Parameter Remote File Inclusion
| [40709] GoSamba inc_group.php include_path Parameter Remote File Inclusion
| [40708] GoSamba inc_freigabe3.php include_path Parameter Remote File Inclusion
| [40707] GoSamba inc_freigabe1.php include_path Parameter Remote File Inclusion
| [40706] GoSamba inc_freigabe.php include_path Parameter Remote File Inclusion
| [40705] GoSamba HTML_oben.php include_path Parameter Remote File Inclusion
| [39191] Samba nmdb send_mailslot() Function GETDC mailslot Request Remote Overflow
| [39180] Samba nmbd Crafted GETDC mailslot Request Remote Overflow
| [39179] Samba nmbd nmbd/nmbd_packets.c reply_netbios_packet Function Remote Overflow
| [39178] Samba idmap_ad.so Winbind nss_info Extension (nsswitch/idmap_ad.c) Local Privilege Escalati
on
| [37795] GSAMBAD /tmp/gsambadtmp Symlink Arbitrary File Overwrite
| [36971] Apple Mac OS X Samba Server Disk Quota Bypass
| [34852] Apple Mac OS X Apple-specific Samba Module (SMB File Server) ACL Handling Overflow
| [34733] Samba DFS RPC Interface DFSEnum Request Remote Overflow
| [34732] Samba SPOOLSS RPC Interface RFNPCNEX Request Remote Overflow
| [34731] Samba SRVSVC RPC Interface NetSetFileSecurity Request Remote Overflow
| [34700] Samba Unfiltered MS-RPC Calls Arbitrary Remote Command Execution
| [34699] Samba LSA RPC Interface Multiple Function Remote Overflow
| [34698] Samba SID/Name Translation Privileged SMB/CIFS Protocol Operation Execution
| [33101] Samba VFS Plugin afsacl.so Format String
| [33098] Samba nss_winbind.so.1 Multiple Function Overflow
| [32336] Sambar FTP Server Malformed SIZE Command DoS
| [27130] Samba smdb Share Connection Saturation DoS
| [24263] Samba winbindd Debug Log Server Credentials Local Disclosure
| [23282] Samba Unspecified Remote Memory Leak Information Disclosure
| [20434] Sambar Server proxy.asp Multiple Field XSS
| [16751] Sambar Server Referer XSS
| [16750] Sambar Server logout RCredirect XSS
| [16749] Sambar Server results.stm indexname XSS
| [14525] Samba Encrypted Password String Conversion Decryption Overflow DoS
| [14233] Sambar Telnet Proxy/Server Long Password Overflow

| [13872] Samba smbclient mput Symlink Arbitrary File Overwrite
| [13871] Samba smbclient more Symlink Arbitrary File Overwrite
| [13870] Samba Printer Queue Query Symlink Arbitrary File Overwrite
| [13397] Samba Multiple Unspecified Overflows
| [12642] Samba .reg File Race Condition Arbitrary File Overwrite
| [11794] Sambar Server whois Script Hostname Remote Overflow
| [11793] Sambar Server finger Script Hostname Remote Overflow
| [11782] Samba QFILEPATHINFO Unicode Filename Request Handler Overflow
| [11555] Samba ms_fnmatch() Function Wildcard Matching Remote DoS
| [11521] Samba Password Field Handling Remote Overflow
| [11479] Microsoft Windows NT Double Dot Samba Client DoS
| [10886] Sambar Web Server Long HTTP GET Request Overflow
| [10464] Samba MS-DOS Path Request Arbitrary File Retrieval
| [9917] Samba nmbd process_logon_packet Function Remote DoS
| [9916] Samba ASN.1 Parsing Function Malformed Request DoS
| [8860] Samba NETBIOS Name Service Daemon DoS
| [8859] Samba smbmnt Race Condition Arbitrary Mount Point
| [8191] Samba Mangling Method Hash Overflow
| [8190] Samba Web Administration Tool (SWAT) HTTP Basic Auth base64 Decoding Remote Overflow
| [7529] Samba wsmbconf Command Execution and Privilege Escalation
| [6585] Sambar Server showini.asp Arbitrary File Access
| [6584] Sambar Server showperf.asp title Parameter XSS
| [6583] Sambar Server show.asp show Parameter XSS
| [5820] Sambar Server vchist.stm Multiple Parameter XSS
| [5819] Sambar Server vccreate.stm Multiple Parameter XSS
| [5818] Sambar Server vccheckin.stm Multiple Parameter XSS
| [5817] Sambar Server update.stm Multiple Parameter XSS
| [5816] Sambar Server template.stm path Parameter XSS
| [5815] Sambar Server sendmail.stm Multiple Parameter XSS
| [5814] Sambar Server rename.stm Multiple Parameter XSS
| [5813] Sambar Server mkdir.stm path Parameter XSS
| [5812] Sambar Server htaccess.stm path Parameter XSS
| [5811] Sambar Server ftp.stm path Parameter XSS
| [5810] Sambar Server info.stm Multiple Parameter XSS
| [5809] Sambar Server create.stm path Parameter XSS
| [5808] Sambar Server iecreate.stm path Parameter XSS
| [5807] Sambar Server edit.stm Multiple Parameter XSS
| [5806] Sambar Server ieedit.stm Multiple Parameter XSS
| [5805] Sambar Server search.dll query Parameter XSS
| [5804] Sambar Server environ.pl param1 Parameter XSS
| [5803] Sambar Server testisa.dll check1 Parameter XSS
| [5802] Sambar Server echo.bat Code Execution
| [5786] Sambar Server results.stm Overflow
| [5785] Sambar Server book.pl E-mail Field XSS
| [5784] Sambar Server dumpenv.pl XSS
| [5783] Sambar Server ssienv.shtml XSS
| [5782] Sambar Server mortgage.pl price Parameter XSS
| [5781] Sambar Server DOS Device Name Code Execution
| [5780] Sambar Server Proxy IP Filter Bypass
| [5468] Sambar Server Password Encryption Scheme Weakness
| [5123] Sambar DOS Device Name DoS
| [5122] Sambar Server Null Terminated URL Arbitrary File Source Disclosure
| [5108] Sambar Server search.stm Multiple Parameter XSS
| [5107] Sambar Server findata.stm Multiple Parameter XSS
| [5106] Sambar Server whodata.stm sitename Parameter XSS

| [5105] Sambar Server showfnc.stm pkg Parameter XSS
| [5104] Sambar Server showfncs.stm pkg Parameter XSS
| [5103] Sambar Server showfunc.stm func Parameter XSS
| [5102] Sambar Server stmex.stm XSS
| [5101] Sambar Server ipdata.stm ipaddr Parameter XSS
| [5100] Sambar Server testcgi.exe XSS
| [5097] Sambar Server index.stm wwwsite Parameter XSS
| [5096] Sambar Server iecreate.stm Directory Listing
| [5095] Sambar Server ieedit.stm Directory Listing
| [5094] Sambar Server testcgi.exe Environment Variable Disclosure
| [5093] Sambar Server environ.pl Environment Variable Disclosure
| [4469] Samba trans2.c call_trans2open() Function Overflow
| [3919] Samba mksmbpasswd.sh Uninitialized Passwords
| [3916] Samba smbmnt Local Privilege Escalation
| [2204] Sambar Server search.pl results.stm Overflow DoS
| [1626] Samba Web Administration Tool (SWAT) cgi.log Permission Weakness Information Disclosure
| [1625] Samba Web Administration Tool (SWAT) Failed Login Logging Failure Weakness
| [1025] Samba smdb Malformed Message Handling Remote Overflow
| [861] Samba enum_csc_policy Data Structure Termination Remote Overflow
| [656] Samba NETBIOS Name Traversal Arbitrary Remote File Creation
| [589] Sambar Web Server pagecount CGI Traversal Arbitrary File Overwrite
| [487] Samba Web Administration Tool (SWAT) Error Message Username Enumeration
| [413] Sambar Server ISAPI Search Utility search.dll Query Parameter Parsing Folder Name Disclosure
| [319] Sambar Server mailit.pl Arbitrary Mail Relay
| [318] Sambar Server Sysadmin Web Interface Default Account
| [317] Sambar sendmail CGI Arbitrary Mail Relay
| [215] Samba Web Administration Tool (SWAT) cgi.log Symlink Arbitrary File Modification
| [194] Sambar Server hello.bat Code Execution
| [52] Sambar Server dumpenv.pl Information Disclosure
| [34] Sambar Server cgitest.exe Crafted GET Request Parsing Remote Overflow
|_
631/tcp open   ipp   CUPS 1.7
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server’s resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| temp: VulDB - https://vuldb.com:
| [102573] Adam Kropelin adk0212 APC UPS Daemon up to 3.14.14 apcupsd.exe access control
| [20177] APC apcupsd 3.8.5 vsprintf memory corruption
| [20070] pdftops xpdf/xpdf-i/CUPS integer coercion
| [16450] APC apcupsd 3.7.2 Process ID File apcupsd.pid path traversal
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2013-1982] Multiple integer overflows in X.org libXext 1.3.1 and earlier allow X servers to trigger al

location of insufficient memory and a buffer overflow via vectors related to the (1) XcupGetReservedColor mapEntries, (2) XcupStoreColors, (3) XdbeGetVisualInfo, (4) XeviGetVisualInfo, (5) XShapeGetRectangle s, and (6) XSyncListSystemCounters functions.
| [CVE-2012-5519] CUPS 1.4.4, when running in certain Linux distributions such as Debian GNU/Linux, st ores the web interface administrator key in /var/run/cups/certs/0 using certain permissions, which allows l ocal users in the lpadmin group to read or write arbitrary files as root by leveraging the web interface.
| [CVE-2011-4405] The cupshelpers scripts in system-config-printer in Ubuntu 11.04 and 11.10, as used b y the automatic printer driver download service, uses an "insecure connection" for queries to the OpenPri nting database, which allows remote attackers to execute arbitrary code via a man-in-the-middle (MITM) a ttack that modifies packages or repositories.
| [CVE-2011-3170] The gif_read_lzw function in filter/image-gif.c in CUPS 1.4.8 and earlier does not prop erly handle the first code word in an LZW stream, which allows remote attackers to trigger a heap-based buffer overflow, and possibly execute arbitrary code, via a crafted stream, a different vulnerability than CV E-2011-2896.
| [CVE-2011-2896] The LZW decompressor in the LWZReadByte function in giftoppm.c in the David Kobl as GIF decoder in PBMPLUS, as used in the gif_read_lzw function in filter/image-gif.c in CUPS before 1.4 .7, the LZWReadByte function in plug-ins/common/file-gif-load.c in GIMP 2.6.11 and earlier, the LZWRea dByte function in img/gifread.c in XPCE in SWI-Prolog 5.10.4 and earlier, and other products, does not pr operly handle code words that are absent from the decompression table when encountered, which allows remote attackers to trigger an infinite loop or a heap-based buffer overflow, and possibly execute arbitrary code, via a crafted compressed stream, a related issue to CVE-2006-1168 and CVE-2011-2895.
| [CVE-2010-2941] ipp.c in cupsd in CUPS 1.4.4 and earlier does not properly allocate memory for attribut e values with invalid string data types, which allows remote attackers to cause a denial of service (use-aft er-free and application crash) or possibly execute arbitrary code via a crafted IPP request.
| [CVE-2010-2432] The cupsDoAuthentication function in auth.c in the client in CUPS before 1.4.4, when HAVE_GSSAPI is omitted, does not properly handle a demand for authorization, which allows remote CU PS servers to cause a denial of service (infinite loop) via HTTP_UNAUTHORIZED responses.
| [CVE-2010-2431] The cupsFileOpen function in CUPS before 1.4.4 allows local users, with lp group me mbership, to overwrite arbitrary files via a symlink attack on the (1) /var/cache/cups/remote.cache or (2) /v ar/cache/cups/job.cache file.
| [CVE-2010-1748] The cgi_initialize_string function in cgi-bin/var.c in the web interface in CUPS before 1. 4.4, as used on Apple Mac OS X 10.5.8, Mac OS X 10.6 before 10.6.4, and other platforms, does not pro perly handle parameter values containing a % (percent) character without two subsequent hex characters , which allows context-dependent attackers to obtain sensitive information from cupsd process memory vi a a crafted request, as demonstrated by the (1) /admin?OP=redirect&URL=% and (2) /admin?URL=/admi n/&OP=% URIs.
| [CVE-2010-1380] Integer overflow in the cgtexttops CUPS filter in Printing in Apple Mac OS X 10.6 befor e 10.6.4 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors related to page sizes.
| [CVE-2010-0542] The _WriteProlog function in texttops.c in texttops in the Text Filter subsystem in CUP S before 1.4.4 does not check the return values of certain calloc calls, which allows remote attackers to c ause a denial of service (NULL pointer dereference or heap memory corruption) or possibly execute arbitr ary code via a crafted file.
| [CVE-2010-0540] Cross-site request forgery (CSRF) vulnerability in the web interface in CUPS before 1. 4.4, as used on Apple Mac OS X 10.5.8, Mac OS X 10.6 before 10.6.4, and other platforms, allows remot e attackers to hijack the authentication of administrators for requests that change settings.
| [CVE-2010-0393] The _cupsGetlang function, as used by lppasswd.c in lppasswd in CUPS 1.2.2, 1.3.7, 1.3.9, and 1.4.1, relies on an environment variable to determine the file that provides localized message s trings, which allows local users to gain privileges via a file that contains crafted localization data with form at string specifiers.
| [CVE-2010-0302] Use-after-free vulnerability in the abstract file-descriptor handling interface in the cups dDoSelect function in scheduler/select.c in the scheduler in cupsd in CUPS before 1.4.4, when kqueue or epoll is used, allows remote attackers to cause a denial of service (daemon crash or hang) via a client dis connection during listing of a large number of print jobs, related to improperly maintaining a reference cou nt. NOTE: some of these details are obtained from third party information. NOTE: this vulnerability exists

because of an incomplete fix for CVE-2009-3553.
| [CVE-2009-3553] Use-after-free vulnerability in the abstract file-descriptor handling interface in the cups dDoSelect function in scheduler/select.c in the scheduler in cupsd in CUPS 1.3.7 and 1.3.10 allows remot e attackers to cause a denial of service (daemon crash or hang) via a client disconnection during listing of a large number of print jobs, related to improperly maintaining a reference count. NOTE: some of these details are obtained from third party information.
| [CVE-2009-2820] The web interface in CUPS before 1.4.2, as used on Apple Mac OS X before 10.6.2 a nd other platforms, does not properly handle (1) HTTP headers and (2) HTML templates, which allows re mote attackers to conduct cross-site scripting (XSS) attacks and HTTP response splitting attacks via vect ors related to (a) the product's web interface, (b) the configuration of the print system, and (c) the titles of printed jobs, as demonstrated by an XSS attack that uses the kerberos parameter to the admin program, and leverages attribute injection and HTTP Parameter Pollution (HPP) issues.
| [CVE-2009-2807] Heap-based buffer overflow in the USB backend in CUPS in Apple Mac OS X 10.5.8 a llows local users to gain privileges via unspecified vectors.
| [CVE-2009-1196] The directory-services functionality in the scheduler in CUPS 1.1.17 and 1.1.22 allows remote attackers to cause a denial of service (cupsd daemon outage or crash) via manipulations of the ti ming of CUPS browse packets, related to a "pointer use-after-delete flaw."
| [CVE-2009-1183] The JBIG2 MMR decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allows remote attackers to cause a denial of service (infinite loop and h ang) via a crafted PDF file.
| [CVE-2009-1182] Multiple buffer overflows in the JBIG2 MMR decoder in Xpdf 3.02pl2 and earlier, CUP S 1.3.9 and earlier, Poppler before 0.10.6, and other products allow remote attackers to execute arbitrary code via a crafted PDF file.
| [CVE-2009-1181] The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler befor e 0.10.6, and other products allows remote attackers to cause a denial of service (crash) via a crafted PD F file that triggers a NULL pointer dereference.
| [CVE-2009-1180] The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler befor e 0.10.6, and other products allows remote attackers to execute arbitrary code via a crafted PDF file that t riggers a free of invalid data.
| [CVE-2009-1179] Integer overflow in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and ear lier, Poppler before 0.10.6, and other products allows remote attackers to execute arbitrary code via a craf ted PDF file.
| [CVE-2009-0949] The ippReadIO function in cups/ipp.c in cupsd in CUPS before 1.3.10 does not properl y initialize memory for IPP request packets, which allows remote attackers to cause a denial of service (N ULL pointer dereference and daemon crash) via a scheduler request with two consecutive IPP_TAG_UN SUPPORTED tags.
| [CVE-2009-0800] Multiple "input validation flaws" in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUP S 1.3.9 and earlier, Poppler before 0.10.6, and other products allow remote attackers to execute arbitrary code via a crafted PDF file.
| [CVE-2009-0799] The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler befor e 0.10.6, and other products allows remote attackers to cause a denial of service (crash) via a crafted PD F file that triggers an out-of-bounds read.
| [CVE-2009-0791] Multiple integer overflows in Xpdf 2.x and 3.x and Poppler 0.x, as used in the pdftops fi lter in CUPS 1.1.17, 1.1.22, and 1.3.7, GPdf, and kdegraphics KPDF, allow remote attackers to cause a d enial of service (application crash) or possibly execute arbitrary code via a crafted PDF file that triggers a heap-based buffer overflow, possibly related to (1) Decrypt.cxx, (2) FoFiTrueType.cxx, (3) gmem.c, (4) JB IG2Stream.cxx, and (5) PSOutputDev.cxx in pdftops/. NOTE: the JBIG2Stream.cxx vector may overlap C VE-2009-1179.
| [CVE-2009-0577] Integer overflow in the WriteProlog function in texttops in CUPS 1.1.17 on Red Hat Ent erprise Linux (RHEL) 3 allows remote attackers to execute arbitrary code via a crafted PostScript file that triggers a heap-based buffer overflow. NOTE: this issue exists because of an incorrect fix for CVE-2008-3640.
| [CVE-2009-0195] Heap-based buffer overflow in Xpdf 3.02pl2 and earlier, CUPS 1.3.9, and probably oth er products, allows remote attackers to execute arbitrary code via a PDF file with crafted JBIG2 symbol di ctionary segments.

| [CVE-2009-0166] The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, and other products allows remote attackers to cause a denial of service (crash) via a crafted PDF file that triggers a free of uninitialized memory.
| [CVE-2009-0164] The web interface for CUPS before 1.3.10 does not validate the HTTP Host header in a client request, which makes it easier for remote attackers to conduct DNS rebinding attacks.
| [CVE-2009-0163] Integer overflow in the TIFF image decoding routines in CUPS 1.3.9 and earlier allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a crafted TIFF image, which is not properly handled by the (1) _cupsImageReadTIFF function in the imagetops filter and (2) imagetoraster filter, leading to a heap-based buffer overflow.
| [CVE-2009-0147] Multiple integer overflows in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, and other products allow remote attackers to cause a denial of service (crash) via a crafted PDF file, related to (1) JBIG2Stream::readSymbolDictSeg, (2) JBIG2Stream::readSymbolDictSeg, and (3) JBIG2Stream::readGenericBitmap.
| [CVE-2009-0146] Multiple buffer overflows in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, and other products allow remote attackers to cause a denial of service (crash) via a crafted PDF file, related to (1) JBIG2SymbolDict::setBitmap and (2) JBIG2Stream::readSymbolDictSeg.
| [CVE-2008-5377] pstopdf in CUPS 1.3.8 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/pstopdf.log temporary file, a different vulnerability than CVE-2001-1333.
| [CVE-2008-5286] Integer overflow in the _cupsImageReadPNG function in CUPS 1.1.17 through 1.3.9 allows remote attackers to execute arbitrary code via a PNG image with a large height value, which bypasses a validation check and triggers a buffer overflow.
| [CVE-2008-5184] The web interface (cgi-bin/admin.c) in CUPS before 1.3.8 uses the guest username when a user is not logged on to the web server, which makes it easier for remote attackers to bypass intended policy and conduct CSRF attacks via the (1) add and (2) cancel RSS subscription functions.
| [CVE-2008-5183] cupsd in CUPS 1.3.9 and earlier allows local users, and possibly remote attackers, to cause a denial of service (daemon crash) by adding a large number of RSS Subscriptions, which triggers a NULL pointer dereference. NOTE: this issue can be triggered remotely by leveraging CVE-2008-5184.
| [CVE-2008-3641] The Hewlett-Packard Graphics Language (HPGL) filter in CUPS before 1.3.9 allows remote attackers to execute arbitrary code via crafted pen width and pen color opcodes that overwrite arbitrary memory.
| [CVE-2008-3640] Integer overflow in the WriteProlog function in texttops in CUPS before 1.3.9 allows remote attackers to execute arbitrary code via a crafted PostScript file that triggers a heap-based buffer overflow.
| [CVE-2008-3639] Heap-based buffer overflow in the read_rle16 function in imagetops in CUPS before 1.3.9 allows remote attackers to execute arbitrary code via an SGI image with malformed Run Length Encoded (RLE) data containing a small image and a large row count.
| [CVE-2008-1722] Multiple integer overflows in (1) filter/image-png.c and (2) filter/image-zoom.c in CUPS 1.3 allow attackers to cause a denial of service (crash) and trigger memory corruption, as demonstrated via a crafted PNG image.
| [CVE-2008-1373] Buffer overflow in the gif_read_lzw function in CUPS 1.3.6 allows remote attackers to have an unknown impact via a GIF file with a large code_size value, a similar issue to CVE-2006-4484.
| [CVE-2008-1033] The scheduler in CUPS in Apple Mac OS X 10.5 before 10.5.3, when debug logging is enabled and a printer requires a password, allows attackers to obtain sensitive information (credentials) by reading the log data, related to "authentication environment variables."
| [CVE-2008-0882] Double free vulnerability in the process_browse_data function in CUPS 1.3.5 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via crafted UDP Browse packets to the cupsd port (631/udp), related to an unspecified manipulation of a remote printer. NOTE: some of these details are obtained from third party information.
| [CVE-2008-0597] Use-after-free vulnerability in CUPS before 1.1.22, and possibly other versions, allows remote attackers to cause a denial of service (crash) via crafted IPP packets.
| [CVE-2008-0596] Memory leak in CUPS before 1.1.22, and possibly other versions, allows remote attackers to cause a denial of service (memory consumption and daemon crash) via a large number of requests to add and remove shared printers.
| [CVE-2008-0053] Multiple buffer overflows in the HP-GL/2-to-PostScript filter in CUPS before 1.3.6 might allow remote attackers to execute arbitrary code via a crafted HP-GL/2 file.

| [CVE-2008-0047] Heap-based buffer overflow in the cgiCompileSearch function in CUPS 1.3.5, and other versions including the version bundled with Apple Mac OS X 10.5.2, when printer sharing is enabled, allows remote attackers to execute arbitrary code via crafted search expressions.
| [CVE-2007-6358] pdftops.pl before 1.20 in alternate pdftops filter allows local users to overwrite arbitrary files via a symlink attack on the pdfin.[PID].tmp temporary file, which is created when pdftops reads a PDF file from stdin, such as when pdftops is invoked by CUPS.
| [CVE-2007-5849] Integer underflow in the asn1_get_string function in the SNMP back end (backend/snmp.c) for CUPS 1.2 through 1.3.4 allows remote attackers to execute arbitrary code via a crafted SNMP response that triggers a stack-based buffer overflow.
| [CVE-2007-5848] Buffer overflow in CUPS in Apple Mac OS X 10.4.11 allows local admin users to execute arbitrary code via a crafted URI to the CUPS service.
| [CVE-2007-4351] Off-by-one error in the ippReadIO function in cups/ipp.c in CUPS 1.3.3 allows remote attackers to cause a denial of service (crash) via a crafted (1) textWithLanguage or (2) nameWithLanguage Internet Printing Protocol (IPP) tag, leading to a stack-based buffer overflow.
| [CVE-2007-1834] Cisco Unified CallManager (CUCM) 5.0 before 5.0(4a)SU1 and Cisco Unified Presence Server (CUPS) 1.0 before 1.0(3) allow remote attackers to cause a denial of service (loss of voice services) via a flood of ICMP echo requests, aka bug ID CSCsf12698.
| [CVE-2007-1826] Unspecified vulnerability in the IPSec Manager Service for Cisco Unified CallManager (CUCM) 5.0 before 5.0(4a)SU1 and Cisco Unified Presence Server (CUPS) 1.0 before 1.0(3) allows remote attackers to cause a denial of service (loss of cluster services) via a "specific UDP packet" to UDP port 8500, aka bug ID CSCsg60949.
| [CVE-2005-4873] Multiple stack-based buffer overflows in the phpcups PHP module for CUPS 1.1.23rc1 might allow context-dependent attackers to execute arbitrary code via vectors that result in long function parameters, as demonstrated by the cups_get_dest_options function in phpcups.c.
| [CVE-2005-2874] The is_path_absolute function in scheduler/client.c for the daemon in CUPS before 1.1.23 allows remote attackers to cause a denial of service (CPU consumption by tight loop) via a "..\.." URL in an HTTP request.
| [CVE-2005-2526] CUPS in Mac OS X 10.3.9 and 10.4.2 allows remote attackers to cause a denial of service (CPU consumption) by sending a partial IPP request and closing the connection.
| [CVE-2005-2525] CUPS in Mac OS X 10.3.9 and 10.4.2 does not properly close file descriptors when handling multiple simultaneous print jobs, which allows remote attackers to cause a denial of service (printing halt).
| [CVE-2004-2154] CUPS before 1.1.21rc1 treats a Location directive in cupsd.conf as case sensitive, which allows attackers to bypass intended ACLs via a printer name containing uppercase or lowercase letters that are different from what is specified in the directive.
| [CVE-2004-1270] lppasswd in CUPS 1.1.22, when run in environments that do not ensure that file descriptors 0, 1, and 2 are open when lppasswd is called, does not verify that the passwd.new file is different from STDERR, which allows local users to control output to passwd.new via certain user input that triggers an error message.
| [CVE-2004-1269] lppasswd in CUPS 1.1.22 does not remove the passwd.new file if it encounters a file-size resource limit while writing to passwd.new, which causes subsequent invocations of lppasswd to fail.
| [CVE-2004-1268] lppasswd in CUPS 1.1.22 ignores write errors when modifying the CUPS passwd file, which allows local users to corrupt the file by filling the associated file system and triggering the write errors.
| [CVE-2004-1267] Buffer overflow in the ParseCommand function in hpgl-input.c in the hpgltops program for CUPS 1.1.22 allows remote attackers to execute arbitrary code via a crafted HPGL file.
| [CVE-2004-0923] CUPS 1.1.20 and earlier records authentication information for a device URI in the error_log file, which allows local users to obtain user names and passwords.
| [CVE-2004-0558] The Internet Printing Protocol (IPP) implementation in CUPS before 1.1.21 allows remote attackers to cause a denial of service (service hang) via a certain UDP packet to the IPP port.
| [CVE-2004-0382] Unknown vulnerability in the CUPS printing system in Mac OS X 10.3.3 and Mac OS X 10.2.8 with unknown impact, possibly related to a configuration file setting.
| [CVE-2003-0788] Unknown vulnerability in the Internet Printing Protocol (IPP) implementation in CUPS before 1.1.19 allows remote attackers to cause a denial of service (CPU consumption from a "busy loop") via certain inputs to the IPP port (TCP 631).

| [CVE-2003-0195] CUPS before 1.1.19 allows remote attackers to cause a denial of service via a partial printing request to the IPP port (631), which does not time out.
| [CVE-2002-1384] Integer overflow in pdftops, as used in Xpdf 2.01 and earlier, xpdf-i, and CUPS before 1.1.18, allows local users to execute arbitrary code via a ColorSpace entry with a large number of elemen ts, as demonstrated by cups-pdf.
| [CVE-2002-1383] Multiple integer overflows in Common Unix Printing System (CUPS) 1.1.14 through 1. 1.17 allow remote attackers to execute arbitrary code via (1) the CUPSd HTTP interface, as demonstrate d by vanilla-coke, and (2) the image handling code in CUPS filters, as demonstrated by mksun.
| [CVE-2002-1372] Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 does not properly check the return values of various file and socket operations, which could allow a remote attacker to cause a de nial of service (resource exhaustion) by causing file descriptors to be assigned and not released, as demo nstrated by fanta.
| [CVE-2002-1371] filters/image-gif.c in Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 doe s not properly check for zero-length GIF images, which allows remote attackers to execute arbitrary code via modified chunk headers, as demonstrated by nogif.
| [CVE-2002-1369] jobs.c in Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 does not prope rly use the strncat function call when processing the options string, which allows remote attackers to exec ute arbitrary code via a buffer overflow attack.
| [CVE-2002-1368] Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by causing negative arguments to be fed into memcpy() calls via HTTP requests with (1) a negative Content-Length value or (2) a negative length in a chunked transfer encoding.
| [CVE-2002-1367] Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allows remote attackers to add printers without authentication via a certain UDP packet, which can then be used to perform unaut horized activities such as stealing the local root certificate for the administration server via a "need authori zation" page, as demonstrated by new-coke.
| [CVE-2002-1366] Common Unix Printing System (CUPS) 1.1.14 through 1.1.17 allows local users with l p privileges to create or overwrite arbitrary files via file race conditions, as demonstrated by ice-cream.
| [CVE-2002-1267] Mac OS X 10.2.2 allows remote attackers to cause a denial of service by accessing th e CUPS Printing Web Administration utility, aka "CUPS Printing Web Administration is Remotely Accessib le."
| [CVE-2002-0063] Buffer overflow in ippRead function of CUPS before 1.1.14 may allow attackers to exe cute arbitrary code via long attribute names or language values.
| [CVE-2001-1333] Linux CUPS before 1.1.6 does not securely handle temporary files, possibly due to a s ymlink vulnerability that could allow local users to overwrite files.
| [CVE-2001-1332] Buffer overflows in Linux CUPS before 1.1.6 may allow remote attackers to execute ar bitrary code.
| [CVE-2001-0194] Buffer overflow in httpGets function in CUPS 1.1.5 allows remote attackers to execute arbitrary commands via a long input line.
| [CVE-2000-0513] CUPS (Common Unix Printing System) 1.04 and earlier allows remote attackers to ca use a denial of service by authenticating with a user name that does not exist or does not have a shadow password.
| [CVE-2000-0512] CUPS (Common Unix Printing System) 1.04 and earlier does not properly delete requ est files, which allows a remote attacker to cause a denial of service.
| [CVE-2000-0511] CUPS (Common Unix Printing System) 1.04 and earlier allows remote attackers to ca use a denial of service via a CGI POST request.
| [CVE-2000-0510] CUPS (Common Unix Printing System) 1.04 and earlier allows remote attackers to ca use a denial of service via a malformed IPP request.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [88563] CUPS CVE-2001-0194 Remote Security Vulnerability
| [88030] CUPS CVE-2001-1333 Local Security Vulnerability
| [86939] Cups CVE-2005-4873 Remote Security Vulnerability
| [85201] cups-filters CVE-2015-8560 Arbitrary Command Execution Vulnerability
| [84720] CUPS CVE-2008-5184 Security Bypass Vulnerability

| [82922] CUPS CVE-2001-1332 Remote Security Vulnerability
| [78524] cups-filters CVE-2015-8327 Arbitrary Command Execution Vulnerability
| [75557] cups-filters CVE-2015-3279 Remote Heap Buffer Overflow Vulnerability
| [75436] cups-filters 'texttopdf' Remote Heap Buffer Overflow Vulnerability
| [75106] CUPS CVE-2015-1159 Cross Site Scripting Vulnerability
| [75098] CUPS CVE-2015-1158 Remote Privilege Escalation Vulnerability
| [73300] CUPS CVE-2014-8166 Arbitrary Code Execution Vulnerability
| [73008] cups-filters 'utils/cups-browsed.c' Arbitrary Command Execution Vulnerability
| [72594] CUPS cupsRasterReadPixels Buffer Overflow Vulnerability
| [69866] Wireshark CUPS Dissector CVE-2014-6425 Denial of Service Vulnerability
| [68847] CUPS Web Interface CVE-2014-5031 Incomplete Fix Local Privilege Escalation Vulnerability
| [68846] CUPS Web Interface CVE-2014-5030 Incomplete Fix Local Privilege Escalation Vulnerability
| [68842] CUPS Web Interface CVE-2014-5029 Incomplete Fix Local Privilege Escalation Vulnerability
| [68788] CUPS Web Interface CVE-2014-3537 Local Privilege Escalation Vulnerability
| [68124] cups-filters CVE-2014-4338 Security Bypass Vulnerability
| [68122] cups-filters CVE-2014-4337 Denial of Service Vulnerability
| [68121] cups-filters CVE-2014-4336 Incomplete Fix Arbitrary Command Execution Vulnerability
| [66788] CUPS Web Interface Cross Site Scripting Vulnerability
| [66624] cups-filters CVE-2014-2707 Arbitrary Command Execution Vulnerability
| [66601] cups-filters 'urftopdf.cpp' Multiple Heap Based Buffer Overflow Vulnerabilities
| [66163] cups-filters 'pdftoopvp' Filter Remote Heap Buffer Overflow Vulnerability
| [66161] cups-filters 'urftopdf.cpp' Multiple Heap Based Buffer Overflow Vulnerabilities
| [66158] cups-filters 'OPVPWrapper::loadDriver()' Function Local Arbitrary Command Execution Vulnerab
ility
| [64985] cups 'systemv/lppasswd.c' Local Privilege Escalation Vulnerability
| [57158] CUPS 'Listen localhost:631' Option Unauthorized Access Vulnerability
| [56494] CUPS CVE-2012-5519 Local Privilege Escalation Vulnerability
| [55911] cups-pk-helper 'cupsGetFile()' and 'cupsPutFile()' Local Security Vulnerabilities
| [55583] OKI Multiple CUPS Printer Drivers Multiple Insecure Temporary File Creation Vulnerabilities
| [49323] CUPS 'gif_read_lzw()' CVE-2011-3170 GIF File Heap Buffer Overflow Vulnerability
| [45710] Ubuntu CUPS Package AppArmor Security Bypass Weakness
| [44530] CUPS Server 'cups/ipp.c' Remote Memory Corruption Vulnerability
| [41131] CUPS 'cupsFileOpen' function Symlink Attack Local Privilege Escalation Vulnerability
| [41126] CUPS 'cupsDoAuthentication()' Infinite Loop Denial of Service Vulnerability
| [40943] CUPS 'texttops' Filter NULL-pointer Dereference Vulnerability
| [40897] CUPS Web Interface Information Disclosure Vulnerability
| [40889] CUPS Web Interface Unspecified Cross Site Request Forgery Vulnerability
| [38524] CUPS 'lppasswd' Tool Localized Message String Security Weakness
| [38510] CUPS File Descriptors Handling Use-After-Free Remote Denial Of Service Vulnerability
| [37048] CUPS File Descriptors Handling Remote Denial Of Service Vulnerability
| [36958] CUPS 'kerberos' Parameter Cross Site Scripting Vulnerability
| [36350] CUPS USB backend Local Heap Based Buffer Overflow Vulnerability
| [35195] CUPS PDF File Multiple Heap Buffer Overflow Vulnerabilities
| [35194] CUPS Scheduler Directory Services Remote Denial Of Service Vulnerability
| [35169] CUPS 'cups/ipp.c' NULL Pointer Dereference Denial Of Service Vulnerability
| [34791] CUPS and Xpdf JBIG2 Symbol Dictionary Processing Heap Buffer Overflow Vulnerability
| [34665] CUPS Insufficient 'Host' Header Validation Weakness
| [34571] CUPS '_cupsImageReadTIFF()' Integer Overflow Vulnerability
| [33418] CUPS '/tmp/pdf.log' Insecure Temporary File Creation Vulnerability
| [32745] CUPS 'pstopdf' Insecure Temporary File Creation Vulnerability
| [32518] CUPS PNG Filter '_cupsImageReadPNG()' Integer Overflow Vulnerability
| [32419] CUPS 'cupsd' RSS Subscriptions NULL Pointer Dereference Local Denial Of Service Vulnerabili
ty
| [31690] CUPS Multiple Heap Based Buffer Overflow Vulnerabilities
| [31688] CUPS 'HP-GL/2' Filter Remote Code Execution Vulnerability

| [29484] Apple Mac OS X CUPS Debug Logging Information Disclosure Vulnerability
| [28781] CUPS PNG Filter Multiple Integer Overflow Vulnerabilities
| [28544] CUPS 'gif_read_lzw()' GIF File Buffer Overflow Vulnerability
| [28334] CUPS Multiple Unspecified Input Validation Vulnerabilities
| [28307] CUPS CGI Interface Remote Buffer Overflow Vulnerability
| [27988] CUPS Multiple Remote Denial of Service Vulnerabilities
| [27906] CUPS 'process_browse_data()' Remote Double Free Denial of Service Vulnerability
| [26919] pdftops.pl Alternate pdftops Filter for CUPS Insecure Temporary File Creation Vulnerability
| [26524] CUPS SSL Negotiation Unspecified Remote Denial of Service Vulnerability
| [26268] CUPS IPP Tag Handling Remote Buffer Overflow Vulnerability
| [23127] CUPS Partial SSL Connection Remote Denial of Service Vulnerability
| [14527] Easy Software Products CUPS Denial of Service Vulnerability
| [14265] Easy Software Products CUPS Access Control List Bypass Vulnerability
| [12200] Easy Software Products CUPS HTTP GET Denial Of Service Vulnerability
| [12007] Easy Software Products LPPassWd CUPS Password File Error Message Injection Vulnerability
| [12004] Easy Software Products LPPassWd CUPS Password File Truncation Vulnerability
| [11968] CUPS HPGL File Processor Buffer Overflow Vulnerability
| [11324] CUPS Error_Log Local Password Disclosure Vulnerability
| [11183] CUPS UDP Packet Remote Denial Of Service Vulnerability
| [10062] CUPS Unspecified Configuration Vulnerability
| [8952] Cups Internet Printing Protocol Job Loop Denial Of Service Vulnerability
| [7637] CUPS Cupsd Request Method Denial Of Service Vulnerability
| [7200] APC apcupsd Multiple Buffer Overflow Vulnerabilities
| [6828] APC apcupsd Client Syslog Format String Vulnerability
| [6475] Xpdf/CUPS pdftops Integer Overflow Vulnerability
| [6440] CUPS File Descriptor Leakage Denial Of Service Vulnerability
| [6439] CUPS Image Filter Zero Width GIF Memory Corruption Vulnerability
| [6438] CUPS strncat() Function Call Buffer Overflow Vulnerability
| [6437] CUPS Negative Length HTTP Header Vulnerability
| [6436] CUPS Remote Printer Addition Vulnerability
| [6435] CUPS Insecure Temporary File Creation Vulnerability
| [6434] CUPS lp Image Handler Integer Overflow Vulnerabilities
| [6433] CUPS HTTP Interface Integer Overflow Vulnerability
| [2070] APC apcupsd Local Denial of Service Vulnerability
| [1373] CUPS (Common UNIX Printing System) Denial of Service Vulnerability
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [80012] CUPS SystemGroup privilege escalation
| [79242] cups-pk-helper file transmission routines privilege escalation
| [78763] Multiple CUPS drivers for OKI printers symlink
| [69380] CUPS gif_read_lzw function buffer overflow
| [68862] HP Linux Imaging and Printing System hpcupsfax.cpp symlink
| [67063] Ubuntu CUPS AppArmor security bypass
| [62882] CUPS cupsd code execution
| [59736] CUPS cupsDoAuthentication() demand for authorization denial of service
| [59735] CUPS cupsFileOpen() symlink
| [59597] CUPS _WriteProlog() function code execution
| [59466] Apple Mac OS X Printing cgtexttops CUPS filter code execution
| [59456] Apple Mac OS X CUPS cupsd information disclosure
| [59455] Apple Mac OS X CUPS Web interface cross-site request forgery
| [56669] CUPS lppasswd tool code execution
| [56668] CUPS file descriptors-handling interface denial of service
| [54326] CUPS cupsdDoSelect() denial of service
| [54189] Apple Mac OS X CUPS response splitting
| [53168] Apple Mac OS X CUPS USB buffer overflow

| [50944] CUPS Scheduler Directory Services denial of service
| [50941] CUPS pdftops filter buffer overflow
| [50926] Apple CUPS IPP tag denial of service
| [49942] CUPS HTTP Host header security bypass
| [49941] CUPS _cupsImageReadTIFF() function buffer overflow
| [48977] CUPS texttops WriteProlog() buffer overflow
| [48210] CUPS pdf.log symlink
| [47249] CUPS pstopdf symlink
| [46933] CUPS _cupsImageReadPNG() integer overflow
| [46773] CUPS Web interface weak security
| [46684] CUPS RSS subscription denial of service
| [45790] CUPS WriteProlog() buffer overflow
| [45789] CUPS read_rle16() buffer overflow
| [45779] CUPS HPGL filter code execution
| [42713] Apple Mac OS X CUPS information disclosure
| [41832] CUPS image-png.c and image-zoom.c buffer overflow
| [41758] CUPS pdftops filter buffer overflow
| [41587] CUPS gif_read_lzw() buffer overflow
| [41497] phpcups PHP module for CUPS multiple function parameters buffer overflows
| [41316] Apple Mac OS X CUPS buffer overflow
| [41272] Apple Mac OS X CUPS input validation unspecified
| [40845] CUPS IPP browse use-after-free denial of service
| [40842] CUPS IPP browse memory leak denial of service
| [40718] CUPS process_browse_data() code execution
| [39101] CUPS SNMP asn1_get_string() buffer overflow
| [39096] Apple Mac OS X CUPS buffer overflow
| [38190] CUPS ippReadIO function buffer overflow
| [35344] Cisco Unified Presence Server (CUPS) and Cisco Unified CallManager (CUCM) SNMP informati
on disclosure
| [35341] Cisco Unified Presence Server (CUPS) and Cisco Unified CallManager (CUCM) system service
denial of service
| [32123] RHSA-2005:878 updates for cups not installed
| [22679] RHSA-2005:053 updates for cups not installed
| [22603] RHSA-2005:571 updates for cups not installed
| [21874] Apple Mac OS X CUPS IPP request denial of service
| [21871] Apple Mac OS X CUPS printing service denial of service
| [21522] CUPS queue name bypass authentication
| [18804] CUPS logic error denial of service
| [18609] CUPS lppasswd modify passwd file
| [18608] CUPS lppasswd denial of service
| [18606] CUPS lppasswd truncate passwd file
| [18604] CUPS ParseCommand HPGL buffer overflow
| [17593] CUPS disclose passwords in log files
| [17389] CUPS UDP packet denial of service
| [15769] Apple Mac OS X CUPS undisclosed configuration security issue
| [13584] CUPS Internet Printing Protocol denial of service
| [12080] CUPS IPP implementation partial request denial of service
| [11491] Apcupsd vsprintf() multiple buffer overflows
| [11334] Apcupsd log_event() format string attack
| [10937] CUPS and Xpdf pdftops filter integer overflow
| [10912] CUPS file descriptor leak denial of service
| [10911] CUPS filters/image-gif.c improperly checks zero width GIF images
| [10910] CUPS strncat() options buffer overflow
| [10909] CUPS negative Content-Length memcpy() buffer overflows
| [10908] CUPS UDP packets could be used to add printers

