M3 – Windows – White Box

Report generated by Nessus™ Mon, 01 Apr 2024 22:55:53 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.0.25

99	347	99	14	176
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 735

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.9	9.0	129718	KB4520003: Windows 7 and Windows Server 2008 R2 October 2019 Security Update
CRITICAL	9.9	9.8	130905	KB4525233: Windows 7 and Windows Server 2008 R2 November 2019 Security Update
CRITICAL	9.9	9.6	136507	KB4556843: Windows 7 and Windows Server 2008 R2 May 2020 Security Update
CRITICAL	9.9	9.2	149392	KB5003233: Windows 7 and Windows Server 2008 R2 Security Update (May 2021)
CRITICAL	9.9	9.5	152436	KB5005089: Windows 7 and Windows Server 2008 R2 Security Update (August 2021)
CRITICAL	9.8	6.7	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	6.7	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	5.9	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	6.7	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	8.4	151425	Apache Struts 2.0.0 < 2.5.26 Possible Remote Code Execution vulnerability (S2-061)
CRITICAL	9.8	7.4	159667	Apache Struts 2.0.0 < 2.5.30 Possible Remote Code Execution vulnerability (S2-062)
CRITICAL	9.8	9.0	102960	Apache Struts 2.1.x >= 2.1.2 / 2.2.x / 2.3.x < 2.3.34 / 2.5.x < 2.5.13 Multiple Vulnerabilities (S2-050 - S2-053)

CRITICAL	9.8	5.9	94336	Apache Struts 2.3.1 < 2.3.31 / 2.5.x < 2.5.5 Convention Plugin Path Traversal RCE (S2-042)
CRITICAL	9.8	7.4	101361	Apache Struts 2.3.x Showcase App Struts 1 Plugin ActionMessage Class Error Message Input Handling RCE (S2-048)
CRITICAL	9.8	9.5	186643	Apache Struts 2.5.0 < 2.5.33 / 6.0.0 < 6.3.0.2 Remote Code Execution (S2-066)
CRITICAL	9.8	7.4	90773	Apache Struts 2.x < 2.3.28.1 Multiple Vulnerabilities
CRITICAL	9.8	8.4	143599	Apache Struts 2.x < 2.5.26 RCE (S2-061)
CRITICAL	9.8	8.4	139607	Apache Struts 2.x <= 2.5.20 Multiple Vulnerabilities
CRITICAL	9.8	6.7	118732	Apache Struts <= 2.3.36 FileUpload Deserialization Vulnerability
CRITICAL	9.8	7.4	95438	Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities
CRITICAL	9.8	6.7	111067	Apache Tomcat 8.0.0 < 8.0.53 Security Constraint Weakness
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	9.6	117418	KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update
CRITICAL	9.8	8.9	118913	KB4467106: Windows 7 and Windows Server 2008 R2 November 2018 Security Update
CRITICAL	9.8	9.7	119582	KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update
CRITICAL	9.8	8.9	122118	KB4486564: Windows 7 and Windows Server 2008 R2 February 2019 Security Update
CRITICAL	9.8	9.7	125063	KB4499175: Windows 7 and Windows Server 2008 R2 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout) (BlueKeep)
CRITICAL	9.8	7.4	127846	KB4512486: Windows 7 and Windows Server 2008 R2 August 2019 Security Update
CRITICAL	9.8	8.9	132866	KB4534314: Windows 7 and Windows Server 2008 R2 January 2020 Security Update
CRITICAL	9.8	9.4	142683	KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update