| [10907] CUPS /etc/cups/certs/ race condition could be used to create and overwrite files
| [10906] CUPS has multiple integer overflows
| [10824] Apple Mac OS X Common Unix Printing System (CUPS) denial of service
| [9998] CUPS temporary file symlink attack
| [9997] CUPS password buffer overflow
| [8192] CUPS ippRead() attribute name buffer overflow
| [6043] CUPS httpGets function denial of service
| [5654] APC apcupsd denial of service
| [5550] Cups allows Internet users to attach to local printers
| [5178] Debian CUPS shadow password authentication
| [4847] CUPS request files denial of service
| [4846] CUPS CGI form POST denial of service
| [4736] CUPS malformed IPP request denial of service
|
| Exploit-DB - https://www.exploit-db.com:
| [24977] CUPS 1.1.x HPGL File Processor Buffer Overflow Vulnerability
| [24599] CUPS 1.1.x UDP Packet Remote Denial of Service Vulnerability
| [22619] CUPS 1.1.x Cupsd Request Method Denial of Service Vulnerability
| [22106] CUPS 1.1.x Negative Length HTTP Header Vulnerability
| [7550] CUPS < 1.3.8-4 (pstopdf filter) Privilege Escalation Exploit
| [7150] CUPS 1.3.7 CSRF (add rss subscription) Remote Crash Exploit
| [1196] CUPS Server <= 1.1 (Get Request) Denial of Service Exploit
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [63843] Debian Security Advisory DSA 1773-1 (cups)
| [62839] Debian Security Advisory DSA 1677-1 (cupsys)
| [90017] Cups < 1.3.8 vulnerability
| [66443] Fedora Core 10 FEDORA-2009-12652 (cups)
| [66435] Fedora Core 10 FEDORA-2009-11062 (cups)
| [66430] Fedora Core 12 FEDORA-2009-11314 (cups)
| [66426] Fedora Core 11 FEDORA-2009-10891 (cups)
| [66269] Debian Security Advisory DSA 1933-1 (cups)
| [64112] Debian Security Advisory DSA 1810-1 (cups, cupsys)
| [63877] Fedora Core 10 FEDORA-2009-3769 (cups)
| [61778] Debian Security Advisory DSA 1656-1 (cupsys)
| [61377] Debian Security Advisory DSA 1625-1 (cupsys)
| [60619] Debian Security Advisory DSA 1530-1 (cupsys)
| [60069] Debian Security Advisory DSA 1437-1 (cupsys)
| [59234] Debian Security Advisory DSA 1407-1 (cupsys)
| [53391] Debian Security Advisory DSA 110-1 (cupsys)
| [16141] CUPS < 1.1.23 Multiple Vulnerabilities
|
| SecurityTracker - https://www.securitytracker.com:
| [1025980] CUPS Buffer Overflow in gif_read_lzw() Lets Remote Users Execute Arbitrary Code
| [1024662] CUPS IPP Request Processing Bug Lets Remote Users Execute Arbitrary Code
| [1024124] CUPS Use After Free in cupsdDoSelect() Lets Remote Users Deny Service
| [1024123] CUPS Administrative Interface Lets Remote Users Obtain Potentially Sensitive Memory Cont
ents
| [1024122] CUPS Web Interface Permits Cross-Site Request Forgery Attacks
| [1024121] CUPS Null Pointer Dereference in 'texttops' Filter Lets Remote Users Execute Arbitrary Code
| [1023678] CUPS lppasswd Format String Bug Lets Local Users Gain Elevated Privileges
| [1023194] CUPS Use After Free in cupsdDoSelect() Lets Remote Users Deny Service
| [1023193] CUPS Input Validation Flaw in 'kerberos' Parameter Permits Cross-Site Scripting and Respon
se Splitting Attacks
| [1022898] CUPS Heap Overflow in USB Backend Lets Local Users Gain Elevated Privileges

| [1022327] CUPS Scheduler Directory Services Use-After-Free Bug Lets Remote Users Deny Service
| [1022326] CUPS Integer Overflow in 'pdftops' Lets Remote Users Execute Arbitrary Code
| [1022321] CUPS IPP_TAG_UNSUPPORTED Structure Initialization Bug Lets Remote Users Deny Servi
ce
| [1022070] CUPS Integer Overflow in Processing TIFF Images Lets Remote Users Execute Arbitrary Cod
e
| [1021637] CUPS on Mandriva Lets Local Users Gain Elevated Privileges
| [1021396] CUPS RSS Subscription Null Pointer Dereference Lets Local Users Deny Service
| [1021298] CUPS Integer Overflow in _cupsImageReadPNG() Lets Remote Users Execute Arbitrary Cod
e
| [1021034] CUPS Heap Overflow in 'texttops' Lets Remote Users Execute Arbitrary Code
| [1021033] CUPS Heap Overflow in 'imagetops' Processing of SGI Image Files Lets Remote Users Exec
ute Arbitrary Code
| [1021031] CUPS Bug in HPGL Filter Lets Remote Users Execute Arbitrary Code
| [1020145] CUPS Scheduler Discloses Information to Local Users
| [1019854] CUPS Integer Overflows in Processing PNG Images May Let Remote Users Execute Arbitrar
y Code
| [1019739] CUPS Buffer Overflow in gif_read_lzw() Lets Remote Users Execute Arbitrary Code
| [1019672] CUPS Bugs Let Remote Users Execute Arbitrary Code or Deny Service
| [1019646] CUPS Heap Overflow Lets Remote Users Execute Arbitrary Code
| [1019497] CUPS Bugs in Adding/Deleting Shared Printers Lets Remote Users Deny Service
| [1019473] CUPS Double Free Bug in process_browse_data() May Let Remote Users Execute Arbitrary
Code
| [1018879] CUPS Buffer Overflow in ippReadIO() Lets Remote Users Execute Arbitrary Code
| [1017750] Mac OS X CUPS SSL Negotiation Lets Remote Users Deny Service
| [1014698] CUPS on Mac OS X Lets Remote Users Deny Service By Submitting Multipe Print Jobs or Pa
rtial IPP Requests
| [1014482] CUPS Case Sensitive Location Directive May Let Remote Users Bypass Access Controls
| [1012811] CUPS Logic Error in Processing '/..' Requests Lets Remote Users Deny Service
| [1012602] CUPS lppasswd Lets Local Users Truncate Files and Deny Service
| [1012566] CUPS HPGL Buffer Overflow in ParseCommand() Lets Remote Users Execute Arbitrary Cod
e
| [1011529] CUPS Log Files May Disclose User Passwords to Local Users
| [1011283] CUPS Browsing Can Be Disabled By Remote Users
| [1009679] Apple Mac OS X CUPS Configuration Flaw Has Unspecified Impact
| [1008774] apcupsd Unsafe File Permissions Let Local Users Kill Arbitrary Processes
| [1008078] CUPS IPP Busy Loop May Let Remote Users Deny Service
| [1006836] CUPS Internet Printing Protocol HTTP Header Processing Flaw Lets Remote Users Deny Ser
vice
| [1006108] Apcupsd Format String Flaw May Let Remote Users Gain Root Access
| [1005853] Common UNIX Printing System (CUPS) 'pdftops' Integer Overflow May Let Remote Users Ca
use Arbitrary Code to Be Executed By a Target User
| [1005835] Common UNIX Printing System (CUPS) Has Multiple Bugs That Let Remote and Local Users
Gain Root Privileges on the System
| [1003551] Common UNIX Printing System (CUPS) Buffer Overflow May Allow a Remote User to Execut
e Arbitrary Code or Crash the Process
|
| OSVDB - http://www.osvdb.org:
| [92076] CUPS cups/http-support.c http_resolve_cb Function Memory Exhaustion Remote DoS
| [92075] CUPS scheduler/job.c load_request_root Function Memory Exhaustion DoS
| [92074] CUPS scheduler/job.c set_time Function NULL Pointer Dereference DoS
| [92073] CUPS cups/ipp.c ippReadIO Function NULL Pointer Dereference DoS
| [92072] CUPS cups/ipp-support.c ippEnumString Function Off-by-one Overflow DoS
| [92052] CUPS cupsd.conf Listen Directive Admin Interface Restriction IPv6 Connection Bypass
| [90648] Cisco Unified Presence Server (CUPS) Crafted SIP Packets CPU Consumption Remote DoS

| [87783] cups-pk-helper cupsGetFile / cupsPutFile Function Arbitrary File Overwrite
| [87635] CUPS on Linux /var/run/cups/certs/0 Permission Weakness Arbitrary File Manipulation
| [77214] system-config-printer cupshelper OpenPrinting Database Query MitM Package Installation Spoo
fing
| [76797] HP Linux Imaging and Printing (HPLIP) prnt/hpijs/hpcupsfax.cpp send_data_to_stdout() Functio
n Symlink Local Arbitrary File Overwrite
| [74673] CUPS filter/image-gif.c gif_read_lzw Function Crafted LZW Stream Remote Overflow
| [68951] CUPS IPP Request Handling Use-After-Free Arbitrary Code Execution
| [65699] CUPS auth.c cupsDoAuthentication Function HTTP_UNAUTHORIZED Response Remote DoS
| [65698] CUPS cupsFileOpen Function Multiple Temporary File Symlink Arbitrary File Overwrite
| [65692] CUPS texttops.c _WriteProlog Function Memory Corruption
| [65569] CUPS Web Interface Form Variable Handling cupsd Process Memory Disclosure
| [65566] Apple Mac OS X Printing cgtexttops CUPS Filter Page Size Overflow
| [65555] Apple Mac OS X CUPS Web Interface Settings Manipulation CSRF
| [62715] CUPS lppasswd.c _cupsGetlang Function Format String Local Privilege Escalation
| [60204] CUPS scheduler/select.c cupsdDoSelect() Function Use-after-free DoS
| [59854] CUPS Web Interface admin/ kerberos Parameter XSS
| [58777] CUPS SSL Negotiation Unspecified Remote DoS
| [57951] Apple Mac OS X CUPS USB Backend Unspecified Local Overflow
| [56176] CUPS pdftops Filter PDF File Handling Multiple Unspecified Overflows
| [56174] CUPS PNG Image Size Validation Unspecified Overflow
| [56173] CUPS Scheduler Unspecified DNS Rebinding
| [55032] CUPS Scheduler Directory-services Functionality Browse Packet Timing Remote DoS
| [55002] CUPS cupsd cups/ipp.c ippReadIO Function IPP Packet Handling Remote DoS
| [54495] CUPS JBIG2 Decoder PDF File Handling Multiple Function Overflows
| [54490] CUPS Crafted PDF File JBIG2 Symbol Dictionary Segments Handling Overflow
| [54488] CUPS JBIG2 Decoder PDF File Handling Unitialized Memory Free DoS
| [54485] CUPS JBIG2 Decoder PDF File Handling Out-of-bounds Read DoS
| [54482] CUPS JBIG2 Decoder PDF File Handling NULL Dereference DoS
| [54479] CUPS JBIG2 Decoder PDF File Handling Invalid Free Arbitrary Code Execution
| [54476] CUPS JBIG2 Decoder PDF File Handling Unspecified Integer Overflow
| [54471] CUPS JBIG2 Decoder PDF File Handling Multiple Unspecified Input Validation Flaws Arbitrary C
ode Execution
| [54468] CUPS JBIG2 MMR Decoder Crafted PDF Handling Arbitrary Code Execution
| [54466] CUPS JBIG2 MMR Decoder Crafted PDF File Handling Infinite Loop DoS
| [54462] CUPS TIFF Image Decoding Routines Multiple Filter File Handling Overflows
| [54461] CUPS Web Interface HTTP Host Header Validation Weakness
| [52937] CUPS on Mandriva Linux /tmp/pdf.log Temporary File Symlink Arbitrary File Overwrite
| [50637] CUPS pstopdf /tmp/pstopdf.log Temporary File Symlink Arbitrary File Overwrite
| [50494] CUPS _cupsImageReadPNG Function PNG File Handling Overflow
| [50352] CUPS cgi-bin/admin.c Multiple RSS Subscription Function Policy Bypass CSRF
| [50351] CUPS cupsd RSS Subscription Saturation NULL Dereference DoS
| [49132] CUPS texttops WriteProlog Function Crafted PostScript File Handling Overflow
| [49131] CUPS imagetops read_rle16 Function Malformed SGI Image Handling Remote Overflow
| [49130] CUPS Hewlett-Packard Graphics Language (HPGL) Filter Multiple Opcode Handling Remote Co
de Execution
| [48699] CUPS cupsaddsmb Temporary File Cleartext Samba Credential Disclosure
| [44398] CUPS PNG File Handling Multiple Overflows
| [44330] CUPS on Red Hat Linux 64-bit pdftops Crafted PDF File Handling Overflow
| [44160] CUPS filter/image-gif.c gif_read_image() Function GIF Image Handling Overflow
| [43889] phpcups PHP module for CUPS Multiple Overflows
| [43382] CUPS Multiple HP-GL/2-to-PostScript Unspecified Input Validation Issues
| [43376] CUPS CGI Backend IPP Request Search Expression Handling (cgiCompileSearch) Remote Ov
erflow
| [42159] CUPS Crafted IPP Packets Remote DoS

| [42158] CUPS Add / Remove Shared Printer Request Saturation DoS
| [42030] CUPS process_browse_data() Function Double-free Arbitrary Code Execution
| [42029] Alternate pdftops Filter for CUPS pdfin.[PID].tmp Symlink Arbitrary File Overwrite
| [42028] CUPS cups/ipp.c ippReadIO Function IPP Tag Handling Overflow
| [40725] Apple Mac OS X CUPS Service Crafted URI Local Overflow
| [40719] CUPS SNMP Back End (backend/snmp.c) asn1_get_string Function Crafted SNMP Response Remote Overflow
| [36124] Cisco CUCM / CUPS Unspecified SNMP Information Disclosure
| [36123] Cisco CUCM / CUPS Unspecified Cluster Services DoS
| [34594] Cisco CUCM / CUPS ICMP Echo Request Saturation DoS
| [34072] CUPS Incomplete SSL Negotiation Remote DoS
| [18797] CUPS on Mac OS X Print Job Saturation DoS
| [18796] CUPS on Mac OS X Partial IPP Request Connection Termination DoS
| [17912] CUPS Case Mismatch Printer Queue Password Bypass
| [15014] Apple Mac OS X CUPS Unspecified Configuration File Issue
| [12834] CUPS Malformed Traversal HTTP Request Remote DoS
| [12454] CUPS lppasswd passwd.new Arbitrary Append
| [12453] CUPS lppasswd passwd.new File Limit DoS
| [12439] CUPS ParseCommand() Function HPGL File Overflow
| [11048] CUPS Debugging Local Authentication Credential Disclosure
| [10749] APC apcupsd vsprintf Function Unspecified Multiple Overflows
| [10748] APC apcupsd Slave Server Request Format String
| [10746] CUPS Image Handler Remote Overflow
| [10745] CUPS HTTP Interface Remote Overflow
| [10744] CUPS File/Socket Return Value File Descriptor Consumption DoS
| [10743] CUPS image-gif.c Zero-Length GIF Image Header Arbitrary Code Execution
| [10742] CUPS jobs.c Options Strings Remote Overflow
| [10741] CUPS HTTP Request Multiple Header Negative Argument Overflow
| [10740] CUPS UDP Packet Arbitrary Printer Addition Privilege Escalation
| [10739] CUPS lp Privilege Arbitrary File Creation/Overwrite
| [10738] CUPS Insecure Temporary File Handling
| [10737] CUPS lppasswd Remote Overflow
| [10499] CUPS Printing Log Password Disclosure
| [9995] CUPS Internet Printing Protocol (IPP) Implementation Empty UDP Datagram Remote DoS
| [7304] CUPS CGI Form POST DoS
| [7303] CUPS Request File Deletion DoS
| [7302] CUPS Invalid Username Authentication Remote DoS
| [7058] Apple Mac OS X CUPS Web Admin Utility DoS
| [6064] CUPS httpGets() Function Overflow DoS
| [5380] CUPS ippRead Function Multiple Variable Overflow
| [4780] CUPS Partial IPP Request DoS
| [2761] CUPS Unspecified DoS
| [1683] APC apcupsd Local DoS
| [1413] CUPS Malformed IPP Request DoS
|_
| http-enum:
| /admin.php: Possible admin folder
| /admin/: Possible admin folder
| /admin/admin/: Possible admin folder
| /administrator/: Possible admin folder
| /adminarea/: Possible admin folder
| /adminLogin/: Possible admin folder
| /admin_area/: Possible admin folder
| /administratorlogin/: Possible admin folder
| /admin/account.php: Possible admin folder

| /admin/index.php: Possible admin folder
| /admin/login.php: Possible admin folder
| /admin/admin.php: Possible admin folder
| /admin_area/admin.php: Possible admin folder
| /admin_area/login.php: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin_area/index.php: Possible admin folder
| /admin/home.php: Possible admin folder
| /admin_area/login.html: Possible admin folder
| /admin_area/index.html: Possible admin folder
| /admin/controlpanel.php: Possible admin folder
| /admincp/: Possible admin folder
| /admincp/index.asp: Possible admin folder
| /admincp/index.html: Possible admin folder
| /admincp/login.php: Possible admin folder
| /admin/account.html: Possible admin folder
| /adminpanel.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin_login.html: Possible admin folder
| /admin/cp.php: Possible admin folder
| /administrator/index.php: Possible admin folder
| /administrator/login.php: Possible admin folder
| /admin/admin_login.php: Possible admin folder
| /admin_login.php: Possible admin folder
| /administrator/account.php: Possible admin folder
| /administrator.php: Possible admin folder
| /admin_area/admin.html: Possible admin folder
| /admin/admin-login.php: Possible admin folder
| /admin-login.php: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin-login.html: Possible admin folder
| /admincontrol.php: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /adminLogin.html: Possible admin folder
| /adminarea/index.html: Possible admin folder
| /adminarea/admin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin.html: Possible admin folder
| /admin/cp.html: Possible admin folder
| /adminpanel.php: Possible admin folder
| /administrator/index.html: Possible admin folder
| /administrator/login.html: Possible admin folder
| /administrator/account.html: Possible admin folder
| /administrator.html: Possible admin folder
| /adminarea/login.html: Possible admin folder
| /admincontrol/login.html: Possible admin folder
| /admincontrol.html: Possible admin folder
| /adminLogin.php: Possible admin folder
| /admin/adminLogin.php: Possible admin folder
| /adminarea/index.php: Possible admin folder
| /adminarea/admin.php: Possible admin folder
| /adminarea/login.php: Possible admin folder

| /admincontrol/login.php: Possible admin folder
| /admin2.php: Possible admin folder
| /admin2/login.php: Possible admin folder
| /admin2/index.php: Possible admin folder
| /administratorlogin.php: Possible admin folder
| /admin/account.cfm: Possible admin folder
| /admin/index.cfm: Possible admin folder
| /admin/login.cfm: Possible admin folder
| /admin/admin.cfm: Possible admin folder
| /admin.cfm: Possible admin folder
| /admin/admin_login.cfm: Possible admin folder
| /admin_login.cfm: Possible admin folder
| /adminpanel.cfm: Possible admin folder
| /admin/controlpanel.cfm: Possible admin folder
| /admincontrol.cfm: Possible admin folder
| /admin/cp.cfm: Possible admin folder
| /admincp/index.cfm: Possible admin folder
| /admincp/login.cfm: Possible admin folder
| /admin_area/admin.cfm: Possible admin folder
| /admin_area/login.cfm: Possible admin folder
| /administrator/login.cfm: Possible admin folder
| /administratorlogin.cfm: Possible admin folder
| /administrator.cfm: Possible admin folder
| /administrator/account.cfm: Possible admin folder
| /adminLogin.cfm: Possible admin folder
| /admin2/index.cfm: Possible admin folder
| /admin_area/index.cfm: Possible admin folder
| /admin2/login.cfm: Possible admin folder
| /admincontrol/login.cfm: Possible admin folder
| /administrator/index.cfm: Possible admin folder
| /adminarea/login.cfm: Possible admin folder
| /adminarea/admin.cfm: Possible admin folder
| /adminarea/index.cfm: Possible admin folder
| /admin/adminLogin.cfm: Possible admin folder
| /admin-login.cfm: Possible admin folder
| /admin/admin-login.cfm: Possible admin folder
| /admin/home.cfm: Possible admin folder
| /admin/account.asp: Possible admin folder
| /admin/index.asp: Possible admin folder
| /admin/login.asp: Possible admin folder
| /admin/admin.asp: Possible admin folder
| /admin_area/admin.asp: Possible admin folder
| /admin_area/login.asp: Possible admin folder
| /admin_area/index.asp: Possible admin folder
| /admin/home.asp: Possible admin folder
| /admin/controlpanel.asp: Possible admin folder
| /admin.asp: Possible admin folder
| /admin/admin-login.asp: Possible admin folder
| /admin-login.asp: Possible admin folder
| /admin/cp.asp: Possible admin folder
| /administrator/account.asp: Possible admin folder
| /administrator.asp: Possible admin folder
| /administrator/login.asp: Possible admin folder
| /admincp/login.asp: Possible admin folder
| /admincontrol.asp: Possible admin folder

| /adminpanel.asp: Possible admin folder
| /admin/admin_login.asp: Possible admin folder
| /admin_login.asp: Possible admin folder
| /adminLogin.asp: Possible admin folder
| /admin/adminLogin.asp: Possible admin folder
| /adminarea/index.asp: Possible admin folder
| /adminarea/admin.asp: Possible admin folder
| /adminarea/login.asp: Possible admin folder
| /administrator/index.asp: Possible admin folder
| /admincontrol/login.asp: Possible admin folder
| /admin2.asp: Possible admin folder
| /admin2/login.asp: Possible admin folder
| /admin2/index.asp: Possible admin folder
| /administratorlogin.asp: Possible admin folder
| /admin/account.aspx: Possible admin folder
| /admin/index.aspx: Possible admin folder
| /admin/login.aspx: Possible admin folder
| /admin/admin.aspx: Possible admin folder
| /admin_area/admin.aspx: Possible admin folder
| /admin_area/login.aspx: Possible admin folder
| /admin_area/index.aspx: Possible admin folder
| /admin/home.aspx: Possible admin folder
| /admin/controlpanel.aspx: Possible admin folder
| /admin.aspx: Possible admin folder
| /admin/admin-login.aspx: Possible admin folder
| /admin-login.aspx: Possible admin folder
| /admin/cp.aspx: Possible admin folder
| /administrator/account.aspx: Possible admin folder
| /administrator.aspx: Possible admin folder
| /administrator/login.aspx: Possible admin folder
| /admincp/index.aspx: Possible admin folder
| /admincp/login.aspx: Possible admin folder
| /admincontrol.aspx: Possible admin folder
| /adminpanel.aspx: Possible admin folder
| /admin/admin_login.aspx: Possible admin folder
| /admin_login.aspx: Possible admin folder
| /adminLogin.aspx: Possible admin folder
| /admin/adminLogin.aspx: Possible admin folder
| /adminarea/index.aspx: Possible admin folder
| /adminarea/admin.aspx: Possible admin folder
| /adminarea/login.aspx: Possible admin folder
| /administrator/index.aspx: Possible admin folder
| /admincontrol/login.aspx: Possible admin folder
| /admin2.aspx: Possible admin folder
| /admin2/login.aspx: Possible admin folder
| /admin2/index.aspx: Possible admin folder
| /administratorlogin.aspx: Possible admin folder
| /admin/index.jsp: Possible admin folder
| /admin/login.jsp: Possible admin folder
| /admin/admin.jsp: Possible admin folder
| /admin_area/admin.jsp: Possible admin folder
| /admin_area/login.jsp: Possible admin folder
| /admin_area/index.jsp: Possible admin folder
| /admin/home.jsp: Possible admin folder
| /admin/controlpanel.jsp: Possible admin folder

| /admin.jsp: Possible admin folder
| /admin/admin-login.jsp: Possible admin folder
| /admin-login.jsp: Possible admin folder
| /admin/cp.jsp: Possible admin folder
| /administrator/account.jsp: Possible admin folder
| /administrator.jsp: Possible admin folder
| /administrator/login.jsp: Possible admin folder
| /admincp/index.jsp: Possible admin folder
| /admincp/login.jsp: Possible admin folder
| /admincontrol.jsp: Possible admin folder
| /admin/account.jsp: Possible admin folder
| /adminpanel.jsp: Possible admin folder
| /admin/admin_login.jsp: Possible admin folder
| /admin_login.jsp: Possible admin folder
| /adminLogin.jsp: Possible admin folder
| /admin/adminLogin.jsp: Possible admin folder
| /adminarea/index.jsp: Possible admin folder
| /adminarea/admin.jsp: Possible admin folder
| /adminarea/login.jsp: Possible admin folder
| /administrator/index.jsp: Possible admin folder
| /admincontrol/login.jsp: Possible admin folder
| /admin2.jsp: Possible admin folder
| /admin2/login.jsp: Possible admin folder
| /admin2/index.jsp: Possible admin folder
| /administratorlogin.jsp: Possible admin folder
| /admin1.php: Possible admin folder
| /administr8.asp: Possible admin folder
| /administr8.php: Possible admin folder
| /administr8.jsp: Possible admin folder
| /administr8.aspx: Possible admin folder
| /administr8.cfm: Possible admin folder
| /administr8/: Possible admin folder
| /administer/: Possible admin folder
| /administracao.php: Possible admin folder
| /administracao.asp: Possible admin folder
| /administracao.aspx: Possible admin folder
| /administracao.cfm: Possible admin folder
| /administracao.jsp: Possible admin folder
| /administracion.php: Possible admin folder
| /administracion.asp: Possible admin folder
| /administracion.aspx: Possible admin folder
| /administracion.jsp: Possible admin folder
| /administracion.cfm: Possible admin folder
| /administrators/: Possible admin folder
| /adminpro/: Possible admin folder
| /admins/: Possible admin folder
| /admins.cfm: Possible admin folder
| /admins.php: Possible admin folder
| /admins.jsp: Possible admin folder
| /admins.asp: Possible admin folder
| /admins.aspx: Possible admin folder
| /administracion-sistema/: Possible admin folder
| /admin108/: Possible admin folder
| /admin_cp.asp: Possible admin folder
| /admin/backup/: Possible backup

```
|   /admin/download/backup.sql: Possible database backup
|   /robots.txt: Robots file
|   /admin/upload.php: Admin File Upload
|   /admin/CiscoAdmin.jhtml: Cisco Collaboration Server
|   /admin-console/: JBoss Console
|   /admin4.nsf: Lotus Domino
|   /admin5.nsf: Lotus Domino
|   /admin.nsf: Lotus Domino
|   /administrator/wp-login.php: Wordpress login page.
|   /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File uploa
d
|   /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind CMS/FCKeditor File
 upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Uploa
d
|   /admin/jscript/upload.php: Lizard Cart/Remote File upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|   /admin/jscript/upload.pl: Lizard Cart/Remote File upload
|   /admin/jscript/upload.asp: Lizard Cart/Remote File upload
|   /admin/environment.xml: Moodle files
|   /classes/: Potentially interesting folder
|   /es/: Potentially interesting folder
|   /helpdesk/: Potentially interesting folder
|   /help/: Potentially interesting folder
|_  /printers/: Potentially interesting folder
|_http-server-header: CUPS/1.7 IPP/2.1
| vulners:
|   cpe:/a:apple:cups:1.7:
|       CVE-2012-5519 7.2 https://vulners.com/cve/CVE-2012-5519
|       SECURITYVULNS:VULN:13879 5.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1387
9
|       PRION:CVE-2014-5031 5.0 https://vulners.com/prion/PRION:CVE-2014-5031
|       CVE-2014-5031 5.0 https://vulners.com/cve/CVE-2014-5031
|       SECURITYVULNS:VULN:13707 4.3 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1370
7
|       PRION:CVE-2014-2856 4.3 https://vulners.com/prion/PRION:CVE-2014-2856
|       CVE-2014-2856 4.3 https://vulners.com/cve/CVE-2014-2856
|       PRION:CVE-2014-5030 1.9 https://vulners.com/prion/PRION:CVE-2014-5030
|       CVE-2014-5030 1.9 https://vulners.com/cve/CVE-2014-5030
|       PRION:CVE-2021-25317 1.7 https://vulners.com/prion/PRION:CVE-2021-25317
|       SECURITYVULNS:VULN:13530 1.2 https://vulners.com/securityvulns/SECURITYVULNS:VULN:1353
0
|       PRION:CVE-2014-3537 1.2 https://vulners.com/prion/PRION:CVE-2014-3537
|       PRION:CVE-2013-6891 1.2 https://vulners.com/prion/PRION:CVE-2013-6891
|       CVE-2014-3537 1.2 https://vulners.com/cve/CVE-2014-3537
|_      CVE-2013-6891 1.2 https://vulners.com/cve/CVE-2013-6891
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
| temp: VulDB - https://vuldb.com:
| [137831] CouchCMS 2 mysql2i.func.php Path information disclosure
| [107083] Xceedium Xsuite 2.3.0/2.4.3.0 MySQL Database Empty sql injection
| [94689] WampServer 3.0.6 wampapache/wampmysqld access control
| [84458] Tutti Nova class.novaRead.mysql.php privileges management
| [84191] Bee-hive Lite mysqlCall.inc.php privileges management
```

| [23289] netenberg fantastico de luxe 2.8 var/lib/mysql information disclosure
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2013-3812] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Replication.
| [CVE-2013-3811] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3806.
| [CVE-2013-3810] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to XA Transactions.
| [CVE-2013-3809] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Audit Log.
| [CVE-2013-3808] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Server Options.
| [CVE-2013-3807] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Server Privileges.
| [CVE-2013-3806] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3811.
| [CVE-2013-3805] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Prepared Statements.
| [CVE-2013-3804] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2013-3802] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Full Text Search.
| [CVE-2013-3801] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Server Options.
| [CVE-2013-3798] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect integrity and availability via unknown vectors related to MemCached.
| [CVE-2013-3796] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2013-3795] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.
| [CVE-2013-3794] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Server Partition.
| [CVE-2013-3793] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.
| [CVE-2013-3783] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Parser.
| [CVE-2013-3561] Multiple integer overflows in Wireshark 1.8.x before 1.8.7 allow remote attackers to ca

use a denial of service (loop or application crash) via a malformed packet, related to a crash of the Websocket dissector, an infinite loop in the MySQL dissector, and a large loop in the ETCH dissector.
| [CVE-2013-3221] The Active Record component in Ruby on Rails 2.3.x, 3.0.x, 3.1.x, and 3.2.x does not ensure that the declared data type of a database column is used during comparisons of input values to stored values in that column, which makes it easier for remote attackers to conduct data-type injection attacks against Ruby on Rails applications via a crafted value, as demonstrated by unintended interaction between the "typed XML" feature and a MySQL database.
| [CVE-2013-2395] Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-1567.
| [CVE-2013-2392] Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2013-2391] Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows local users to affect confidentiality and integrity via unknown vectors related to Server Install.
| [CVE-2013-2389] Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
| [CVE-2013-2381] Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server Privileges.
| [CVE-2013-2378] Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, 5.5.29 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Information Schema.
| [CVE-2013-2376] Unspecified vulnerability in Oracle MySQL 5.5.30 and earlier and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Stored Procedure.
| [CVE-2013-2375] Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.
| [CVE-2013-1861] MariaDB 5.5.x before 5.5.30, 5.3.x before 5.3.13, 5.2.x before 5.2.15, and 5.1.x before 5.1.68, and Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, and 5.6.11 and earlier allows remote attackers to cause a denial of service (crash) via a crafted geometry feature that specifies a large number of points, which is not properly handled when processing the binary representation of this feature, related to a numeric calculation error.
| [CVE-2013-1570] Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote attackers to affect availability via unknown vectors related to MemCached.
| [CVE-2013-1567] Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-2395.
| [CVE-2013-1566] Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
| [CVE-2013-1555] Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, and 5.5.29 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Partition.
| [CVE-2013-1552] Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.
| [CVE-2013-1548] Unspecified vulnerability in Oracle MySQL 5.1.63 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Types.
| [CVE-2013-1544] Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.
| [CVE-2013-1532] Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Information Schema.
| [CVE-2013-1531] Unspecified vulnerability in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors rela

ted to Server Privileges.
| [CVE-2013-1526] Unspecified vulnerability in Oracle MySQL 5.5.29 and earlier allows remote authentica ted users to affect availability via unknown vectors related to Server Replication.
| [CVE-2013-1523] Unspecified vulnerability in Oracle MySQL 5.5.29 and earlier and 5.6.10 and earlier all ows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors rela ted to Server Optimizer.
| [CVE-2013-1521] Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier all ows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors rela ted to Server Locking.
| [CVE-2013-1512] Unspecified vulnerability in Oracle MySQL 5.5.29 and earlier allows remote authentica ted users to affect availability via unknown vectors related to Data Manipulation Language.
| [CVE-2013-1511] Unspecified vulnerability in Oracle MySQL 5.5.30 and earlier and 5.6.10 and earlier all ows remote authenticated users to affect availability via unknown vectors related to InnoDB.
| [CVE-2013-1506] Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, 5.5.29 and earlier, and 5 .6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Se rver Locking.
| [CVE-2013-1502] Unspecified vulnerability in Oracle MySQL 5.5.30 and earlier and 5.6.9 and earlier allo ws local users to affect availability via unknown vectors related to Server Partition.
| [CVE-2013-1492] Buffer overflow in yaSSL, as used in MySQL 5.1.x before 5.1.68 and 5.5.x before 5.5. 30, has unspecified impact and attack vectors, a different vulnerability than CVE-2012-0553.
| [CVE-2013-0389] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote authenticated users to affect availability via unknown vectors relate d to Server Optimizer.
| [CVE-2013-0386] Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Stored Procedure.
| [CVE-2013-0385] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows local users to affect confidentiality and integrity via unknown vectors relate d to Server Replication.
| [CVE-2013-0384] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote authenticated users to affect availability via unknown vectors relate d to Information Schema.
| [CVE-2013-0383] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote attackers to affect availability via unknown vectors related to Server Locking.
| [CVE-2013-0375] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.1.28 and earlier, allows remote authenticated users to affect confidentiality and integrity via unkno wn vectors related to Server Replication.
| [CVE-2013-0371] Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability, related to MyISAM.
| [CVE-2013-0368] Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
| [CVE-2013-0367] Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Partition.
| [CVE-2012-5615] MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a, 5.3.11, 5.2.13, 5.1.6 6, and possibly other versions, generates different error messages with different time delays depending o n whether a user name exists, which allows remote attackers to enumerate valid usernames.
| [CVE-2012-5614] Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier, and MariaDB 5.5.28a and po ssibly other versions, allows remote authenticated users to cause a denial of service (mysqld crash) via a SELECT command with an UpdateXML command containing XML with a large number of unique, nested elements.
| [CVE-2012-5613] ** DISPUTED ** MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a an d possibly other versions, when configured to assign the FILE privilege to users who should not have adm inistrative privileges, allows remote authenticated users to gain privileges by leveraging the FILE privilege to create files as the MySQL administrator. NOTE: the vendor disputes this issue, stating that this is only a vulnerability when the administrator does not follow recommendations in the product’s installation docu

mentation. NOTE: it could be argued that this should not be included in CVE because it is a configuration issue.
| [CVE-2012-5612] Heap-based buffer overflow in Oracle MySQL 5.5.19 and other versions through 5.5.28, and MariaDB 5.5.28a and possibly other versions, allows remote authenticated users to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code, as demonstrated using certain variations of the (1) USE, (2) SHOW TABLES, (3) DESCRIBE, (4) SHOW FIELDS FROM, (5) SHOW COLUMNS FROM, (6) SHOW INDEX FROM, (7) CREATE TABLE, (8) DROP TABLE, (9) ALTER TABLE, (10) DELETE FROM, (11) UPDATE, and (12) SET PASSWORD commands.
| [CVE-2012-5611] Stack-based buffer overflow in the acl_get function in Oracle MySQL 5.5.19 and other versions through 5.5.28, and 5.1.53 and other versions through 5.1.66, and MariaDB 5.5.2.x before 5.5.28a, 5.3.x before 5.3.11, 5.2.x before 5.2.13 and 5.1.x before 5.1.66, allows remote authenticated users to execute arbitrary code via a long argument to the GRANT FILE command.
| [CVE-2012-5383] ** DISPUTED ** Untrusted search path vulnerability in the installation functionality in Oracle MySQL 5.5.28, when installed in the top-level C:\ directory, might allow local users to gain privileges via a Trojan horse DLL in the "C:\MySQL\MySQL Server 5.5\bin" directory, which may be added to the PATH system environment variable by an administrator, as demonstrated by a Trojan horse wlbsctrl.dll file used by the "IKE and AuthIP IPsec Keying Modules" system service in Windows Vista SP1, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 Release Preview. NOTE: CVE disputes this issue because the unsafe PATH is established only by a separate administrative action that is not a default part of the MySQL installation.
| [CVE-2012-5096] Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users with Server Privileges to affect availability via unknown vectors.
| [CVE-2012-5060] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.65 and earlier and 5.5.27 and earlier allows remote authenticated users to affect availability, related to GIS Extension.
| [CVE-2012-4452] MySQL 5.0.88, and possibly other versions and platforms, allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL data home directory, related to incorrect calculation of the mysql_unpacked_real_data_home value. NOTE: this vulnerability exists because of a CVE-2009-4030 regression, which was not omitted in other packages and versions such as MySQL 5.0.95 in Red Hat Enterprise Linux 6.
| [CVE-2012-4414] Multiple SQL injection vulnerabilities in the replication code in Oracle MySQL possibly before 5.5.29, and MariaDB 5.1.x through 5.1.62, 5.2.x through 5.2.12, 5.3.x through 5.3.7, and 5.5.x through 5.5.25, allow remote authenticated users to execute arbitrary SQL commands via vectors related to the binary log. NOTE: as of 20130116, Oracle has not commented on claims from a downstream vendor that the fix in MySQL 5.5.29 is incomplete.
| [CVE-2012-4255] MySQLDumper 1.24.4 allows remote attackers to obtain sensitive information via a direct request to learn/cubemail/refresh_dblist.php, which reveals the installation path in an error message.
| [CVE-2012-4254] MySQLDumper 1.24.4 allows remote attackers to obtain sensitive information (Notices) via a direct request to (1) learn/cubemail/restore.php or (2) learn/cubemail/dump.php.
| [CVE-2012-4253] Multiple directory traversal vulnerabilities in MySQLDumper 1.24.4 allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) language parameter to learn/cubemail/install.php or (2) f parameter learn/cubemail/filemanagement.php, or execute arbitrary local files via a .. (dot dot) in the (3) config parameter to learn/cubemail/menu.php.
| [CVE-2012-4252] Multiple cross-site request forgery (CSRF) vulnerabilities in MySQLDumper 1.24.4 allow remote attackers to hijack the authentication of administrators for requests that (1) remove file access restriction via a deletehtaccess action, (2) drop a database via a kill value in a db action, (3) uninstall the application via a 101 value in the phase parameter to learn/cubemail/install.php, (4) delete config.php via a 2 value in the phase parameter to learn/cubemail/install.php, (5) change a password via a schutz action, or (6) execute arbitrary SQL commands via the sql_statement parameter to learn/cubemail/sql.php.
| [CVE-2012-4251] Multiple cross-site scripting (XSS) vulnerabilities in MySQLDumper 1.24.4 allow remote attackers to inject arbitrary web script or HTML via the (1) page parameter to index.php, (2) phase parameter to install.php, (3) tablename or (4) dbid parameter to sql.php, or (5) filename parameter to restore.php in learn/cubemail/.
| [CVE-2012-3951] The MySQL component in Plixer Scrutinizer (aka Dell SonicWALL Scrutinizer) 9.0.1.1

9899 and earlier has a default password of admin for the (1) scrutinizer and (2) scrutremote accounts, whi
ch allows remote attackers to execute arbitrary SQL commands via a TCP session.
| [CVE-2012-3441] The database creation script (module/idoutils/db/scripts/create_mysqldb.sh) in Icinga 1
.7.1 grants access to all databases to the icinga user, which allows icinga users to access other database
s via unspecified vectors.
| [CVE-2012-3197] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 an
d earlier, and 5.5.26 and earlier, allows remote authenticated users to affect availability via unknown vect
ors related to Server Replication.
| [CVE-2012-3180] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.65 an
d earlier, and 5.5.27 and earlier, allows remote authenticated users to affect availability via unknown vect
ors related to Server Optimizer.
| [CVE-2012-3177] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.65 an
d earlier, and 5.5.27 and earlier, allows remote authenticated users to affect availability via unknown vect
ors related to Server.
| [CVE-2012-3173] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.63 an
d earlier, and 5.5.25 and earlier, allows remote authenticated users to affect availability via unknown vect
ors related to InnoDB Plugin.
| [CVE-2012-3167] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.63 an
d earlier, and 5.5.25 and earlier, allows remote authenticated users to affect availability via unknown vect
ors related to Server Full Text Search.
| [CVE-2012-3166] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.63 an
d earlier, and 5.5.25 and earlier, allows remote authenticated users to affect availability via unknown vect
ors related to InnoDB.
| [CVE-2012-3163] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 an
d earlier, and 5.5.26 and earlier, allows remote authenticated users to affect confidentiality, integrity, and
availability via unknown vectors related to Information Schema.
| [CVE-2012-3160] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.65 an
d earlier, and 5.5.27 and earlier, allows local users to affect confidentiality via unknown vectors related to
Server Installation.
| [CVE-2012-3158] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 an
d earlier, and 5.5.26 and earlier, allows remote attackers to affect confidentiality, integrity, and availability
via unknown vectors related to Protocol.
| [CVE-2012-3156] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.25 an
d earlier allows remote authenticated users to affect availability via unknown vectors related to Server.
| [CVE-2012-3150] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 an
d earlier, and 5.5.26 and earlier, allows remote authenticated users to affect availability via unknown vect
ors related to Server Optimizer.
| [CVE-2012-3149] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 an
d earlier allows remote authenticated users to affect confidentiality, related to MySQL Client.
| [CVE-2012-3147] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 an
d earlier allows remote attackers to affect integrity and availability, related to MySQL Client.
| [CVE-2012-3144] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 an
d earlier allows remote authenticated users to affect availability via unknown vectors related to Server.
| [CVE-2012-2750] Unspecified vulnerability in MySQL 5.5.x before 5.5.23 has unknown impact and attac
k vectors related to a "Security Fix", aka Bug #59533. NOTE: this might be a duplicate of CVE-2012-1689
, but as of 20120816, Oracle has not commented on this possibility.
| [CVE-2012-2749] MySQL 5.1.x before 5.1.63 and 5.5.x before 5.5.24 allows remote authenticated users
to cause a denial of service (mysqld crash) via vectors related to incorrect calculation and a sort order ind
ex.
| [CVE-2012-2122] sql/password.c in Oracle MySQL 5.1.x before 5.1.63, 5.5.x before 5.5.24, and 5.6.x be
fore 5.6.6, and MariaDB 5.1.x before 5.1.62, 5.2.x before 5.2.12, 5.3.x before 5.3.6, and 5.5.x before 5.5.2
3, when running in certain environments with certain implementations of the memcmp function, allows re
mote attackers to bypass authentication by repeatedly authenticating with the same incorrect password, w
hich eventually causes a token comparison to succeed due to an improperly-checked return value.
| [CVE-2012-2102] MySQL 5.1.x before 5.1.62 and 5.5.x before 5.5.22 allows remote authenticated users

to cause a denial of service (assertion failure and mysqld abort) by deleting a record and using HANDLER READ NEXT.
| [CVE-2012-1757] Unspecified vulnerability in Oracle MySQL Server 5.5.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
| [CVE-2012-1756] Unspecified vulnerability in Oracle MySQL Server 5.5.23 and earlier allows remote authenticated users to affect availability via unknown vectors.
| [CVE-2012-1735] Unspecified vulnerability in Oracle MySQL Server 5.5.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-1734] Unspecified vulnerability in Oracle MySQL Server 5.1.62 and earlier, and 5.5.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-1705] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-1703] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.61 and earlier, and 5.5.21 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-1702] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote attackers to affect availability via unknown vectors.
| [CVE-2012-1697] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Partition.
| [CVE-2012-1696] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.19 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-1690] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.61 and earlier, and 5.5.21 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-1689] Unspecified vulnerability in Oracle MySQL Server 5.1.62 and earlier, and 5.5.22 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-1688] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.61 and earlier, and 5.5.21 and earlier, allows remote authenticated users to affect availability, related to Server DML.
| [CVE-2012-0937] ** DISPUTED ** wp-admin/setup-config.php in the installation component in WordPress 3.3.1 and earlier does not limit the number of MySQL queries sent to external MySQL database servers, which allows remote attackers to use WordPress as a proxy for brute-force attacks or denial of service attacks via the dbhost parameter, a different vulnerability than CVE-2011-4898. NOTE: the vendor disputes the significance of this issue because an incomplete WordPress installation might be present on the network for only a short time.
| [CVE-2012-0882] Buffer overflow in yaSSL, as used in MySQL 5.5.20 and possibly other versions including 5.5.x before 5.5.22 and 5.1.x before 5.1.62, allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VulnDisco Pack Professional 9.17. NOTE: as of 20120224, this disclosure has no actionable information. However, because the module author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes. NOTE: due to lack of details, it is not clear whether this issue is a duplicate of CVE-2012-0492 or another CVE.
| [CVE-2012-0583] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.60 and earlier, and 5.5.19 and earlier, allows remote authenticated users to affect availability, related to MyISAM.
| [CVE-2012-0578] Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
| [CVE-2012-0574] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote authenticated users to affect availability via unknown vectors.
| [CVE-2012-0572] Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

| [CVE-2012-0553] Buffer overflow in yaSSL, as used in MySQL 5.1.x before 5.1.68 and 5.5.x before 5.5.28, has unspecified impact and attack vectors, a different vulnerability than CVE-2013-1492.
| [CVE-2012-0540] Unspecified vulnerability in Oracle MySQL Server 5.1.62 and earlier and 5.5.23 and earlier allows remote authenticated users to affect availability, related to GIS Extension.
| [CVE-2012-0496] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect confidentiality and integrity via unknown vectors.
| [CVE-2012-0495] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, and CVE-2012-0493.
| [CVE-2012-0494] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows local users to affect availability via unknown vectors.
| [CVE-2012-0493] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, and CVE-2012-0495.
| [CVE-2012-0492] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0485.
| [CVE-2012-0491] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0493, and CVE-2012-0495.
| [CVE-2012-0490] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect availability via unknown vectors.
| [CVE-2012-0489] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.
| [CVE-2012-0488] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0487, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.
| [CVE-2012-0487] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0486, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.
| [CVE-2012-0486] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0117, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and CVE-2012-0495.
| [CVE-2012-0485] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0492.
| [CVE-2012-0484] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect confidentiality via unknown vectors.
| [CVE-2012-0120] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0485, and CVE-2012-0492.
| [CVE-2012-0119] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.
| [CVE-2012-0118] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0113.

| [CVE-2012-0117] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.x allo
ws remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE
-2012-0486, CVE-2012-0487, CVE-2012-0488, CVE-2012-0489, CVE-2012-0491, CVE-2012-0493, and
CVE-2012-0495.
| [CVE-2012-0116] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and
5.5.x allows remote authenticated users to affect confidentiality and integrity via unknown vectors.
| [CVE-2012-0115] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and
5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability t
han CVE-2012-0112, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.
| [CVE-2012-0114] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.
x, and 5.5.x allows local users to affect confidentiality and integrity via unknown vectors.
| [CVE-2012-0113] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and
5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a diff
erent vulnerability than CVE-2012-0118.
| [CVE-2012-0112] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and
5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability t
han CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.
| [CVE-2012-0102] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and
5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability t
han CVE-2012-0087 and CVE-2012-0101.
| [CVE-2012-0101] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and
5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability t
han CVE-2012-0087 and CVE-2012-0102.
| [CVE-2012-0087] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and
5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability t
han CVE-2012-0101 and CVE-2012-0102.
| [CVE-2012-0075] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.
x, and 5.5.x allows remote authenticated users to affect integrity via unknown vectors.
| [CVE-2011-5049] MySQL 5.5.8, when running on Windows, allows remote attackers to cause a denial of
service (NULL pointer dereference) via a crafted packet to TCP port 3306.
| [CVE-2011-4959] SQL injection vulnerability in the addslashes method in SilverStripe 2.3.x before 2.3.12
and 2.4.x before 2.4.6, when connected to a MySQL database using far east character encodings, allows
remote attackers to execute arbitrary SQL commands via unspecified vectors.
| [CVE-2011-4899] ** DISPUTED ** wp-admin/setup-config.php in the installation component in WordPres
s 3.3.1 and earlier does not ensure that the specified MySQL database service is appropriate, which allow
s remote attackers to configure an arbitrary database via the dbhost and dbname parameters, and subse
quently conduct static code injection and cross-site scripting (XSS) attacks via (1) an HTTP request or (2)
a MySQL query. NOTE: the vendor disputes the significance of this issue
| [CVE-2011-4898] ** DISPUTED ** wp-admin/setup-config.php in the installation component in WordPres
s 3.3.1 and earlier generates different error messages for requests lacking a dbname parameter dependin
g on whether the MySQL credentials are valid, which makes it easier for remote attackers to conduct brut
e-force attacks via a series of requests with different uname and pwd parameters. NOTE: the vendor disp
utes the significance of this issue
| [CVE-2011-3989] SQL injection vulnerability in DBD::mysqlPP 0.04 and earlier allows remote attackers t
o execute arbitrary SQL commands via unspecified vectors.
| [CVE-2011-3805] TaskFreak! multi-mysql-0.6 allows remote attackers to obtain sensitive information via
a direct request to a .php file, which reveals the installation path in an error message, as demonstrated by
include/language/zh/register_info.php and certain other files.
| [CVE-2011-2688] SQL injection vulnerability in mysql/mysql-auth.pl in the mod_authnz_external module
3.2.5 and earlier for the Apache HTTP Server allows remote attackers to execute arbitrary SQL command
s via the user field.
| [CVE-2011-2531] Prosody 0.8.x before 0.8.1, when MySQL is used, assigns an incorrect data type to th
e value column in certain tables, which might allow remote attackers to cause a denial of service (data tru
ncation) by sending a large amount of data.
| [CVE-2011-2262] Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and

5.5.x allows remote attackers to affect availability via unknown vectors.
| [CVE-2011-1906] Trustwave WebDefend Enterprise before 5.0 7.01.903-1.4 stores specific user-account credentials in a MySQL database, which makes it easier for remote attackers to read the event collection table via requests to the management port, a different vulnerability than CVE-2011-0756.
| [CVE-2011-1513] Static code injection vulnerability in install_.php in e107 CMS 0.7.24 and probably earlier versions, when the installation script is not removed, allows remote attackers to inject arbitrary PHP code into e107_config.php via a crafted MySQL server name.
| [CVE-2011-0432] Multiple SQL injection vulnerabilities in the get_userinfo method in the MySQLAuthHandler class in DAVServer/mysqlauth.py in PyWebDAV before 0.9.4.1 allow remote attackers to execute arbitrary SQL commands via the (1) user or (2) pw argument. NOTE: some of these details are obtained from third party information.
| [CVE-2010-5104] The escapeStrForLike method in TYPO3 4.2.x before 4.2.16, 4.3.x before 4.3.9, and 4.4.x before 4.4.5 does not properly escape input when the MySQL database is set to sql_mode NO_BACKSLASH_ESCAPES, which allows remote attackers to obtain sensitive information via wildcard characters in a LIKE query.
| [CVE-2010-4822] core/model/MySQLDatabase.php in SilverStripe 2.4.x before 2.4.4, when the site is running in "live mode," allows remote attackers to obtain the SQL queries for a page via the showqueries and ajax parameters.
| [CVE-2010-4700] The set_magic_quotes_runtime function in PHP 5.3.2 and 5.3.3, when the MySQLi extension is used, does not properly interact with use of the mysqli_fetch_assoc function, which might make it easier for context-dependent attackers to conduct SQL injection attacks via crafted input that had been properly handled in earlier PHP versions.
| [CVE-2010-3840] The Gis_line_string::init_from_wkb function in sql/spatial.cc in MySQL 5.1 before 5.1.51 allows remote authenticated users to cause a denial of service (server crash) by calling the PolyFromWKB function with Well-Known Binary (WKB) data containing a crafted number of (1) line strings or (2) line points.
| [CVE-2010-3839] MySQL 5.1 before 5.1.51 and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (infinite loop) via multiple invocations of a (1) prepared statement or (2) stored procedure that creates a query with nested JOIN statements.
| [CVE-2010-3838] MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a query that uses the (1) GREATEST or (2) LEAST function with a mixed list of numeric and LONGBLOB arguments, which is not properly handled when the function’s result is "processed using an intermediate temporary table."
| [CVE-2010-3837] MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a prepared statement that uses GROUP_CONCAT with the WITH ROLLUP modifier, probably triggering a use-after-free error when a copied object is modified in a way that also affects the original object.
| [CVE-2010-3836] MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (assertion failure and server crash) via vectors related to view preparation, pre-evaluation of LIKE predicates, and IN Optimizers.
| [CVE-2010-3835] MySQL 5.1 before 5.1.51 and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (mysqld server crash) by performing a user-variable assignment in a logical expression that is calculated and stored in a temporary table for GROUP BY, then causing the expression value to be used after the table is created, which causes the expression to be re-evaluated instead of accessing its value from the table.
| [CVE-2010-3834] Unspecified vulnerability in MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via vectors related to "materializing a derived table that required a temporary table for grouping" and "user variable assignments."
| [CVE-2010-3833] MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 does not properly propagate type errors, which allows remote attackers to cause a denial of service (server crash) via crafted arguments to extreme-value functions such as (1) LEAST and (2) GREATEST, related to KILL_BAD_DATA and a "CREATE TABLE ... SELECT."
| [CVE-2010-3683] Oracle MySQL 5.1 before 5.1.49 and 5.5 before 5.5.5 sends an OK packet when a LOAD DATA INFILE request generates SQL errors, which allows remote authenticated users to cause a den

ial of service (mysqld daemon crash) via a crafted request.
| [CVE-2010-3682] Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated us ers to cause a denial of service (mysqld daemon crash) by using EXPLAIN with crafted "SELECT ... UNIO N ... ORDER BY (SELECT ... WHERE ...)" statements, which triggers a NULL pointer dereference in the It em_singlerow_subselect::store function.
| [CVE-2010-3681] Oracle MySQL 5.1 before 5.1.49 and 5.5 before 5.5.5 allows remote authenticated use rs to cause a denial of service (mysqld daemon crash) by using the HANDLER interface and performing " alternate reads from two indexes on a table," which triggers an assertion failure.
| [CVE-2010-3680] Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by creating temporary tables with nullable columns while using InnoDB, which triggers an assertion failure.
| [CVE-2010-3679] Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via certain arguments to the BINLOG command, which triggers an acc ess of uninitialized memory, as demonstrated by valgrind.
| [CVE-2010-3678] Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (crash) via (1) IN or (2) CASE operations with NULL arguments that are explicitly specified or in directly provided by the WITH ROLLUP modifier.
| [CVE-2010-3677] Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated us ers to cause a denial of service (mysqld daemon crash) via a join query that uses a table with a unique S ET column.
| [CVE-2010-3676] storage/innobase/dict/dict0crea.c in mysqld in Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (assertion failure) by modifying the (1) innodb_file _format or (2) innodb_file_per_table configuration parameters for the InnoDB storage engine, then executi ng a DDL statement.
| [CVE-2010-3064] Stack-based buffer overflow in the php_mysqlnd_auth_write function in the Mysqlnd e xtension in PHP 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long (1) username or (2) database name argument to the (a) m ysql_connect or (b) mysqli_connect function.
| [CVE-2010-3063] The php_mysqlnd_read_error_from_line function in the Mysqlnd extension in PHP 5.3 through 5.3.2 does not properly calculate a buffer length, which allows context-dependent attackers to trig ger a heap-based buffer overflow via crafted inputs that cause a negative length value to be used.
| [CVE-2010-3062] mysqlnd_wireprotocol.c in the Mysqlnd extension in PHP 5.3 through 5.3.2 allows rem ote attackers to (1) read sensitive memory via a modified length value, which is not properly handled by th e php_mysqlnd_ok_read function
| [CVE-2010-3056] Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 2.11.x before 2.11.10 .1 and 3.x before 3.3.5.1 allow remote attackers to inject arbitrary web script or HTML via vectors related t o (1) db_search.php, (2) db_sql.php, (3) db_structure.php, (4) js/messages.php, (5) libraries/common.lib.p hp, (6) libraries/database_interface.lib.php, (7) libraries/dbi/mysql.dbi.lib.php, (8) libraries/dbi/mysqli.dbi.lib .php, (9) libraries/db_info.inc.php, (10) libraries/sanitizing.lib.php, (11) libraries/sqlparser.lib.php, (12) serv er_databases.php, (13) server_privileges.php, (14) setup/config.php, (15) sql.php, (16) tbl_replace.php, a nd (17) tbl_sql.php.
| [CVE-2010-2008] MySQL before 5.1.48 allows remote authenticated users with alter database privileges to cause a denial of service (server crash and database loss) via an ALTER DATABASE command with a #mysql50# string followed by a . (dot), .. (dot dot), ../ (dot dot slash) or similar sequence, and an UPGR ADE DATA DIRECTORY NAME command, which causes MySQL to move certain directories to the serve r data directory.
| [CVE-2010-2003] Cross-site scripting (XSS) vulnerability in misc/get_admin.php in Advanced Poll 2.08 al lows remote attackers to inject arbitrary web script or HTML via the mysql_host parameter.
| [CVE-2010-1865] Multiple SQL injection vulnerabilities in ClanSphere 2009.0.3 and earlier allow remote attackers to execute arbitrary SQL commands via (1) the IP address to the cs_getip function in generate.p hp in the Captcha module, or (2) the s_email parameter to the cs_sql_select function in the MySQL datab ase driver (mysql.php).
| [CVE-2010-1850] Buffer overflow in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote auth enticated users to execute arbitrary code via a COM_FIELD_LIST command with a long table name.
| [CVE-2010-1849] The my_net_skip_rest function in sql/net_serv.cc in MySQL 5.0 through 5.0.91 and 5.

1 before 5.1.47 allows remote attackers to cause a denial of service (CPU and bandwidth consumption) b y sending a large number of packets that exceed the maximum length.
| [CVE-2010-1848] Directory traversal vulnerability in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 all ows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables , and on 5.1 to read or delete content of arbitrary tables, via a .. (dot dot) in a table name.
| [CVE-2010-1626] MySQL before 5.1.46 allows local users to delete the data and index files of another u ser's MyISAM table via a symlink attack in conjunction with the DROP TABLE command, a different vulne rability than CVE-2008-4098 and CVE-2008-7247.
| [CVE-2010-1621] The mysql_uninstall_plugin function in sql/sql_plugin.cc in MySQL 5.1 before 5.1.46 d oes not check privileges before uninstalling a plugin, which allows remote attackers to uninstall arbitrary pl ugins via the UNINSTALL PLUGIN command.
| [CVE-2010-1583] SQL injection vulnerability in the loadByKey function in the TznDbConnection class in t zn_mysql.php in Tirzen (aka TZN) Framework 1.5, as used in TaskFreak! before 0.6.3, allows remote atta ckers to execute arbitrary SQL commands via the username field in a login action.
| [CVE-2010-0336] Unspecified vulnerability in the kiddog_mysqldumper (kiddog_mysqldumper) extension 0.0.3 and earlier for TYPO3 allows remote attackers to obtain sensitive information via unknown attack v ectors.
| [CVE-2010-0124] Employee Timeclock Software 0.99 places the database password on the mysqldump command line, which allows local users to obtain sensitive information by listing the process.
| [CVE-2009-5026] The executable comment feature in MySQL 5.0.x before 5.0.93 and 5.1.x before 5.1.5 0, when running in certain slave configurations in which the slave is running a newer version than the mas ter, allows remote attackers to execute arbitrary SQL commands via custom comments.
| [CVE-2009-4833] MySQL Connector/NET before 6.0.4, when using encryption, does not verify SSL certif icates during connection, which allows remote attackers to perform a man-in-the-middle attack with a spo ofed SSL certificate.
| [CVE-2009-4484] Multiple stack-based buffer overflows in the CertDecoder::GetName function in src/asn .cpp in TaoCrypt in yaSSL before 1.9.9, as used in mysqld in MySQL 5.0.x before 5.0.90, MySQL 5.1.x be fore 5.1.43, MySQL 5.5.x through 5.5.0-m2, and other products, allow remote attackers to execute arbitrar y code or cause a denial of service (memory corruption and daemon crash) by establishing an SSL conne ction and sending an X.509 client certificate with a crafted name field, as demonstrated by mysql_overflo w1.py and the vd_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: this was originally reporte d for MySQL 5.0.51a.
| [CVE-2009-4030] MySQL 5.1.x before 5.1.41 allows local users to bypass certain privilege checks by cal ling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTOR Y arguments that are originally associated with pathnames without symlinks, and that can point to tables c reated at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MyS QL data home directory, related to incorrect calculation of the mysql_unpacked_real_data_home value. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4098 and CVE-2008-2079.
| [CVE-2009-4028] The vio_verify_callback function in viosslfactories.c in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41, when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates, w hich allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certific ate, as demonstrated by a certificate presented by a server linked against the yaSSL library.
| [CVE-2009-4019] mysqld in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 does not (1) properly ha ndle errors during execution of certain SELECT statements with subqueries, and does not (2) preserve ce rtain null_value flags during execution of statements that use the GeomFromWKB function, which allows r emote authenticated users to cause a denial of service (daemon crash) via a crafted statement.
| [CVE-2009-3696] Cross-site scripting (XSS) vulnerability in phpMyAdmin 2.11.x before 2.11.9.6 and 3.x before 3.2.2.1 allows remote attackers to inject arbitrary web script or HTML via a crafted name for a MyS QL table.
| [CVE-2009-3102] The doHotCopy subroutine in socket-server.pl in Zmanda Recovery Manager (ZRM) fo r MySQL 2.x before 2.1.1 allows remote attackers to execute arbitrary commands via vectors involving a c rafted $MYSQL_BINPATH variable.
| [CVE-2009-2942] The mysql-ocaml bindings 1.0.4 for MySQL do not properly support the mysql_real_es cape_string function, which might allow remote attackers to leverage escaping issues involving multibyte character encodings.

| [CVE-2009-2446] Multiple format string vulnerabilities in the dispatch_command function in libmysqld/sql_parse.cc in mysqld in MySQL 4.0.0 through 5.0.83 allow remote authenticated users to cause a denial of service (daemon crash) and possibly have unspecified other impact via format string specifiers in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request. NOTE: some of these details are obtained from third party information.
| [CVE-2009-1246] Multiple directory traversal vulnerabilities in Blogplus 1.0 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) row_mysql_blocks_center_down[file] parameter to includes/block_center_down.php
| [CVE-2009-1208] SQL injection vulnerability in auth2db 0.2.5, and possibly other versions before 0.2.7, uses the addslashes function instead of the mysql_real_escape_string function, which allows remote attackers to conduct SQL injection attacks using multibyte character encodings.
| [CVE-2009-0919] XAMPP installs multiple packages with insecure default passwords, which makes it easier for remote attackers to obtain access via (1) the "lampp" default password for the "nobody" account within the included ProFTPD installation, (2) a blank default password for the "root" account within the included MySQL installation, (3) a blank default password for the "pma" account within the phpMyAdmin installation, and possibly other unspecified passwords. NOTE: this was originally reported as a problem in DFLabs PTK, but this issue affects any product that is installed within the XAMPP environment, and should not be viewed as a vulnerability within that product. NOTE: DFLabs states that PTK is intended for use in a laboratory with "no contact from / to internet."
| [CVE-2009-0819] sql/item_xmlfunc.cc in MySQL 5.1 before 5.1.32 and 6.0 before 6.0.10 allows remote authenticated users to cause a denial of service (crash) via "an XPath expression employing a scalar expression as a FilterExpr with ExtractValue() or UpdateXML()," which triggers an assertion failure.
| [CVE-2009-0617] Cisco Application Networking Manager (ANM) before 2.0 uses a default MySQL root password, which makes it easier for remote attackers to execute arbitrary operating-system commands or change system files.
| [CVE-2009-0543] ProFTPD Server 1.3.1, with NLS support enabled, allows remote attackers to bypass SQL injection protection mechanisms via invalid, encoded multibyte characters, which are not properly handled in (1) mod_sql_mysql and (2) mod_sql_postgres.
| [CVE-2008-7247] sql/sql_table.cc in MySQL 5.0.x through 5.0.88, 5.1.x through 5.1.41, and 6.0 before 6.0.9-alpha, when the data home directory contains a symlink to a different filesystem, allows remote authenticated users to bypass intended access restrictions by calling CREATE TABLE with a (1) DATA DIRECTORY or (2) INDEX DIRECTORY argument referring to a subdirectory that requires following this symlink.
| [CVE-2008-6992] GreenSQL Firewall (greensql-fw), possibly before 0.9.2 or 0.9.4, allows remote attackers to bypass the SQL injection protection mechanism via a WHERE clause containing an expression such as "x=y=z", which is successfully parsed by MySQL.
| [CVE-2008-6813] SQL injection vulnerability in index.php in phpWebNews 0.2 MySQL Edition allows remote attackers to execute arbitrary SQL commands via the id_kat parameter.
| [CVE-2008-6812] SQL injection vulnerability in bukutamu.php in phpWebNews 0.2 MySQL Edition allows remote attackers to execute arbitrary SQL commands via the det parameter.
| [CVE-2008-6655] Multiple cross-site scripting (XSS) vulnerabilities in GEDCOM_TO_MYSQL 2 allow remote attackers to inject arbitrary web script or HTML via the (1) nom_branche and (2) nom parameters to php/prenom.php
| [CVE-2008-6287] Multiple PHP remote file inclusion vulnerabilities in Broadcast Machine 0.1 allow remote attackers to execute arbitrary PHP code via a URL in the baseDir parameter to (1) MySQLController.php, (2) SQLController.php, (3) SetupController.php, (4) VideoController.php, and (5) ViewController.php in controllers/.
| [CVE-2008-6193] Sam Crew MyBlog stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.
| [CVE-2008-5847] Constructr CMS 3.02.5 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information by reading the hash column.
| [CVE-2008-5738] Nodstrum MySQL Calendar 1.1 and 1.2 allows remote attackers to bypass authentication and gain administrative access by setting the nodstrumCalendarV2 cookie to 1. NOTE: some of these details are obtained from third party information.
| [CVE-2008-5737] SQL injection vulnerability in index.php in Nodstrum MySQL Calendar 1.1 and 1.2 allo

ws remote attackers to execute arbitrary SQL commands via the username parameter.
| [CVE-2008-5069] SQL injection vulnerability in go.php in Panuwat PromoteWeb MySQL, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the id parameter.
| [CVE-2008-4456] Cross-site scripting (XSS) vulnerability in the command-line client in MySQL 5.0.26 through 5.0.45, and other versions including versions later than 5.0.45, when the --html option is enabled, allows attackers to inject arbitrary web script or HTML by placing it in a database cell, which might be accessed by this client when composing an HTML document. NOTE: as of 20081031, the issue has not been fixed in MySQL 5.0.67.
| [CVE-2008-4455] Directory traversal vulnerability in index.php in EKINdesigns MySQL Quick Admin 1.5.5 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to read and execute arbitrary files via a .. (dot dot) in the language cookie.
| [CVE-2008-4454] Directory traversal vulnerability in EKINdesigns MySQL Quick Admin 1.5.5 allows remote attackers to read and execute arbitrary files via a .. (dot dot) in the lang parameter to actions.php. NOTE: the provenance of this information is unknown
| [CVE-2008-4180] Unspecified vulnerability in db.php in NooMS 1.1 allows remote attackers to conduct brute force attacks against passwords via a username in the g_dbuser parameter and a password in the g_dbpwd parameter, and possibly a "localhost" g_dbhost parameter value, related to a "Mysql Remote Brute Force Vulnerability."
| [CVE-2008-4106] WordPress before 2.6.2 does not properly handle MySQL warnings about insertion of username strings that exceed the maximum column width of the user_login column, and does not properly handle space characters when comparing usernames, which allows remote attackers to change an arbitrary user’s password to a random value by registering a similar username and then requesting a password reset, related to a "SQL column truncation vulnerability." NOTE: the attacker can discover the random password by also exploiting CVE-2008-4107.
| [CVE-2008-4098] MySQL before 5.0.67 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL home data directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4097.
| [CVE-2008-4097] MySQL 5.0.51a allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are associated with symlinks within pathnames for subdirectories of the MySQL home data directory, which are followed when tables are created in the future. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-2079.
| [CVE-2008-3963] MySQL 5.0 before 5.0.66, 5.1 before 5.1.26, and 6.0 before 6.0.6 does not properly handle a b’’ (b single-quote single-quote) token, aka an empty bit-string literal, which allows remote attackers to cause a denial of service (daemon crash) by using this token in a SQL statement.
| [CVE-2008-3846] Cross-site scripting (XSS) vulnerability in mysql-lists 1.2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
| [CVE-2008-3840] Crafty Syntax Live Help (CSLH) 2.14.6 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.
| [CVE-2008-3820] Cisco Security Manager 3.1 and 3.2 before 3.2.2, when Cisco IPS Event Viewer (IEV) is used, exposes TCP ports used by the MySQL daemon and IEV server, which allows remote attackers to obtain "root access" to IEV via unspecified use of TCP sessions to these ports.
| [CVE-2008-3582] SQL injection vulnerability in login.php in Keld PHP-MySQL News Script 0.7.1 allows remote attackers to execute arbitrary SQL commands via the username parameter.
| [CVE-2008-3090] Multiple SQL injection vulnerabilities in index.php in BlognPlus (BURO GUN +) 2.5.5 MySQL and PostgreSQL editions allow remote attackers to execute arbitrary SQL commands via the (1) p, (2) e, (3) d, and (4) m parameters, a different vulnerability than CVE-2008-2819.
| [CVE-2008-2881] Relative Real Estate Systems 3.0 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.
| [CVE-2008-2857] AlstraSoft AskMe Pro 2.1 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.
| [CVE-2008-2819] SQL injection vulnerability in BlognPlus (BURO GUN +) 2.5.4 and earlier MySQL and PostgreSQL editions allows remote attackers to execute arbitrary SQL commands via unspecified vectors

.
| [CVE-2008-2667] SQL injection vulnerability in the Courier Authentication Library (aka courier-authlib) be fore 0.60.6 on SUSE openSUSE 10.3 and 11.0, and other platforms, when MySQL and a non-Latin chara cter set are used, allows remote attackers to execute arbitrary SQL commands via the username and uns pecified other vectors.
| [CVE-2008-2384] SQL injection vulnerability in mod_auth_mysql.c in the mod-auth-mysql (aka libapache 2-mod-auth-mysql) module for the Apache HTTP Server 2.x, when configured to use a multibyte characte r set that allows a \ (backslash) as part of the character encoding, allows remote attackers to execute arbit rary SQL commands via unspecified inputs in a login request.
| [CVE-2008-2079] MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL ho me data directory, which can point to tables that are created in the future.
| [CVE-2008-2029] Multiple SQL injection vulnerabilities in (1) setup_mysql.php and (2) setup_options.php in miniBB 2.2 and possibly earlier, when register_globals is enabled, allow remote attackers to execute ar bitrary SQL commands via the xtr parameter in a userinfo action to index.php.
| [CVE-2008-1711] Terong PHP Photo Gallery (aka Advanced Web Photo Gallery) 1.0 stores passwords i n cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive informatio n.
| [CVE-2008-1567] phpMyAdmin before 2.11.5.1 stores the MySQL (1) username and (2) password, and t he (3) Blowfish secret key, in cleartext in a Session file under /tmp, which allows local users to obtain sen sitive information.
| [CVE-2008-1486] SQL injection vulnerability in Phorum before 5.2.6, when mysql_use_ft is disabled, allo ws remote attackers to execute arbitrary SQL commands via the non-fulltext search.
| [CVE-2008-0249] PHP Webquest 2.6 allows remote attackers to retrieve database credentials via a dire ct request to admin/backup_phpwebquest.php, which leaks the credentials in an error message if a call to /usr/bin/mysqldump fails. NOTE: this might only be an issue in limited environments.
| [CVE-2008-0227] yaSSL 1.7.5 and earlier, as used in MySQL and possibly other products, allows remot e attackers to cause a denial of service (crash) via a Hello packet containing a large size value, which trig gers a buffer over-read in the HASHwithTransform::Update function in hash.cpp.
| [CVE-2008-0226] Multiple buffer overflows in yaSSL 1.7.5 and earlier, as used in MySQL and possibly ot her products, allow remote attackers to execute arbitrary code via (1) the ProcessOldClientHello function i n handshake.cpp or (2) "input_buffer& operator>>" in yassl_imp.cpp.
| [CVE-2007-6512] PHP MySQL Banner Exchange 2.2.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain database information via a direct r equest to inc/lib.inc.
| [CVE-2007-6418] The libdspam7-drv-mysql cron job in Debian GNU/Linux includes the MySQL dspam d atabase password in a command line argument, which might allow local users to read the password by lis ting the process and its arguments.
| [CVE-2007-6345] SQL injection vulnerability in aurora framework before 20071208 allows remote attack ers to execute arbitrary SQL commands via unspecified vectors, possibly the value parameter to the pack _var function in module/db.lib/db_mysql.lib. NOTE: some of these details are obtained from third party inf ormation.
| [CVE-2007-6313] MySQL Server 5.1.x before 5.1.23 and 6.0.x before 6.0.4 does not check the rights of t he entity executing BINLOG, which allows remote authorized users to execute arbitrary BINLOG stateme nts.
| [CVE-2007-6304] The federated engine in MySQL 5.0.x before 5.0.51a, 5.1.x before 5.1.23, and 6.0.x b efore 6.0.4, when performing a certain SHOW TABLE STATUS query, allows remote MySQL servers to c ause a denial of service (federated handler crash and daemon crash) via a response that lacks the minim um required number of columns.
| [CVE-2007-6303] MySQL 5.0.x before 5.0.51a, 5.1.x before 5.1.23, and 6.0.x before 6.0.4 does not upd ate the DEFINER value of a view when the view is altered, which allows remote authenticated users to ga in privileges via a sequence of statements including a CREATE SQL SECURITY DEFINER VIEW statem ent and an ALTER VIEW statement.
| [CVE-2007-6081] AdventNet EventLog Analyzer build 4030 for Windows, and possibly other versions an

d platforms, installs a mysql instance with a default "root" account without a password, which allows remot e attackers to gain privileges and modify logs.
| [CVE-2007-5970] MySQL 5.1.x before 5.1.23 and 6.0.x before 6.0.4 allows remote authenticated users t o gain privileges on arbitrary tables via unspecified vectors involving use of table-level DATA DIRECTOR Y and INDEX DIRECTORY options when creating a partitioned table with the same name as a table on w hich the user lacks privileges.
| [CVE-2007-5969] MySQL Community Server 5.0.x before 5.0.51, Enterprise Server 5.0.x before 5.0.52, Server 5.1.x before 5.1.23, and Server 6.0.x before 6.0.4, when a table relies on symlinks created through explicit DATA DIRECTORY and INDEX DIRECTORY options, allows remote authenticated users to over write system table information and gain privileges via a RENAME TABLE statement that changes the sym link to point to an existing file.
| [CVE-2007-5925] The convert_search_mode_to_innobase function in ha_innodb.cc in the InnoDB engin e in MySQL 5.1.23-BK and earlier allows remote authenticated users to cause a denial of service (databa se crash) via a certain CONTAINS operation on an indexed column, which triggers an assertion error.
| [CVE-2007-5646] SQL injection vulnerability in Sources/Search.php in Simple Machines Forum (SMF) 1. 1.3, when MySQL 5 is used, allows remote attackers to execute arbitrary SQL commands via the userspe c parameter in a search2 action to index.php.
| [CVE-2007-5626] make_catalog_backup in Bacula 2.2.5, and probably earlier, sends a MySQL passwor d as a command line argument, and sometimes transmits cleartext e-mail containing this command line, which allows context-dependent attackers to obtain the password by listing the process and its arguments , or by sniffing the network.
| [CVE-2007-5488] Multiple SQL injection vulnerabilities in cdr_addon_mysql in Asterisk-Addons before 1. 2.8, and 1.4.x before 1.4.4, allow remote attackers to execute arbitrary SQL commands via the (1) source and (2) destination numbers, and probably (3) SIP URI, when inserting a record.
| [CVE-2007-4889] The MySQL extension in PHP 5.2.4 and earlier allows remote attackers to bypass safe _mode and open_basedir restrictions via the MySQL (1) LOAD_FILE, (2) INTO DUMPFILE, and (3) INTO OUTFILE functions, a different issue than CVE-2007-3997.
| [CVE-2007-3997] The (1) MySQL and (2) MySQLi extensions in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to bypass safe_mode and open_basedir restrictions via MySQL LOCAL INF ILE operations, as demonstrated by a query with LOAD DATA LOCAL INFILE.
| [CVE-2007-3782] MySQL Community Server before 5.0.45 allows remote authenticated users to gain up date privileges for a table in another database via a view that refers to this external table.
| [CVE-2007-3781] MySQL Community Server before 5.0.45 does not require privileges such as SELECT for the source table in a CREATE TABLE LIKE statement, which allows remote authenticated users to obt ain sensitive information such as the table structure.
| [CVE-2007-3780] MySQL Community Server before 5.0.45 allows remote attackers to cause a denial of service (daemon crash) via a malformed password packet in the connection protocol.
| [CVE-2007-3567] MySQLDumper 1.21b through 1.23 REV227 uses a "Limit GET" statement in the .htac cess authentication mechanism, which allows remote attackers to bypass authentication requirements via HTTP POST requests.
| [CVE-2007-2857] PHP remote file inclusion vulnerability in sample/xls2mysql in ABC Excel Parser Pro 4. 0 allows remote attackers to execute arbitrary PHP code via a URL in the parser_path parameter.
| [CVE-2007-2766] lib/backup-methods.sh in Backup Manager before 0.7.6 provides the MySQL passwor d as a plaintext command line argument, which allows local users to obtain this password by listing the pr ocess and its arguments, related to lib/backup-methods.sh.
| [CVE-2007-2693] MySQL before 5.1.18 allows remote authenticated users without SELECT privileges to obtain sensitive information from partitioned tables via an ALTER TABLE statement.
| [CVE-2007-2692] The mysql_change_db function in MySQL 5.0.x before 5.0.40 and 5.1.x before 5.1.18 does not restore THD::db_access privileges when returning from SQL SECURITY INVOKER stored routin es, which allows remote authenticated users to gain privileges.
| [CVE-2007-2691] MySQL before 4.1.23, 5.0.x before 5.0.42, and 5.1.x before 5.1.18 does not require th e DROP privilege for RENAME TABLE statements, which allows remote authenticated users to rename a rbitrary tables.
| [CVE-2007-2583] The in_decimal::set function in item_cmpfunc.cc in MySQL before 5.0.40, and 5.1 befo re 5.1.18-beta, allows context-dependent attackers to cause a denial of service (crash) via a crafted IF cla

use that results in a divide-by-zero error and a NULL pointer dereference.
| [CVE-2007-2554] Associated Press (AP) Newspower 4.0.1 and earlier uses a default blank password for the MySQL root account, which allows remote attackers to insert or modify news articles via shows.tblscript.
| [CVE-2007-2429] ManageEngine PasswordManager Pro (PMP) allows remote attackers to obtain administrative access to a database by injecting a certain command line for the mysql program, as demonstrated by the "-port 2345" and "-u root" arguments. NOTE: the provenance of this information is unknown
| [CVE-2007-2364] Multiple PHP remote file inclusion vulnerabilities in burnCMS 0.2 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the root parameter to (1) mysql.class.php or (2) postgres.class.php in lib/db/
| [CVE-2007-2204] Multiple PHP remote file inclusion vulnerabilities in GPL PHP Board (GPB) unstable-2001.11.14-1 allow remote attackers to execute arbitrary PHP code via a URL in the root_path parameter to (1) db.mysql.inc.php or (2) gpb.inc.php in include/, or the (3) theme parameter to themes/ubb/login.php.
| [CVE-2007-2016] Cross-site scripting (XSS) vulnerability in mysql/phpinfo.php in phpMyAdmin 2.6.1 allows remote attackers to inject arbitrary web script or HTML via the lang[] parameter.
| [CVE-2007-1779] Multiple SQL injection vulnerabilities in the MySQL back-end in Advanced Website Creator (AWC) before 1.9.0 might allow remote attackers to execute arbitrary SQL commands via unspecified parameters, related to use of mysql_escape_string instead of mysql_real_escape_string.
| [CVE-2007-1778] PHP remote file inclusion vulnerability in db/mysql.php in the Eve-Nuke 0.1 (EN-Forums) module for PHP-Nuke allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.
| [CVE-2007-1548] SQL injection vulnerability in functions/functions_filters.asp in Web Wiz Forums before 8.05a (MySQL version) does not properly filter certain characters in SQL commands, which allows remote attackers to execute arbitrary SQL commands via \"' (backslash double-quote quote) sequences, which are collapsed into \'', as demonstrated via the name parameter to forum/pop_up_member_search.asp.
| [CVE-2007-1455] Multiple absolute path traversal vulnerabilities in Fantastico, as used with cPanel 10.x, allow remote authenticated users to include and execute arbitrary local files via (1) the userlanguage parameter to includes/load_language.php or (2) the fantasticopath parameter to includes/mysqlconfig.php and certain other files.
| [CVE-2007-1439] PHP remote file inclusion vulnerability in ressourcen/dbopen.php in bitesser MySQL Commander 2.7 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the home parameter.
| [CVE-2007-1420] MySQL 5.x before 5.0.36 allows local users to cause a denial of service (database crash) by performing information_schema table subselects and using ORDER BY to sort a single-row result, which prevents certain structure elements from being initialized and triggers a NULL dereference in the filesort function.
| [CVE-2007-1167] inc/filebrowser/browser.php in deV!L‘z Clanportal (DZCP) 1.4.5 and earlier allows remote attackers to obtain MySQL data via the inc/mysql.php value of the file parameter.
| [CVE-2007-1111] Multiple cross-site scripting (XSS) vulnerabilities in ActiveCalendar 1.2.0 allow remote attackers to inject arbitrary web script or HTML via the css parameter to (1) flatevents.php, (2) js.php, (3) mysqlevents.php, (4) m_2.php, (5) m_3.php, (6) m_4.php, (7) xmlevents.php, (8) y_2.php, or (9) y_3.php in data/.
| [CVE-2007-0926] The dologin function in guestbook.php in KvGuestbook 1.0 Beta allows remote attackers to gain administrative privileges, probably via modified $mysql['pass'] and $gbpass variables.
| [CVE-2007-0890] Cross-site scripting (XSS) vulnerability in scripts/passwdmysql in cPanel WebHost Manager (WHM) 11.0.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the password parameter.
| [CVE-2007-0828] PHP remote file inclusion vulnerability in affichearticles.php3 in MySQLNewsEngine allows remote attackers to execute arbitrary PHP code via a URL in the newsenginedir parameter.
| [CVE-2007-0167] Multiple PHP file inclusion vulnerabilities in WGS-PPC (aka PPC Search Engine), as distributed with other aliases, allow remote attackers to execute arbitrary PHP code via a URL in the INC parameter in (1) config_admin.php, (2) config_main.php, (3) config_member.php, and (4) mysql_config.php in config/
| [CVE-2007-0124] Unspecified vulnerability in Drupal before 4.6.11, and 4.7 before 4.7.5, when MySQL is used, allows remote authenticated users to cause a denial of service by poisoning the page cache via u

nspecified vectors, which triggers erroneous 404 HTTP errors for pages that exist.
| [CVE-2006-7232] sql_select.cc in MySQL 5.0.x before 5.0.32 and 5.1.x before 5.1.14 allows remote auth enticated users to cause a denial of service (crash) via an EXPLAIN SELECT FROM on the INFORMATI ON_SCHEMA table, as originally demonstrated using ORDER BY.
| [CVE-2006-7194] PHP remote file inclusion vulnerability in modules/Mysqlfinder/MysqlfinderAdmin.php i n Agora 1.4 RC1, when register_globals is enabled, allows remote attackers to execute arbitrary PHP cod e via a URL in the _SESSION[PATH_COMPOSANT] parameter.
| [CVE-2006-6948] MyODBC Japanese conversion edition 3.51.06, 2.50.29, and 2.50.25 allows remote at tackers to cause a denial of service via a certain string in a response, which has unspecified impact on th e MySQL database.
| [CVE-2006-6457] tiki-wiki_rss.php in Tikiwiki 1.9.5, 1.9.2, and possibly other versions allows remote atta ckers to obtain sensitive information (MySQL username and password) via an invalid (large or negative) v er parameter, which leaks the information in an error message.
| [CVE-2006-6378] BTSaveMySql 1.2 stores sensitive data under the web root with insufficient access co ntrol, which allows remote attackers to obtain configuration and save files via direct requests.
| [CVE-2006-6254] administration/telecharger.php in Cahier de texte 2.0 allows remote attackers to obtain unparsed content (source code) of files via the chemin parameter, as demonstrated using directory traver sal sequences to obtain the MySQL username and password from conn_cahier_de_texte.php. NOTE: it i s not clear whether the scope of this issue extends above the web document root, and whether directory t raversal is the primary vulnerability.
| [CVE-2006-5893] Multiple PHP remote file inclusion vulnerabilities in iWonder Designs Storystream 0.4. 0.0 allow remote attackers to execute arbitrary PHP code via a URL in the baseDir parameter to (1) mysql .php and (2) mysqli.php in include/classes/pear/DB/.
| [CVE-2006-5702] Tikiwiki 1.9.5 allows remote attackers to obtain sensitive information (MySQL usernam e and password) via an empty sort_mode parameter in (1) tiki-listpages.php, (2) tiki-lastchanges.php, (3) messu-archive.php, (4) messu-mailbox.php, (5) messu-sent.php, (6) tiki-directory_add_site.php, (7) tiki-dir ectory_ranking.php, (8) tiki-directory_search.php, (9) tiki-forums.php, (10) tiki-view_forum.php, (11) tiki-fri ends.php, (12) tiki-list_blogs.php, (13) tiki-list_faqs.php, (14) tiki-list_trackers.php, (15) tiki-list_users.php, (16) tiki-my_tiki.php, (17) tiki-notepad_list.php, (18) tiki-orphan_pages.php, (19) tiki-shoutbox.php, (20) tiki -usermenu.php, and (21) tiki-webmail_contacts.php, which reveal the information in certain database erro r messages.
| [CVE-2006-5675] Multiple unspecified vulnerabilities in Pentaho Business Intelligence (BI) Suite before 1 .2 RC3 (1.2.0.470-RC3) have unknown impact and attack vectors, related to "MySQL Scripts need chang es for security," possibly SQL injection vulnerabilities associated with these scripts.
| [CVE-2006-5381] Contenido CMS stores sensitive data under the web root with insufficient access contr ol, which allows remote attackers to obtain database credentials and other information via a direct request to (1) db_msql.inc, (2) db_mssql.inc, (3) db_mysqli.inc, (4) db_oci8.inc, (5) db_odbc.inc, (6) db_oracle.inc , (7) db_pgsql.inc, or (8) db_sybase.inc in the conlib/ directory.
| [CVE-2006-5264] Cross-site scripting (XSS) vulnerability in sql.php in MysqlDumper 1.21 b6 allows remo te attackers to inject arbitrary web script or HTML via the db parameter.
| [CVE-2006-5127] Multiple cross-site scripting (XSS) vulnerabilities in Bartels Schoene ConPresso before 4.0.5a allow remote attackers to inject arbitrary web script or HTML via (1) the nr parameter in detail.php, (2) the msg parameter in db_mysql.inc.php, and (3) the pos parameter in index.php.
| [CVE-2006-5079] PHP remote file inclusion vulnerability in class.mysql.php in Matt Humphrey paBugs 2. 0 Beta 3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the path_to_bt_d ir parameter.
| [CVE-2006-5065] PHP remote file inclusion vulnerability in libs/dbmax/mysql.php in ZoomStats 1.0.2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a U RL in the GLOBALS[lib][db][path] parameter.
| [CVE-2006-5029] SQL injection vulnerability in thread.php in WoltLab Burning Board (wBB) 2.3.x allows remote attackers to obtain the version numbers of PHP, MySQL, and wBB via the page parameter. NOT E: this issue might be a forced SQL error. Also, the original report was disputed by a third party for 2.3.3 a nd 2.3.4.
| [CVE-2006-5027] Jeroen Vennegoor JevonCMS, possibly pre alpha, allows remote attackers to obtain s ensitive information via a direct request for php/main/phplib files (1) db_msql.inc, (2) db_mssql.inc, (3) db