CRITICAL	9.8	7.5	146342	KB4601363: Windows 7 and Windows Server 2008 R2 February 2021 Security Update
CRITICAL	9.8	10.0	147231	KB5000851: Windows 7 and Windows Server 2008 R2 March 2021 Security Update
CRITICAL	9.8	9.8	156069	KB5008282: Windows 7 and Windows Server 2008 R2 Security Update (December 2021)
CRITICAL	9.8	9.4	159672	KB5012649: Windows 7 and Windows Server 2008 R2 Security Update (April 2022)
CRITICAL	9.8	7.4	160937	KB5013999: Windows 7 and Windows Server 2008 R2 Security Update (May 2022)
CRITICAL	9.8	9.5	163952	KB5016679: Windows 7 and Windows Server 2008 R2 Security Update (August 2022)
CRITICAL	9.8	9.2	165002	KB5017373: Windows Server 2008 R2 Security Update (September 2022)
CRITICAL	9.8	9.0	171440	KB5022874: Windows Server 2008 R2 Security Update (February 2023)
CRITICAL	9.8	7.4	172517	KB5023759: Windows Server 2008 R2 Security Update (March 2023)
CRITICAL	9.8	9.4	174103	KB5025277: Windows Server 2008 R2 Security Update (April 2023)
CRITICAL	9.8	9.4	175344	KB5026426: Windows Server 2008 R2 Security Update (May 2023)
CRITICAL	9.8	6.7	177241	KB5027256: Windows Server 2008 R2 Security Update (June 2023)
CRITICAL	9.8	9.4	178168	KB5028224: Windows Server 2008 R2 Security Update (July 2023)
CRITICAL	9.8	9.6	179489	KB5029307: Windows Server 2008 R2 Security Update (August 2023)
CRITICAL	9.8	6.7	182857	KB5031441: Windows Server 2008 R2 Security Update (October 2023)
CRITICAL	9.8	9.6	185587	KB5032250: Windows Server 2008 R2 Security Update (November 2023)
CRITICAL	9.8	7.4	51956	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) (uncredentialed check)
CRITICAL	9.8	5.9	89757	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass (3141780)

CRITICAL	9.8	7.4	91605	MS16-077: Security Update for WPAD (3165191)
CRITICAL	9.8	8.9	94017	MS16-120: Security Update for Microsoft Graphics Component (3192884)
CRITICAL	9.8	5.9	139377	ManageEngine Desktop Central < 10 Build 10.0.533 Integer Overflow
CRITICAL	9.8	8.9	155865	ManageEngine Desktop Central < 10.1.2127.18 / 10.1.2128.0 < 10.1.2137.3 Authentication Bypass (CVE-2021-44515)
CRITICAL	9.8	9.7	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	9.8	-	134942	Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)
CRITICAL	9.8	6.7	118233	MySQL 5.5.x < 5.5.62 Multiple Vulnerabilities (October 2018 CPU)
CRITICAL	9.8	5.9	119612	Security Updates for Microsoft .NET Framework (December 2018)
CRITICAL	9.8	6.7	117431	Security Updates for Microsoft .NET Framework (September 2018)
CRITICAL	9.8	6.7	101367	Windows 7 and Windows Server 2008 R2 July 2017 Security Updates
CRITICAL	9.8	9.5	100761	Windows 7 and Windows Server 2008 R2 June 2017 Security Updates
CRITICAL	9.8	8.9	103746	Windows 7 and Windows Server 2008 R2 October 2017 Security Updates (KRACK)
CRITICAL	9.4	9.8	150368	KB5003694: Windows 7 and Windows Server 2008 R2 Security Update (June 2021)
CRITICAL	9.1	5.2	121120	Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control
CRITICAL	9.1	9.5	128640	KB4516033: Windows 7 and Windows Server 2008 R2 September 2019 Security Update
CRITICAL	9.1	5.2	148038	ManageEngine Desktop Central < 10.0.647 Multiple Vulnerabilities
CRITICAL	9.1	5.2	156790	ManageEngine Desktop Central < 10.1.2137.9 Authentication Bypass (CVE-2021-44757)
CRITICAL	9.0	6.5	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.0	8.9	87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)

CRITICAL	10.0	10.0	97576	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (S2-045) (S2-046)
CRITICAL	10.0	-	182281	Apache Struts SEoL (2.3.0.x <= x <= 2.3.37.x)
CRITICAL	10.0	-	171342	Apache Tomcat SEoL (8.0.x)
CRITICAL	10.0	-	171356	Apache httpd SEoL (2.1.x <= x <= 2.2.x)
CRITICAL	10.0	9.5	139491	KB4571719: Windows 7 and Windows Server 2008 R2 August 2020 Security Update
CRITICAL	10.0	-	87893	MS KB3118753: Update for ActiveX Kill Bits
CRITICAL	10.0	-	72704	Microsoft .NET Framework Unsupported
CRITICAL	10.0	-	22024	Microsoft Internet Explorer Unsupported Version Detection
CRITICAL	10.0	-	122615	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0	-	34460	Unsupported Web Server Detection
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.4	51904	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)
CRITICAL	10.0*	5.9	53377	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)
CRITICAL	10.0*	6.7	56736	MS11-083: Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)
CRITICAL	10.0*	7.4	61529	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)
CRITICAL	10.0*	8.9	62907	MS12-075: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)
CRITICAL	10.0*	8.9	63225	MS12-078: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)
CRITICAL	10.0*	5.9	63419	MS13-001: Vulnerabilities in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)