_mysql.inc, (4) db_oci8.inc, (5) db_odbc.inc, (6) db_oracle.inc, and (7) db_pgsql.inc
| [CVE-2006-5014] Unspecified vulnerability in cPanel before 10.9.0 12 Tree allows remote authenticated users to gain privileges via unspecified vectors in (1) mysqladmin and (2) hooksadmin.
| [CVE-2006-4994] Multiple unquoted Windows search path vulnerabilities in Apache Friends XAMPP 1.5.2 might allow local users to gain privileges via a malicious program file in %SYSTEMDRIVE%, which is run when XAMPP attempts to execute (1) FileZillaServer.exe, (2) mysqld-nt.exe, (3) Perl.exe, or (4) xamppcontrol.exe with an unquoted "Program Files" pathname.
| [CVE-2006-4835] Bluview Blue Magic Board (BMB) (aka BMForum) 5.5 allows remote attackers to obtain sensitive information via a direct request to (1) footer.php, (2) header.php, (3) db_mysql_error.php, (4) langlist.php, (5) sendmail.php, or (6) style.php, which reveals the path in various error messages.
| [CVE-2006-4578] export.php in The Address Book 1.04e writes username and password hash information into a publicly accessible file when dumping the MySQL database contents, which allows remote attackers to obtain sensitive information.
| [CVE-2006-4380] MySQL before 4.1.13 allows local users to cause a denial of service (persistent replication slave crash) via a query with multiupdate and subselects.
| [CVE-2006-4277] Multiple PHP remote file inclusion vulnerabilities in Tutti Nova 1.6 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the TNLIB_DIR parameter to (1) include/novalib/class.novaAdmin.mysql.php and (2) novalib/class.novaRead.mysql.php. NOTE: the provenance of this information is unknown
| [CVE-2006-4276] PHP remote file inclusion vulnerability in Tutti Nova 1.6 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the TNLIB_DIR parameter to novalib/class.novaEdit.mysql.php.
| [CVE-2006-4227] MySQL before 5.0.25 and 5.1 before 5.1.12 evaluates arguments of suid routines in the security context of the routine’s definer instead of the routine’s caller, which allows remote authenticated users to gain privileges through a routine that has been made available using GRANT EXECUTE.
| [CVE-2006-4226] MySQL before 4.1.21, 5.0 before 5.0.25, and 5.1 before 5.1.12, when run on case-sensitive filesystems, allows remote authenticated users to create or access a database when the database name differs only in case from a database for which they have permissions.
| [CVE-2006-4031] MySQL 4.1 before 4.1.21 and 5.0 before 5.0.24 allows a local user to access a table through a previously created MERGE table, even after the user’s privileges are revoked for the original table, which might violate intended security policy.
| [CVE-2006-3965] Banex PHP MySQL Banner Exchange 2.21 stores lib.inc under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information such as database usernames and passwords.
| [CVE-2006-3964] PHP remote file inclusion vulnerability in members.php in Banex PHP MySQL Banner Exchange 2.21 allows remote attackers to execute arbitrary PHP code via a URL in the cfg_root parameter.
| [CVE-2006-3963] Multiple SQL injection vulnerabilities in Banex PHP MySQL Banner Exchange 2.21 allow remote attackers to execute arbitrary SQL commands via the (1) site_name parameter to (a) signup.php, and the (2) id, (3) deleteuserbanner, (4) viewmem, (5) viewmemunb, (6) viewunmem,or (7) deleteuser parameters to (b) admin.php.
| [CVE-2006-3878] Opsware Network Automation System (NAS) 6.0 installs /etc/init.d/mysql with insecure permissions, which allows local users to read the root password for the MySQL MAX database or gain privileges by modifying /etc/init.d/mysql.
| [CVE-2006-3486] ** DISPUTED ** Off-by-one buffer overflow in the Instance_options::complete_initialization function in instance_options.cc in the Instance Manager in MySQL before 5.0.23 and 5.1 before 5.1.12 might allow local users to cause a denial of service (application crash) via unspecified vectors, which triggers the overflow when the convert_dirname function is called. NOTE: the vendor has disputed this issue via e-mail to CVE, saying that it is only exploitable when the user has access to the configuration file or the Instance Manager daemon. Due to intended functionality, this level of access would already allow the user to disrupt program operation, so this does not cross security boundaries and is not a vulnerability.
| [CVE-2006-3469] Format string vulnerability in time.cc in MySQL Server 4.1 before 4.1.21 and 5.0 before 1 April 2006 allows remote authenticated users to cause a denial of service (crash) via a format string instead of a date as the first parameter to the date_format function, which is later used in a formatted print call to display the error message.

| [CVE-2006-3330] Cross-site scripting (XSS) vulnerability in AddAsset1.php in PHP/MySQL Classifieds (PHP Classifieds) allows remote attackers to execute arbitrary SQL commands via the (1) ProductName (" Title" field), (2) url, and (3) Description parameters, possibly related to issues in add1.php.
| [CVE-2006-3329] SQL injection vulnerability in search.php in PHP/MySQL Classifieds (PHP Classifieds) allows remote attackers to execute arbitrary SQL commands via the rate parameter.
| [CVE-2006-3081] mysqld in MySQL 4.1.x before 4.1.18, 5.0.x before 5.0.19, and 5.1.x before 5.1.6 allow s remote authorized users to cause a denial of service (crash) via a NULL second argument to the str_to_ date function.
| [CVE-2006-2753] SQL injection vulnerability in MySQL 4.1.x before 4.1.20 and 5.0.x before 5.0.22 allow s context-dependent attackers to execute arbitrary SQL commands via crafted multibyte encodings in cha racter sets such as SJIS, BIG5, and GBK, which are not properly handled when the mysql_real_escape fu nction is used to escape the input.
| [CVE-2006-2750] Cross-site scripting (XSS) vulnerability in the do_mysql_query function in core.php for Open Searchable Image Catalogue (OSIC) before 0.7.0.1 allows remote attackers to inject arbitrary web scripts or HTML via failed SQL queries, which is reflected in an error message.
| [CVE-2006-2748] SQL injection vulnerability in the do_mysql_query function in core.php for Open Searc hable Image Catalogue (OSIC) before 0.7.0.1 allows remote attackers to inject arbitrary SQL commands via multiple vectors, as demonstrated by the (1) type parameter in adminfunctions.php and the (2) catalog ue_id parameter in editcatalogue.php.
| [CVE-2006-2742] SQL injection vulnerability in Drupal 4.6.x before 4.6.7 and 4.7.0 allows remote attacke rs to execute arbitrary SQL commands via the (1) count and (2) from variables to (a) database.mysql.inc, (b) database.pgsql.inc, and (c) database.mysqli.inc.
| [CVE-2006-2543] Xtreme Topsites 1.1 allows remote attackers to trigger MySQL errors and possibly con duct SQL injection attacks via unspecified vectors in join.php.
| [CVE-2006-2329] AngelineCMS 0.6.5 and earlier allow remote attackers to obtain sensitive information v ia a direct request for (1) adodb-access.inc.php, (2) adodb-ado.inc.php, (3) adodb-ado_access.inc, (4) ad odb-ado_mssql.inc.php, (5) adodb-borland_ibase, (6) adodb-csv.inc.php, (7) adodb-db2.inc.php, (8) adod b-fbsql.inc.php, (9) adodb-firebird.inc.php, (10) adodb-ibase.inc.php, (11) adodb-informix.inc.php, (12) ad odb-informix72.inc, (13) adodb-mssql.inc.php, (14) adodb-mssqlpo.inc.php, (15) adodb-mysql.inc.php, (16) adodb-mysqlt.inc.php, (17) adodb-oci8.inc.php, (18) adodb-oci805.inc.php, (19) adodb-oci8po.inc.php, a nd (20) adodb-odbc.inc.php, which reveal the path in various error messages
| [CVE-2006-2042] Adobe Dreamweaver 8 before 8.0.2 and MX 2004 can generate code that allows SQL injection attacks in the (1) ColdFusion, (2) PHP mySQL, (3) ASP, (4) ASP.NET, and (5) JSP server model s.
| [CVE-2006-1930] ** DISPUTED ** Multiple SQL injection vulnerabilities in userscript.php in Green Minut e 1.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) huserid, (2) pituus , or (3) date parameters. NOTE: this issue has been disputed by the vendor, saying "those parameters m entioned ARE checked (preg_match) before they are used in SQL-query... If someone decided to add S QL-injection stuff to certain parameter, they would see an error text, but only because _nothing_ was pas sed inside that parameter (to MySQL-database)." As allowed by the vendor, CVE investigated this report on 20060525 and found that the demo site demonstrated a non-sensitive SQL error when given standard SQL injection manipulations.
| [CVE-2006-1518] Buffer overflow in the open_table function in sql_base.cc in MySQL 5.0.x up to 5.0.20 might allow remote attackers to execute arbitrary code via crafted COM_TABLE_DUMP packets with inva lid length values.
| [CVE-2006-1517] sql_parse.cc in MySQL 4.0.x up to 4.0.26, 4.1.x up to 4.1.18, and 5.0.x up to 5.0.20 all ows remote attackers to obtain sensitive information via a COM_TABLE_DUMP request with an incorrect packet length, which includes portions of memory in an error message.
| [CVE-2006-1516] The check_connection function in sql_parse.cc in MySQL 4.0.x up to 4.0.26, 4.1.x up t o 4.1.18, and 5.0.x up to 5.0.20 allows remote attackers to read portions of memory via a username witho ut a trailing null byte, which causes a buffer over-read.
| [CVE-2006-1451] MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6, when setting up a new MySQ L database server, does not use the "New MySQL root password" that is provided, which causes the MyS QL root password to be blank and allows local users to gain full privileges to that database.
| [CVE-2006-1396] Multiple cross-site scripting (XSS) vulnerabilities in Cholod MySQL Based Message B

oard allow remote attackers to inject arbitrary web script or HTML via unknown vectors. NOTE: the prove nance of this information is unknown
| [CVE-2006-1395] SQL injection vulnerability in mb.cgi in Cholod MySQL Based Message Board allows r emote attackers to execute arbitrary SQL commands via unspecified vectors in a showmessage action, p ossibly the username parameter. NOTE: the provenance of this information is unknown
| [CVE-2006-1324] Cross-site scripting (XSS) vulnerability in acp/lib/class_db_mysql.php in Woltlab Burni ng Board (wBB) 2.3.4 allows remote attackers to inject arbitrary web script or HTML via the errormsg para meter when a SQL error is generated.
| [CVE-2006-1211] IBM Tivoli Micromuse Netcool/NeuSecure 3.0.236 configures a MySQL database to all ow connections from any source IP address with the ns database account, which allows remote attackers to bypass the Netcool/NeuSecure application layer and perform unauthorized database actions. NOTE: I BM has privately confirmed to CVE that a fix is available for these issues.
| [CVE-2006-1210] The web interface for IBM Tivoli Micromuse Netcool/NeuSecure 3.0.236 includes the MySQL database username and password in cleartext in body.phtml, which allows remote attackers to ga in privileges by reading the source. NOTE: IBM has privately confirmed to CVE that a fix is available for t hese issues.
| [CVE-2006-1112] Aztek Forum 4.0 allows remote attackers to obtain sensitive information via a long logi n value in a register form, which displays the installation path in a MySQL error message.
| [CVE-2006-1111] Aztek Forum 4.0 allows remote attackers to obtain sensitive information via a "*/*" in th e msg parameter to index.php, which reveals usernames and passwords in a MySQL error message, pos sibly due to a forced SQL error or SQL injection.
| [CVE-2006-0909] Invision Power Board (IPB) 2.1.4 and earlier allows remote attackers to view sensitive information via a direct request to multiple PHP scripts that include the full path in error messages, includi ng (1) PEAR/Text/Diff/Renderer/inline.php, (2) PEAR/Text/Diff/Renderer/unified.php, (3) PEAR/Text/Diff3. php, (4) class_db.php, (5) class_db_mysql.php, and (6) class_xml.php in the ips_kernel/ directory
| [CVE-2006-0903] MySQL 5.0.18 and earlier allows local users to bypass logging mechanisms via SQL q ueries that contain the NULL character, which are not properly handled by the mysql_real_query function. NOTE: this issue was originally reported for the mysql_query function, but the vendor states that since m ysql_query expects a null character, this is not an issue for mysql_query.
| [CVE-2006-0692] Multiple SQL injection vulnerabilities in Carey Briggs PHP/MYSQL Timesheet 1 and 2 allow remote attackers to execute arbitrary SQL commands via the (1) yr, (2) month, (3) day, and (4) job p arameters in (a) index.php and (b) changehrs.php.
| [CVE-2006-0369] ** DISPUTED ** MySQL 5.0.18 allows local users with access to a VIEW to obtain se nsitive information via the "SELECT * FROM information_schema.views
| [CVE-2006-0200] Format string vulnerability in the error-reporting feature in the mysqli extension in PHP 5.1.0 and 5.1.1 might allow remote attackers to execute arbitrary code via format string specifiers in MyS QL error messages.
| [CVE-2006-0146] The server.php test script in ADOdb for PHP before 4.70, as used in multiple products including (1) Mantis, (2) PostNuke, (3) Moodle, (4) Cacti, (5) Xaraya, (6) PHPOpenChat, (7) MAXdev MD-Pro, and (8) MediaBeez, when the MySQL root password is empty, allows remote attackers to execute ar bitrary SQL commands via the sql parameter.
| [CVE-2006-0097] Stack-based buffer overflow in the create_named_pipe function in libmysql.c in PHP 4. 3.10 and 4.4.x before 4.4.3 for Windows allows attackers to execute arbitrary code via a long (1) arg_host or (2) arg_unix_socket argument, as demonstrated by a long named pipe variable in the host argument t o the mysql_connect function.
| [CVE-2006-0056] Double free vulnerability in the authentication and authentication token alteration code in PAM-MySQL 0.6.x before 0.6.2 and 0.7.x before 0.7pre3 allows remote attackers to cause a denial of s ervice (application crash) and possibly execute arbitrary code via crafted passwords, which lead to a doub le free of a pointer that was created by the pam_get_item function. NOTE: this issue only occurs in certai n configurations in which there are multiple PAM modules, PAM-MySQL is not evaluated first, and there a re no requisite modules before PAM-MySQL.
| [CVE-2005-4713] Unspecified vulnerability in the SQL logging facility in PAM-MySQL 0.6.x before 0.6.2 and 0.7.x before 0.7pre3 allows remote attackers to cause a denial of service (segmentation fault) via uns pecified vectors, probably involving the pam_mysql_sql_log function when being used in vsftpd, which do es not include the IP address argument to an sprintf call.

| [CVE-2005-4661] The notifyendsubs cron job in Campsite before 2.3.3 sends an e-mail message containing a certain unencrypted MySQL password, which allows remote attackers to sniff the password.
| [CVE-2005-4626] The default configuration of Recruitment Software installs admin/site.xml under the web document root with insufficient access control, which might allow remote attackers to obtain sensitive information (MySQL database credentials) via a direct request.
| [CVE-2005-4237] Cross-site scripting (XSS) vulnerability in MySQL Auction 3.0 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified search module parameters, possibly the keyword parameter in the SearchZoom module.
| [CVE-2005-2865] Multiple PHP remote file inclusion vulnerabilities in aMember Pro 2.3.4 allow remote attackers to execute arbitrary PHP code via the config[root_dir] parameter to (1) mysql.inc.php, (2) efsnet.inc.php, (3) theinternetcommerce.inc.php, (4) cdg.inc.php, (5) compuworld.inc.php, (6) directone.inc.php, (7) authorize_aim.inc.php, (8) beanstream.inc.php, (9) config.inc.php, (10) eprocessingnetwork.inc.php, (11) eway.inc.php, (12) linkpoint.inc.php, (13) logiccommerce.inc.php, (14) netbilling.inc.php, (15) payflow_pro.inc.php, (16) paymentsgateway.inc.php, (17) payos.inc.php, (18) payready.inc.php, or (19) plugnplay.inc.php.
| [CVE-2005-2573] The mysql_create_function function in sql_udf.cc for MySQL 4.0 before 4.0.25, 4.1 before 4.1.13, and 5.0 before 5.0.7-beta, when running on Windows, uses an incomplete blacklist in a directory traversal check, which allows attackers to include arbitrary files via the backslash (\) character.
| [CVE-2005-2572] MySQL, when running on Windows, allows remote authenticated users with insert privileges on the mysql.func table to cause a denial of service (server hang) and possibly execute arbitrary code via (1) a request for a non-library file, which causes the Windows LoadLibraryEx function to block, or (2) a request for a function in a library that has the XXX_deinit or XXX_init functions defined but is not tailored for mySQL, such as jpeg1x32.dll and jpeg2x32.dll.
| [CVE-2005-2571] FunkBoard 0.66CF, and possibly earlier versions, does not properly restrict access to the (1) admin/mysql_install.php and (2) admin/pg_install.php scripts, which allows attackers to obtain the database username and password or inject arbitrary PHP code into info.php.
| [CVE-2005-2558] Stack-based buffer overflow in the init_syms function in MySQL 4.0 before 4.0.25, 4.1 before 4.1.13, and 5.0 before 5.0.7-beta allows remote authenticated users who can create user-defined functions to execute arbitrary code via a long function_name field.
| [CVE-2005-2468] Multiple SQL injection vulnerabilities in MySQL Eventum 1.5.5 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) isCorrectPassword or (2) userExist function in class.auth.php, getCustomFieldReport function in (4) custom_fields.php, (5) custom_fields_graph.php, or (6) class.report.php, or the insert function in (7) releases.php or (8) class.release.php.
| [CVE-2005-2467] Multiple cross-site scripting (XSS) vulnerabilities in MySQL Eventum 1.5.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter to view.php, (2) release parameter to list.php, or (3) F parameter to get_jsrs_data.php.
| [CVE-2005-2174] Bugzilla 2.17.x, 2.18 before 2.18.2, 2.19.x, and 2.20 before 2.20rc1 inserts a bug into the database before it is marked private, which introduces a race condition and allows attackers to access information about the bug via buglist.cgi before MySQL replication is complete.
| [CVE-2005-1944] xmysqladmin 1.0 and earlier allows local users to delete arbitrary files via a symlink attack on a database backup file in /tmp.
| [CVE-2005-1636] mysql_install_db in MySQL 4.1.x before 4.1.12 and 5.x up to 5.0.4 creates the mysql_install_db.X file with a predictable filename and insecure permissions, which allows local users to execute arbitrary SQL commands by modifying the file’s contents.
| [CVE-2005-1274] Stack-based buffer overflow in the getIfHeader function in the WebDAV functionality in MySQL MaxDB before 7.5.00.26 allows remote attackers to execute arbitrary code via an HTTP unlock request and a long "If" parameter.
| [CVE-2005-1121] Format string vulnerability in the my_xlog function in lib.c for Oops! Proxy Server 1.5.23 and earlier, as called by the auth functions in the passwd_mysql and passwd_pgsql modules, may allow attackers to execute arbitrary code via a URL.
| [CVE-2005-0799] MySQL 4.1.9, and possibly earlier versions, allows remote attackers with certain privileges to cause a denial of service (application crash) via a use command followed by an MS-DOS device name such as (1) LPT1 or (2) PRN.
| [CVE-2005-0711] MySQL 4.0.23 and earlier, and 4.1.x up to 4.1.10, uses predictable file names when creating temporary tables, which allows local users with CREATE TEMPORARY TABLE privileges to overw

rite arbitrary files via a symlink attack.
| [CVE-2005-0710] MySQL 4.0.23 and earlier, and 4.1.x up to 4.1.10, allows remote authenticated users with INSERT and DELETE privileges to bypass library path restrictions and execute arbitrary libraries by using INSERT INTO to modify the mysql.func table, which is processed by the udf_init function.
| [CVE-2005-0709] MySQL 4.0.23 and earlier, and 4.1.x up to 4.1.10, allows remote authenticated users with INSERT and DELETE privileges to execute arbitrary code by using CREATE FUNCTION to access li bc calls, as demonstrated by using strcat, on_exit, and exit.
| [CVE-2005-0684] Multiple buffer overflows in the web tool for MySQL MaxDB before 7.5.00.26 allows re mote attackers to execute arbitrary code via (1) an HTTP GET request with a long file parameter after a p ercent ("%") sign or (2) a long Lock-Token string to the WebDAV functionality, which is not properly handl ed by the getLockTokenHeader function in WDVHandler_CommonUtils.c.
| [CVE-2005-0646] SQL injection vulnerability in auth.php in paNews 2.0.4b allows remote attackers to ex ecute arbitrary SQL via the mysql_prefix parameter.
| [CVE-2005-0544] phpMyAdmin 2.6.1 allows remote attackers to obtain the full path of the server via dire ct requests to (1) sqlvalidator.lib.php, (2) sqlparser.lib.php, (3) select_theme.lib.php, (4) select_lang.lib.ph p, (5) relation_cleanup.lib.php, (6) header_meta_style.inc.php, (7) get_foreign.lib.php, (8) display_tbl_link s.lib.php, (9) display_export.lib.php, (10) db_table_exists.lib.php, (11) charset_conversion.lib.php, (12) ufp df.php, (13) mysqli.dbi.lib.php, (14) setup.php, or (15) cookie.auth.lib.php, which reveals the path in a PH P error message.
| [CVE-2005-0111] Stack-based buffer overflow in the websql CGI program in MySQL MaxDB 7.5.00 allo ws remote attackers to execute arbitrary code via a long password parameter.
| [CVE-2005-0083] MySQL MaxDB 7.5.00 for Windows, and possibly earlier versions and other platforms, allows remote attackers to cause a denial of service (application crash) via invalid parameters to the (1) DBMCli_String::ReallocString, (2) DBMCli_String::operator, (3) DBMCli_Buffer::ForceResize, (4) DBMCli_ Wizard::InstallDatabase, (5) DBMCli_Devspaces::Complete, (6) DBMWeb_TemplateWizard::askForWrite CountStep5, or (7) DBMWeb_DBMWeb::wizardDB functions, which triggers a null dereference.
| [CVE-2005-0082] The sapdbwa_GetUserData function in MySQL MaxDB 7.5.0.0, and other versions bef ore 7.5.0.21, allows remote attackers to cause a denial of service (crash) via invalid parameters to the We bDAV handler code, which triggers a null dereference that causes the SAP DB Web Agent to crash.
| [CVE-2005-0081] MySQL MaxDB 7.5.0.0, and other versions before 7.5.0.21, allows remote attackers to cause a denial of service (crash) via an HTTP request with invalid headers.
| [CVE-2005-0004] The mysqlaccess script in MySQL 4.0.23 and earlier, 4.1.x before 4.1.10, 5.0.x before 5.0.3, and other versions including 3.x, allows local users to overwrite arbitrary files or read temporary file s via a symlink attack on temporary files.
| [CVE-2004-2632] phpMyAdmin 2.5.1 up to 2.5.7 allows remote attackers to modify configuration settings and gain unauthorized access to MySQL servers via modified $cfg['Servers'] variables.
| [CVE-2004-2398] Netenberg Fantastico De Luxe 2.8 uses database file names that contain the associat ed usernames, which allows local users to determine valid usernames and conduct brute force attacks by reading the file names from /var/lib/mysql, which is assigned world-readable permissions by cPanel 9.3.0 R5.
| [CVE-2004-2357] The embedded MySQL 4.0 server for Proofpoint Protection Server does not require a password for the root user of MySQL, which allows remote attackers to read or modify the backend datab ase.
| [CVE-2004-2354] SQL injection vulnerability in 4nGuestbook 0.92 for PHP-Nuke 6.5 through 6.9 allows r emote attackers to modify SQL statements via the entry parameter to modules.php, which can also facilita te cross-site scripting (XSS) attacks when MySQL errors are triggered.
| [CVE-2004-2149] Buffer overflow in the prepared statements API in libmysqlclient for MySQL 4.1.3 beta and 4.1.4 allows remote attackers to cause a denial of service via a large number of placeholders.
| [CVE-2004-2138] Cross-site scripting (XSS) vulnerability in AWSguest.php in AllWebScripts MySQLGue st allows remote attackers to inject arbitrary HTML and PHP code via the (1) Name, (2) Email, (3) Homep age or (4) Comments field.
| [CVE-2004-1228] The install scripts in SugarCRM Sugar Sales 2.0.1c and earlier are not removed after i nstallation, which allows attackers to obtain the MySQL administrative password in cleartext from an instal lation form, or to cause a denial of service by changing database settings to the default.
| [CVE-2004-0957] Unknown vulnerability in MySQL 3.23.58 and earlier, when a local user has privileges f

or a database whose name includes a "_" (underscore), grants privileges to other databases that have si milar names, which can allow the user to conduct unauthorized activities.
| [CVE-2004-0956] MySQL before 4.0.20 allows remote attackers to cause a denial of service (application crash) via a MATCH AGAINST query with an opening double quote but no closing double quote.
| [CVE-2004-0931] MySQL MaxDB before 7.5.00.18 allows remote attackers to cause a denial of service (crash) via an HTTP request to webdbm with high ASCII values in the Server field, which triggers an asser t error in the IsAscii7 function.
| [CVE-2004-0837] MySQL 4.x before 4.0.21, and 3.x before 3.23.49, allows attackers to cause a denial o f service (crash or hang) via multiple threads that simultaneously alter MERGE table UNIONs.
| [CVE-2004-0836] Buffer overflow in the mysql_real_connect function in MySQL 4.x before 4.0.21, and 3. x before 3.23.49, allows remote DNS servers to cause a denial of service and possibly execute arbitrary c ode via a DNS response with a large address length (h_length).
| [CVE-2004-0835] MySQL 3.x before 3.23.59, 4.x before 4.0.19, 4.1.x before 4.1.2, and 5.x before 5.0.1, checks the CREATE/INSERT rights of the original table instead of the target table in an ALTER TABLE R ENAME operation, which could allow attackers to conduct unauthorized activities.
| [CVE-2004-0628] Stack-based buffer overflow in MySQL 4.1.x before 4.1.3, and 5.0, allows remote attac kers to cause a denial of service (crash) and possibly execute arbitrary code via a long scramble string.
| [CVE-2004-0627] The check_scramble_323 function in MySQL 4.1.x before 4.1.3, and 5.0, allows remot e attackers to bypass authentication via a zero-length scrambled string.
| [CVE-2004-0457] The mysqlhotcopy script in mysql 4.0.20 and earlier, when using the scp method from the mysql-server package, allows local users to overwrite arbitrary files via a symlink attack on temporary files.
| [CVE-2004-0388] The mysqld_multi script in MySQL allows local users to overwrite arbitrary files via a s ymlink attack.
| [CVE-2004-0381] mysqlbug in MySQL allows local users to overwrite arbitrary files via a symlink attack o n the failed-mysql-bugreport temporary file.
| [CVE-2003-1480] MySQL 3.20 through 4.1.0 uses a weak algorithm for hashed passwords, which make s it easier for attackers to decrypt the password via brute force methods.
| [CVE-2003-1421] Unspecified vulnerability in mod_mysql_logger shared object in SuckBot 0.006 allows remote attackers to cause a denial of service (seg fault) via unknown attack vectors.
| [CVE-2003-1383] WEB-ERP 0.1.4 and earlier allows remote attackers to obtain sensitive information via an HTTP request for the logicworks.ini file, which contains the MySQL database username and password.
| [CVE-2003-1331] Stack-based buffer overflow in the mysql_real_connect function in the MySql client libr ary (libmysqlclient) 4.0.13 and earlier allows local users to execute arbitrary code via a long socket name, a different vulnerability than CVE-2001-1453.
| [CVE-2003-0780] Buffer overflow in get_salt_from_password from sql_acl.cc for MySQL 4.0.14 and earli er, and 3.23.x, allows attackers with ALTER TABLE privileges to execute arbitrary code via a long Passw ord field.
| [CVE-2003-0515] SQL injection vulnerabilities in the (1) PostgreSQL or (2) MySQL authentication modul es for teapop 0.3.5 and earlier allow attackers to execute arbitrary SQL and possibly gain privileges.
| [CVE-2003-0150] MySQL 3.23.55 and earlier creates world-writeable files and allows mysql users to gai n root privileges by using the "SELECT * INFO OUTFILE" operator to overwrite a configuration file and ca use mysql to run as root upon restart, as demonstrated by modifying my.cnf.
| [CVE-2003-0073] Double-free vulnerability in mysqld for MySQL before 3.23.55 allows attackers with My SQL access to cause a denial of service (crash) via mysql_change_user.
| [CVE-2002-2043] SQL injection vulnerability in the LDAP and MySQL authentication patch for Cyrus SA SL 1.5.24 and 1.5.27 allows remote attackers to execute arbitrary SQL commands and log in as arbitrary POP mail users via the password.
| [CVE-2002-1952] phpRank 1.8 does not properly check the return codes for MySQL operations when au thenticating users, which could allow remote attackers to authenticate using a NULL password when data base errors occur or if the database is unavailable.
| [CVE-2002-1923] The default configuration in MySQL 3.20.32 through 3.23.52, when running on Windo ws, does not have logging enabled, which could allow remote attackers to conduct activities without detec tion.
| [CVE-2002-1921] The default configuration of MySQL 3.20.32 through 3.23.52, when running on Windo

ws, does set the bind address to the loopback interface, which allows remote attackers to connect to the d atabase.
| [CVE-2002-1809] The default configuration of the Windows binary release of MySQL 3.23.2 through 3.2 3.52 has a NULL root password, which could allow remote attackers to gain unauthorized root access to t he MySQL database.
| [CVE-2002-1479] Cacti before 0.6.8 stores a MySQL username and password in plaintext in config.php, which has world-readable permissions, which allows local users modify databases as the Cacti user and possibly gain privileges.
| [CVE-2002-1376] libmysqlclient client library in MySQL 3.x to 3.23.54, and 4.x to 4.0.6, does not properly verify length fields for certain responses in the (1) read_rows or (2) read_one_row routines, which allows remote attackers to cause a denial of service and possibly execute arbitrary code.
| [CVE-2002-1375] The COM_CHANGE_USER command in MySQL 3.x before 3.23.54, and 4.x to 4.0.6, allows remote attackers to execute arbitrary code via a long response.
| [CVE-2002-1374] The COM_CHANGE_USER command in MySQL 3.x before 3.23.54, and 4.x before 4. 0.6, allows remote attackers to gain privileges via a brute force attack using a one-character password, w hich causes MySQL to only compare the provided password against the first character of the real passwo rd.
| [CVE-2002-1373] Signed integer vulnerability in the COM_TABLE_DUMP package for MySQL 3.23.x be fore 3.23.54 allows remote attackers to cause a denial of service (crash or hang) in mysqld by causing lar ge negative integers to be provided to a memcpy call.
| [CVE-2002-0969] Buffer overflow in MySQL daemon (mysqld) before 3.23.50, and 4.0 beta before 4.02, on the Win32 platform, allows local users to execute arbitrary code via a long "datadir" parameter in the m y.ini initialization file, whose permissions on Windows allow Full Control to the Everyone group.
| [CVE-2002-0229] Safe Mode feature (safe_mode) in PHP 3.0 through 4.1.0 allows attackers with access to the MySQL database to bypass Safe Mode access restrictions and read arbitrary files using "LOAD D ATA INFILE LOCAL" SQL statements.
| [CVE-2001-1454] Buffer overflow in MySQL before 3.23.33 allows remote attackers to execute arbitrary code via a long drop database request.
| [CVE-2001-1453] Buffer overflow in libmysqlclient.so in MySQL 3.23.33 and earlier allows remote attack ers to execute arbitrary code via a long host parameter.
| [CVE-2001-1275] MySQL before 3.23.31 allows users with a MySQL account to use the SHOW GRANT S command to obtain the encrypted administrator password from the mysql.user table and possibly gain p rivileges via password cracking.
| [CVE-2001-1274] Buffer overflow in MySQL before 3.23.31 allows attackers to cause a denial of service and possibly gain privileges.
| [CVE-2001-1255] WinMySQLadmin 1.1 stores the MySQL password in plain text in the my.ini file, which allows local users to obtain unathorized access the MySQL database.
| [CVE-2001-1226] AdCycle 1.17 and earlier allow remote attackers to modify SQL queries, which are not properly sanitized before being passed to the MySQL database.
| [CVE-2001-1044] Basilix Webmail 0.9.7beta, and possibly other versions, stores *.class and *.inc files un der the document root and does not restrict access, which could allows remote attackers to obtain sensitiv e information such as MySQL passwords and usernames from the mysql.class file.
| [CVE-2001-0990] Inter7 vpopmail 4.10.35 and earlier, when using the MySQL module, compiles authenti cation information in cleartext into the libvpopmail.a library, which allows local users to obtain the MySQL username and password by inspecting the vpopmail programs that use the library.
| [CVE-2001-0645] Symantec/AXENT NetProwler 3.5.x contains several default passwords, which could a llow remote attackers to (1) access to the management tier via the "admin" password, or (2) connect to a MySQL ODBC from the management tier using a blank password.
| [CVE-2001-0407] Directory traversal vulnerability in MySQL before 3.23.36 allows local users to modify arbitrary files and gain privileges by creating a database whose name starts with .. (dot dot).
| [CVE-2000-0981] MySQL Database Engine uses a weak authentication method which leaks information that could be used by a remote attacker to recover the password.
| [CVE-2000-0957] The pluggable authentication module for mysql (pam_mysql) before 0.4.7 does not pro perly cleanse user input when constructing SQL statements, which allows attackers to obtain plaintext pa sswords or hashes.

| [CVE-2000-0707] PCCS MySQLDatabase Admin Tool Manager 1.2.4 and earlier installs the file dbconnect.inc within the web root, which allows remote attackers to obtain sensitive information such as the administrative password.
| [CVE-2000-0148] MySQL 3.22 allows remote attackers to bypass password authentication and access a database via a short check string.
| [CVE-2000-0045] MySQL allows local users to modify passwords for arbitrary MySQL users via the GRANT privilege.
| [CVE-1999-1188] mysqld in MySQL 3.21 creates log files with world-readable permissions, which allows local users to obtain passwords for users who are added to the user database.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [104370] MySQL Multi-Master Replication Manager Multiple Remote Command Injection Vulnerabilities
| [103954] Oracle MySQL CVE-2018-2767 Incomplete Fix SSL Certificate Validation Security Bypass Vulnerability
| [103876] Oracle MySQL Server CVE-2018-2769 Remote Security Vulnerability
| [103845] Oracle MySQL Server CVE-2018-2839 Remote Security Vulnerability
| [103838] Oracle MySQL Cluster CVE-2018-2877 Local Security Vulnerability
| [103836] Oracle MySQL Server CVE-2018-2812 Remote Security Vulnerability
| [103831] Oracle MySQL Server CVE-2018-2805 Remote Security Vulnerability
| [103830] Oracle MySQL Server CVE-2018-2813 Remote Security Vulnerability
| [103828] Oracle MySQL Server CVE-2018-2771 Remote Security Vulnerability
| [103825] Oracle MySQL Server CVE-2018-2781 Remote Security Vulnerability
| [103824] Oracle MySQL Server CVE-2018-2818 Remote Security Vulnerability
| [103820] Oracle MySQL Server CVE-2018-2761 Remote Security Vulnerability
| [103818] Oracle MySQL Server CVE-2018-2817 Remote Security Vulnerability
| [103814] Oracle MySQL Server CVE-2018-2819 Remote Security Vulnerability
| [103811] Oracle MySQL Server CVE-2018-2773 Local Security Vulnerability
| [103807] Oracle MySQL Server CVE-2018-2755 Local Security Vulnerability
| [103805] Oracle MySQL Server CVE-2018-2766 Remote Security Vulnerability
| [103804] Oracle MySQL Server CVE-2018-2787 Remote Security Vulnerability
| [103802] Oracle MySQL Server CVE-2018-2758 Remote Security Vulnerability
| [103801] Oracle MySQL Server CVE-2018-2784 Remote Security Vulnerability
| [103799] Oracle MySQL Server CVE-2018-2782 Remote Security Vulnerability
| [103794] Oracle MySQL Server CVE-2018-2762 Remote Security Vulnerability
| [103791] Oracle MySQL Server CVE-2018-2776 Remote Security Vulnerability
| [103790] Oracle MySQL Server CVE-2018-2846 Remote Security Vulnerability
| [103789] Oracle MySQL Server CVE-2018-2816 Remote Security Vulnerability
| [103787] Oracle MySQL Server CVE-2018-2779 Remote Security Vulnerability
| [103785] Oracle MySQL Server CVE-2018-2778 Remote Security Vulnerability
| [103783] Oracle MySQL Server CVE-2018-2810 Remote Security Vulnerability
| [103781] Oracle MySQL Server CVE-2018-2777 Remote Security Vulnerability
| [103780] Oracle MySQL Server CVE-2018-2759 Remote Security Vulnerability
| [103779] Oracle MySQL Server CVE-2018-2786 Remote Security Vulnerability
| [103778] Oracle MySQL Server CVE-2018-2780 Remote Security Vulnerability
| [103777] Oracle MySQL Server CVE-2018-2775 Remote Security Vulnerability
| [102714] Oracle MySQL Server CVE-2018-2591 Remote Security Vulnerability
| [102713] Oracle MySQL Server CVE-2018-2562 Remote Security Vulnerability
| [102712] Oracle MySQL Server CVE-2018-2565 Remote Security Vulnerability
| [102711] Oracle MySQL Server CVE-2018-2647 Remote Security Vulnerability
| [102710] Oracle MySQL Server CVE-2018-2573 Remote Security Vulnerability
| [102709] Oracle MySQL Server CVE-2018-2612 Remote Security Vulnerability
| [102708] Oracle MySQL Server CVE-2018-2583 Remote Security Vulnerability
| [102706] Oracle MySQL Server CVE-2018-2622 Remote Security Vulnerability
| [102704] Oracle MySQL Server CVE-2018-2703 Remote Security Vulnerability
| [102703] Oracle MySQL Server CVE-2018-2646 Remote Security Vulnerability

| [102701] Oracle MySQL Server CVE-2018-2696 Remote Security Vulnerability
| [102700] Oracle MySQL Server CVE-2018-2586 Remote Security Vulnerability
| [102698] Oracle MySQL Server CVE-2018-2645 Remote Security Vulnerability
| [102697] Oracle MySQL Server CVE-2018-2590 Remote Security Vulnerability
| [102696] Oracle MySQL Server CVE-2018-2600 Remote Security Vulnerability
| [102695] Oracle MySQL Server CVE-2018-2576 Remote Security Vulnerability
| [102685] Oracle MySQL Server CVE-2018-2667 Remote Security Vulnerability
| [102682] Oracle MySQL Server CVE-2018-2668 Remote Security Vulnerability
| [102681] Oracle MySQL Server CVE-2018-2665 Remote Security Vulnerability
| [102678] Oracle MySQL Server CVE-2018-2640 Remote Security Vulnerability
| [102674] Oracle MySQL Connectors CVE-2018-2585 Remote Security Vulnerability
| [101448] Oracle MySQL Server CVE-2017-10313 Remote Security Vulnerability
| [101446] Oracle MySQL Server CVE-2017-10311 Remote Security Vulnerability
| [101444] Oracle MySQL Server CVE-2017-10294 Remote Security Vulnerability
| [101441] Oracle MySQL Server CVE-2017-10276 Remote Security Vulnerability
| [101439] Oracle MySQL Connectors CVE-2017-10277 Remote Security Vulnerability
| [101433] Oracle MySQL Server CVE-2017-10167 Remote Security Vulnerability
| [101429] Oracle MySQL Server CVE-2017-10365 Remote Security Vulnerability
| [101424] Oracle MySQL Server CVE-2017-10165 Remote Security Vulnerability
| [101420] Oracle MySQL Server CVE-2017-10283 Remote Security Vulnerability
| [101415] Oracle MySQL Server CVE-2017-10379 Remote Security Vulnerability
| [101410] Oracle MySQL Server CVE-2017-10320 Remote Security Vulnerability
| [101406] Oracle MySQL Server CVE-2017-10384 Remote Security Vulnerability
| [101402] Oracle MySQL Server CVE-2017-10155 Remote Security Vulnerability
| [101397] Oracle MySQL Server CVE-2017-10286 Remote Security Vulnerability
| [101390] Oracle MySQL Server CVE-2017-10268 Local Security Vulnerability
| [101385] Oracle MySQL Server CVE-2017-10284 Remote Security Vulnerability
| [101381] Oracle MySQL Enterprise Monitor CVE-2017-10424 Remote Security Vulnerability
| [101375] Oracle MySQL Server CVE-2017-10378 Remote Security Vulnerability
| [101373] Oracle MySQL Server CVE-2017-10296 Remote Security Vulnerability
| [101337] Oracle MySQL Server CVE-2017-10227 Remote Security Vulnerability
| [101324] Oracle MySQL Connectors CVE-2017-10203 Remote Security Vulnerability
| [101316] Oracle MySQL Server CVE-2017-10279 Remote Security Vulnerability
| [101314] Oracle MySQL Server CVE-2017-10314 Remote Security Vulnerability
| [99810] Oracle MySQL Server CVE-2017-3653 Remote Security Vulnerability
| [99808] Oracle MySQL Server CVE-2017-3650 Remote Security Vulnerability
| [99805] Oracle MySQL Server CVE-2017-3652 Remote Security Vulnerability
| [99802] Oracle MySQL Server CVE-2017-3651 Remote Security Vulnerability
| [99799] Oracle MySQL Server CVE-2017-3649 Remote Security Vulnerability
| [99796] Oracle MySQL Server CVE-2017-3647 Remote Security Vulnerability
| [99789] Oracle MySQL Server CVE-2017-3648 Remote Security Vulnerability
| [99786] Oracle MySQL Server CVE-2017-3646 Remote Security Vulnerability
| [99783] Oracle MySQL Server CVE-2017-3645 Remote Security Vulnerability
| [99779] Oracle MySQL Server CVE-2017-3642 Remote Security Vulnerability
| [99778] Oracle MySQL Server CVE-2017-3638 Remote Security Vulnerability
| [99775] Oracle MySQL Server CVE-2017-3644 Remote Security Vulnerability
| [99772] Oracle MySQL Server CVE-2017-3643 Remote Security Vulnerability
| [99767] Oracle MySQL Server CVE-2017-3641 Remote Security Vulnerability
| [99765] Oracle MySQL Server CVE-2017-3640 Remote Security Vulnerability
| [99753] Oracle MySQL Server CVE-2017-3639 Remote Security Vulnerability
| [99748] Oracle MySQL Server CVE-2017-3637 Remote Security Vulnerability
| [99746] Oracle MySQL Server CVE-2017-3529 Remote Security Vulnerability
| [99736] Oracle MySQL Server CVE-2017-3636 Local Security Vulnerability
| [99730] Oracle MySQL Connectors/MySQL Server CVE-2017-3635 Remote Security Vulnerability
| [99729] Oracle MySQL Server CVE-2017-3634 Remote Security Vulnerability

| [99722] Oracle MySQL Server CVE-2017-3633 Remote Security Vulnerability
| [99374] Perl DBD::mysql Module CVE-2017-10788 Use After Free Denial of Service Vulnerability
| [99364] Perl DBD::mysql Module CVE-2017-10789 Man in the Middle Security Bypass Vulnerability
| [97982] Oracle MySQL Connectors CVE-2017-3523 Remote Security Vulnerability
| [97960] MySQL-GUI-tools CVE-2010-4178 Local Information Disclosure Vulnerability
| [97959] MySQL-GUI-tools CVE-2010-4177 Local Information Disclosure Vulnerability
| [97851] Oracle MySQL Server CVE-2017-3462 Remote Security Vulnerability
| [97849] Oracle MySQL Server CVE-2017-3463 Remote Security Vulnerability
| [97848] Oracle MySQL Server CVE-2017-3468 Remote Security Vulnerability
| [97847] Oracle MySQL Server CVE-2017-3459 Remote Security Vulnerability
| [97845] Oracle MySQL Server CVE-2017-3457 Remote Security Vulnerability
| [97844] Oracle MySQL Enterprise Monitor CVE-2017-3307 Remote Security Vulnerability
| [97840] Oracle MySQL Connectors CVE-2017-3590 Local Security Vulnerability
| [97837] Oracle MySQL Server CVE-2017-3458 Remote Security Vulnerability
| [97836] Oracle MySQL Connectors CVE-2017-3589 Local Security Vulnerability
| [97833] Oracle MySQL Workbench CVE-2017-3469 Remote Security Vulnerability
| [97831] Oracle MySQL Server CVE-2017-3456 Remote Security Vulnerability
| [97826] Oracle MySQL Server CVE-2017-3460 Remote Security Vulnerability
| [97825] Oracle MySQL Server CVE-2017-3467 Remote Security Vulnerability
| [97822] Oracle MySQL Server CVE-2017-3465 Remote Security Vulnerability
| [97820] Oracle MySQL Server CVE-2017-3455 Remote Security Vulnerability
| [97818] Oracle MySQL Server CVE-2017-3464 Remote Security Vulnerability
| [97815] Oracle MySQL Cluster CVE-2017-3304 Remote Security Vulnerability
| [97812] Oracle MySQL Server CVE-2017-3461 Remote Security Vulnerability
| [97791] Oracle MySQL Server CVE-2017-3454 Remote Security Vulnerability
| [97784] Oracle MySQL Connectors CVE-2017-3586 Remote Security Vulnerability
| [97779] Oracle MySQL Server CVE-2017-3452 Remote Security Vulnerability
| [97776] Oracle MySQL Server CVE-2017-3453 Remote Security Vulnerability
| [97772] Oracle MySQL Server CVE-2017-3331 Remote Security Vulnerability
| [97765] Oracle MySQL Server CVE-2017-3600 Remote Security Vulnerability
| [97763] Oracle MySQL Server CVE-2017-3329 Remote Security Vulnerability
| [97754] Oracle MySQL Server CVE-2017-3599 Remote Security Vulnerability
| [97747] Oracle MySQL Server CVE-2017-3450 Remote Security Vulnerability
| [97742] Oracle MySQL Server CVE-2017-3309 Remote Security Vulnerability
| [97725] Oracle MySQL Server CVE-2017-3308 Remote Security Vulnerability
| [97724] Oracle MySQL Enterprise Monitor CVE-2017-3306 Remote Security Vulnerability
| [97023] MySQL CVE-2017-3305 Man in the Middle Security Bypass Vulnerability
| [96300] PHP 'ext/mysqli/mysqli.c' Denial of Service Vulnerability
| [96162] MariaDB and MySQL CVE-2017-3302 Denial of Service Vulnerability
| [95592] Oracle MySQL Cluster CVE-2016-5541 Remote Security Vulnerability
| [95589] Oracle MySQL Server CVE-2017-3257 Remote Security Vulnerability
| [95588] Oracle MySQL Server CVE-2017-3318 Local Security Vulnerability
| [95585] Oracle MySQL Server CVE-2017-3317 Local Security Vulnerability
| [95583] Oracle MySQL Server CVE-2017-3273 Remote Security Vulnerability
| [95580] Oracle MySQL Server CVE-2016-8318 Remote Security Vulnerability
| [95575] Oracle MySQL Cluster CVE-2017-3323 Remote Security Vulnerability
| [95574] Oracle MySQL Cluster CVE-2017-3322 Remote Security Vulnerability
| [95571] Oracle MySQL Server CVE-2017-3238 Remote Security Vulnerability
| [95565] Oracle MySQL Server CVE-2017-3244 Remote Security Vulnerability
| [95562] Oracle MySQL Cluster CVE-2017-3321 Remote Security Vulnerability
| [95560] Oracle MySQL Server CVE-2017-3258 Remote Security Vulnerability
| [95542] Oracle MySQL Enterprise Monitor CVE-2016-5590 Remote Security Vulnerability
| [95538] Oracle MySQL Server CVE-2017-3243 Remote Security Vulnerability
| [95527] Oracle MySQL Server CVE-2017-3313 Local Security Vulnerability
| [95520] Oracle MySQL Server CVE-2017-3265 Local Security Vulnerability

| [95501] Oracle MySQL Server CVE-2017-3291 Local Security Vulnerability
| [95491] Oracle MySQL Server CVE-2017-3312 Local Security Vulnerability
| [95486] Oracle MySQL Server CVE-2017-3256 Remote Security Vulnerability
| [95482] Oracle MySQL Server CVE-2017-3251 Remote Security Vulnerability
| [95479] Oracle MySQL Server CVE-2017-3319 Remote Security Vulnerability
| [95470] Oracle MySQL Server CVE-2017-3320 Remote Security Vulnerability
| [95146] Pivotal MySQL for PCF CVE-2016-0898 Information Disclosure Vulnerability
| [94350] DBD::mysql CVE-2016-1249 Out-Of-Bounds Read Information Disclosure Vulnerability
| [93755] Oracle MySQL CVE-2016-8284 Local Security Vulnerability
| [93745] Oracle MySQL CVE-2016-8286 Remote Security Vulnerability
| [93740] Oracle MySQL CVE-2016-8288 Remote Security Vulnerability
| [93737] Oracle MySQL CVE-2016-8283 Remote Security Vulnerability
| [93735] Oracle MySQL CVE-2016-5584 Remote Security Vulnerability
| [93733] Oracle MySQL CVE-2016-8290 Remote Security Vulnerability
| [93727] Oracle MySQL CVE-2016-8287 Remote Security Vulnerability
| [93720] Oracle MySQL CVE-2016-8289 Local Security Vulnerability
| [93715] Oracle MySQL CVE-2016-5635 Remote Security Vulnerability
| [93709] Oracle MySQL CVE-2016-5634 Remote Security Vulnerability
| [93702] Oracle MySQL CVE-2016-5633 Remote Security Vulnerability
| [93693] Oracle MySQL CVE-2016-5632 Remote Security Vulnerability
| [93684] Oracle MySQL CVE-2016-5631 Remote Security Vulnerability
| [93678] Oracle MySQL CVE-2016-5507 Remote Security Vulnerability
| [93674] Oracle MySQL CVE-2016-5630 Remote Security Vulnerability
| [93670] Oracle MySQL CVE-2016-3495 Remote Security Vulnerability
| [93668] Oracle MySQL CVE-2016-5629 Remote Security Vulnerability
| [93662] Oracle MySQL CVE-2016-5628 Remote Security Vulnerability
| [93659] Oracle MySQL CVE-2016-7440 Local Security Vulnerability
| [93653] Oracle MySQL Connector CVE-2016-5598 Remote Security Vulnerability
| [93650] Oracle MySQL CVE-2016-3492 Remote Security Vulnerability
| [93642] Oracle MySQL CVE-2016-5627 Remote Security Vulnerability
| [93638] Oracle MySQL CVE-2016-5626 Remote Security Vulnerability
| [93635] Oracle MySQL CVE-2016-5624 Remote Security Vulnerability
| [93630] Oracle MySQL CVE-2016-5612 Remote Security Vulnerability
| [93622] Oracle MySQL CVE-2016-5609 Remote Security Vulnerability
| [93617] Oracle MySQL CVE-2016-5625 Local Security Vulnerability
| [93614] RETIRED: Oracle MySQL CVE-2016-5616 Local Security Vulnerability
| [93612] Oracle MySQL CVE-2016-6664 Local Security Vulnerability
| [93480] Pivotal Cloud Foundry cf-mysql CVE-2016-6653 Information Disclosure Vulnerability
| [93337] perl-DBD-MySQL CVE-2016-1246 Remote Buffer Overflow Vulnerability
| [92912] Oracle MySQL CVE-2016-6662 Remote Code Execution Vulnerability
| [92911] Oracle MySQL CVE-2016-6663 Unspecified Security Vulnerability
| [92149] DBD::mysql CVE-2014-9906 Incomplete Fix Use After Free Remote Code Execution Vulnerabili
ty
| [92118] DBD::mysql 'my_login()' Function Use After Free Remote Code Execution Vulnerability
| [91999] Oracle MySQL CVE-2016-3452 Remote Security Vulnerability
| [91992] Oracle MySQL CVE-2016-3614 Remote Security Vulnerability
| [91987] Oracle MySQL CVE-2016-5444 Remote Security Vulnerability
| [91983] Oracle MySQL CVE-2016-3588 Remote Security Vulnerability
| [91980] Oracle MySQL CVE-2016-3486 Remote Security Vulnerability
| [91976] Oracle MySQL CVE-2016-3424 Remote Security Vulnerability
| [91974] Oracle MySQL CVE-2016-5442 Remote Security Vulnerability
| [91969] Oracle MySQL CVE-2016-5439 Remote Security Vulnerability
| [91967] Oracle MySQL CVE-2016-3518 Remote Security Vulnerability
| [91963] Oracle MySQL CVE-2016-5443 Local Security Vulnerability
| [91960] Oracle MySQL CVE-2016-3615 Remote Security Vulnerability

| [91953] Oracle MySQL CVE-2016-5440 Remote Security Vulnerability
| [91949] Oracle MySQL CVE-2016-3501 Remote Security Vulnerability
| [91943] Oracle MySQL CVE-2016-3459 Remote Security Vulnerability
| [91932] Oracle MySQL CVE-2016-3521 Remote Security Vulnerability
| [91917] Oracle MySQL CVE-2016-5437 Remote Security Vulnerability
| [91915] Oracle MySQL CVE-2016-5441 Remote Security Vulnerability
| [91913] Oracle MySQL CVE-2016-3471 Local Security Vulnerability
| [91910] Oracle MySQL CVE-2016-3440 Remote Security Vulnerability
| [91906] Oracle MySQL CVE-2016-5436 Remote Security Vulnerability
| [91902] Oracle MySQL CVE-2016-3477 Local Security Vulnerability
| [90165] MySQL CVE-2005-0799 Denial-Of-Service Vulnerability
| [89812] xMySQLadmin CVE-2005-1944 Local Security Vulnerability
| [89412] MySQL CVE-2005-2573 Directory Traversal Vulnerability
| [88627] MySQL CVE-1999-1188 Local Security Vulnerability
| [88032] MySQL CVE-2001-1275 Local Security Vulnerability
| [87310] Btsavemysql CVE-2006-6378 Remote Security Vulnerability
| [86999] MySQL CVE-2001-1274 Denial-Of-Service Vulnerability
| [86513] Oracle MySQL CVE-2016-0665 Remote Security Vulnerability
| [86511] Oracle MySQL CVE-2016-0661 Remote Security Vulnerability
| [86509] Oracle MySQL CVE-2016-0666 Remote Security Vulnerability
| [86506] Oracle MySQL CVE-2016-0662 Remote Security Vulnerability
| [86504] Oracle MySQL CVE-2016-0654 Remote Security Vulnerability
| [86501] Oracle MySQL CVE-2016-0651 Remote Security Vulnerability
| [86498] Oracle MySQL CVE-2016-0649 Remote Security Vulnerability
| [86496] Oracle MySQL CVE-2016-0650 Remote Security Vulnerability
| [86495] Oracle MySQL CVE-2016-0647 Remote Security Vulnerability
| [86493] Oracle MySQL CVE-2016-0659 Remote Security Vulnerability
| [86489] Oracle MySQL CVE-2016-3461 Remote Security Vulnerability
| [86486] Oracle MySQL CVE-2016-0643 Remote Security Vulnerability
| [86484] Oracle MySQL CVE-2016-0667 Remote Security Vulnerability
| [86470] Oracle MySQL CVE-2016-0641 Remote Security Vulnerability
| [86467] Oracle MySQL CVE-2016-0668 Remote Security Vulnerability
| [86463] Oracle MySQL CVE-2016-0658 Remote Security Vulnerability
| [86457] Oracle MySQL CVE-2016-0648 Remote Security Vulnerability
| [86454] Oracle MySQL CVE-2016-0652 Remote Security Vulnerability
| [86451] Oracle MySQL CVE-2016-0663 Remote Security Vulnerability
| [86445] Oracle MySQL CVE-2016-0642 Remote Security Vulnerability
| [86442] Oracle MySQL CVE-2016-0644 Remote Security Vulnerability
| [86439] Oracle MySQL CVE-2016-0653 Remote Security Vulnerability
| [86436] Oracle MySQL CVE-2016-0646 Remote Security Vulnerability
| [86433] Oracle MySQL CVE-2016-0657 Remote Security Vulnerability
| [86431] Oracle MySQL CVE-2016-0656 Remote Security Vulnerability
| [86427] Oracle MySQL CVE-2016-0640 Remote Security Vulnerability
| [86424] Oracle MySQL CVE-2016-0655 Remote Security Vulnerability
| [86418] Oracle MySQL CVE-2016-0639 Remote Security Vulnerability
| [85985] MariaDB and MySQL CVE-2015-5969 Local Information Disclosure Vulnerability
| [85262] MySQL CVE-2007-5970 Remote Security Vulnerability
| [85246] Mysql Community Server CVE-2007-6313 Remote Security Vulnerability
| [85215] Mysql Banner Exchange CVE-2007-6512 Denial-Of-Service Vulnerability
| [83639] MySQLDumper CVE-2006-5264 Cross-Site Scripting Vulnerability
| [83232] MySQL Connector/Net CVE-2006-4227 Remote Security Vulnerability
| [83194] MySQL CVE-2004-0628 Denial Of Service Vulnerability
| [82913] MySQL CVE-2001-1453 Remote Security Vulnerability
| [82911] MySQL CVE-2001-1454 Remote Security Vulnerability
| [81810] MariaDB/MySQL/Percona Server CVE-2016-2047 SSL Certificate Validation Security Bypass V

ulnerability
| [81258] Oracle MySQL CVE-2016-0609 Remote Security Vulnerability
| [81253] Oracle MySQL CVE-2016-0605 Remote Security Vulnerability
| [81245] Oracle MySQL CVE-2015-7744 Remote Security Vulnerability
| [81238] Oracle MySQL CVE-2016-0607 Remote Security Vulnerability
| [81226] Oracle MySQL CVE-2016-0608 Remote Security Vulnerability
| [81211] Oracle MySQL CVE-2016-0601 Remote Security Vulnerability
| [81203] Oracle MySQL CVE-2016-0599 Remote Security Vulnerability
| [81198] Oracle MySQL CVE-2016-0610 Remote Security Vulnerability
| [81188] Oracle MySQL CVE-2016-0600 Remote Security Vulnerability
| [81182] Oracle MySQL CVE-2016-0598 Remote Security Vulnerability
| [81176] Oracle MySQL CVE-2016-0616 Remote Security Vulnerability
| [81164] Oracle MySQL CVE-2016-0611 Remote Security Vulnerability
| [81151] Oracle MySQL CVE-2016-0597 Remote Security Vulnerability
| [81136] Oracle MySQL CVE-2016-0502 Remote Security Vulnerability
| [81130] Oracle MySQL CVE-2016-0596 Remote Security Vulnerability
| [81126] Oracle MySQL CVE-2016-0503 Remote Security Vulnerability
| [81121] Oracle MySQL CVE-2016-0595 Remote Security Vulnerability
| [81108] Oracle MySQL CVE-2016-0594 Remote Security Vulnerability
| [81088] Oracle MySQL CVE-2016-0505 Remote Security Vulnerability
| [81077] Oracle MySQL CVE-2016-0504 Remote Security Vulnerability
| [81066] Oracle MySQL CVE-2016-0546 Local Security Vulnerability
| [79408] Mysql-Ocaml CVE-2009-2942 Remote Security Vulnerability
| [79044] kiddog_mysqldumper CVE-2010-0336 Information Disclosure Vulnerability
| [78373] MySQL CVE-2011-5049 Denial-Of-Service Vulnerability
| [77237] Oracle MySQL Server CVE-2015-4826 Remote Security Vulnerability
| [77234] Oracle MySQL Server CVE-2015-4910 Remote Security Vulnerability
| [77232] Oracle MySQL Server CVE-2015-4766 Local Security Vulnerability
| [77231] Oracle MySQL Server CVE-2015-4890 Remote Security Vulnerability
| [77228] Oracle MySQL Server CVE-2015-4830 Remote Security Vulnerability
| [77222] Oracle MySQL Server CVE-2015-4815 Remote Security Vulnerability
| [77219] Oracle MySQL Server CVE-2015-4904 Remote Security Vulnerability
| [77216] Oracle MySQL Server CVE-2015-4800 Remote Security Vulnerability
| [77213] Oracle MySQL Server CVE-2015-4791 Remote Security Vulnerability
| [77208] Oracle MySQL Server CVE-2015-4870 Remote Security Vulnerability
| [77205] Oracle MySQL Server CVE-2015-4807 Remote Security Vulnerability
| [77199] Oracle MySQL Server CVE-2015-4730 Remote Security Vulnerability
| [77196] Oracle MySQL Server CVE-2015-4819 Local Security Vulnerability
| [77190] Oracle MySQL Server CVE-2015-4836 Remote Security Vulnerability
| [77187] Oracle MySQL Server CVE-2015-4864 Remote Security Vulnerability
| [77171] Oracle MySQL Server CVE-2015-4792 Remote Security Vulnerability
| [77170] Oracle MySQL Server CVE-2015-4833 Remote Security Vulnerability
| [77165] Oracle MySQL Server CVE-2015-4802 Remote Security Vulnerability
| [77153] Oracle MySQL Server CVE-2015-4913 Remote Security Vulnerability
| [77147] Oracle MySQL Server CVE-2015-4862 Remote Security Vulnerability
| [77145] Oracle MySQL Server CVE-2015-4858 Remote Security Vulnerability
| [77143] Oracle MySQL Server CVE-2015-4905 Remote Security Vulnerability
| [77140] Oracle MySQL Server CVE-2015-4879 Remote Security Vulnerability
| [77137] Oracle MySQL Server CVE-2015-4861 Remote Security Vulnerability
| [77136] Oracle MySQL Server CVE-2015-4895 Remote Security Vulnerability
| [77134] Oracle MySQL Server CVE-2015-4816 Remote Security Vulnerability
| [77132] Oracle MySQL Server CVE-2015-4866 Remote Security Vulnerability
| [77015] Oracle MySQL Multiple Buffer Overflow Vulnerabilities
| [75849] Oracle MySQL Server CVE-2015-4752 Remote Security Vulnerability
| [75844] Oracle MySQL Server CVE-2015-4767 Remote Security Vulnerability

| [75837] Oracle MySQL Server CVE-2015-2620 Remote Security Vulnerability
| [75835] Oracle MySQL Server CVE-2015-4771 Remote Security Vulnerability
| [75830] Oracle MySQL Server CVE-2015-2643 Remote Security Vulnerability
| [75822] Oracle MySQL Server CVE-2015-2648 Remote Security Vulnerability
| [75815] Oracle MySQL Server CVE-2015-2641 Remote Security Vulnerability
| [75813] Oracle MySQL Server CVE-2015-2661 Local Security Server Vulnerability
| [75802] Oracle MySQL Server CVE-2015-4737 Remote Security Vulnerability
| [75785] Oracle MySQL Server CVE-2015-4756 Remote Security Vulnerability
| [75781] Oracle MySQL Server CVE-2015-4772 Remote Security Vulnerability
| [75774] Oracle MySQL Server CVE-2015-2617 Remote Security Vulnerability
| [75770] Oracle MySQL Server CVE-2015-4761 Remote Security Vulnerability
| [75762] Oracle MySQL Server CVE-2015-2611 Remote Security Vulnerability
| [75760] Oracle MySQL Server CVE-2015-2639 Remote Security Vulnerability
| [75759] Oracle MySQL Server CVE-2015-4757 Remote Security Vulnerability
| [75753] Oracle MySQL Server CVE-2015-4769 Remote Security Vulnerability
| [75751] Oracle MySQL Server CVE-2015-2582 Remote Security Vulnerability
| [75397] MySql Lite Administrator Multiple Cross Site Scripting Vulnerabilities
| [75394] WordPress wp-instance-rename Plugin ’mysqldump_download.php’ Arbitrary File Download Vul
nerability
| [74695] Tiny MySQL ’tinymy.php’ Cross Site Scripting Vulnerability
| [74398] Oracle MySQL CVE-2015-3152 SSL Certificate Validation Security Bypass Vulnerability
| [74137] Oracle MySQL Utilities CVE-2015-2576 Local Security Vulnerability
| [74133] Oracle MySQL Server CVE-2015-0498 Remote Security Vulnerability
| [74130] Oracle MySQL Server CVE-2015-0511 Remote Security Vulnerability
| [74126] Oracle MySQL Server CVE-2015-2566 Remote Security Vulnerability
| [74123] Oracle MySQL Server CVE-2015-2567 Remote Security Vulnerability
| [74121] Oracle MySQL Server CVE-2015-0507 Remote Security Vulnerability
| [74120] Oracle MySQL Server CVE-2015-0506 Remote Security Vulnerability
| [74115] Oracle MySQL Server CVE-2015-0499 Remote Security Vulnerability
| [74112] Oracle MySQL Server CVE-2015-0505 Remote Security Vulnerability
| [74110] Oracle MySQL Server CVE-2015-0405 Remote Security Vulnerability
| [74103] Oracle MySQL Server CVE-2015-0441 Remote Security Vulnerability
| [74102] Oracle MySQL Server CVE-2015-0503 Remote Security Vulnerability
| [74098] Oracle MySQL Server CVE-2015-0438 Remote Security Vulnerability
| [74095] Oracle MySQL Server CVE-2015-2571 Remote Security Vulnerability
| [74091] Oracle MySQL Server CVE-2015-0423 Remote Security Vulnerability
| [74089] Oracle MySQL Server CVE-2015-0433 Remote Security Vulnerability
| [74086] Oracle MySQL Server CVE-2015-0508 Remote Security Vulnerability
| [74085] Oracle MySQL Server CVE-2015-0439 Remote Security Vulnerability
| [74081] Oracle MySQL Server CVE-2015-0500 Remote Security Vulnerability
| [74078] Oracle MySQL Server CVE-2015-2573 Remote Security Vulnerability
| [74075] Oracle MySQL Connectors CVE-2015-2575 Remote Security Vulnerability
| [74073] Oracle MySQL Server CVE-2015-2568 Remote Security Vulnerability
| [74070] Oracle MySQL Server CVE-2015-0501 Remote Security Vulnerability
| [72728] RubyGems xaviershay-dm-rails ’storage.rb’ MySQL Credential Information Disclosure Vulnerabil
ity
| [72229] Oracle MySQL Server CVE-2015-0385 Remote Security Vulnerability
| [72227] Oracle MySQL Server CVE-2015-0374 Remote Security Vulnerability
| [72223] Oracle MySQL Server CVE-2015-0409 Remote Security Vulnerability
| [72217] Oracle MySQL Server CVE-2015-0432 Remote Security Vulnerability
| [72214] Oracle MySQL Server CVE-2015-0381 Remote Security Vulnerability
| [72210] Oracle MySQL Server CVE-2014-6568 Remote Security Vulnerability
| [72205] Oracle MySQL Server CVE-2015-0391 Remote Security Vulnerability
| [72200] Oracle MySQL Server CVE-2015-0382 Remote Security Vulnerability
| [72191] Oracle MySQL Server CVE-2015-0411 Remote Security Vulnerability

| [70550] Oracle MySQL Server CVE-2014-6507 Remote Security Vulnerability
| [70540] RETIRED: Oracle MySQL Server CVE-2012-5615 Remote Security Vulnerability
| [70532] Oracle MySQL Server CVE-2014-6463 Remote Security Vulnerability
| [70530] Oracle MySQL Server CVE-2014-6555 Remote Security Vulnerability
| [70525] Oracle MySQL Server CVE-2014-6489 Remote Security Vulnerability
| [70517] Oracle MySQL Server CVE-2014-4287 Remote Security Vulnerability
| [70516] Oracle MySQL Server CVE-2014-6505 Remote Security Vulnerability
| [70511] Oracle MySQL Server CVE-2014-6564 Remote Security Vulnerability
| [70510] Oracle MySQL Server CVE-2014-6520 Remote Security Vulnerability
| [70497] Oracle MySQL Server CVE-2014-6494 Remote Security Vulnerability
| [70496] Oracle MySQL Server CVE-2014-6495 Remote Security Vulnerability
| [70489] Oracle MySQL Server CVE-2014-6478 Remote Security Vulnerability
| [70487] Oracle MySQL Server CVE-2014-6559 Remote Security Vulnerability
| [70486] Oracle MySQL Server CVE-2014-6530 Remote Security Vulnerability
| [70478] Oracle MySQL Server CVE-2014-6500 Remote Security Vulnerability
| [70469] Oracle MySQL Server CVE-2014-6496 Remote Security Vulnerability
| [70462] Oracle MySQL Server CVE-2014-6551 Local Security Vulnerability
| [70455] Oracle MySQL Server CVE-2014-6484 Remote Security Vulnerability
| [70451] Oracle MySQL Server CVE-2014-6464 Remote Security Vulnerability
| [70448] Oracle MySQL Server CVE-2014-6474 Remote Security Vulnerability
| [70446] Oracle MySQL Server CVE-2014-6469 Remote Security Vulnerability
| [70444] Oracle MySQL Server CVE-2014-6491 Remote Security Vulnerability
| [69743] Oracle MySQL Client yaSSL Certificate Decode Buffer Overflow Vulnerability
| [69732] MySQL MyISAM Insecure Temporary File Creation Vulnerability
| [68736] RubyGems lean-ruport MySQL Credential Local Information Disclosure Vulnerability
| [68607] Oracle MySQL Server CVE-2014-4214 Remote Security Vulnerability
| [68602] Oracle MySQL Server CVE-2014-4240 Local Security Vulnerability
| [68598] Oracle MySQL Server CVE-2014-4233 Remote Security Vulnerability
| [68593] Oracle MySQL Server CVE-2014-4207 Remote Security Vulnerability
| [68587] Oracle MySQL Server CVE-2014-4238 Remote Security Vulnerability
| [68579] Oracle MySQL Server CVE-2014-2494 Remote Security Vulnerability
| [68573] Oracle MySQL Server CVE-2014-4260 Remote Security Vulnerability
| [68564] Oracle MySQL Server CVE-2014-4258 Remote Security Vulnerability
| [66896] Oracle MySQL Server CVE-2014-2436 Remote Security Vulnerability
| [66890] Oracle MySQL Server CVE-2014-2431 Remote Security Vulnerability
| [66885] Oracle MySQL Server CVE-2014-2444 Remote Security Vulnerability
| [66880] Oracle MySQL Server CVE-2014-2419 Remote Security Vulnerability
| [66872] Oracle MySQL Server CVE-2014-2434 Remote Security Vulnerability
| [66863] Oracle MySQL Server CVE-2014-2450 Remote Security Vulnerability
| [66858] Oracle MySQL Server CVE-2014-2430 Remote Security Vulnerability
| [66853] Oracle MySQL Server CVE-2014-2435 Remote Security Vulnerability
| [66850] Oracle MySQL Client CVE-2014-2440 Remote Security Vulnerability
| [66846] Oracle MySQL Server CVE-2014-2438 Remote Security Vulnerability
| [66835] Oracle MySQL Server CVE-2014-0384 Remote Security Vulnerability
| [66828] Oracle MySQL Server CVE-2014-2451 Remote Security Vulnerability
| [66823] Oracle MySQL Server CVE-2014-2442 Remote Security Vulnerability
| [66153] lighttpd ’mod_mysql_vhost.c’ SQL Injection Vulnerability
| [65890] InterWorx MySQL Password Information Disclosure Vulnerability
| [65621] Percona Toolkit for MySQL Automatic Version Check Information Disclosure Vulnerability
| [65298] Oracle MySQL Client ’main()’ Function Buffer Overflow Vulnerability
| [64908] Oracle MySQL Server CVE-2014-0402 Remote Security Vulnerability
| [64904] Oracle MySQL Server CVE-2014-0386 Remote Security Vulnerability
| [64898] Oracle MySQL Server CVE-2014-0401 Remote Security Vulnerability
| [64897] Oracle MySQL Server CVE-2014-0431 Remote Security Vulnerability
| [64896] Oracle MySQL Server CVE-2013-5908 Remote Security Vulnerability

| [64895] Oracle MySQL Server CVE-2014-0433 Remote Security Vulnerability
| [64893] Oracle MySQL Server CVE-2014-0430 Remote Security Vulnerability
| [64891] Oracle MySQL Server CVE-2013-5891 Remote Security Vulnerability
| [64888] Oracle MySQL Server CVE-2014-0420 Remote Security Vulnerability
| [64885] Oracle MySQL Server CVE-2013-5881 Remote Security Vulnerability
| [64880] Oracle MySQL Server CVE-2014-0412 Remote Security Vulnerability
| [64877] Oracle MySQL Server CVE-2014-0393 Remote Security Vulnerability
| [64873] Oracle MySQL Server CVE-2013-5894 Remote Security Vulnerability
| [64868] Oracle MySQL Server CVE-2014-0427 Remote Security Vulnerability
| [64864] Oracle MySQL Server CVE-2013-5860 Remote Security Vulnerability
| [64854] Oracle MySQL Server CVE-2013-5882 Remote Security Vulnerability
| [64849] Oracle MySQL Server CVE-2014-0437 Remote Security Vulnerability
| [64731] CSP MySQL User Manager 'login.php' Script SQL Injection Vulnerability
| [64630] Zen Cart 'mysql_zencart.sql' Information Disclosure Vulnerability
| [63125] Oracle MySQL Server CVE-2012-2750 Remote Security Vulnerability
| [63119] Oracle MySQL Server CVE-2013-5770 Remote Security Vulnerability
| [63116] Oracle MySQL Server CVE-2013-5793 Remote Security Vulnerability
| [63113] Oracle MySQL Server CVE-2013-5767 Remote Security Vulnerability
| [63109] Oracle MySQL Server CVE-2013-3839 Remote Security Vulnerability
| [63107] Oracle MySQL Server CVE-2013-5786 Remote Security Vulnerability
| [63105] Oracle MySQL Server CVE-2013-5807 Remote Security Vulnerability
| [62358] Oracle MySQL CVE-2005-2572 Remote Code Execution Vulnerability
| [61274] Oracle MySQL Server CVE-2013-3798 Remote Security Vulnerability
| [61272] Oracle MySQL Server CVE-2013-3809 Remote Security Vulnerability
| [61269] Oracle MySQL Server CVE-2013-3801 Remote Security Vulnerability
| [61264] Oracle MySQL Server CVE-2013-3793 Remote Security Vulnerability
| [61260] Oracle MySQL Server CVE-2013-3804 Remote Security Vulnerability
| [61256] Oracle MySQL Server CVE-2013-3805 Remote Security Vulnerability
| [61252] Oracle MySQL Server CVE-2013-3811 Remote Security Vulnerability
| [61249] Oracle MySQL Server CVE-2013-3812 Remote Security Vulnerability
| [61244] Oracle MySQL Server CVE-2013-3802 Remote Security Vulnerability
| [61241] Oracle MySQL Server CVE-2013-3795 Remote Security Vulnerability
| [61238] Oracle MySQL Server CVE-2013-3807 Remote Security Vulnerability
| [61235] Oracle MySQL Server CVE-2013-3806 Remote Security Vulnerability
| [61233] Oracle MySQL Server CVE-2013-3796 Remote Security Vulnerability
| [61227] Oracle MySQL Server CVE-2013-3808 Remote Security Vulnerability
| [61222] Oracle MySQL Server CVE-2013-3794 Remote Security Vulnerability
| [61214] Oracle MySQL Server CVE-2013-3810 Remote Security Vulnerability
| [61210] Oracle MySQL Server CVE-2013-3783 Remote Security Vulnerability
| [60424] Debian mysql-server CVE-2013-2162 Insecure File Creation Vulnerability
| [60001] Wireshark MySQL Dissector Denial of Service Vulnerability
| [59242] Oracle MySQL CVE-2013-2391 Local MySQL Server Vulnerability
| [59239] Oracle MySQL CVE-2013-1502 Local MySQL Server Vulnerability
| [59237] Oracle MySQL CVE-2013-1506 Remote MySQL Server Vulnerability
| [59232] Oracle MySQL CVE-2013-1567 Remote MySQL Server Vulnerability
| [59229] Oracle MySQL Server CVE-2013-1544 Remote Security Vulnerability
| [59227] Oracle MySQL CVE-2013-2376 Remote MySQL Server Vulnerability
| [59225] Oracle MySQL CVE-2013-1523 Remote MySQL Server Vulnerability
| [59224] Oracle MySQL Server CVE-2013-2392 Remote Security Vulnerability
| [59223] Oracle MySQL Server CVE-2013-1548 Remote Security Vulnerability
| [59222] RETIRED: Oracle MySQL CVE-2012-5614 Remote MySQL Server Vulnerability
| [59218] Oracle MySQL Server CVE-2013-1512 Remote Security Vulnerability
| [59217] Oracle MySQL CVE-2013-1526 Remote MySQL Server Vulnerability
| [59216] Oracle MySQL CVE-2013-1570 Remote MySQL Server Vulnerability
| [59215] Oracle MySQL Server CVE-2013-2381 Remote Security Vulnerability

| [59211] Oracle MySQL Server CVE-2013-1532 Remote Security Vulnerability
| [59210] Oracle MySQL CVE-2013-1555 Remote MySQL Server Vulnerability
| [59209] Oracle MySQL CVE-2013-2375 Remote MySQL Server Vulnerability
| [59207] Oracle MySQL Server CVE-2013-2389 Remote Security Vulnerability
| [59205] Oracle MySQL Server CVE-2013-1566 Remote Security Vulnerability
| [59202] Oracle MySQL CVE-2013-1531 Remote MySQL Server Vulnerability
| [59201] Oracle MySQL Server CVE-2013-1511 Remote Security Vulnerability
| [59196] Oracle MySQL CVE-2013-1552 Remote MySQL Server Vulnerability
| [59188] Oracle MySQL CVE-2013-2378 Remote MySQL Server Vulnerability
| [59180] Oracle MySQL CVE-2013-1521 Remote MySQL Server Vulnerability
| [59173] Oracle MySQL CVE-2013-2395 Remote MySQL Server Vulnerability
| [58511] MySQL and MariaDB Geometry Query Denial Of Service Vulnerability
| [57418] Oracle MySQL Server CVE-2013-0386 Remote Security Vulnerability
| [57417] Oracle MySQL Server CVE-2013-0389 Remote Security Vulnerability
| [57416] Oracle MySQL Server CVE-2013-0384 Remote Security Vulnerability
| [57415] Oracle MySQL Server CVE-2013-0371 Remote Security Vulnerability
| [57414] Oracle MySQL Server CVE-2012-0574 Remote Security Vulnerability
| [57412] Oracle MySQL Server CVE-2013-0385 Local Security Vulnerability
| [57411] Oracle MySQL Server CVE-2012-5060 Remote Security Vulnerability
| [57410] Oracle MySQL Server CVE-2012-1705 Remote Security Vulnerability
| [57408] Oracle MySQL Server CVE-2013-0367 Remote Security Vulnerability
| [57405] Oracle MySQL Server CVE-2013-0383 Remote Security Vulnerability
| [57400] Oracle MySQL Server CVE-2012-5096 Remote Security Vulnerability
| [57397] Oracle MySQL Server CVE-2013-0368 Remote Security Vulnerability
| [57391] Oracle MySQL Server CVE-2013-0375 Remote Security Vulnerability
| [57388] Oracle MySQL Server CVE-2012-1702 Remote Security Vulnerability
| [57385] Oracle MySQL Server CVE-2012-0572 Remote Security Vulnerability
| [57334] Oracle MySQL Server CVE-2012-0578 Remote Security Vulnerability
| [56837] Oracle MySQL and MariaDB CVE-2012-5627 Insecure Salt Generation Security Bypass Weakn
ess
| [56791] Oracle MySQL Remote Code Execution Vulnerability
| [56776] Oracle MySQL CVE-2012-5614 Denial of Service Vulnerability
| [56772] Oracle MySQL Remote Code Execution Vulnerability
| [56771] Oracle MySQL Server Privilege Escalation Vulnerability
| [56769] Oracle MySQL and MariaDB 'acl_get()' Buffer Overflow Vulnerability
| [56768] Oracle MySQL Server Heap Overflow Vulnerability
| [56766] Oracle MySQL Server Username Enumeration Weakness
| [56041] Oracle MySQL Server CVE-2012-3173 Remote MySQL Security Vulnerability
| [56036] Oracle MySQL Server CVE-2012-3163 Remote MySQL Security Vulnerability
| [56028] Oracle MySQL Server CVE-2012-3166 Remote Security Vulnerability
| [56027] Oracle MySQL Server CVE-2012-3160 Local Security Vulnerability
| [56022] Oracle MySQL Server CVE-2012-3147 Remote Security Vulnerability
| [56021] Oracle MySQL Server CVE-2012-3197 Remote Security Vulnerability
| [56018] Oracle MySQL Server CVE-2012-3167 Remote Security Vulnerability
| [56017] Oracle MySQL Server CVE-2012-3158 Remote Security Vulnerability
| [56013] Oracle MySQL Server CVE-2012-3156 Remote Security Vulnerability
| [56008] Oracle MySQL Server CVE-2012-3144 Remote Security Vulnerability
| [56006] Oracle MySQL Server CVE-2012-3149 Remote Security Vulnerability
| [56005] Oracle MySQL Server CVE-2012-3177 Remote Security Vulnerability
| [56003] Oracle MySQL Server CVE-2012-3180 Remote Security Vulnerability
| [55990] Oracle MySQL Server CVE-2012-3150 Remote Security Vulnerability
| [55715] MySQL MyISAM Table Symbolic Link CVE-2012-4452 Local Privilege Escalation Vulnerability
| [55120] Oracle MySQL CVE-2012-2749 Denial Of Service Vulnerability
| [54551] Oracle MySQL Server CVE-2012-0540 Remote Security Vulnerability
| [54549] Oracle MySQL Server CVE-2012-1735 Remote Security Vulnerability