CRITICAL	10.0*	5.9	64576	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2800277)
CRITICAL	10.0*	6.7	69327	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)
CRITICAL	10.0*	6.7	70335	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)
CRITICAL	10.0*	9.2	73805	MS14-021: Security Update for Internet Explorer (2965111)
CRITICAL	10.0*	6.7	73985	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)
CRITICAL	10.0*	8.9	74427	MS14-035: Cumulative Security Update for Internet Explorer (2969262)
CRITICAL	10.0*	5.9	78432	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)
CRITICAL	10.0*	9.2	82771	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)
CRITICAL	10.0*	7.3	90192	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE
CRITICAL	10.0*	5.9	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.8	5.9	88714	Apache Struts 2.x < 2.3.24.1 Multiple Vulnerabilities (S2-026) (S2-027)
HIGH	8.8	5.9	90153	Apache Struts 2.x < 2.3.28 Multiple Vulnerabilities (S2-028) (S2-029) (S2-030) (S2-034)
HIGH	8.8	7.4	91812	Apache Struts 2.x < 2.3.29 Multiple Vulnerabilities (S2-035 - S2-040)
HIGH	8.8	8.9	108966	KB4093108: Windows 7 and Windows Server 2008 R2 April 2018 Security Update
HIGH	8.8	9.4	111689	KB4343899: Windows 7 and Windows Server 2008 R2 August 2018 Security Update (Foreshadow)
HIGH	8.8	9.7	118001	KB4462915: Windows 7 and Windows Server 2008 R2 October 2018 Security Update
HIGH	8.8	9.4	121017	KB4480960: Windows 7 and Windows Server 2008 R2 January 2019 Security Update
HIGH	8.8	9.6	122782	KB4489885: Windows 7 and Windows Server 2008 R2 March 2019 Security Update

HIGH	8.8	9.7	123945	KB4493448: Windows 7 and Windows Server 2008 R2 April 2019 Security Update
HIGH	8.8	9.8	125824	KB4503269: Windows 7 and Windows Server 2008 R2 June 2019 Security Update
HIGH	8.8	9.6	126571	KB4507456: Windows 7 and Windows Server 2008 R2 July 2019 Security Update (SWAPGS)
HIGH	8.8	9.6	131934	KB4530692: Windows 7 and Windows Server 2008 R2 December 2019 Security Update
HIGH	8.8	9.8	134864	KB4537813: Windows 7 and Windows Server 2008 R2 February 2020 Security Update
HIGH	8.8	9.7	134865	KB4541500: Windows 7 and Windows Server 2008 R2 March 2020 Security Update
HIGH	8.8	9.7	135472	KB4550965: Windows 7 and Windows Server 2008 R2 April 2020 Security Update
HIGH	8.8	8.9	137260	KB4561669: Windows 7 and Windows Server 2008 R2 June 2020 Security Update
HIGH	8.8	8.9	138460	KB4565539: Windows 7 and Windows Server 2008 R2 July 2020 Security Update
HIGH	8.8	7.4	140422	KB4577053: Windows 7 and Windows Server 2008 R2 September 2020 Security Update
HIGH	8.8	7.4	141431	KB4580387: Windows 7 and Windows Server 2008 R2 October 2020 Security Update
HIGH	8.8	7.4	144877	KB4598289: Windows 7 and Windows Server 2008 R2 January 2021 Security Update
HIGH	8.8	7.4	148466	KB5001335: Windows 7 and Windows Server 2008 R2 Security Update (Apr 2021)
HIGH	8.8	9.0	151611	KB5004307: Windows 7 and Windows Server 2008 R2 Security Update (July 2021)
HIGH	8.8	9.8	151476	KB5004951: Windows 7 and Windows Server 2008 R2 OOB Security Update RCE (July 2021)
HIGH	8.8	8.9	153379	KB5005615: Windows 7 and Windows Server 2008 R2 September 2021 Security Update

HIGH	8.8	9.2	154035	KB5006728: Windows 7 and Windows Server 2008 R2 Security Update (October 2021)
HIGH	8.8	8.9	154984	KB5007233: Windows 7 and Windows Server 2008 R2 Security Update (November 2021)
HIGH	8.8	9.5	156627	KB5009621: Windows 7 and Windows Server 2008 R2 Security Update (January 2022)
HIGH	8.8	6.7	158718	KB5011529: Windows 7 and Windows Server 2008 R2 (March 2022) Security Update
HIGH	8.8	9.8	162191	KB5014742: Windows 7 and Windows Server 2008 R2 Security Update (June 2022)
HIGH	8.8	9.0	163050	KB5015862: Windows 7 and Windows Server 2008 R2 Security Update (July 2022)
HIGH	8.8	7.4	166024	KB5018479: Windows 7 / Windows Server 2008 R2 Security Update (October 2022)
HIGH	8.8	8.1	167103	KB5020013: Windows Server 2008 R2 Security Update (November 2022)
HIGH	8.8	9.2	169781	KB5022339: Windows Server 2008 R2 Security Update (January 2023)
HIGH	8.8	6.7	186781	KB5033424: Windows Server 2008 R2 Security Update (December 2023)
HIGH	8.8	8.4	190478	KB5034809: Windows Server 2008 R2 Security Update (February 2024)
HIGH	8.8	8.4	191933	KB5035919: Windows Server 2008 R2 Security Update (March 2024)
HIGH	8.8	9.7	59042	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)
HIGH	8.8	8.9	81735	MS15-020: Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (3041836) (EASYHOOKUP)
HIGH	8.8	6.7	85845	MS15-094: Cumulative Security Update for Internet Explorer (3089548)
HIGH	8.8	6.7	87892	MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)
HIGH	8.8	8.9	89749	MS16-026: Security Update for Graphic Fonts to Address Remote Code Execution (3143148)

HIGH	8.8	9.4	90433	MS16-039: Security Update for Microsoft Graphics Component (3148522)
HIGH	8.8	7.4	90434	MS16-040: Security Update for Microsoft XML Core Services (3148541)
HIGH	8.8	8.9	91005	MS16-055: Security Update for Microsoft Graphics Component (3156754)
HIGH	8.8	5.9	91011	MS16-061: Security Update for Microsoft RPC (3155520)
HIGH	8.8	8.9	91596	MS16-063: Cumulative Security Update for Internet Explorer (3163649)
HIGH	8.8	5.9	91604	MS16-076: Security Update for Netlogon (3167691)
HIGH	8.8	5.9	93473	MS16-114: Security Update for Windows SMBv1 Server (3185879)
HIGH	8.8	8.9	94633	MS16-132: Security Update for Microsoft Graphics Component (3199120)
HIGH	8.8	8.9	95764	MS16-144: Cumulative Security Update for Internet Explorer (3204059)
HIGH	8.8	8.9	95765	MS16-146: Security Update for Microsoft Graphics Component (3204066)
HIGH	8.8	6.7	95766	MS16-147: Security Update for Microsoft Uniscribe (3204063)
HIGH	8.8	9.0	97732	MS17-011: Security Update for Microsoft Uniscribe (4013076)
HIGH	8.8	6.7	117639	ManageEngine Desktop Central 10 < Build 100282 Remote Privilege Escalation
HIGH	8.8	5.9	122234	Security Updates for Microsoft .NET Framework (February 2019)
HIGH	8.8	7.4	126600	Security Updates for Microsoft .NET Framework (July 2019)
HIGH	8.8	6.7	102267	Windows 7 and Windows Server 2008 R2 August 2017 Security Updates
HIGH	8.8	8.9	103127	Windows 7 and Windows Server 2008 R2 September 2017 Security Updates
HIGH	8.6	5.9	154344	Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)
HIGH	8.5	8.1	168681	KB5021288: Windows Server 2008 R2 Security Update (December 2022)