| [54547] Oracle MySQL Server CVE-2012-1689 Remote Security Vulnerability
| [54540] Oracle MySQL Server CVE-2012-1734 Remote Security Vulnerability
| [54526] Oracle MySQL Server CVE-2012-1757 Remote Security Vulnerability
| [54524] Oracle MySQL Server CVE-2012-1756 Remote Security Vulnerability
| [53922] RETIRED: MySQL and MariaDB 'sql/password.c' Authentication Bypass Vulnerability
| [53911] Oracle MySQL CVE-2012-2122 User Login Security Bypass Vulnerability
| [53310] MySQLDumper 'menu.php' Remote PHP Code Execution Vulnerability
| [53306] MySQLDumper Multiple Security Vulnerabilities
| [53074] Oracle MySQL CVE-2012-1690 Remote MySQL Server Vulnerability
| [53071] Oracle MySQL CVE-2012-1696 Remote MySQL Server Vulnerability
| [53067] Oracle MySQL CVE-2012-1688 Remote MySQL Server Vulnerability
| [53064] Oracle MySQL CVE-2012-1697 Remote MySQL Server Vulnerability
| [53061] Oracle MySQL CVE-2012-0583 Remote MySQL Server Vulnerability
| [53058] Oracle MySQL CVE-2012-1703 Remote MySQL Server Vulnerability
| [52931] Oracle MySQL Server Multiple Unspecified Security Vulnerabilities
| [52154] RETIRED: MySQL 5.5.20 Unspecified Remote Code Execution Vulnerability
| [51925] MySQL Unspecified Remote Code Execution Vulnerability
| [51526] Oracle MySQL CVE-2012-0075 Remote MySQL Server Vulnerability
| [51525] Oracle MySQL CVE-2012-0493 Remote Vulnerability
| [51524] Oracle MySQL Server CVE-2012-0490 Remote Security Vulnerability
| [51523] Oracle MySQL Server CVE-2012-0494 Local Security Vulnerability
| [51522] Oracle MySQL Server CVE-2012-0495 Remote Security Vulnerability
| [51521] Oracle MySQL Server CVE-2012-0117 Remote MySQL Server Vulnerability
| [51520] Oracle MySQL Server CVE-2012-0114 Local Security Vulnerability
| [51519] Oracle MySQL Server CVE-2012-0112 Remote MySQL Server Vulnerability
| [51518] Oracle MySQL Server CVE-2012-0491 Remote Security Vulnerability
| [51517] Oracle MySQL CVE-2012-0120 Remote Vulnerability
| [51516] Oracle MySQL Server CVE-2012-0492 Remote MySQL Server Vulnerability
| [51515] Oracle MySQL Server CVE-2012-0484 Remote Security Vulnerability
| [51514] Oracle MySQL Server CVE-2012-0486 Remote Security Vulnerability
| [51513] Oracle MySQL Server CVE-2012-0485 Remote Security Vulnerability
| [51512] Oracle MySQL CVE-2012-0119 Remote Vulnerability
| [51511] Oracle MySQL CVE-2012-0118 Remote MySQL Server Vulnerability
| [51510] Oracle MySQL Server CVE-2012-0489 Remote MySQL Server Vulnerability
| [51509] Oracle MySQL Server CVE-2012-0087 Remote Security Vulnerability
| [51508] Oracle MySQL CVE-2012-0116 Remote MySQL Server Vulnerability
| [51507] Oracle MySQL Server CVE-2012-0496 Remote Security Vulnerability
| [51506] Oracle MySQL Server CVE-2012-0488 Remote MySQL Server Vulnerability
| [51505] Oracle MySQL Server CVE-2012-0101 Remote Security Vulnerability
| [51504] Oracle MySQL CVE-2012-0115 Remote Vulnerability
| [51503] Oracle MySQL Server CVE-2012-0487 Remote MySQL Server Vulnerability
| [51502] Oracle MySQL Server CVE-2012-0102 Remote Security Vulnerability
| [51493] Oracle MySQL CVE-2011-2262 Remote MySQL Server Vulnerability
| [51488] Oracle MySQL CVE-2012-0113 Remote MySQL Server Vulnerability
| [50139] DBD::mysqlPP Unspecified SQL Injection Vulnerability
| [48466] MySQLDriverCS SQL Injection Vulnerability
| [47919] Zend Framework 'PDO_MySql' Security Bypass Vulnerability
| [47871] Oracle MySQL Prior to 5.1.52 Multiple Denial Of Service Vulnerabilities
| [47693] DirectAdmin 'mysql_backup' Folder Permissions Information Disclosure Vulnerability
| [46655] pywebdav MySQL Authentication Module SQL Injection Vulnerability
| [46456] MySQL Eventum 'full_name' Field HTML Injection Vulnerability
| [46380] MySQL Eventum Multiple HTML Injection Vulnerabilities
| [46056] PHP MySQLi Extension 'set_magic_quotes_runtime' Function Security-Bypass Weakness
| [43884] phpFK - PHP Forum Script ohne MySQL 'page_bottom.php' Local File Include Vulnerability
| [43677] Oracle MySQL Prior to 5.1.50 Privilege Escalation Vulnerability

| [43676] Oracle MySQL Prior to 5.1.51 Multiple Denial Of Service Vulnerabilities
| [42646] Oracle MySQL Prior to 5.1.49 'JOIN' Statement Denial Of Service Vulnerability
| [42643] Oracle MySQL Prior to 5.1.49 'DDL' Statements Denial Of Service Vulnerability
| [42638] Oracle MySQL Prior to 5.1.49 Malformed 'BINLOG' Arguments Denial Of Service Vulnerability
| [42633] Oracle MySQL 'HANDLER' interface Denial Of Service Vulnerability
| [42625] Oracle MySQL 'LOAD DATA INFILE' Denial Of Service Vulnerability
| [42599] Oracle MySQL 'EXPLAIN' Denial Of Service Vulnerability
| [42598] Oracle MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability
| [42596] Oracle MySQL Prior to 5.1.49 'WITH ROLLUP' Denial Of Service Vulnerability
| [42586] RETIRED: Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service Vulnerabilities
| [42417] Zmanda Recovery Manager for MySQL Multiple Local Privilege Escalation Vulnerabilities
| [41440] phpFK - PHP Forum Script ohne MySQL 'upload.php' Arbitrary File Upload Vulnerability
| [41198] Oracle MySQL 'ALTER DATABASE' Remote Denial Of Service Vulnerability
| [40537] MySQL Enterprise Monitor Multiple Unspecified Cross Site Request Forgery Vulnerabilities
| [40506] RETIRED: phpGraphy 'mysql_cleanup.php' Remote File Include Vulnerability
| [40461] PHP Mysqlnd Extension Information Disclosure and Multiple Buffer Overflow Vulnerabilities
| [40257] Oracle MySQL DROP TABLE MyISAM Symbolic Link Local Security Bypass Vulnerability
| [40109] Oracle MySQL 'COM_FIELD_LIST' Command Packet Security Bypass Vulnerability
| [40106] Oracle MySQL 'COM_FIELD_LIST' Command Buffer Overflow Vulnerability
| [40100] Oracle MySQL Malformed Packet Handling Remote Denial of Service Vulnerability
| [40045] Advanced Poll 'mysql_host' Parameter Cross Site Scripting Vulnerability
| [39918] FlexAppsStore Flex MySQL Connector Unauthorized Access Vulnerability
| [39543] MySQL UNINSTALL PLUGIN Security Bypass Vulnerability
| [38642] Timeclock Software 'mysqldump' Local Information Disclosure Vulnerability
| [38043] MySQL 'sql/sql_table.cc' CREATE TABLE Security Bypass Vulnerability
| [37943] MySQL with yaSSL SSL Certificate Handling Remote Stack Buffer Overflow Vulnerability
| [37770] TYPO3 kiddog_mysqldumper Unspecified Information Disclosure Vulnerability
| [37640] MySQL 5.0.51a Unspecified Remote Code Execution Vulnerability
| [37297] MySQL Multiple Remote Denial Of Service Vulnerabilities
| [37076] MySQL OpenSSL Server Certificate yaSSL Security Bypass Vulnerability
| [37075] MySQL MyISAM Table Symbolic Link Local Privilege Escalation Vulnerability
| [36242] MySQL 5.x Unspecified Buffer Overflow Vulnerability
| [35858] MySQL Connector/J Unicode Character String SQL Injection Vulnerability
| [35609] MySQL 'sql_parse.cc' Multiple Format String Vulnerabilities
| [35514] MySQL Connector/Net SSL Certificate Validation Security Bypass Vulnerability
| [33972] MySQL XPath Expression Remote Denial Of Service Vulnerability
| [33392] 'mod_auth_mysql' Package Multibyte Character Encoding SQL Injection Vulnerability
| [32978] MySQL Calendar 'username' Parameter SQL Injection Vulnerability
| [32914] MySQL Calendar Cookie Authentication Bypass Vulnerability
| [32157] MySQL Quick Admin 'actions.php' Local File Include Vulnerability
| [32000] Agora 'MysqlfinderAdmin.php' Remote File Include Vulnerability
| [31517] MySQL Quick Admin 'index.php' Local File Include Vulnerability
| [31486] MySQL Command Line Client HTML Special Characters HTML Injection Vulnerability
| [31425] PromoteWeb MySQL 'go.php' SQL Injection Vulnerability
| [31081] MySQL Empty Binary String Literal Remote Denial Of Service Vulnerability
| [30835] mysql-lists Unspecified Cross Site Scripting Vulnerability
| [30529] Keld PHP-MySQL News Script 'login.php' SQL Injection Vulnerability
| [30383] phpwebnews-mysql Multiple SQL Injection Vulnerabilities
| [29106] MySQL MyISAM Table Privileges Secuity Bypass Vulnerability
| [29048] GEDCOM_to_MySQL2 Multiple Cross-Site Scripting Vulnerabilities
| [28351] MySQL INFORMATION_SCHEMA Remote Denial Of Service Vulnerability
| [27938] DSPAM Debian 'libdspam7-drv-mysql' Cron Job MySQL Calls Local Information Disclosure Vuln
erability
| [27202] PHP Webquest MySQL Credentials Information Disclosure Vulnerability
| [27032] PHP MySQL Open Source Help Desk 'form.php' Code Injection Vulnerability

| [26947] MySQL Server Unspecified Remote Arbitrary Command Execution Vulnerability
| [26832] MySQL Server Privilege Escalation And Denial Of Service Vulnerabilities
| [26829] aurora framework Db_mysql.LIB SQL Injection Vulnerability
| [26765] MySQL Server RENAME TABLE System Table Overwrite Vulnerability
| [26353] MySQL Server InnoDB CONVERT_SEARCH_MODE_TO_INNOBASE Function Denial Of Servi
ce Vulnerability
| [26304] AdventNet EventLog Analyzer Insecure Default MySQL Password Unauthorized Access Vulnera
bility
| [26156] Bacula MySQL Password Information Disclosure Vulnerability
| [26095] Asterisk 'asterisk-addons' CDR_ADDON_MYSQL Module SQL Injection Vulnerability
| [25017] MySQL Access Validation and Denial of Service Vulnerabilities
| [24759] MySQLDumper Apache Access Control Authentication Bypass Vulnerability
| [24016] MySQL Rename Table Function Access Validation Vulnerability
| [24011] MySQL Security Invoker Privilege Escalation Vulnerability
| [24008] MySQL Alter Table Function Information Disclosure Vulnerability
| [23911] MySQL IF Query Handling Remote Denial Of Service Vulnerability
| [23176] Eve-Nuke Forums MySQL.PHP Remote File Include Vulnerability
| [22941] MySQL Commander Remote File Include Vulnerability
| [22900] MySQL Single Row SubSelect Remote Denial Of Service Vulnerability
| [22474] CPanel PassWDMySQL Cross-Site Scripting Vulnerability
| [22431] MySQLNewsEngine Affichearticles.PHP3 Remote File Include Vulnerability
| [20460] MySQLDumper SQL.PHP Cross-Site Scripting Vulnerability
| [20222] PABugs Class.MySQL.PHP Remote File Include Vulnerability
| [20165] ZoomStats MySQL.PHP Remote File Include Vulnerability
| [19794] MySQL Multiupdate and Subselects Denial Of Service Vulnerability
| [19559] MySQL Privilege Elevation and Security Bypass Vulnerabilities
| [19279] MySQL MERGE Privilege Revoke Bypass Vulnerability
| [19240] Banex PHP MySQL Banner Exchange Multiple Remote Vulnerabilities
| [19032] MySQL Server Date_Format Denial Of Service Vulnerability
| [18717] PHP/MySQL Classifieds AddAsset1.PHP Multiple HTML Injection Vulnerabilities
| [18439] MySQL Server Str_To_Date Remote Denial Of Service Vulnerability
| [18219] MySQL Mysql_real_escape Function SQL Injection Vulnerability
| [17780] MySQL Remote Information Disclosure and Buffer Overflow Vulnerabilities
| [17224] Cholod MySQL Based Message Board Mb.CGI SQL Injection Vulnerability
| [17223] Cholod MySQL Based Message Board Multiple HTML Injection Vulnerabilities
| [17147] Woltlab Burning Board Class_DB_MySQL.PHP Cross-Site Scripting Vulnerability
| [16850] MySQL Query Logging Bypass Vulnerability
| [16620] PHP/MYSQL Timesheet Multiple SQL Injection Vulnerabilities
| [16564] PAM-MySQL Code Execution And Denial Of Service Vulnerabilities
| [16219] PHP MySQLI Error Logging Remote Format String Vulnerability
| [16145] PHP MySQL_Connect Remote Buffer Overflow Vulnerability
| [15852] MySQL Auction Search Module Cross-Site Scripting Vulnerability
| [14509] MySQL User-Defined Function Buffer Overflow Vulnerability
| [14437] MySQL Eventum Multiple SQL Injection Vulnerabilities
| [14436] MySQL Eventum Multiple Cross-Site Scripting Vulnerabilities
| [13913] xMySQLadmin Insecure Temporary File Creation Vulnerability
| [13660] MySQL mysql_install_db Insecure Temporary File Creation Vulnerability
| [13378] MySQL MaxDB WebDAV IF Parameter Remote Buffer Overflow Vulnerability
| [13369] MySQL MaxDB WebDAV Lock Token Remote Buffer Overflow Vulnerability
| [13368] MySQL MaxDB HTTP GET Request Remote Buffer Overflow Vulnerability
| [12805] MySQL MaxDB WebAgent Input Validation Multiple Remote Denial Of Service Vulnerabilities
| [12781] MySQL AB MySQL Multiple Remote Vulnerabilities
| [12313] MySQL MaxDB WebAgent Remote Denial of Service Vulnerabilities
| [12277] MySQL Database MySQLAccess Local Insecure Temporary File Creation Vulnerability
| [12265] MySQL MaxDB WebAgent WebSQL Password Parameter Remote Buffer Overflow Vulnerability

| [12133] MySQL Eventum Multiple Input Validation Vulnerabilities
| [11844] MySQL MaxDB WebDav Handler Overwrite Header Remote Buffer Overflow Vulnerability
| [11843] MySQL MaxDB WAHTTP Server Remote Denial Of Service Vulnerability
| [11435] MySQL Database Unauthorized GRANT Privilege Vulnerability
| [11432] MySQL Remote FULLTEXT Search Denial Of Service Vulnerability
| [11357] MySQL Multiple Local Vulnerabilities
| [11346] MySQL MaxDB WebDBM Server Name Denial of Service Vulnerability
| [11291] MySQL Unspecified Insecure Temporary File Creation Vulnerability
| [11261] MySQL Bounded Parameter Statement Execution Remote Buffer Overflow Vulnerability
| [11234] AllWebScripts MySQLGuest HTML Injection Vulnerability
| [10986] Ben Yacoub Hatem MySQL Backup Pro Undisclosed 'getbackup()' Vulnerability
| [10981] MySQL Mysql_real_connect Function Potential Remote Buffer Overflow Vulnerability
| [10969] MySQL Mysqlhotcopy Script Insecure Temporary File Creation Vulnerability
| [10655] MySQL Password Length Remote Buffer Overflow Vulnerability
| [10654] MySQL Authentication Bypass Vulnerability
| [10142] MySQL MYSQLD_Multi Insecure Temporary File Creation Vulnerability
| [9976] MySQL Aborted Bug Report Insecure Temporary File Creation Vulnerability
| [8796] MySQL Multiple Vulnerabilities
| [8590] MySQL Password Handler Buffer Overflow Vulnerability
| [8245] MySQL AB ODBC Driver Plain Text Password Vulnerability
| [7887] MySQL libmysqlclient Library mysql_real_connect() Buffer Overrun Vulnerability
| [7500] MySQL Weak Password Encryption Vulnerability
| [7052] MySQL mysqld Privilege Escalation Vulnerability
| [7041] MySQL Control Center Insecure Default File Permission Vulnerability
| [6718] MySQL Double Free Heap Corruption Vulnerability
| [6375] MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability
| [6374] MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerability
| [6373] MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability
| [6370] MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability
| [6368] MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
| [5948] PHPRank MySQL Error Unauthorized Access Vulnerability
| [5853] MySQL DataDir Parameter Local Buffer Overflow Vulnerability
| [5513] MySQL Logging Not Enabled Weak Default Configuration Vulnerability
| [5511] MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability
| [5503] MySQL Null Root Password Weak Default Configuration Vulnerability
| [4409] Cyrus SASL LDAP+MySQL Authentication Patch SQL Command Execution Vulnerability
| [4026] PHP MySQL Safe_Mode Filesystem Circumvention Vulnerability
| [3907] Conectiva Linux MySQL World Readable Log File Vulnerability
| [3381] WinMySQLadmin Plain Text Password Storage Vulnerability
| [3284] Inter7 vpopmail MySQL Authentication Data Recovery Vulnerability
| [3255] Apache mod_auth_mysql Remote SQL Query Manipulation Vulnerability
| [2522] MySQL Root Operation Symbolic Link File Overwriting Vulnerability
| [2380] MySQL SHOW GRANTS Pasword Hash Disclosure Vulnerability
| [2262] Mysql Local Buffer Overflow Vulnerability
| [1850] pam_mysql Authentication Input Validation Vulnerability
| [1826] MySQL Authentication Algorithm Vulnerability
| [1557] PCCS Mysql Database Admin Tool Username/Password Exposure Vulnerability
| [975] MySQL Unauthenticated Remote Access Vulnerability
| [926] MySQL GRANT Global Password Changing Vulnerability
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [85724] Oracle MySQL Server XA Transactions denial of service
| [85723] Oracle MySQL Server Server Replication denial of service
| [85722] Oracle MySQL Server InnoDB denial of service
| [85721] Oracle MySQL Server Server Privileges unspecified

| [85720] Oracle MySQL Server Server Partition denial of service
| [85719] Oracle MySQL Server Server Parser denial of service
| [85718] Oracle MySQL Server Server Options denial of service
| [85717] Oracle MySQL Server Server Options denial of service
| [85716] Oracle MySQL Server Server Optimizer denial of service
| [85715] Oracle MySQL Server Server Optimizer denial of service
| [85714] Oracle MySQL Server Prepared Statements denial of service
| [85713] Oracle MySQL Server InnoDB denial of service
| [85712] Oracle MySQL Server Full Text Search denial of service
| [85711] Oracle MySQL Server Data Manipulation Language denial of service
| [85710] Oracle MySQL Server Data Manipulation Language denial of service
| [85709] Oracle MySQL Server Audit Log unspecified
| [85708] Oracle MySQL Server MemCached unspecified
| [84846] Debian mysql-server package information disclosure
| [84375] Wireshark MySQL dissector denial of service
| [83554] Oracle MySQL Server Server Partition denial of service
| [83553] Oracle MySQL Server Server Locking denial of service
| [83552] Oracle MySQL Server Server Install unspecified
| [83551] Oracle MySQL Server Server Types denial of service
| [83550] Oracle MySQL Server Server Privileges unspecified
| [83549] Oracle MySQL Server InnoDB denial of service
| [83548] Oracle MySQL Server InnoDB denial of service
| [83547] Oracle MySQL Server Data Manipulation Language denial of service
| [83546] Oracle MySQL Server Stored Procedure denial of service
| [83545] Oracle MySQL Server Server Replication denial of service
| [83544] Oracle MySQL Server Server Partition denial of service
| [83543] Oracle MySQL Server Server Optimizer denial of service
| [83542] Oracle MySQL Server InnoDB denial of service
| [83541] Oracle MySQL Server Information Schema denial of service
| [83540] Oracle MySQL Server Data Manipulation Language denial of service
| [83539] Oracle MySQL Server Data Manipulation Language denial of service
| [83538] Oracle MySQL Server Server Optimizer unspecified
| [83537] Oracle MySQL Server MemCached denial of service
| [83536] Oracle MySQL Server Server Privileges unspecified
| [83535] Oracle MySQL Server Server Privileges unspecified
| [83534] Oracle MySQL Server Server unspecified
| [83533] Oracle MySQL Server Information Schema unspecified
| [83532] Oracle MySQL Server Server Locking unspecified
| [83531] Oracle MySQL Server Data Manipulation Language denial of service
| [83388] MySQL administrative login attempt detected
| [82963] Mambo MySQL database information disclosure
| [82946] Oracle MySQL buffer overflow
| [82945] Oracle MySQL buffer overflow
| [82895] Oracle MySQL and MariaDB geometry queries denial of service
| [81577] MySQL2JSON extension for TYPO3 unspecified SQL injection
| [81325] Oracle MySQL Server Server Privileges denial of service
| [81324] Oracle MySQL Server Server Partition denial of service
| [81323] Oracle MySQL Server Server Optimizer denial of service
| [81322] Oracle MySQL Server Server Optimizer denial of service
| [81321] Oracle MySQL Server Server denial of service
| [81320] Oracle MySQL Server MyISAM denial of service
| [81319] Oracle MySQL Server InnoDB denial of service
| [81318] Oracle MySQL Server InnoDB denial of service
| [81317] Oracle MySQL Server Server Locking denial of service
| [81316] Oracle MySQL Server Server denial of service

| [81315] Oracle MySQL Server Server Replication unspecified
| [81314] Oracle MySQL Server Server Replication unspecified
| [81313] Oracle MySQL Server Stored Procedure denial of service
| [81312] Oracle MySQL Server Server Optimizer denial of service
| [81311] Oracle MySQL Server Information Schema denial of service
| [81310] Oracle MySQL Server GIS Extension denial of service
| [80790] Oracle MySQL yaSSL buffer overflow
| [80553] Oracle MySQL and MariaDB salt security bypass
| [80443] Oracle MySQL Server unspecified code execution
| [80442] Oracle MySQL Server acl_get() buffer overflow
| [80440] Oracle MySQL Server table buffer overflow
| [80435] Oracle MySQL Server database privilege escalation
| [80434] Oracle MySQL Server COM_BINLOG_DUMP denial of service
| [80433] Oracle MySQL Server Stuxnet privilege escalation
| [80432] Oracle MySQL Server authentication information disclosure
| [79394] Oracle MySQL Server Server Installation information disclosure
| [79393] Oracle MySQL Server Server Replication denial of service
| [79392] Oracle MySQL Server Server Full Text Search denial of service
| [79391] Oracle MySQL Server Server denial of service
| [79390] Oracle MySQL Server Client information disclosure
| [79389] Oracle MySQL Server Server Optimizer denial of service
| [79388] Oracle MySQL Server Server Optimizer denial of service
| [79387] Oracle MySQL Server Server denial of service
| [79386] Oracle MySQL Server InnoDB Plugin denial of service
| [79385] Oracle MySQL Server InnoDB denial of service
| [79384] Oracle MySQL Server Client unspecified
| [79383] Oracle MySQL Server Server denial of service
| [79382] Oracle MySQL Server Protocol unspecified
| [79381] Oracle MySQL Server Information Schema unspecified
| [78954] SilverStripe MySQLDatabase.php information disclosure
| [78948] MySQL MyISAM table symlink
| [77865] MySQL unknown vuln
| [77864] MySQL sort order denial of service
| [77768] MySQLDumper refresh_dblist.php information disclosure
| [77177] MySQL Squid Access Report unspecified cross-site scripting
| [77065] Oracle MySQL Server Optimizer denial of service
| [77064] Oracle MySQL Server Optimizer denial of service
| [77063] Oracle MySQL Server denial of service
| [77062] Oracle MySQL InnoDB denial of service
| [77061] Oracle MySQL GIS Extension denial of service
| [77060] Oracle MySQL Server Optimizer denial of service
| [76189] MySQL unspecified error
| [76188] MySQL attempts security bypass
| [75287] MySQLDumper restore.php information disclosure
| [75286] MySQLDumper filemanagement.php directory traversal
| [75285] MySQLDumper main.php cross-site request forgery
| [75284] MySQLDumper install.php cross-site scripting
| [75283] MySQLDumper install.php file include
| [75282] MySQLDumper menu.php code execution
| [75022] Oracle MySQL Server Server Optimizer denial of service
| [75021] Oracle MySQL Server Server Optimizer denial of service
| [75020] Oracle MySQL Server Server DML denial of service
| [75019] Oracle MySQL Server Partition denial of service
| [75018] Oracle MySQL Server MyISAM denial of service
| [75017] Oracle MySQL Server Server Optimizer denial of service

| [74672] Oracle MySQL Server multiple unspecified
| [73092] MySQL unspecified code execution
| [72540] Oracle MySQL Server denial of service
| [72539] Oracle MySQL Server unspecified
| [72538] Oracle MySQL Server denial of service
| [72537] Oracle MySQL Server denial of service
| [72536] Oracle MySQL Server unspecified
| [72535] Oracle MySQL Server denial of service
| [72534] Oracle MySQL Server denial of service
| [72533] Oracle MySQL Server denial of service
| [72532] Oracle MySQL Server denial of service
| [72531] Oracle MySQL Server denial of service
| [72530] Oracle MySQL Server denial of service
| [72529] Oracle MySQL Server denial of service
| [72528] Oracle MySQL Server denial of service
| [72527] Oracle MySQL Server denial of service
| [72526] Oracle MySQL Server denial of service
| [72525] Oracle MySQL Server information disclosure
| [72524] Oracle MySQL Server denial of service
| [72523] Oracle MySQL Server denial of service
| [72522] Oracle MySQL Server denial of service
| [72521] Oracle MySQL Server denial of service
| [72520] Oracle MySQL Server denial of service
| [72519] Oracle MySQL Server denial of service
| [72518] Oracle MySQL Server unspecified
| [72517] Oracle MySQL Server unspecified
| [72516] Oracle MySQL Server unspecified
| [72515] Oracle MySQL Server denial of service
| [72514] Oracle MySQL Server unspecified
| [71965] MySQL port denial of service
| [70680] DBD::mysqlPP unspecified SQL injection
| [70370] TaskFreak! multi-mysql unspecified path disclosure
| [68799] mod_authnz_external module for Apache mysql-auth.pl SQL injection
| [68294] MySQLDriverCS statement.cs sql injection
| [68175] Prosody MySQL denial of service
| [67539] Zend Framework MySQL PDO security bypass
| [67254] DirectAdmin MySQL information disclosure
| [66567] Xoops mysql.sql information disclosure
| [65871] PyWebDAV MySQLAuthHandler class SQL injection
| [65543] MySQL Select Arbitrary data into a File
| [65529] MySQL Eventum full_name field cross-site scripting
| [65380] Oracle MySQL Eventum forgot_password.php cross-site scripting
| [65379] Oracle MySQL Eventum list.php cross-site scripting
| [65266] Accellion File Transfer Appliance MySQL default password
| [64878] MySQL Geometry denial of service
| [64877] MySQL EXPLAIN EXTENDED denial of service
| [64876] MySQL prepared statement denial of service
| [64845] MySQL extreme-value denial of service
| [64844] MySQL Gis_line_string::init_from_wkb denial of service
| [64843] MySQL user-variable denial of service
| [64842] MySQL view preparation denial of service
| [64841] MySQL prepared statement denial of service
| [64840] MySQL LONGBLOB denial of service
| [64839] MySQL invocations denial of service
| [64838] MySQL Gis_line_string::init_from_wkb denial of service

| [64689] MySQL dict0crea.c denial of service
| [64688] MySQL SET column denial of service
| [64687] MySQL BINLOG command denial of service
| [64686] MySQL InnoDB denial of service
| [64685] MySQL HANDLER interface denial of service
| [64684] MySQL Item_singlerow_subselect::store denial of service
| [64683] MySQL OK packet denial of service
| [63518] MySQL Query Browser GUI Tools information disclosure
| [63517] MySQL Administrator GUI Tools information disclosure
| [62272] MySQL PolyFromWKB() denial of service
| [62269] MySQL LIKE predicates denial of service
| [62268] MySQL joins denial of service
| [62267] MySQL GREATEST() or LEAST() denial of service
| [62266] MySQL GROUP_CONCAT() denial of service
| [62265] MySQL expression values denial of service
| [62264] MySQL temporary table denial of service
| [62263] MySQL LEAST() or GREATEST() denial of service
| [62262] MySQL replication privilege escalation
| [61739] MySQL WITH ROLLUP denial of service
| [61343] MySQL LOAD DATA INFILE denial of service
| [61342] MySQL EXPLAIN denial of service
| [61341] MySQL HANDLER denial of service
| [61340] MySQL BINLOG denial of service
| [61339] MySQL IN() or CASE denial of service
| [61338] MySQL SET denial of service
| [61337] MySQL DDL denial of service
| [61318] PHP mysqlnd_wireprotocol.c buffer overflow
| [61317] PHP php_mysqlnd_read_error_from_line buffer overflow
| [61316] PHP php_mysqlnd_auth_write buffer overflow
| [61274] MySQL TEMPORARY InnoDB denial of service
| [59905] MySQL ALTER DATABASE denial of service
| [59841] CMySQLite updateUser.php cross-site request forgery
| [59112] MySQL Enterprise Monitor unspecified cross-site request forgery
| [59075] PHP php_mysqlnd_auth_write() buffer overflow
| [59074] PHP php_mysqlnd_read_error_from_line() buffer overflow
| [59073] PHP php_mysqlnd_rset_header_read() buffer overflow
| [59072] PHP php_mysqlnd_ok_read() information disclosure
| [58842] MySQL DROP TABLE file deletion
| [58676] Template Shares MySQL information disclosure
| [58531] MySQL COM_FIELD_LIST buffer overflow
| [58530] MySQL packet denial of service
| [58529] MySQL COM_FIELD_LIST security bypass
| [58311] ClanSphere the captcha generator and MySQL driver SQL injection
| [57925] MySQL UNINSTALL PLUGIN security bypass
| [57006] Quicksilver Forums mysqldump information disclosure
| [56800] Employee Timeclock Software mysqldump information disclosure
| [56200] Flex MySQL Connector ActionScript SQL injection
| [55877] MySQL yaSSL buffer overflow
| [55622] kiddog_mysqldumper extension for TYPO3 information disclosure
| [55416] MySQL unspecified buffer overflow
| [55382] Ublog UblogMySQL.sql information disclosure
| [55251] PHP-MySQL-Quiz editquiz.php SQL injection
| [54597] MySQL sql_table.cc security bypass
| [54596] MySQL mysqld denial of service
| [54365] MySQL OpenSSL security bypass

| [54364] MySQL MyISAM table symlink
| [53950] The mysql-ocaml mysql_real_escape_string weak security
| [52978] Zmanda Recovery Manager for MySQL mysqlhotcopy privilege escalation
| [52977] Zmanda Recovery Manager for MySQL socket-server.pl command execution
| [52660] iScouter PHP Web Portal MySQL Password Retrieval
| [52220] aa33code mysql.inc information disclosure
| [52122] MySQL Connector/J unicode SQL injection
| [51614] MySQL dispatch_command() denial of service
| [51406] MySQL Connector/NET SSL spoofing
| [49202] MySQL UDF command execution
| [49050] MySQL XPath denial of service
| [48919] Cisco Application Networking Manager MySQL default account password
| [48163] libapache2-mod-auth-mysql module for Debian multibyte encoding SQL injection
| [47544] MySQL Calendar index.php SQL injection
| [47476] MySQL Calendar index.php nodstrumCalendarV2 security bypass
| [45649] MySQL MyISAM symlink security bypass
| [45648] MySQL MyISAM symlinks security bypass
| [45607] MySQL Quick Admin actions.php file include
| [45606] MySQL Quick Admin index.php file include
| [45590] MySQL command-line client cross-site scripting
| [45436] PromoteWeb MySQL go.php SQL injection
| [45042] MySQL empty bit-string literal denial of service
| [44662] mysql-lists unspecified cross-site scripting
| [42267] MySQL MyISAM security bypass
| [42211] GEDCOM_to_MySQL2 index.php, info.php and prenom.php cross-site scripting
| [42014] miniBB setup_mysql.php and setup_options.php SQL injection
| [40920] MySQL sql_select.cc denial of service
| [40734] MySQL Server BINLOG privilege escalation
| [40350] MySQL password information disclosure
| [39415] Debian GNU/Linux libdspam7-drv-mysql cron job password disclosure
| [39402] PHP LOCAL INFILE and MySQL extension security bypass
| [38999] aurora framework db_mysql.lib SQL injection
| [38990] MySQL federated engine denial of service
| [38989] MySQL DEFINER value privilege escalation
| [38988] MySQL DATA DIRECTORY and INDEX DIRECTORY privilege escalation
| [38964] MySQL RENAME TABLE symlink
| [38733] ManageEngine EventLog Analyzer MySQL default password
| [38284] MySQL ha_innodb.cc convert_search_mode_to_innobase() denial of service
| [38189] MySQL default root password
| [37235] Asterisk-Addons cdr_addon_mysql module SQL injection
| [37099] RHSA update for MySQL case sensistive database name privilege escalation not installed
| [36555] PHP MySQL extension multiple functions security bypass
| [35960] MySQL view privilege escalation
| [35959] MySQL CREATE TABLE LIKE information disclosure
| [35958] MySQL connection protocol denial of service
| [35291] MySQLDumper main.php security bypass
| [34811] MySQL udf_init and mysql_create_function command execution
| [34809] MySQL mysql_update privilege escalation
| [34349] MySQL ALTER information disclosure
| [34348] MySQL mysql_change_db privilege escalation
| [34347] MySQL RENAME TABLE weak security
| [34232] MySQL IF clause denial of service
| [33388] Advanced Website Creator (AWC) mysql_escape_string SQL injection
| [33285] Eve-Nuke mysql.php file include
| [32957] MySQL Commander dbopen.php file include

| [32933] cPanel load_language.php and mysqlconfig.php file include
| [32911] MySQL filesort function denial of service
| [32462] cPanel passwdmysql cross-site scripting
| [32288] RHSA-2006:0544 updates for mysql not installed
| [32266] MySQLNewsEngine affichearticles.php3 file include
| [31244] The Address Book MySQL export.php password information disclosure
| [31037] Php/Mysql Site Builder (PHPBuilder) htm2php.php directory traversal
| [30760] BTSaveMySql URL file disclosure
| [30191] StoryStream mysql.php and mysqli.php file include
| [30085] MySQL MS-DOS device name denial of service
| [30031] Agora MysqlfinderAdmin.php file include
| [29438] MySQLDumper mysqldumper_path/sql.php cross-site scripting
| [29179] paBugs class.mysql.php file include
| [29120] ZoomStats MySQL file include
| [28448] MySQL case sensitive database name privilege escalation
| [28442] MySQL GRANT EXECUTE privilege escalation
| [28387] FunkBoard admin/mysql_install.php and admin/pg_install.php unauthorized access
| [28202] MySQL multiupdate subselect query denial of service
| [28180] MySQL MERGE table security bypass
| [28176] PHP MySQL Banner Exchange lib.inc information disclosure
| [27995] Opsware Network Automation System MySQL plaintext password
| [27904] MySQL date_format() format string
| [27635] MySQL Instance Manager denial of service
| [27212] MySQL SELECT str_to_date denial of service
| [26875] MySQL ASCII escaping SQL injection
| [26420] Apple Mac OS X MySQL Manager blank password
| [26236] MySQL login packet information disclosure
| [26232] MySQL COM_TABLE_DUMP buffer overflow
| [26228] MySQL sql_parce.cc information disclosure
| [26042] MySQL running
| [25313] WoltLab Burning Board class_db_mysql.php cross-site scripting
| [24966] MySQL mysql_real_query logging bypass
| [24653] PAM-MySQL logging function denial of service
| [24652] PAM-MySQL authentication double free code execution
| [24567] PHP/MYSQL Timesheet index.php and changehrs.php SQL injection
| [24095] PHP ext/mysqli exception handling format string
| [23990] PHP mysql_connect() buffer overflow
| [23596] MySQL Auction search module could allow cross-site scripting
| [22642] RHSA-2005:334 updates for mysql not installed
| [21757] MySQL UDF library functions command execution
| [21756] MySQL LoadLibraryEx function denial of service
| [21738] MySQL UDF mysql_create_function function directory traversal
| [21737] MySQL user defined function buffer overflow
| [21640] MySQL Eventum multiple class SQL injection
| [21638] MySQL Eventum multiple scripts cross-site scripting
| [20984] xmysqladmin temporary file symlink
| [20656] MySQL mysql_install_db script symlink
| [20333] Plans MySQL password information disclosure
| [19659] MySQL CREATE TEMPORARY TABLE command creates insecure files
| [19658] MySQL udf_init function gain access
| [19576] auraCMS mysql_fetch_row function path disclosure
| [18922] MySQL mysqlaccess script symlink attack
| [18824] MySQL UDF root privileges
| [18464] mysql_auth unspecified vulnerability
| [18449] Sugar Sales plaintext MySQL password

| [17783] MySQL underscore allows elevated privileges
| [17768] MySQL MATCH ... AGAINST SQL statement denial of service
| [17667] MySQL UNION change denial of service
| [17666] MySQL ALTER TABLE RENAME bypass restriction
| [17493] MySQL libmysqlclient bulk inserts buffer overflow
| [17462] MySQLGuest AWSguest.php script cross-site scripting
| [17047] MySQL mysql_real_connect buffer overflow
| [17030] MySQL mysqlhotcopy insecure temporary file
| [16612] MySQL my_rnd buffer overflow
| [16604] MySQL check_scramble_323 function allows unauthorized access
| [15883] MySQL mysqld_multi script symlink attack
| [15617] MySQL mysqlbug script symlink attack
| [15417] Confixx db_mysql_loeschen2.php SQL injection
| [15280] Proofpoint Protection Server MySQL allows unauthorized access
| [13404] HP Servicecontrol Manager multiple vulnerabilities in MySQL could allow execution of code
| [13153] MySQL long password buffer overflow
| [12689] MySQL AB ODBC Driver stores ODBC passwords and usernames in plain text
| [12540] Teapop PostSQL and MySQL modules SQL injection
| [12337] MySQL mysql_real_connect function buffer overflow
| [11510] MySQL datadir/my.cnf modification could allow root privileges
| [11493] mysqlcc configuration and connection files are world writable
| [11340] SuckBot mod_mysql_logger denial of service
| [11199] MySQL mysql_change_user() double-free memory pointer denial of service
| [10850] MySQL libmysql client read_one_row buffer overflow
| [10849] MySQL libmysql client read_rows buffer overflow
| [10848] MySQL COM_CHANGE_USER password buffer overflow
| [10847] MySQL COM_CHANGE_USER command password authentication bypass
| [10846] MySQL COM_TABLE_DUMP unsigned integer denial of service
| [10483] Bugzilla stores passwords in plain text in the MySQL database
| [10455] gBook MySQL could allow administrative access
| [10243] MySQL my.ini &quot
| [9996] MySQL SHOW GRANTS command discloses adminstrator‘s encrypted password
| [9909] MySQL logging disabled by default on Windows
| [9908] MySQL binding to the loopback adapter is disabled
| [9902] MySQL default root password could allow unauthorized access
| [8748] Cyrus SASL LDAP+MySQL patch allows user unauthorized POP access
| [8105] PHP MySQL client library allows an attacker to bypass safe_mode restrictions
| [7923] Conectiva Linux MySQL /var/log/mysql file has insecure permissions
| [7206] WinMySQLadmin stores MySQL password in plain text
| [6617] MySQL &quot
| [6419] MySQL drop database command buffer overflow
| [6418] MySQL libmysqlclient.so buffer overflow
| [5969] MySQL select buffer overflow
| [5447] pam_mysql authentication input
| [5409] MySQL authentication algorithm obtain password hash
| [5057] PCCS MySQL Database Admin Tool could reveal username and password
| [4228] MySQL unauthenticated remote access
| [3849] MySQL default test account could allow any user to connect to the database
| [1568] MySQL creates readable log files
|
| Exploit-DB - https://www.exploit-db.com:
| [30744] MySQL <= 5.1.23 Server InnoDB CONVERT_SEARCH_MODE_TO_INNOBASE Function Denial Of Service Vulnerability
| [30677] Asterisk ’asterisk-addons’ 1.2.7/1.4.3 CDR_ADDON_MYSQL Module SQL Injection Vulnerability
| [30020] MySQL 5.0.x - IF Query Handling Remote Denial of Service Vulnerability