HIGH	8.4	-	65057	Insecure Windows Service Permissions
HIGH	8.3	7.3	138522	Oracle Java SE 1.7.0_271 / 1.8.0_261 / 1.11.0_8 / 1.14.0_2 Multiple Vulnerabilities (Jul 2020 CPU)
HIGH	8.1	8.4	112036	Apache Struts CVE-2018-11776 Results With No Namespace Possible Remote Code Execution (S2-057)
HIGH	8.1	9.2	103697	Apache Tomcat 8.0.0.RC1 < 8.0.47 Multiple Vulnerabilities
HIGH	8.1	6.7	110486	KB4284867: Windows 7 and Windows Server 2008 R2 June 2018 Security Update
HIGH	8.1	8.9	110982	KB4338823: Windows 7 and Windows Server 2008 R2 July 2018 Security Update
HIGH	8.1	6.7	143572	KB4592503: Windows 7 and Windows Server 2008 R2 December 2020 Security Update
HIGH	8.1	6.7	187805	KB5034167: Windows Server 2008 R2 Security Update (January 2024)
HIGH	8.1	6.7	76406	MS14-037: Cumulative Security Update for Internet Explorer (2975687)
HIGH	8.1	8.9	86367	MS15-106: Cumulative Security Update for Internet Explorer (3096441)
HIGH	8.1	9.2	87890	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (3124901)
HIGH	8.1	6.7	91600	MS16-072: Security Update for Group Policy (3163622)
HIGH	8.1	6.7	92018	MS16-087: Security Update for Windows Print Spooler (3170005)
HIGH	8.1	9.7	97737	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya)
HIGH	8.1	9.7	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	8.1	8.9	97743	MS17-012: Security Update for Microsoft Windows (4013078)
HIGH	8.1	9.8	99304	Windows 7 and Windows 2008 R2 April 2017 Security Updates (Petya)

HIGH	8.1	8.9	100058	Windows 7 and Windows Server 2008 R2 May 2017 Security Updates
HIGH	7.8	5.9	180360	7-Zip < 23.00 Multiple Vulnerabilities
HIGH	7.8	8.9	108757	KB4100480: Windows Kernel Elevation of Privilege Vulnerability
HIGH	7.8	9.8	109604	KB4103712: Windows 7 and Windows Server 2008 R2 May 2018 Security Update
HIGH	7.8	9.7	157427	KB5010422: Windows 7 and Windows Server 2008 R2 Security Update (February 2022)
HIGH	7.8	6.7	181299	KB5030261: Windows Server 2008 R2 Security Update (September 2023)
HIGH	7.8	8.9	87881	MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege (3124605)
HIGH	7.8	9.5	88646	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228)
HIGH	7.8	5.9	88650	MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)
HIGH	7.8	6.7	89753	MS16-030: Security Update for Windows OLE to Address Remote Code Execution (3143136)
HIGH	7.8	5.9	89754	MS16-031: Security Update for Microsoft Windows to Address Elevation of Privilege (3140410)
HIGH	7.8	9.7	89755	MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege (3143141)
HIGH	7.8	8.9	89756	MS16-034: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3143145)
HIGH	7.8	5.9	90437	MS16-044: Security Update for Windows OLE (3146706)
HIGH	7.8	5.9	91010	MS16-060: Security Update for Windows Kernel (3154846)
HIGH	7.8	8.9	91012	MS16-062: Security Update for Windows Kernel-Mode Drivers (3158222)
HIGH	7.8	5.9	91601	MS16-073: Security Update for Windows Kernel-Mode Drivers (3164028)
HIGH	7.8	8.9	91602	MS16-074: Security Update for Microsoft Graphics Component (3164036)

HIGH	7.8	9.4	91603	MS16-075: Security Update for Windows SMB Server (3164038)
HIGH	7.8	8.9	92843	MS16-097: Security Update for Microsoft Graphics Component (3177393)
HIGH	7.8	9.5	92821	MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466)
HIGH	7.8	6.7	92823	MS16-101: Security Update for Windows Authentication Methods (3178465)
HIGH	7.8	5.9	93466	MS16-106: Security Update for Microsoft Graphics Component (3185848)
HIGH	7.8	7.2	93470	MS16-111: Security Update for Windows Kernel (3186973)
HIGH	7.8	8.9	94012	MS16-123: Security Update for Windows Kernel-Mode Drivers (3192892)
HIGH	7.8	5.9	94631	MS16-130: Security Update for Microsoft Windows (3199172)
HIGH	7.8	5.9	94635	MS16-134: Security Update for Common Log File System Driver (3193706)
HIGH	7.8	9.7	94636	MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135)
HIGH	7.8	5.9	94638	MS16-137: Security Update for Windows Authentication Methods (3199173)
HIGH	7.8	5.9	95813	MS16-149: Security Update for Microsoft Windows (3205655)
HIGH	7.8	7.4	95768	MS16-151: Security Update for Windows Kernel-Mode Drivers (3205651)
HIGH	7.8	8.4	97794	MS17-013: Security Update for Microsoft Graphics Component (4013075)
HIGH	7.8	9.6	97733	MS17-017: Security Update for Windows Kernel (4013081)
HIGH	7.8	9.4	97738	MS17-018: Security Update for Windows Kernel-Mode Drivers (4013083)
HIGH	7.8	6.7	63155	Microsoft Windows Unquoted Service Path Enumeration
HIGH	7.8	6.0	174511	Oracle Java SE Multiple Vulnerabilities (April 2023 CPU)
HIGH	7.8	5.9	139598	Security Updates for Microsoft .NET Framework (August 2020)