| [29724] MySQL 5.0.x Single Row SubSelect Remote Denial of Service Vulnerability
| [29653] Active Calendar 1.2 data/mysqlevents.php css Parameter XSS
| [29572] CPanel <= 11 PassWDMySQL Cross-Site Scripting Vulnerability
| [29569] MySQLNewsEngine Affichearticles.PHP3 Remote File Include Vulnerability
| [28783] MySQLDumper 1.21 SQL.PHP Cross-Site Scripting Vulnerability
| [28398] MySQL 4/5 SUID Routine Miscalculation Arbitrary DML Statement Execution
| [28308] Banex PHP MySQL Banner Exchange 2.21 members.php cfg_root Parameter Remote File Inclu
sion
| [28307] Banex PHP MySQL Banner Exchange 2.21 admin.php Multiple Parameter SQL Injection
| [28306] Banex PHP MySQL Banner Exchange 2.21 signup.php site_name Parameter SQL Injection
| [28234] MySQL 4.x/5.x Server Date_Format Denial of Service Vulnerability
| [28026] MySQL Server 4/5 Str_To_Date Remote Denial of Service Vulnerability
| [27464] Cholod MySQL Based Message Board Mb.CGI SQL Injection Vulnerability
| [27444] Woltlab Burning Board 2.3.4 Class_DB_MySQL.PHP Cross-Site Scripting Vulnerability
| [27326] MySQL 5.0.18 Query Logging Bypass Vulnerability
| [26058] MySQL AB Eventum 1.x get_jsrs_data.php F Parameter XSS
| [26057] MySQL AB Eventum 1.x list.php release Parameter XSS
| [26056] MySQL AB Eventum 1.x view.php id Parameter XSS
| [25211] MySQL 4.x CREATE TEMPORARY TABLE Symlink Privilege Escalation
| [25210] MySQL 4.x CREATE FUNCTION mysql.func Table Arbitrary Library Injection
| [25209] MySQL 4.x CREATE FUNCTION Arbitrary libc Code Execution
| [24805] MySQL MaxDB 7.5 WAHTTP Server Remote Denial of Service Vulnerability
| [24669] MySQL 3.x/4.x ALTER TABLE/RENAME Forces Old Permission Checks
| [24250] MySQL 4.1/5.0 Authentication Bypass Vulnerability
| [23179] Oracle MySQL for Microsoft Windows MOF Execution
| [23138] MySQL 3.23.x/4.0.x Password Handler Buffer Overflow Vulnerability
| [23083] MySQL Windows Remote System Level Exploit (Stuxnet technique) 0day
| [23081] MySQL Remote Preauth User Enumeration Zeroday
| [23078] MySQL Denial of Service Zeroday PoC
| [23077] MySQL (Linux) Database Privilege Elevation Zeroday Exploit
| [23076] MySQL (Linux) Heap Based Overrun PoC Zeroday
| [23075] MySQL (Linux) Stack Based Buffer Overrun PoC Zeroday
| [23073] MySQL 5.1/5.5 WiNDOWS REMOTE R00T (mysqljackpot)
| [22946] MySQL AB ODBC Driver 3.51 Plain Text Password Vulnerability
| [22565] MySQL 3.x/4.0.x Weak Password Encryption Vulnerability
| [22340] MySQL 3.23.x mysqld Privilege Escalation Vulnerability
| [22085] MySQL 3.23.x/4.0.x COM_CHANGE_USER Password Memory Corruption Vulnerability
| [22084] MySQL 3.23.x/4.0.x COM_CHANGE_USER Password Length Account Compromise Vulnerabilit
y
| [21726] MySQL 3.20.32/3.22.x/3.23.x Null Root Password Weak Default Configuration Vulnerability (2)
| [21725] MySQL 3.20.32/3.22.x/3.23.x Null Root Password Weak Default Configuration Vulnerability (1)
| [21266] PHP 4.x/5.x MySQL Safe_Mode Filesystem Circumvention Vulnerability (3)
| [21265] PHP 4.x/5.x MySQL Safe_Mode Filesystem Circumvention Vulnerability (2)
| [21264] PHP 4.x/5.x MySQL Safe_Mode Filesystem Circumvention Vulnerability (1)
| [20718] MySQL 3.20.32 a/3.23.34 Root Operation Symbolic Link File Overwriting Vulnerability
| [20581] Mysql 3.22.x/3.23.x Local Buffer Overflow Vulnerability
| [20355] Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
| [20055] MySQL Squid Access Report 2.1.4 HTML Injection
| [20044] Symantec Web Gateway 5.0.3.18 Blind SQLi Backdoor via MySQL Triggers
| [19721] MySQL 3.22.27/3.22.29/3.23.8 GRANT Global Password Changing Vulnerability
| [19092] MySQL Remote Root Authentication Bypass
| [18269] MySQL 5.5.8 - Remote Denial of Service (DOS)
| [16957] Oracle MySQL for Microsoft Windows Payload Execution
| [16850] MySQL yaSSL CertDecoder::GetName Buffer Overflow
| [16849] MySQL yaSSL SSL Hello Message Buffer Overflow

| [16701] MySQL yaSSL SSL Hello Message Buffer Overflow
| [15467] Oracle MySQL < 5.1.49 'WITH ROLLUP' Denial of Service Vulnerability
| [14654] CMSQLite <= 1.2 & CMySQLite <= 1.3.1 - Remote Code Execution Exploit
| [14537] Oracle MySQL 'ALTER DATABASE' Remote Denial of Service Vulnerability
| [14096] CMSQlite & CMySQLite CSRF Vulnerability
| [10876] PHP-MySQL-Quiz SQL Injection Vulnerability
| [10450] Linkster PHP/MySQL SQL Injection Vulnerability
| [10260] Robert Zimmerman PHP / MYSQL Scripts Admin Bypass
| [9953] MySQL <= 6.0 yaSSL <= 1.7.5 Hello Message Buffer Overflow
| [9085] MySQL <= 5.0.45 COM_CREATE_DB Format String PoC (auth)
| [8037] ProFTPd with mod_mysql Authentication Bypass Vulnerability
| [7856] MySQL 4/5/6 UDF for Command Execution
| [7020] MySQL Quick Admin 1.5.5 - Local File Inclusion Vulnerability
| [6641] MySQL Quick Admin <= 1.5.5 (COOKIE) Local File Inclusion Vulnerability
| [6577] PromoteWeb MySQL (go.php id) Remote SQL Injection Vulnerability
| [6136] phpWebNews 0.2 MySQL Edition (SQL) Insecure Cookie Handling Vuln
| [5999] phpWebNews 0.2 MySQL Edition (det) SQL Injection Vulnerability
| [5998] phpWebNews 0.2 MySQL Edition (id_kat) SQL Injection Vulnerability
| [5913] MyBlog: PHP and MySQL Blog/CMS software (SQL/XSS) Vulnerabilities
| [4615] MySQL <= 5.0.45 (Alter) Denial of Service Vulnerability
| [4392] PHP <= 4.4.7 / 5.2.3 MySQL/MySQLi Safe Mode Bypass Vulnerability
| [3685] MyBlog: PHP and MySQL Blog/CMS software RFI Vulnerability
| [3591] PHP-Nuke Module Eve-Nuke 0.1 (mysql.php) RFI Vulnerability
| [3468] MySQL Commander <= 2.7 (home) Remote File Inclusion Vulnerability
| [3450] NukeSentinel <= 2.5.06 (MySQL => 4.0.24) - Remote SQL Injection Exploit
| [3344] PHP-Nuke <= 8.0 Final (INSERT) Blind SQL Injection Exploit (mysql)
| [3274] MySQL 4.x/5.0 User-Defined Function Command Execution Exploit (win)
| [2969] Php/Mysql Site Builder 0.0.2 (htm2php.php) File Disclosure Vulnerability
| [2726] Agora 1.4 RC1 (MysqlfinderAdmin.php) Remote File Include Vulnerability
| [2554] cPanel <= 10.8.x (cpwrap via mysqladmin) Local Root Exploit (php)
| [2466] cPanel <= 10.8.x (cpwrap via mysqladmin) Local Root Exploit
| [2437] paBugs <= 2.0 Beta 3 (class.mysql.php) Remote File Include Exploit
| [2420] ZoomStats <= 1.0.2 (mysql.php) Remote File Include Vulnerability
| [1742] MySQL (<= 4.1.18, 5.0.20) Local/Remote Information Leakage Exploit
| [1741] MySQL <= 5.0.20 COM_TABLE_DUMP Memory Leak/Remote BoF Exploit
| [1518] MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit
| [1406] PHP <= 4.4.0 (mysql_connect function) Local Buffer Overflow Exploit
| [1181] MySQL 4.0.17 UDF Dynamic Library Exploit
| [1134] MySQL Eventum <= 1.5.5 (login.php) SQL Injection Exploit
| [960] MySQL MaxDB Webtool <= 7.5.00.23 Remote Stack Overflow Exploit
| [311] MySQL 4.1/5.0 zero-length password Auth. Bypass Exploit
| [98] MySQL 3.23.x/4.0.x Remote Exploit
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [902675] MySQLDumper Multiple Vulnerabilities
| [881549] CentOS Update for mysql CESA-2012:1551 centos6
| [881538] CentOS Update for mysql CESA-2012:1462 centos6
| [881225] CentOS Update for mysql CESA-2012:0105 centos6
| [881185] CentOS Update for mysql CESA-2012:0127 centos5
| [881061] CentOS Update for mysql CESA-2012:0874 centos6
| [880760] CentOS Update for mysql CESA-2009:1289 centos5 i386
| [880613] CentOS Update for mysql CESA-2010:0109 centos5 i386
| [880577] CentOS Update for mysql CESA-2010:0442 centos5 i386
| [880452] CentOS Update for mysql CESA-2010:0824 centos4 i386
| [880366] CentOS Update for mysql CESA-2010:0110 centos4 i386

| [880329] CentOS Update for mysql CESA-2007:1155 centos4 x86_64
| [880324] CentOS Update for mysql CESA-2007:1155 centos4 i386
| [870870] RedHat Update for mysql RHSA-2012:1551-01
| [870861] RedHat Update for mysql RHSA-2012:1462-01
| [870778] RedHat Update for mysql RHSA-2012:0874-04
| [870736] RedHat Update for mysql RHSA-2011:0164-01
| [870647] RedHat Update for mysql RHSA-2012:0105-01
| [870547] RedHat Update for mysql RHSA-2012:0127-01
| [870357] RedHat Update for mysql RHSA-2010:0824-01
| [870356] RedHat Update for mysql RHSA-2010:0825-01
| [870272] RedHat Update for mysql RHSA-2010:0442-01
| [870218] RedHat Update for mysql RHSA-2010:0110-01
| [870216] RedHat Update for mysql RHSA-2010:0109-01
| [870195] RedHat Update for mysql RHSA-2007:1155-01
| [870069] RedHat Update for mysql RHSA-2008:0364-01
| [870033] RedHat Update for mysql RHSA-2008:0768-01
| [864951] Fedora Update for mysql FEDORA-2012-19823
| [864945] Fedora Update for mysql FEDORA-2012-19833
| [864504] Fedora Update for mysql FEDORA-2012-9324
| [864474] Fedora Update for mysql FEDORA-2012-9308
| [863910] Fedora Update for mysql FEDORA-2012-0972
| [863725] Fedora Update for mysql FEDORA-2012-0987
| [862844] Fedora Update for mod_auth_mysql FEDORA-2011-0100
| [862840] Fedora Update for mod_auth_mysql FEDORA-2011-0114
| [862676] Fedora Update for mysql FEDORA-2010-15147
| [862444] Fedora Update for mysql FEDORA-2010-15166
| [862300] Fedora Update for mysql FEDORA-2010-11126
| [862290] Fedora Update for mysql FEDORA-2010-11135
| [862149] Fedora Update for mysql FEDORA-2010-9053
| [862148] Fedora Update for mysql FEDORA-2010-9061
| [862136] Fedora Update for mysql FEDORA-2010-9016
| [861948] Fedora Update for mysql FEDORA-2010-7355
| [861936] Fedora Update for mysql FEDORA-2010-7414
| [861707] Fedora Update for mysql FEDORA-2010-1300
| [861651] Fedora Update for mysql FEDORA-2010-1348
| [861544] Fedora Update for php-pear-MDB2-Driver-mysql FEDORA-2007-3369
| [861392] Fedora Update for mysql FEDORA-2007-4471
| [861180] Fedora Update for php-pear-MDB2-Driver-mysqli FEDORA-2007-3369
| [861162] Fedora Update for php-pear-MDB2-Driver-mysql FEDORA-2007-3376
| [861108] Fedora Update for php-pear-MDB2-Driver-mysqli FEDORA-2007-3376
| [861033] Fedora Update for mysql FEDORA-2007-4465
| [855481] Solaris Update for mysql 120292-02
| [855333] Solaris Update for mysql 120293-02
| [850182] SuSE Update for mysql openSUSE-SU-2012:0860-1 (mysql)
| [841248] Ubuntu Update for mysql-5.5 USN-1658-1
| [841207] Ubuntu Update for mysql-5.5 USN-1621-1
| [841039] Ubuntu Update for mysql-5.5 USN-1467-1
| [840989] Ubuntu Update for mysql-5.1 USN-1427-1
| [840944] Ubuntu Update for mysql-5.1 USN-1397-1
| [840533] Ubuntu Update for MySQL vulnerabilities USN-1017-1
| [840442] Ubuntu Update for MySQL vulnerabilities USN-950-1
| [840384] Ubuntu Update for MySQL vulnerabilities USN-897-1
| [840292] Ubuntu Update for mysql-dfsg-5.0 vulnerabilities USN-671-1
| [840240] Ubuntu Update for mysql-dfsg-5.0 regression USN-588-2
| [840219] Ubuntu Update for mysql-dfsg-5.0 vulnerabilities USN-588-1

| [840106] Ubuntu Update for mysql-dfsg-5.0 vulnerabilities USN-559-1
| [840042] Ubuntu Update for mysql-dfsg-5.0 vulnerabilities USN-528-1
| [840012] Ubuntu Update for mysql-dfsg-5.0 vulnerability USN-440-1
| [835096] HP-UX Update for on HP 9000 Servers Running MySQL HPSBUX00287
| [831755] Mandriva Update for mysql MDVSA-2012:178 (mysql)
| [831684] Mandriva Update for mysql MDVA-2012:049 (mysql)
| [831547] Mandriva Update for mysql MDVA-2012:022 (mysql)
| [831532] Mandriva Update for mysql MDVA-2012:005 (mysql)
| [831519] Mandriva Update for mysql MDVA-2011:099 (mysql)
| [831425] Mandriva Update for mysql MDVA-2011:025 (mysql)
| [831327] Mandriva Update for mysql MDVA-2011:005 (mysql)
| [831315] Mandriva Update for mysql MDVSA-2011:012 (mysql)
| [831295] Mandriva Update for mysql MDVA-2010:240 (mysql)
| [831244] Mandriva Update for mysql MDVSA-2010:155-1 (mysql)
| [831243] Mandriva Update for mysql MDVSA-2010:222 (mysql)
| [831237] Mandriva Update for mysql MDVSA-2010:223 (mysql)
| [831202] Mandriva Update for mysql MDVA-2010:210 (mysql)
| [831134] Mandriva Update for mysql MDVSA-2010:155 (mysql)
| [831049] Mandriva Update for mysql MDVSA-2010:107 (mysql)
| [831048] Mandriva Update for mysql MDVSA-2010:101 (mysql)
| [831034] Mandriva Update for mysql MDVA-2010:146 (mysql)
| [831033] Mandriva Update for mysql MDVSA-2010:093 (mysql)
| [830902] Mandriva Update for mysql MDVSA-2010:044 (mysql)
| [830821] Mandriva Update for mysql MDVSA-2010:011 (mysql)
| [830806] Mandriva Update for mysql MDVSA-2010:012 (mysql)
| [830772] Mandriva Update for mysql MDVSA-2008:150 (mysql)
| [830664] Mandriva Update for mysql MDVA-2008:018 (mysql)
| [830659] Mandriva Update for mysql MDVSA-2008:017 (mysql)
| [830513] Mandriva Update for mysql MDVSA-2008:028 (mysql)
| [830421] Mandriva Update for mysql MDVSA-2008:149 (mysql)
| [830297] Mandriva Update for MySQL MDKSA-2007:177 (MySQL)
| [830223] Mandriva Update for perl-DBD-mysql MDKA-2007:066 (perl-DBD-mysql)
| [830063] Mandriva Update for MySQL MDKSA-2007:139 (MySQL)
| [830032] Mandriva Update for MySQL MDKSA-2007:243 (MySQL)
| [801593] Oracle MySQL Eventum Multiple Cross Site Scripting Vulnerabilities
| [801205] MySQL Connector/Net SSL Certificate Validation Security Bypass Vulnerability
| [103051] PHP MySQLi Extension ’set_magic_quotes_runtime’ Function Security-Bypass Weakness
| [100662] PHP Mysqlnd Extension Information Disclosure and Multiple Buffer Overflow Vulnerabilities
| [71475] Debian Security Advisory DSA 2496-1 (mysql-5.1)
| [71233] Debian Security Advisory DSA 2429-1 (mysql-5.1)
| [70803] Gentoo Security Advisory GLSA 201201-02 (MySQL)
| [70586] FreeBSD Ports: proftpd, proftpd-mysql
| [67541] Debian Security Advisory DSA 2057-1 (mysql-dfsg-5.0)
| [66577] Fedora Core 11 FEDORA-2009-13504 (mysql)
| [66573] Fedora Core 12 FEDORA-2009-13466 (mysql)
| [66553] Mandriva Security Advisory MDVSA-2009:189-1 (apache-mod_auth_mysql)
| [66508] Fedora Core 10 FEDORA-2009-12180 (mysql)
| [66425] Mandriva Security Advisory MDVSA-2009:326 (mysql)
| [66256] Fedora Core 11 FEDORA-2009-10701 (ocaml-mysql)
| [66251] Fedora Core 10 FEDORA-2009-10582 (ocaml-mysql)
| [66056] Debian Security Advisory DSA 1910-1 (mysql-ocaml)
| [66035] Mandrake Security Advisory MDVSA-2009:279 (ocaml-mysql)
| [65937] SLES10: Security update for MySQL
| [65884] SLES10: Security update for MySQL
| [65827] SLES10: Security update for MySQL

| [65710] SLES11: Security update for MySQL
| [65610] SLES9: Security update for MySQL
| [65566] SLES9: Security update for MySQL
| [65507] SLES9: Security update for MySQL
| [65502] SLES9: Security update for mysql
| [65426] SLES9: Security update for MySQL
| [65385] SLES9: Security update for mysql
| [65341] SLES9: Security update for MySQL
| [65181] SLES9: Security update for MySQL
| [65176] SLES9: Security update for MySQL
| [64932] CentOS Security Advisory CESA-2009:1289 (mysql)
| [64820] Debian Security Advisory DSA 1877-1 (mysql-dfsg-5.0)
| [64532] Mandrake Security Advisory MDVSA-2009:189 (apache-mod_auth_mysql)
| [64522] Mandrake Security Advisory MDVSA-2009:179 (mysql)
| [64461] Mandrake Security Advisory MDVSA-2009:159 (mysql)
| [63872] Mandrake Security Advisory MDVSA-2009:094 (mysql)
| [63630] FreeBSD Ports: proftpd, proftpd-mysql
| [63171] FreeBSD Ports: mysql-server
| [63170] FreeBSD Ports: mysql-server
| [63169] FreeBSD Ports: mysql-server
| [63168] FreeBSD Ports: mysql-server
| [63095] FreeBSD Ports: mysql-server
| [61852] Debian Security Advisory DSA 1662-1 (mysql-dfsg-5.0)
| [61699] FreeBSD Ports: mysql-client
| [61656] FreeBSD Ports: proftpd, proftpd-mysql
| [61618] FreeBSD Ports: mysql-server
| [61599] Gentoo Security Advisory GLSA 200809-04 (mysql)
| [61283] Debian Security Advisory DSA 1608-1 (mysql-dfsg-5.0)
| [60804] Gentoo Security Advisory GLSA 200804-04 (mysql)
| [60271] Debian Security Advisory DSA 1478-1 (mysql-dfsg-5.0)
| [60106] Debian Security Advisory DSA 1451-1 (mysql-dfsg-5.0)
| [60017] Slackware Advisory SSA:2007-348-01 mysql
| [59638] Debian Security Advisory DSA 1413-1 (mysql-dfsg, mysql-dfsg-5.0, mysql-dfsg-4.1)
| [59245] Gentoo Security Advisory GLSA 200711-25 (mysql)
| [58863] FreeBSD Ports: freeradius, freeradius-mysql
| [58545] Gentoo Security Advisory GLSA 200708-10 (mysql)
| [58261] Gentoo Security Advisory GLSA 200705-11 (MySQL)
| [57859] Gentoo Security Advisory GLSA 200608-09 (mysql)
| [57725] FreeBSD Ports: proftpd, proftpd-mysql
| [57576] FreeBSD Ports: proftpd, proftpd-mysql
| [57527] FreeBSD Ports: mysql-server
| [57526] FreeBSD Ports: mysql-server
| [57337] Debian Security Advisory DSA 1169-1 (mysql-dfsg-4.1)
| [57257] FreeBSD Ports: mysql-server
| [57167] Slackware Advisory SSA:2006-211-01 mysql
| [57109] Debian Security Advisory DSA 1112-1 (mysql-dfsg-4.1)
| [56964] Gentoo Security Advisory GLSA 200606-18 (pam_mysql)
| [56940] Gentoo Security Advisory GLSA 200606-13 (MySQL)
| [56924] Debian Security Advisory DSA 1092-1 (mysql-dfsg-4.1)
| [56861] Slackware Advisory SSA:2006-155-01 mysql
| [56850] FreeBSD Ports: mysql-server
| [56849] FreeBSD Ports: mysql-server
| [56833] Debian Security Advisory DSA 1079-1 (mysql-dfsg)
| [56789] Debian Security Advisory DSA 1073-1 (mysql-dfsg-4.1)
| [56788] Debian Security Advisory DSA 1071-1 (mysql)

| [56730] Slackware Advisory SSA:2006-129-02 mysql
| [56728] Gentoo Security Advisory GLSA 200605-13 (MySQL)
| [56714] FreeBSD Ports: mysql-server
| [55520] Debian Security Advisory DSA 833-2 (mysql-dfsg-4.1)
| [55514] Debian Security Advisory DSA 833-1 (mysql-dfsg-4.1)
| [55493] Debian Security Advisory DSA 829-1 (mysql)
| [55492] Debian Security Advisory DSA 831-1 (mysql-dfsg)
| [55164] Debian Security Advisory DSA 783-1 (mysql-dfsg-4.1)
| [54884] Gentoo Security Advisory GLSA 200503-19 (mysql)
| [54819] Gentoo Security Advisory GLSA 200501-33 (mysql)
| [54713] Gentoo Security Advisory GLSA 200410-22 (MySQL)
| [54659] Gentoo Security Advisory GLSA 200409-02 (MySQL)
| [54580] Gentoo Security Advisory GLSA 200405-20 (MySQL)
| [54483] FreeBSD Ports: proftpd, proftpd-mysql
| [54201] FreeBSD Ports: mysql-server
| [53776] Debian Security Advisory DSA 013-1 (mysql)
| [53755] Debian Security Advisory DSA 483-1 (mysql)
| [53750] Debian Security Advisory DSA 707-1 (mysql)
| [53666] Debian Security Advisory DSA 381-1 (mysql)
| [53595] Debian Security Advisory DSA 303-1 (mysql)
| [53585] Debian Security Advisory DSA 212-1 (mysql)
| [53481] Debian Security Advisory DSA 647-1 (mysql)
| [53251] Debian Security Advisory DSA 562-1 (mysql)
| [53230] Debian Security Advisory DSA 540-1 (mysql)
| [52466] FreeBSD Ports: exim, exim-ldap2, exim-mysql, exim-postgresql
| [52459] FreeBSD Ports: mysql-client
| [52419] FreeBSD Ports: mysql-scripts
| [52406] FreeBSD Ports: mysql-server
| [52375] FreeBSD Ports: mysql-server, mysql-client
| [52274] FreeBSD Ports: mysql-server
| [52273] FreeBSD Ports: mysql-server
| [52272] FreeBSD Ports: mysql-server
| [52271] FreeBSD Ports: mysql-server
| [52270] FreeBSD Ports: mysql-server
| [52233] FreeBSD Ports: mysql-scripts
| [52158] FreeBSD Ports: mysql-server
| [16093] MySQL Eventum Multiple flaws
| [12639] MySQL Authentication bypass through a zero-length password
| [10783] PCCS-Mysql User/Password Exposure
|
| SecurityTracker - https://www.securitytracker.com:
| [1028790] MySQL Multiple Bugs Let Remote Users Deny Service and Partially Access and Modify Data
| [1028449] MySQL Multiple Bugs Let Remote Authenticated Users Deny Service and Partially Access an
d Modify Data
| [1028004] MySQL Multiple Bugs Let Remote Authenticated Users Take Full Control or Deny Service and
 Let Local Users Access and Modify Data
| [1027829] MySQL Bug in UpdateXML() Lets Remote Authenticated Users Deny Service
| [1027828] MySQL Heap Overflow May Let Remote Authenticated Users Execute Arbitrary Code
| [1027827] MySQL Stack Overflow May Let Remote Authenticated Users Execute Arbitrary Code
| [1027665] MySQL Multiple Bugs Let Remote Authenticated Users Access and Modify Data and Deny Se
rvice and Local Users Access Data
| [1027263] MySQL Multiple Bugs Let Remote Authenticated Users Deny Service
| [1027143] MySQL memcmp() Comparison Error Lets Remote Users Bypass Authentication
| [1026934] MySQL Multiple Bugs Let Remote Users Deny Service
| [1026896] MySQL Unspecified Flaws Have Unspecified Impact

| [1026659] MySQL Unspecified Flaw Lets Remote Users Execute Arbitrary Code
| [1026530] MySQL Multiple Bugs Let Local and Remote Users Partially Access and Modifiy Data and Partially Deny Service
| [1024508] MySQL Replication Flaw Lets Remote Authenticated Users Gain Elevated Privileges
| [1024507] MySQL Multiple Flaws Let Remote Authenticated Users Deny Service
| [1024360] MySQL Multiple Flaws Let Remote Authenticated Users Deny Service
| [1024160] MySQL ALTER DATABASE Processing Error Lets Remote Authenticated Users Deny Service
| [1024033] MySQL COM_FIELD_LIST Packet Buffer Overflow Lets Remote Authenticated Users Execute Arbitrary Code
| [1024032] MySQL Large Packet Processing Flaw in my_net_skip_rest() Lets Remote Users Deny Service
| [1024031] MySQL COM_FIELD_LIST Validation Flaw Lets Remote Authenticated Users Gain Elevated Privileges
| [1024004] MySQL mi_delete_table() Symlink Flaw Lets Remote Authenticated Users Delete Data and Index Files
| [1023402] MySQL Unspecified Flaw Lets Remote Users Execute Arbitrary Code
| [1023220] MySQL Client Fails to Check Server Certificates in Certain Cases
| [1022812] MySQL Unspecified Buffer Overflow Lets Remote Users Execute Arbitrary Code
| [1022533] MySQL Format String Bug in dispatch_command() Lets Remote Users Deny Service
| [1022482] MySQL Connector/Net is Missing SSL Certificate Validation
| [1021786] MySQL Bug in ExtractValue()/UpdateXML() in Processing XPath Expressions Lets Remote Authenticated Users Deny Service
| [1021714] (Red Hat Issues Fix) mod_auth_mysql Input Validation Flaw Lets Remote Users Inject SQL Commands
| [1020858] MySQL Item_bin_string::Item_bin_string() Binary Value Processing Bug Lets Remote Authenticated Users Deny Service
| [1019995] MySQL MyISAM Options Let Local Users Overwrite Table Files
| [1019085] MySQL Bugs Let Remote Authenticated Users Gain Elevated Privileges and Deny Service
| [1019084] MySQL DATA DIRECTORY and INDEX DIRECTORY Options May Let Remote Authenticated Users Gain Elevated Privileges
| [1019083] MySQL BINLOG Filename Path Bug May Let Remote Authenticated Users Gain Elevated Privileges
| [1019060] MySQL Rename Table Bug Lets Remote Authenticated Users Modify System Table Information
| [1018978] MySQL convert_search_mode_to_innobase() Bug Lets Remote Authenticated Users Deny Service
| [1018824] Asterisk-Addons Input Validation Flaw in cdr_addon_mysql Lets Remote Users Inject SQL Commands
| [1018663] MySQL Table View Access Bug Lets Remote Authenticated Users Gain Elevated Privileges
| [1018629] MySQL Authentication Protocol Bug Lets Remote Users Deny Service
| [1018071] MySQL ALTER TABLE Function Lets Remote Authenticated Users Obtain Potentially Sensitive Information
| [1018070] MySQL SQL SECURITY INVOKER Routines Let Remote Authenticated Users Gain Elevated Privileges
| [1018069] MySQL Lets Remote Authenticated Users Issue the RENAME TABLE Command
| [1017746] MySQL Single Row Subselect Statements Let Remote Users Deny Service
| [1016790] MySQL Replication Error Lets Local Users Deny Service
| [1016710] MySQL Case-Sensitive Database Names May Let Users Access Restricted Databases
| [1016709] MySQL Error in Checking suid Routine Arguments May Let Users Gain Elevated Privileges
| [1016617] MySQL MERGE Access Control Error May Let Users Access a Restricted Table
| [1016566] Opsware Network Automation System Discloses MySQL Password to Local Users
| [1016216] MySQL Error in Parsing Multibyte Encoded Data in mysql_real_escape() Lets Remote Users Inject SQL Commands
| [1016077] Apple MySQL Manager Database Initialization Bug May Let Local Users Access the Databas

e
| [1016017] MySQL Anonymous Login Processing May Disclose Some Memory Contents to Remote User
s
| [1016016] MySQL COM_TABLE_DUMP Processing Lets Remote Authenticated Users Execute Arbitrary
Code or Obtain Information
| [1015789] Woltlab Burning Board Input Validation Hole in 'class_db_mysql.php' Permits Cross-Site Scrip
ting Attacks
| [1015693] MySQL Query Bug Lets Remote Users Bypass Query Logging
| [1015603] PAM-MySQL pam_get_item() Double Free May Let Remote Users Execute Arbitrary Code
| [1015485] PHP mysqli Extension Error Mode Format String Flaw May Let Users Execute Arbitrary Code
| [1014603] MySQL Eventum Input Validation Hole in 'class.auth.php' Permits SQL Injection and Other In
put Validation Bugs Permit Cross-Site Scripting Attacks
| [1014172] xMySQLadmin Lets Local Users Delete Files
| [1013995] MySQL 'mysql_install_db' Uses Unsafe Temporary Files and May Let Local Users Gain Eleva
ted Privilege
| [1013994] MySQL Non-existent '--user' Error May Allow the Database to Run With Incorrect Privileges
| [1013415] MySQL CREATE FUNCTION Lets Authenticated Users Invoke libc Functions to Execute Arbit
rary Code
| [1013414] MySQL udf_init() Path Validation Flaw Lets Authenticated Users Execute Arbitrary Libraries
| [1013413] MySQL CREATE TEMPORARY TABLE Uses Predictable Temporary Files That May Let User
s Gain Elevated Privileges
| [1012914] MySQL 'mysqlaccess.sh' Unsafe Temporary Files May Let Local Users Gain Elevated Privileg
es
| [1012893] MySQL MaxDB Buffer Overflow in websql Password Parameter Lets Remote Users Execute
Arbitrary Code
| [1012500] mysql_auth Memory Leak Has Unspecified Impact
| [1011741] MySQL Access Control Error in Databases With Underscore Wildcard Character May Grant U
nauthorized Access
| [1011606] MySQL May Let Remote Authenticated Users Access Restricted Tables or Crash the System
| [1011408] MySQL libmysqlclient Buffer Overflow in Executing Prepared Statements Has Unspecified Im
pact
| [1011376] MySQLGuest Lack of Input Validation Lets Remote Users Conduct Cross-Site Scripting Attac
ks
| [1011008] MySQL Buffer Overflow in mysql_real_connect() May Let Remote Users Execute Arbitrary Co
de
| [1010979] MySQL 'mysqlhotcopy' Unsafe Temporary Files May Let Local Users Gain Elevated Privilege
s
| [1010645] MySQL check_scramble_323() Zero-Length Comparison Lets Remote Users Bypass Authenti
cation
| [1009784] MySQL 'mysqld_multi' Temporary File Flaw Lets Local Users Overwrite Files
| [1009554] MySQL 'mysqlbug' Temporary File Flaw Lets Local Users Overwrite Files
| [1007979] MySQL mysql_change_user() Double Free Error Lets Remote Authenticated Users Crash my
sqld
| [1007673] MySQL acl_init() Buffer Overflow Permits Remote Authenticated Administrators to Execute Ar
bitrary Code
| [1007518] DWebPro Discloses MySQL Database Password to Local Users
| [1007312] MySQL World-Writable Configuration File May Let Local Users Gain Root Privileges
| [1006976] MySQL Buffer Overflow in 'mysql_real_connect()' Client Function May Let Remote or Local U
sers Execute Arbitrary Code
| [1005800] MySQL Overflow and Authentication Bugs May Let Remote Users Execute Code or Access D
atabase Accounts
| [1005345] MySQL Buffer Overflow Lets Local Users Gain System Privileges on Windows NT
| [1004506] vBulletin PHP-based Forum Software Has Unspecified Security Flaw in the 'db_mysql.php' M
odule
| [1004172] PHP-Survey Script Discloses Underlying MySQL Database Username and Password to Rem

ote Users
| [1003955] 3rd Party Patch for Cyrus SASL ('auxprop for mysql and ldap') Lets Remote Users Access Pr
otected POP Mail Accounts Without Authentication
| [1003290] Conectiva Linux MySQL Distribution May Allow Local Users to Obtain Sensitive Information
| [1002993] PurePostPro Script Add-on for PureFTPd and MySQL Allows Remote Users to Execute SQL
Commands on the Server
| [1002485] WinMySQLadmin Database Administration Tool Discloses MySQL Password to Local Users
| [1002324] Vpopmail Mail Server Discloses Database Password to Local Users When Installed with MyS
QL
| [1001411] phpMyAdmin Administration Tool for MySQL Allows Remote Users to Execute Commands on
the Server
| [1001118] MySQL Database Allows Authorized Users to Modify Server Files to Deny Service or Obtain
Additional Access
|
| OSVDB - http://www.osvdb.org:
| [95337] Oracle MySQL Server XA Transactions Subcomponent Unspecified Remote DoS
| [95336] Oracle MySQL Server Replication Subcomponent Unspecified Remote DoS
| [95335] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS
| [95334] Oracle MySQL Server Privileges Subcomponent Unspecified Remote Issue
| [95333] Oracle MySQL Server Partition Subcomponent Unspecified Remote DoS
| [95332] Oracle MySQL Server Parser Subcomponent Unspecified Remote DoS
| [95331] Oracle MySQL Server Options Subcomponent Unspecified Remote DoS (2013-3801)
| [95330] Oracle MySQL Server Options Subcomponent Unspecified Remote DoS (2013-3808)
| [95329] Oracle MySQL Server Optimizer Subcomponent Unspecified Remote DoS (2013-3796)
| [95328] Oracle MySQL Server Optimizer Subcomponent Unspecified Remote DoS (2013-3804)
| [95327] Oracle MySQL Server Prepared Statements Subcomponent Unspecified Remote DoS
| [95326] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS
| [95325] Oracle MySQL Server Full Text Search Subcomponent Unspecified Remote DoS
| [95324] Oracle MySQL Server Data Manipulation Language Subcomponent Unspecified Remote DoS (2
013-3795)
| [95323] Oracle MySQL Server Data Manipulation Language Subcomponent Unspecified Remote DoS (2
013-3793)
| [95322] Oracle MySQL Server Audit Log Subcomponent Unspecified Remote Issue
| [95321] Oracle MySQL Server MemCached Subcomponent Unspecified Remote Issue
| [95131] AutoMySQLBackup /usr/sbin/automysqlbackup Database Name Arbitrary Code Injection
| [94076] Debian Linux MySQL Server mysql-server-5.5.postinst Race Condition debian.cnf Plaintext Cred
ential Local Disclosure
| [93505] Wireshark MySQL Dissector (packet-mysql.c) Malformed Packet Handling Infinite Loop Remote
DoS
| [93174] MySQL Crafted Derived Table Handling DoS
| [92967] MySQL2JSON (mn_mysql2json) Extension for TYPO3 Unspecified SQL Injection
| [92950] MySQL Running START SLAVE Statement Process Listing Plaintext Local Password Disclosure
| [92485] Oracle MySQL Server Partition Subcomponent Unspecified Local DoS
| [92484] Oracle MySQL Server Locking Subcomponent Unspecified Remote DoS (2013-1506)
| [92483] Oracle MySQL Server Install Subcomponent Unspecified Local Issue
| [92482] Oracle MySQL Server Types Subcomponent Unspecified Remote DoS
| [92481] Oracle MySQL Server Privileges Subcomponent Unspecified Remote Issue (2013-2381)
| [92480] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS (2013-1566)
| [92479] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS (2013-1511)
| [92478] Oracle MySQL Server Data Manipulation Language Subcomponent Unspecified Remote DoS (2
013-1567)
| [92477] Oracle MySQL Server Stored Procedure Subcomponent Unspecified Remote DoS
| [92476] Oracle MySQL Server Replication Subcomponent Unspecified Remote DoS
| [92475] Oracle MySQL Server Partition Subcomponent Unspecified Remote DoS
| [92474] Oracle MySQL Server Optimizer Subcomponent Unspecified Remote DoS

| [92473] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS (2013-2389)
| [92472] Oracle MySQL Server Information Schema Subcomponent Unspecified Remote DoS
| [92471] Oracle MySQL Server Data Manipulation Language Subcomponent Unspecified Remote DoS (2013-1512)
| [92470] Oracle MySQL Server Data Manipulation Language Subcomponent Unspecified Remote DoS (2013-1544)
| [92469] Oracle MySQL Server Optimizer Subcomponent Unspecified Remote Issue
| [92468] Oracle MySQL Server MemCached Subcomponent Unspecified Remote DoS
| [92467] Oracle MySQL Server Privileges Subcomponent Unspecified Remote Issue (2013-2375)
| [92466] Oracle MySQL Server Privileges Subcomponent Unspecified Remote Issue (2013-1531)
| [92465] Oracle MySQL Server Server Subcomponent Unspecified Remote Issue
| [92464] Oracle MySQL Server Information Schema Subcomponent Unspecified Remote Issue
| [92463] Oracle MySQL Server Locking Subcomponent Unspecified Remote Issue (2013-1521)
| [92462] Oracle MySQL Server Data Manipulation Language Subcomponent Unspecified Remote DoS (2013-2395)
| [91536] Oracle MySQL yaSSL Unspecified Overflow (2012-0553)
| [91534] Oracle MySQL yaSSL Unspecified Overflow (2013-1492)
| [91415] MySQL Raw Geometry Object String Conversion Remote DoS
| [91108] Juju mysql Charm Install Script mysql.passwd MySQL Password Plaintext Local Disclosure
| [89970] Site Go /site-go/admin/extra/mysql/index.php idm Parameter Traversal Arbitrary File Access
| [89265] Oracle MySQL Server Server Privileges Subcomponent Unspecified Remote DoS
| [89264] Oracle MySQL Server Server Partition Subcomponent Unspecified Remote DoS
| [89263] Oracle MySQL Server Server Optimizer Subcomponent Unspecified Remote DoS (2012-0578)
| [89262] Oracle MySQL Server Server Optimizer Subcomponent Unspecified Remote DoS (2012-1705)
| [89261] Oracle MySQL Server Server Subcomponent Unspecified Remote DoS (2012-0574)
| [89260] Oracle MySQL Server MyISAM Subcomponent Unspecified Remote DoS
| [89259] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS (2012-0572)
| [89258] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS (2013-0368)
| [89257] Oracle MySQL Server Server Locking Subcomponent Unspecified Remote DoS
| [89256] Oracle MySQL Server Server Subcomponent Unspecified Remote DoS (2012-1702)
| [89255] Oracle MySQL Server Server Replication Subcomponent Unspecified Remote Issue
| [89254] Oracle MySQL Server Server Replication Subcomponent Unspecified Local Issue
| [89253] Oracle MySQL Server Stored Procedure Subcomponent Unspecified Remote DoS
| [89252] Oracle MySQL Server Server Optimizer Subcomponent Unspecified Remote DoS
| [89251] Oracle MySQL Server Information Schema Subcomponent Unspecified Remote DoS
| [89250] Oracle MySQL Server GIS Extension Subcomponent Unspecified Remote DoS
| [89042] ViciBox Server MySQL cron Service Default Credentials
| [88415] Oracle MySQL Server COM_CHANGE_USER Account Password Brute-Force Weakness
| [88118] Oracle MySQL Server FILE Privilege Database Privilege Escalation
| [88067] Oracle MySQL Server Authentication Error Message User Enumeration
| [88066] Oracle MySQL Server for Linux Access Rights Checking Routine Database Name Handling Stack Buffer Overflow
| [88065] Oracle MySQL Server COM_BINLOG_DUMP Invalid Data Handling DoS
| [88064] Oracle MySQL Server Multiple-Table DELETE Heap Buffer Overflow
| [87704] CodeIgniter MySQL / MySQLi Driver Database Client Multi-byte Character Set Unspecified SQL Injection
| [87507] Oracle MySQL Statement Logging Multiple Log Plaintext Local Password Disclosure
| [87501] Oracle MySQL optimizer_switch Malformed Value Processing Local DoS
| [87494] Oracle MySQL on Windows Field_new_decimal::store_value dbug_buff Variable Overflow DoS
| [87480] MySQL Malformed XML Comment Handling DoS
| [87466] MySQL SSL Certificate Revocation Weakness
| [87356] Oracle MySQL do_div_mod DIV Expression Handling Remote DoS
| [87355] Oracle MySQL handler::pushed_cond Table Cache Handling mysqld DoS
| [87354] Oracle MySQL Polygon Union / Intersection Spatial Operations DoS
| [86273] Oracle MySQL Server Server Installation Subcomponent Unspecified Local Information Disclosu

re
| [86272] Oracle MySQL Server Server Replication Subcomponent Unspecified Remote DoS
| [86271] Oracle MySQL Server Server Full Text Search Subcomponent Unspecified Remote DoS
| [86270] Oracle MySQL Server Server Subcomponent Unspecified Remote DoS (2012-3156)
| [86269] Oracle MySQL Server MySQL Client Subcomponent Unspecified Remote Information Disclosur
e
| [86268] Oracle MySQL Server Server Optimizer Subcomponent Unspecified Remote DoS (2012-3180)
| [86267] Oracle MySQL Server Server Optimizer Subcomponent Unspecified Remote DoS (2012-3150)
| [86266] Oracle MySQL Server Server Subcomponent Unspecified Remote DoS (2012-3144)
| [86265] Oracle MySQL Server InnoDB Plugin Subcomponent Unspecified Remote DoS
| [86264] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS
| [86263] Oracle MySQL Server MySQL Client Subcomponent Unspecified Remote Issue
| [86262] Oracle MySQL Server Server Subcomponent Unspecified Remote DoS (2012-3177)
| [86261] Oracle MySQL Server Protocol Subcomponent Unspecified Remote Issue
| [86260] Oracle MySQL Server Information Schema Subcomponent Unspecified Remote Code Execution
| [86175] Oracle MySQL on Windows Path Subversion Arbitrary DLL Injection Code Execution
| [85155] Icinga module/idoutils/db/scripts/create_mysqldb.sh Icinga User Database Access Restriction By
pass
| [84755] Oracle MySQL Sort Order Index Calculation Remote DoS
| [84719] MySQLDumper index.php page Parameter XSS
| [84680] MySQL Squid Access Report access.log File Path XSS
| [83980] Oracle MySQL Server Optimizer Subcomponent Unspecified Remote DoS (2012-1689)
| [83979] Oracle MySQL Server Optimizer Subcomponent Unspecified Remote DoS (2012-1734)
| [83978] Oracle MySQL Server Subcomponent Unspecified Remote DoS
| [83977] Oracle MySQL Server InnoDB Subcomponent Unspecified Remote DoS
| [83976] Oracle MySQL Server GIS Extension Subcomponent Unspecified Remote DoS
| [83975] Oracle MySQL Server Optimizer Subcomponent Unspecified Remote DoS (2012-1735)
| [83661] Oracle MySQL Unspecified Issue (59533)
| [82804] Oracle MySQL Authentication Protocol Token Comparison Casting Failure Password Bypass
| [82803] Oracle MySQL Unspecified Issue (59387)
| [82120] Oracle MySQL Version Specific Comment Handling Arbitrary SQL Command Execution
| [81897] Viscacha classes/database/mysql.inc.php Multiple Parameter SQL Injection
| [81616] MySQLDumper Multiple Script Direct Request Information Disclosure
| [81615] MySQLDumper filemanagement.php f Parameter Traversal Arbitrary File Access
| [81614] MySQLDumper File Upload PHP Code Execution
| [81613] MySQLDumper main.php Multiple Function CSRF
| [81612] MySQLDumper restore.php filename Parameter XSS
| [81611] MySQLDumper sql.php Multiple Parameter XSS
| [81610] MySQLDumper install.php Multiple Parameter XSS
| [81609] MySQLDumper install.php language Parameter Traversal Arbitrary File Access
| [81378] Oracle MySQL Server Server Optimizer Component Unspecified Remote DoS (2012-1690)
| [81377] Oracle MySQL Server Server Optimizer Component Unspecified Remote DoS (2012-1696)
| [81376] Oracle MySQL Server Server DML Component Unspecified Remote DoS
| [81375] Oracle MySQL Server Partition Component Unspecified Remote DoS
| [81374] Oracle MySQL Server MyISAM Component Unspecified Remote DoS
| [81373] Oracle MySQL Server Server Optimizer Component Unspecified Remote DoS (2012-1703)
| [81059] Oracle MySQL Server Multiple Unspecified Issues
| [79038] Webmin Process Listing MySQL Password Local Disclosure
| [78919] Oracle MySQL Unspecified Pre-authentication Remote Code Execution
| [78710] WordPress wp-admin/setup-config.php MySQL Query Saturation Brute-Force Proxy Weakness
| [78708] WordPress wp-admin/setup-config.php MySQL Database Verification Code Injection Weakness
| [78707] WordPress wp-admin/setup-config.php MySQL Credentials Error Message Brute-Force Weakne
ss
| [78394] Oracle MySQL Server Unspecified Remote DoS (2012-0493)
| [78393] Oracle MySQL Server Unspecified Remote DoS (2012-0492)

| [78392] Oracle MySQL Server Unspecified Remote DoS (2012-0117)
| [78391] Oracle MySQL Server Unspecified Remote DoS (2012-0112)
| [78390] Oracle MySQL Server Unspecified Remote DoS (2012-0495)
| [78389] Oracle MySQL Server Unspecified Remote DoS (2012-0491)
| [78388] Oracle MySQL Server Unspecified Remote DoS (2012-0490)
| [78387] Oracle MySQL Server Unspecified Remote DoS (2012-0489)
| [78386] Oracle MySQL Server Unspecified Remote DoS (2012-0488)
| [78385] Oracle MySQL Server Unspecified Remote DoS (2012-0487)
| [78384] Oracle MySQL Server Unspecified Remote DoS (2012-0486)
| [78383] Oracle MySQL Server Unspecified Remote DoS (2012-0485)
| [78382] Oracle MySQL Server Unspecified Remote DoS (2012-0120)
| [78381] Oracle MySQL Server Unspecified Remote DoS (2012-0119)
| [78380] Oracle MySQL Server Unspecified Remote DoS (2012-0115)
| [78379] Oracle MySQL Server Unspecified Remote DoS (2012-0102)
| [78378] Oracle MySQL Server Unspecified Remote DoS (2012-0101)
| [78377] Oracle MySQL Server Unspecified Remote DoS (2012-0087)
| [78376] Oracle MySQL Server Unspecified Remote DoS (2011-2262)
| [78375] Oracle MySQL Server Unspecified Local DoS
| [78374] Oracle MySQL Server Unspecified Remote Issue (2012-0075)
| [78373] Oracle MySQL Server Unspecified Local Issue
| [78372] Oracle MySQL Server Unspecified Remote Information Disclosure
| [78371] Oracle MySQL Server Unspecified Remote Issue (2012-0496)
| [78370] Oracle MySQL Server Unspecified Remote Issue (2012-0118)
| [78369] Oracle MySQL Server Unspecified Remote Issue (2012-0116)
| [78368] Oracle MySQL Server Unspecified Remote Issue (2012-0113)
| [78283] Oracle MySQL NULL Pointer Dereference Packet Parsing Remote DoS
| [77042] e107 CMS install_.php MySQL Server Name Parsing Remote PHP Code Execution
| [77040] DBD::mysqlPP Unspecified SQL Injection
| [75888] TaskFreak! multi-mysql Multiple Script Direct Request Path Disclosure
| [74120] Apache HTTP Server mod_authnz_external mysql/mysql-auth.pl user Field SQL Injection
| [73555] Prosody MySQL Value Column Invalid Data Type Handling DoS
| [73387] Zend Framework PDO_MySql Character Set Security Bypass
| [72836] Arctic Fox CMS Multiple Script Direct Request MySQL Settings Disclosure
| [72660] MySQL GUI Tools Administrator / Query Browser Command Line Credentials Local Disclosure
| [72120] DirectAdmin mysql_backups Folder MySQL Database Backup Local Disclosure
| [71368] Accellion File Transfer Appliance Weak MySQL root Password
| [70967] MySQL Eventum Admin User Creation CSRF
| [70966] MySQL Eventum preferences.php full_name Parameter XSS
| [70961] MySQL Eventum list.php Multiple Parameter XSS
| [70960] MySQL Eventum forgot_password.php URI XSS
| [70947] PyWebDAV DAVServer/mysqlauth.py get_userinfo() Multiple Parameter SQL Injection
| [70610] PHP MySQLi Extension set_magic_quotes_runtime Function mysqli_fetch_assoc Function Inter
action Weakness
| [69885] SilverStripe modules/sapphire/trunk/core/model/MySQLDatabase.php showqueries Parameter S
QL Command Disclosure
| [69395] MySQL Derived Table Grouping DoS
| [69394] MySQL Temporary Table Expression Re-Evaluation DoS
| [69393] MySQL GROUP_CONCAT() WITH ROLLUP Modifier DoS
| [69392] MySQL Extreme-Value Functions Mixed Arguments DoS
| [69391] MySQL Stored Procedures / Prepared Statements Nested Joins DoS
| [69390] MySQL Extreme-Value Functions Argument Parsing Type Error DoS
| [69389] MySQL CONVERT_TZ() Function Empty SET Column DoS
| [69388] MySQL InnoDB Storage Engine Table Handling Overflow
| [69387] MySQL LIKE Predicates Pre-Evaluation DoS
| [69001] MySQL PolyFromWKB() Function WKB Data Remote DoS

| [69000] MySQL HANDLER Interface Unspecified READ Request DoS
| [68997] MySQL Prepared-Statement Mode EXPLAIN DoS
| [68996] MySQL EXPLAIN EXTENDED Statement DoS
| [68995] MySQL GeometryCollection non-Geometry Value Assignment DoS
| [67488] phpMyAdmin libraries/dbi/mysqli.dbi.lib.php Unspecified Parameter XSS
| [67487] phpMyAdmin libraries/dbi/mysql.dbi.lib.php Unspecified Parameter XSS
| [67421] PHP Mysqlnd Extension mysqlnd_wireprotocol.c php_mysqlnd_rset_header_read Function Over flow
| [67420] PHP Mysqlnd Extension mysqlnd_wireprotocol.c php_mysqlnd_ok_read Function Arbitrary Mem ory Content Disclosure
| [67419] PHP Mysqlnd Extension php_mysqlnd_read_error_from_line Function Negative Buffer Length V alue Overflow
| [67418] PHP Mysqlnd Extension php_mysqlnd_auth_write Function Multiple Overflows
| [67384] MySQL LOAD DATA INFILE Statement Incorrect OK Packet DoS
| [67383] MySQL EXPLAIN Statement Item_singlerow_subselect::store Function NULL Dereference DoS
| [67381] MySQL InnoDB Temporary Table Handling DoS
| [67380] MySQL BINLOG Statement Unspecified Argument DoS
| [67379] MySQL Multiple Operation NULL Argument Handling DoS
| [67378] MySQL Unique SET Column Join Statement Remote DoS
| [67377] MySQL DDL Statement Multiple Configuration Parameter DoS
| [66800] PHP Multiple mysqlnd_* Function Unspecified Overflow
| [66799] PHP mysqlnd Error Packet Handling Multiple Overflows
| [66731] PHP Bundled MySQL Library Unspecified Issue
| [66665] PHP MySQL LOAD DATA LOCAL open_basedir Bypass
| [65851] MySQL ALTER DATABASE #mysql50# Prefix Handling DoS
| [65450] phpGraphy mysql_cleanup.php include_path Parameter Remote File Inclusion
| [65085] MySQL Enterprise Monitor Unspecified CSRF
| [64843] MySQL DROP TABLE Command Symlink MyISAM Table Local Data Deletion
| [64588] MySQL sql/net_serv.cc my_net_skip_rest Function Large Packet Handling Remote DoS
| [64587] MySQL COM_FIELD_LIST Command Packet Table Name Argument Overflow
| [64586] MySQL COM_FIELD_LIST Command Packet Authentication Bypass
| [64524] Advanced Poll misc/get_admin.php mysql_host Parameter XSS
| [64447] Tirzen Framework (TZN) tzn_mysql.php Username Parameter SQL Injection Authentication Byp ass
| [64320] ClanSphere MySQL Driver s_email Parameter SQL Injection
| [63903] MySQL sql/sql_plugin.cc mysql_uninstall_plugin Function UNINSTALL PLUGIN Command Privil ege Check Weakness
| [63115] Quicksilver Forums mysqldump Process List Database Password Disclosure
| [62830] Employee Timeclock Software mysqldump Command-line Database Password Disclosure
| [62640] PHP mysqli_real_escape_string() Function Error Message Path Disclosure
| [62216] Flex MySQL Connector ActionScript SQL Query Arbitrary Code Execution
| [61752] kiddog_mysqldumper Extension for TYPO3 Unspecified Information Disclosure
| [61497] microTopic admin/mysql.php rating Parameter SQL Injection
| [60665] MySQL CREATE TABLE MyISAM Table mysql_unpacked_real_data_home Local Restriction By pass
| [60664] MySQL sql/sql_table.cc Data Home Directory Symlink CREATE TABLE Access Restriction Bypa ss
| [60516] RADIO istek scripti estafresgaftesantusyan.inc Direct Request MySQL Database Credentials Dis closure
| [60489] MySQL GeomFromWKB() Function First Argument Geometry Value Handling DoS
| [60488] MySQL SELECT Statement WHERE Clause Sub-query DoS
| [60487] MySQL vio_verify_callback() Function Crafted Certificate MiTM Weakness
| [60356] MySql Client Library (libmysqlclient) mysql_real_connect Function Local Overflow
| [59907] MySQL on Windows bind-address Remote Connection Weakness
| [59906] MySQL on Windows Default Configuration Logging Weakness

| [59616] MySQL Hashed Password Weakness
| [59609] Suckbot mod_mysql_logger Shared Object Unspecified Remote DoS
| [59495] Cyrus SASL LDAP / MySQL Authentication Patch password Field SQL Injection Authentication Bypass
| [59062] phpMyAdmin Extension for TYPO3 MySQL Table Name Unspecified XSS
| [59045] phpMyAdmin Crafted MYSQL Table Name XSS
| [59030] mysql-ocaml for MySQL mysql_real_escape_string() Function Character Escaping Weakness
| [57587] Zmanda Recovery Manager for MySQL socket-server.pl system() Function Local Privilege Escalation
| [57586] Zmanda Recovery Manager for MySQL socket-server.pl system() Function Remote Shell Command Execution
| [56741] MySQL Connector/J Unicode w/ SJIS/Windows-31J Charset SQL Injection
| [56134] Virtualmin MySQL Module Execute SQL Feature Arbitrary File Access
| [55734] MySQL sql_parse.cc dispatch_command() Function Format String DoS
| [55566] MySQL Connector/NET SSL Certificate Verification Weakness
| [53525] MyBlog /config/mysqlconnection.inc Direct Request Information Disclosure
| [53524] blog+ includes/window_top.php row_mysql_bloginfo[theme] Parameter Traversal Local File Inclusion
| [53523] blog+ includes/block_center_down.php row_mysql_blocks_center_down[file] Parameter Traversal Local File Inclusion
| [53522] blog+ includes/block_center_top.php row_mysql_blocks_center_top[file] Parameter Traversal Local File Inclusion
| [53521] blog+ includes/block_left.php row_mysql_blocks_left[file] Parameter Traversal Local File Inclusion
| [53520] blog+ includes/block_right.php row_mysql_blocks_right[file] Parameter Traversal Local File Inclusion
| [53519] blog+ includes/window_down.php row_mysql_bloginfo[theme] Parameter Traversal Local File Inclusion
| [53366] GEDCOM_TO_MYSQL php/info.php Multiple Parameter XSS
| [53365] GEDCOM_TO_MYSQL php/index.php nom_branche Parameter XSS
| [53364] GEDCOM_TO_MYSQL php/prenom.php Multiple Parameter XSS
| [53360] Blogplus includes/window_top.php row_mysql_bloginfo[theme] Parameter Traversal Local File Inclusion
| [53359] Blogplus includes/window_down.php row_mysql_bloginfo[theme] Parameter Traversal Local File Inclusion
| [53358] Blogplus includes/block_right.php row_mysql_blocks_right[file] Parameter Traversal Local File Inclusion
| [53357] Blogplus includes/block_left.php row_mysql_blocks_left[file] Parameter Traversal Local File Inclusion
| [53356] Blogplus block_center_top.php row_mysql_blocks_center_top[file] Parameter Traversal Local File Inclusion
| [53355] Blogplus includes/block_center_down.php row_mysql_blocks_center_down[file] Parameter Traversal Local File Inclusion
| [53110] XOOPS Cube Legacy ErrorHandler::show() Function MySQL Error Message XSS
| [52729] Asterisk-addon cdr_addon_mysql.c Call Detail Record SQL Injection
| [52728] Tribox cdr_addon_mysql.c Call Detail Record XSS
| [52727] FreePBX cdr_addon_mysql.c Call Detail Record XSS
| [52726] Areski cdr_addon_mysql.c Call Detail Record XSS
| [52464] MySQL charset Column Truncation Weakness
| [52453] MySQL sql/item_xmlfunc.cc ExtractValue() / UpdateXML() Functions Scalar XPath DoS
| [52378] Cisco ANM MySQL root Account Default Password
| [52264] Broadcast Machine MySQLController.php controllers/baseDir Parameter Remote File Inclusion
| [51923] Apache HTTP Server mod-auth-mysql Module mod_auth_mysql.c Multibyte Character Encoding SQL Injection
| [51171] MySQL InnoDB convert_search_mode_to_innobase Function DoS

| [50892] MySQL Calendar index.php username Parameter SQL Injection
| [50827] Nodstrum MySQL Calendar nodstrumCalendarV2 Cookie Manipulation Admin Authentication By pass
| [49875] PromoteWeb MySQL go.php id Parameter SQL Injection
| [48710] MySQL Command Line Client HTML Output XSS
| [48709] MySQL Quick Admin actions.php lang Parameter Traversal Local File Inclusion
| [48708] MySQL Quick Admin index.php language Cookie Traversal Local File Inclusion
| [48021] MySQL Empty Bit-String Literal Token SQL Statement DoS
| [47789] mysql-lists Unspecified XSS
| [47394] Keld PHP-MySQL News Script login.php username Parameter SQL Injection
| [45073] MySQLDumper Extension for TYPO3 Unspecified Authentication Bypass
| [44937] MySQL MyISAM Table CREATE TABLE Privilege Check Bypass
| [44138] Debian GNU/Linux libdspam7-drv-mysql Cron MySQL dspam Database Password Local Disclos ure
| [44071] Phorum /include/db/mysql.php Unspecified Search SQL Injection
| [43180] MySQL sql_select.cc INFORMATION_SCHEMA Table Crafted Query Remote DoS
| [43179] MySQL Server BINLOG Statement Rights Checking Failure
| [42610] MySQL DEFINER View Value Crafted Statements Remote Privilege Escalation
| [42609] MySQL Federated Engine SHOW TABLE STATUS Query Remote DoS
| [42608] MySQL RENAME TABLE Symlink System Table Overwrite
| [42607] MySQL Multiple table-level DIRECTORY Remote Privilege Escalation
| [42460] MySQLDumper HTTP POST Request Remote Authentication Bypass
| [42423] AdventNet EventLog Analyzer MySQL Installation Default root Account
| [41861] Bacula make_catalog_backup Function MySQL Director Password Cleartext Disclosure
| [40232] PHP MySQL Banner Exchange inc/lib.inc Direct Request Database Disclosure
| [40188] Password Manager Pro (PMP) mysql Unspecified Remote Command Injection
| [39279] PHP mysql_error() Function XSS
| [39145] aurora framework db_mysql.lib pack_var() value Parameter SQL Injection
| [38567] NetClassifieds Mysql_db.php Halt_On_Error Setting Error Message Path Disclosure
| [38112] Excel Parser Pro sample/xls2mysql parser_path Parameter Remote File Inclusion
| [37880] Asterisk-Addons source/destination Numbers cdr_addon_mysql Module SQL Injection
| [37784] PHP MySQL Extension Multiple Function Security Restriction Bypass
| [37783] MySQL Community Server CREATE TABLE LIKE Table Structure Disclosure
| [37782] MySQL Community Server External Table View Privilege Escalation
| [37781] MySQL ALTER TABLE Information Disclosure
| [37539] GPL PHP Board db.mysql.inc.php root_path Parameter Remote File Inclusion
| [37195] Eve-Nuke Module for PHP-Nuke db/mysql.php phpbb_root_path
| [37015] paBugs class.mysql.php path_to_bt_dir Parameter Remote File Inclusion
| [36868] PHP MySQLi Extension LOCAL INFILE Operation Security Restriction Bypass
| [36867] PHP MySQL Extension LOCAL INFILE Operation Security Restriction Bypass
| [36771] InterWorx-CP SiteWorx mysql.php PATH_INFO Parameter XSS
| [36757] InterWorx-CP NodeWorx mysql.php PATH_INFO Parameter XSS
| [36732] MySQL Community Server Connection Protocol Malformed Password Packet Remote DoS
| [36251] Associated Press (AP) Newspower Default MySQL root Password
| [35168] Study Planner (Studiewijzer) db/mysql/db.inc.php SPL_CFG[dirroot] Parameter Remote File Incl usion
| [35037] Fantastico for cPanel includes/mysqlconfig.php fantasticopath Parameter Traversal Local File In clusion
| [34780] Backup Manager Command Line Cleartext MySQL Password Disclosure
| [34766] MySQL RENAME TABLE Statement Arbitrary Table Name Modification
| [34765] MySQL mysql_change_db Function THD::db_access Privilege Escalation
| [34734] MySQL Crafted IF Clause Divide-by-zero NULL Dereference DoS
| [34038] MySQL Commander ressourcen/dbopen.php home Parameter Remote File Inclusion
| [33974] MySQL information_schema Table Subselect Single-Row DoS
| [33678] MySQLNewsEngine affichearticles.php3 newsenginedir Parameter Remote File Inclusion

| [33447] WGS-PPC (PPC Search Engine) config/mysql_config.php INC Parameter Remote File Inclusion
| [33372] deV!L'z Clanportal inc/filebrowser/browser.php MySQL Data Disclosure
| [33147] ActiveCalendar data/mysqlevents.php css Parameter XSS
| [32784] Storystream mysqli.php baseDir Parameter Remote File Inclusion
| [32783] Storystream mysql.php baseDir Parameter Remote File Inclusion
| [32421] Contenido CMS conlib/db_mysqli.inc Direct Request Path Disclosure
| [32272] JevonCMS /phplib/db_mysql.inc Direct Request Path Disclosure
| [32171] Blue Magic Board db_mysql_error.php Direct Request Path Disclosure
| [32056] BTSaveMySql Direct Request Config File Disclosure
| [32044] cPanel WebHost Manager (WHM) scripts/passwdmysql password Parameter XSS
| [32024] TikiWiki tiki-wiki_rss.php ver MySQL Credential Disclosure
| [31963] Agora MysqlfinderAdmin.php _SESSION[PATH_COMPOSANT] Parameter Remote File Inclusio
n
| [31431] ZoomStats libs/dbmax/mysql.php GLOBALS[lib][db][path] Parameter Remote File Inclusion
| [30172] TikiWiki Multiple Script Empty sort_mode Parameter MySQL Authentication Credential Disclosur
e
| [29696] MySQLDumper sql.php db Parameter XSS
| [29453] ConPresso CMS db_mysql.inc.php msg Parameter XSS
| [29122] cPanel mysqladmin/hooksadmin Unspecified Privilege Escalation
| [28296] MySQL Crafted multiupdate / subselects Query Local DoS
| [28288] MySQL Instance_options::complete_initialization Function Overflow
| [28030] Tutti Nova class.novaRead.mysql.php TNLIB_DIR Parameter Remote File Inclusion
| [28029] Tutti Nova class.novaAdmin.mysql.php TNLIB_DIR Parameter Remote File Inclusion
| [28028] Tutti Nova class.novaEdit.mysql.php TNLIB_DIR Parameter Remote File Inclusion
| [28013] MySQL SUID Routine Miscalculation Arbitrary DML Statement Execution
| [28012] MySQL Case Sensitivity Unauthorized Database Creation
| [27919] MySQL VIEW Access information_schema.views Information Disclosure
| [27703] MySQL MERGE Table Privilege Persistence
| [27593] Drupal database.mysqli.inc Multiple Parameter SQL Injection
| [27549] Opsware NAS /etc/init.d/mysqll MySQL root Cleartext Password Local Disclosure
| [27416] MySQL Server time.cc date_format Function Format String
| [27054] MySQL mysqld str_to_date Function NULL Argument DoS
| [26923] PHP/MySQL Classifieds (PHP Classifieds) search.php rate Parameter SQL Injection
| [26922] PHP/MySQL Classifieds (PHP Classifieds) AddAsset1.php Multiple Field XSS
| [26822] Bee-hive Lite include/listall.inc.php mysqlcall Parameter Remote File Inclusion
| [26821] Bee-hive Lite conad/include/mysqlCall.inc.php config Parameter Remote File Inclusion
| [26820] Bee-hive Lite conad/logout.inc.php mysqlCall Parameter Remote File Inclusion
| [26819] Bee-hive Lite conad/login.inc.php mysqlCall Parameter Remote File Inclusion
| [26818] Bee-hive Lite conad/checkPasswd.inc.php mysqlCall Parameter Remote File Inclusion
| [26817] Bee-hive Lite conad/changeUserDetails.inc.php mysqlCall Parameter Remote File Inclusion
| [26816] Bee-hive Lite conad/changeEmail.inc.php mysqlCall Parameter Remote File Inclusion
| [26125] Open Searchable Image Catalogue core.php do_mysql_query Function Error Message XSS
| [26123] Open Searchable Image Catalogue core.php do_mysql_query Function SQL Injection
| [25987] MySQL Multibyte Encoding SQL Injection Filter Bypass
| [25908] Drupal database.mysql.inc Multiple Parameter SQL Injection
| [25595] Apple Mac OS X MySQL Manager Blank root Password
| [25228] MySQL Crafted COM_TABLE_DUMP Request Arbitrary Memory Disclosure
| [25227] MySQL COM_TABLE_DUMP Packet Overflow
| [25226] MySQL Malformed Login Packet Remote Memory Disclosure
| [24245] Cholod Mysql Based Message Board Unspecified XSS
| [24244] Cholod Mysql Based Message Board mb.cgi showmessage Action SQL Injection
| [23963] WoltLab Burning Board class_db_mysql.php SQL Error Message XSS
| [23915] Netcool/NeuSecure MySQL Database Connection Restriction Bypass
| [23611] Aztek Forum index.php msg Variable Forced MySQL Error Information Disclosure
| [23526] MySQL Query NULL Charcter Logging Bypass

| [23157] PHP/MYSQL Timesheet changehrs.php Multiple Parameter SQL Injection
| [23156] PHP/MYSQL Timesheet index.php Multiple Parameter SQL Injection
| [22995] PAM-MySQL Authentication pam_get_item() Function Unspecified Privilege Escalation
| [22994] PAM-MySQL SQL Logging Facility Segfault DoS
| [22485] Recruitment Software admin/site.xml MySQL Authentication Credential Disclosure
| [22479] PHP mysqli Extension Error Message Format String
| [22232] PHP Pipe Variable mysql_connect() Function Overflow
| [21685] MySQL Auction Search Module keyword XSS
| [20698] Campsite notifyendsubs Cron MySQL Password Cleartext Remote Disclosure
| [20145] Proofpoint Protection Server Embedded MySQL Server Unpassworded root Account
| [19457] aMember Pro mysql.inc.php Remote File Inclusion
| [19377] MAXdev MD-Pro /MySQL_Tools/admin.php Path Disclosure
| [18899] MySQL UDF Library Arbitrary Function Load Privilege Escalation
| [18898] MySQL UDF LoadLibraryEx Function Nonexistent Library Load DoS
| [18897] MySQL on Windows UDF Create Function Traversal Privilege Escalation
| [18896] MySQL User-Defined Function init_syms() Function Overflow
| [18895] MySQL libmysqlclient.so host Parameter Remote Overflow
| [18894] MySQL drop database Request Remote Overflow
| [18622] FunkBoard mysql_install.php Email Field Arbitrary PHP Code Injection
| [18620] FunkBoard mysql_install.php Admin/Database Password Manipulation
| [18406] MySQL Eventum releases.php SQL Injection
| [18405] MySQL Eventum custom_fields_graph.php SQL Injection
| [18404] MySQL Eventum custom_fields.php SQL Injection
| [18403] MySQL Eventum login.php email Parameter SQL Injection Authentication Bypass
| [18402] MySQL Eventum get_jsrs_data.php F Parameter XSS
| [18401] MySQL Eventum list.php release Parameter XSS
| [18400] MySQL Eventum view.php id Parameter XSS
| [18173] MySQL on Windows USE Command MS-DOS Device Name DoS
| [17801] Bugzilla MySQL Replication Race Condition Information Disclosure
| [17223] xMySQLadmin Symlink Arbitrary File Deletion
| [16727] MySQL Nonexistent '--user' Error Incorrect Privilege Database Invocation
| [16689] MySQL mysql_install_db Symlink Arbitrary File Overwrite
| [16056] Plans Unspecified mySQL Remote Password Disclosure
| [15993] MySQL MaxDB Webtool Remote getIfHeader() WebDAV Function Remote Overflow
| [15817] MySQL MaxDB Web Tool getLockTokenHeader() Function Remote Overflow
| [15816] MySQL MaxDB Web Administration Service Malformed GET Request Overflow
| [15451] paNews auth.php mysql_prefix Parameter SQL Injection
| [14748] MySQL MS-DOS Device Names Request DoS
| [14678] MySQL CREATE FUNCTION Arbitrary libc Code Execution
| [14677] MySQL CREATE FUNCTION mysql.func Table Arbitrary Library Injection
| [14676] MySQL CREATE TEMPORARY TABLE Symlink Privilege Escalation
| [14386] phpMyAdmin mysqli.dbi.lib.php Path Disclosure
| [14052] Symantec Brightmail AntiSpam Multiple Default MySQL Accounts
| [13086] MySQL MaxDB Web Agent Malformed HTTP Header DoS
| [13085] MySQL MaxDB Web Agent WebDAV sapdbwa_GetUserData() Function Remote DoS
| [13013] MySQL mysqlaccess.sh Symlink Arbitrary File Manipulation
| [12919] MySQL MaxDB WebAgent websql Remote Overflow
| [12779] MySQL User Defined Function Privilege Escalation
| [12609] MySQL Eventum projects.php Multiple Parameter XSS
| [12608] MySQL Eventum preferences.php Multiple Parameter XSS
| [12607] MySQL Eventum forgot_password.php email Parameter XSS
| [12606] MySQL Eventum index.php email Parameter XSS
| [12605] MySQL Eventum Default Vendor Account
| [12275] MySQL MaxDB Web Tools wahttp Nonexistent File Request DoS
| [12274] MySQL MaxDB Web Tools WebDAV Handler Remote Overflow

| [11689] Roxen Web Server MySQL Socket Permission Weakness
| [10985] MySQL MATCH..AGAINST Query DoS
| [10959] MySQL GRANT ALL ON Privilege Escalation
| [10660] MySQL ALTER TABLE/RENAME Forces Old Permission Checks
| [10659] MySQL ALTER MERGE Tables to Change the UNION DoS
| [10658] MySQL mysql_real_connect() Function Remote Overflow
| [10532] MySQL MaxDB webdbm Server Field DoS
| [10491] AWS MySQLguest AWSguest.php Script Insertion
| [10244] MySQL libmysqlclient Prepared Statements API Overflow
| [10226] MySQLGuest AWSguest.php Multiple Field XSS
| [9912] PHP safe_mode MySQL Database Access Restriction Bypass
| [9911] Inter7 vpopmail MySQL Module Authentication Credential Disclosure
| [9910] MySQL mysql_change_user() Double-free Memory Pointer DoS
| [9909] MySQL datadir/my.cnf Modification Privilege Escalation
| [9908] MySQL my.ini Initialization File datadir Parameter Overflow
| [9907] MySQL SELECT Statement String Handling Overflow
| [9906] MySQL GRANT Privilege Arbitrary Password Modification
| [9509] teapop MySQL Authentication Module SQL Injection
| [9018] MySQL Backup Pro getbackup() Method Unspecified Issue
| [9015] MySQL mysqlhotcopy Insecure Temporary File Creation
| [8997] Cacti config.php MySQL Authentication Credential Cleartext Disclosure
| [8979] MySQL SHOW GRANTS Encrypted Password Disclosure
| [8889] MySQL COM_TABLE_DUMP Package Negative Integer DoS
| [8888] MySQL COM_CHANGE_USER Command Long Repsonse Overflow
| [8887] MySQL COM_CHANGE_USER Command One Character Password Brute Force
| [8886] MySQL libmysqlclient Library read_one_row Overflow
| [8885] MySQL libmysqlclient Library read_rows Overflow
| [7476] MySQL Protocol 4.1 Authentication Scramble String Overflow
| [7475] MySQL Zero-length Scrambled String Crafted Packet Authentication Bypass
| [7245] MySQL Pluggable Authentication Module (pam_mysql) Password Disclosure
| [7128] MySQL show database Database Name Exposure
| [6716] MySQL Database Engine Weak Authentication Information Disclosure
| [6605] MySQL mysqld Readable Log File Information Disclosure
| [6443] PowerPhlogger db_dump.php View Arbitrary mySQL Dump
| [6421] MySQL mysqld_multi Symlink Arbitrary File Overwrite
| [6420] MySQL mysqlbug Symlink Arbitrary File Overwrite
| [2537] MySQL sql_acl.cc get_salt_from_password Function Password Handling Remote Overflow
| [2144] WinMySQLadmin my.ini Cleartext Password Disclosure
| [653] PCCS-Linux MySQL Database Admin Tool Authentication Credential Disclosure
| [520] MySQL Database Name Traversal Arbitrary File Modification
| [380] MySQL Server on Windows Default Null Root Password
| [261] MySQL Short Check String Authentication Bypass
|_
8080/tcp open http Jetty 8.1.7.v20120910
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.15
| Found the following possible CSRF vulnerabilities:
|
| Path: http://10.0.2.15:8080/continuum/security/login.action;jsessionid=v5ik1vlhpbiabqmq93k7irmv
| Form id: loginform
| Form action: /continuum/security/login_submit.action;jsessionid=mvsuavsh7nifpsldojpycqwr
|
| Path: http://10.0.2.15:8080/continuum/security/login.action;jsessionid=mvsuavsh7nifpsldojpycqwr
| Form id: loginform
| Form action: /continuum/security/login_submit.action;jsessionid=mvsuavsh7nifpsldojpycqwr

|
| Path: http://10.0.2.15:8080/continuum/security/login_submit.action;jsessionid=mvsuavsh7nifpsldojpyc
qwr
| Form id: loginform
| Form action: /continuum/security/login_submit.action;jsessionid=mvsuavsh7nifpsldojpycqwr
|
| Path: http://10.0.2.15:8080/continuum/security/passwordReset.action;jsessionid=mvsuavsh7nifpsldojp
ycqwr
| Form id: passwordresetform
| Form action: /continuum/security/passwordReset_submit.action;jsessionid=mvsuavsh7nifpsldojpycqw
r
|
| Path: http://10.0.2.15:8080/continuum/security/login.action;jsessionid=v5ik1vlhpbiabqmq93k7irmv
| Form id: loginform
| Form action: /continuum/security/login_submit.action;jsessionid=mvsuavsh7nifpsldojpycqwr
|
| Path: http://10.0.2.15:8080/continuum/security/register.action;jsessionid=mvsuavsh7nifpsldojpycqwr
| Form id: registerform
| Form action: /continuum/security/register_submit.action;jsessionid=mvsuavsh7nifpsldojpycqwr
|
| Path: http://10.0.2.15:8080/continuum/security/login.action;jsessionid=v5ik1vlhpbiabqmq93k7irmv
| Form id: loginform
| Form action: /continuum/security/login_submit.action;jsessionid=mvsuavsh7nifpsldojpycqwr
|
| Path: http://10.0.2.15:8080/continuum/security/passwordReset_submit.action;jsessionid=mvsuavsh7ni
fpsldojpycqwr
| Form id: passwordresetform
| Form action: /continuum/security/passwordReset_submit.action;jsessionid=mvsuavsh7nifpsldojpycqw
r
|
| Path: http://10.0.2.15:8080/continuum/security/register_submit.action;jsessionid=mvsuavsh7nifpsldojp
ycqwr
| Form id: registerform
|_   Form action: /continuum/security/register_submit.action;jsessionid=mvsuavsh7nifpsldojpycqwr
|_http-server-header: Jetty(8.1.7.v20120910)
| temp: VulDB - https://vuldb.com:
| [177419] Eclipse Jetty up to 9.4.40/10.0.2/11.0.2 sessionDestroyed session expiration
| [163627] Eclipse Jetty up to 9.4.32.v20200/10.0.0.beta2/11.0.0.beta2O on Unix temp file
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2011-4461] Jetty 8.1.0.RC2 and earlier computes hash values for form parameters without restricti
ng the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of serv
ice (CPU consumption) by sending many crafted parameters.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [99104] Jetty CVE-2017-9735 Security Bypass Vulnerability
| [90945] Jetty CVE-2016-4800 Security Bypass Vulnerability
| [79858] Jetty CVE-2006-2758 Directory Traversal Vulnerability
| [79857] Jetty CVE-2006-2759 Remote Security Vulnerability
| [72768] Jetty CVE-2015-2080 Information Disclosure Vulnerability
| [63970] Jetty NTFS Remote Security Bypass Vulnerability
| [51199] Jetty Hash Collision Denial Of Service Vulnerability
| [50723] Jetty Web Server Directory Traversal Vulnerability
| [37929] Jetty Terminal Escape Sequence in Logs Command Injection Vulnerability
| [37927] Jetty JSP Snoop Page Multiple Cross-Site Scripting Vulnerabilities

| [34800] Jetty Cross Site Scripting and Information Disclosure Vulnerabilities
| [27117] Jetty Double Slash URI Information Disclosure Vulnerability
| [26697] Jetty Dump Servlet Cross Site Scripting Vulnerability
| [26696] Jetty Unspecified HTTP Response Splitting Vulnerability
| [26695] Jetty Cookie Names Session Hijacking Vulnerability
| [22405] Jetty Insecure Random Number Generation Vulnerability
| [15515] Jetty URL Encoded Backslash Source Code Disclosure Vulnerability
| [11330] Jetty Directory Traversal Vulnerability
| [9917] Jetty Unspecified Denial Of Service Vulnerability
| [5852] Jetty Servlet Engine Arbitrary Command Execution Vulnerability
| [5821] Jetty Servlet Engine Cross Site Scripting Vulnerability
| [4360] Jetty Double-Slash Request Arbitrary File Access Vulnerability
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [72017] Jetty hash denial of service
| [71356] VMware vCenter Update Manager vSphere Update Manager Jetty unspecified directory traversa
|
| [55652] Jetty WebApp JSP Snoop page cross-site scripting
| [55651] Jetty dump.jsp cross-site scripting
| [55650] Jetty Dump Servlet information disclosure
| [53777] Jetty CookieDump.java cross-site scripting
| [50411] Jetty DispatchServlet denial of service
| [50301] Jetty listing path cross-site scripting
| [50298] Jetty HTTP server directory traversal
| [39407] Jetty multiple characters information disclosure
| [38899] Jetty unspecified CRLF injection
| [38897] Jetty HTTP cookie session hijacking
| [38894] Jetty Dump Servlet cross-site scripting
| [32240] Jetty session identifiers session hijacking
| [31286] Jetty .jsp extension source code disclosure
| [28060] Jetty URL encoded format directory traversal
| [23165] Jetty JSP source code disclosure
| [17600] Jetty multiple products HTTP directory traversal
| [15537] Jetty unknown denial of service
| [10246] Jetty CGIServlet directory traversal could be used to execute commands
| [10219] Jetty HTTP Server and Servlet Engine cross-site scripting
|
| Exploit-DB - https://www.exploit-db.com:
| [21895] Jetty 3.1.6/3.1.7/4.1 Servlet Engine Arbitrary Command Execution Vulnerability
| [21875] Jetty 4.1 Servlet Engine Cross Site Scripting Vulnerability
| [9887] jetty 6.x - 7.x xss, information disclosure, injection
| [8646] Mortbay Jetty <= 7.0.0-pre5 Dispatcher Servlet Denial of Service Exploit
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [864104] Fedora Update for jetty FEDORA-2012-0752
| [864103] Fedora Update for jetty FEDORA-2012-0730
| [860534] Fedora Update for jetty FEDORA-2008-6164
| [860529] Fedora Update for jetty FEDORA-2008-6141
| [840993] Ubuntu Update for jetty USN-1429-1
| [100183] Jetty Cross Site Scripting and Information Disclosure Vulnerabilities
| [66126] Mandriva Security Advisory MDVSA-2009:291 (jetty5)
| [64091] Fedora Core 10 FEDORA-2009-5513 (jetty)
| [64090] Fedora Core 11 FEDORA-2009-5509 (jetty)
| [64089] Fedora Core 9 FEDORA-2009-5500 (jetty)
| [60397] FreeBSD Ports: jetty

| [60296] FreeBSD Ports: jetty
| [59976] FreeBSD Ports: jetty
| [17348] Jetty < 4.2.19 Denial of Service
|
| SecurityTracker - https://www.securitytracker.com:
| [1026475] Jetty Hash Table Collision Bug Lets Remote Users Deny Service
| [1026341] VMware vCenter Update Manager Directory Traversal Flaw in Jetty Component Lets Remote Users View Files
| [1016168] jetty6 Input Validation Flaws Let Remote Users Traverse the Directory
| [1005348] Jetty Java Server Bug in CGI Servlet Lets Remote Users Execute Specified Binaries
| [1005311] Jetty Java Server Input Validation Hole Lets Remote Users Conduct Cross-Site Scripting Attacks
|
| OSVDB - http://www.osvdb.org:
| [94643] Jetty Cookie Name Session Hijacking Weakness
| [94641] Jetty Privileged Process Termination Weakness
| [94640] Jetty Dispatch Servlet Non-existent Servlet Name XSS
| [94639] Jetty Dispatcher Servlet (com.acme.DispatchServlet) Recursive Inclusion Remote DoS
| [94275] Apache Solr JettySolrRunner.java Can Not Find Error Message XSS
| [88638] Jetty on Windows Mixed Case WEB-INF Request Security Bypass
| [88589] Jetty with JBoss Role Authentication Failure Object Leak Weakness
| [88230] Jetty servletConfig Unspecified Downcast Issue
| [88227] Jetty Malformed URL Request Handling Remote DoS
| [87500] Jetty servlet.jar HTTP Method Header Request Entity Too Large XSS
| [87493] Jetty Malformed MultiPart Form Request Handling Remote Filter DoS
| [87488] Jetty TLS Renegotiation Handshakes MiTM Plaintext Data Injection
| [87487] Jetty Multi-byte UTF-8 Character Handling Overflow
| [87482] Jetty Error Handler Exception Message XSS
| [87468] Jetty Malformed If-Modified-Since Header Handling Remote DoS
| [87465] Jetty HttpTester POST Request Handling Overflow DoS
| [87455] Jetty with mod_jk AJP Malformed Request Unspecified Issue
| [87449] Jetty Chunk Handling Infinite Loop Remote DoS
| [87447] Jetty HTTPS Session Cookie Secure / HttpOnly Flag Weakness
| [87438] Jetty HttpFields Cache Unspecified Overflow
| [87431] Jetty Canonical Path Crafted Traversal Unspecified Issue
| [78117] Jetty Hash Collision Form Parameter Parsing Remote DoS
| [75808] Jetty Backtrace Data Manipulation Remote Code Execution
| [65054] Apache ActiveMQ Jetty Error Handler XSS
| [64020] Apache ActiveMQ Jetty ResourceHandler Crafted Request JSP File Source Disclosure
| [61768] Jetty Dump Servlet URI getPathTranslated Variable Value Information Disclosure
| [61767] Jetty Session Dump Servlet URI Multiple Parameter XSS
| [61766] Jetty JSP Dump Feature jsp/dump.jsp Query String XSS
| [61765] Jetty WebApp JSP Snoop Page URI PATH_INFO Parameter XSS
| [58883] Jetty CookieDump.java Sample Application cookie/ GET Request Value Parameter XSS
| [58736] Jetty on Windows Double Slash (//) Path Aliasing Unspecified Issue
| [54187] Jetty Directory Listing Semicolon Character XSS
| [54186] Jetty HTTP Server Document Root Traversal Arbitrary File Access
| [44989] Jetty .jsp Mixed Case Request JSP Source Disclosure
| [43255] Jetty SslEngine Unspecified Overflow
| [43254] Jetty UTF-8 Handling Unspecified Overflow
| [43253] Jetty mod_jk AJPParser Packet Handling Overflow
| [43252] Jetty Unspecified Security Issue
| [43209] Jetty jasper2 Unspecified Client Scripting Issue
| [43208] Jetty Trailing Slash Suffix Matching Weakness
| [43207] Jetty Crafted Slash Request Constraint Bypass

| [43206] Jetty Null Byte File Request Restriction Bypass
| [43205] Jetty Error Page Unspecified Script Issue
| [43204] Jetty Cookie Date Handling Overflow
| [42497] Jetty Dump Servlet (webapps/test/jsp/dump.jsp) Unspecified XSS
| [42496] Jetty HTML Cookie Parameter Unspecified Character Sequence Hijacking Weakness
| [42495] Jetty Unspecified CRLF Injection
| [39855] Jetty URL Multiple Slash Character Information Disclosure
| [33108] Jetty Predictable Session Identifier Issue
| [21000] Jetty Unspecified JSP Source Code Disclosure
| [10490] IBM Trading Partner Interchange Jetty Server Traversal Arbitrary File Access
| [9543] Jetty CGI+windows Unspecified Security Issue
| [9209] Jetty JSP Servlet Engine .jsp Encoded Newline XSS
| [8948] Jetty HTTP Server CGIServlet Double Dot Arbitrary File Access
| [4387] Jetty HTTP Server HttpRequest.java Content-Length Handling Remote Overflow DoS
|_
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
8181/tcp closed intermapper
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.1.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
| VULNERABLE:
| Service regsvc in Microsoft Windows systems vulnerable to denial of service
| State: VULNERABLE
| The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by
a null deference
| pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron
Bowes
| while working on smb-enum-sessions.
|_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 359.78 seconds