HIGH	7.8	6.7	109652	Security Updates for Microsoft .NET Framework (May 2018)
HIGH	7.8	6.7	99365	Security and Quality Rollup for .NET Framework (April 2017)
HIGH	7.8	9.7	103137	Security and Quality Rollup for .NET Framework (Sep 2017)
HIGH	7.8	8.9	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
HIGH	7.8	8.9	104553	Windows 7 and Windows Server 2008 R2 November 2017 Security Updates
HIGH	7.5	4.4	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	3.6	118731	Apache Struts 2.3.x < 2.3.33 Denial of Service (S2-049)
HIGH	7.5	3.6	177225	Apache Struts < 2.5.31 / 6.1.2.1 Denial of Service (S2-064)
HIGH	7.5	3.6	108760	Apache Struts XStream Handler REST Plugin XML Request Handling Remote DoS (S2-056)
HIGH	7.5	4.4	96003	Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure
HIGH	7.5	6.0	94578	Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities
HIGH	7.5	3.6	99367	Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure
HIGH	7.5	4.4	121119	Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service
HIGH	7.5	4.4	100681	Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation
HIGH	7.5	3.6	121124	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service
HIGH	7.5	8.4	105552	KB4056897: Windows 7 and Windows Server 2008 R2 January 2018 Security Update (Meltdown)(Spectre)
HIGH	7.5	8.9	106802	KB4074587: Windows 7 and Windows Server 2008 R2 February 2018 Security Update
HIGH	7.5	8.9	108290	KB4088878: Windows 7 and Windows Server 2008 R2 March 2018 Security Update (Meltdown)(Spectre)

HIGH	7.5	9.7	72930	MS14-012: Cumulative Security Update for Internet Explorer (2925418)
HIGH	7.5	8.9	77169	MS14-051: Cumulative Security Update for Internet Explorer (2976627)
HIGH	7.5	6.7	87877	MS16-001: Cumulative Security Update for Internet Explorer (3124903)
HIGH	7.5	4.4	88651	MS16-019: Security Update for .NET Framework to Address Denial of Service (3137893)
HIGH	7.5	3.6	92022	MS16-091: Security Update for .NET Framework (3170048)
HIGH	7.5	6.7	93651	MS16-116: Security Update in OLE Automation for VBScript Scripting Engine (3188724)
HIGH	7.5	6.7	94011	MS16-118: Cumulative Security Update for Internet Explorer (3192887)
HIGH	7.5	6.7	94643	MS16-142: Cumulative Security Update for Internet Explorer (3198467)
HIGH	7.5	5.1	96393	MS17-004: Security Update for Local Security Authority Subsystem Service (3216771)
HIGH	7.5	4.4	110192	Oracle GlassFish Server Path Traversal
HIGH	7.5	-	110612	Oracle GlassFish Server URL normalization Denial of Service
HIGH	7.5	6.7	152020	Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU)
HIGH	7.5	4.4	161241	Oracle Java SE Multiple Vulnerabilities (April 2022 CPU)
HIGH	7.5	6.0	189116	Oracle Java SE Multiple Vulnerabilities (January 2024 CPU)
HIGH	7.5	4.4	163304	Oracle Java SE Multiple Vulnerabilities (July 2022 CPU)
HIGH	7.5	4.4	178485	Oracle Java SE Multiple Vulnerabilities (July 2023 CPU)
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	4.9	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	8.9	104896	Security Updates for Internet Explorer (September 2017)

HIGH	7.5	5.1	168395	Security Updates for Microsoft .NET Framework (April 2022)
HIGH	7.5	3.6	111693	Security Updates for Microsoft .NET Framework (August 2018)
HIGH	7.5	4.4	121021	Security Updates for Microsoft .NET Framework (January 2019)
HIGH	7.5	3.6	168397	Security Updates for Microsoft .NET Framework (January 2022)
HIGH	7.5	4.4	125074	Security Updates for Microsoft .NET Framework (May 2019)
HIGH	7.5	3.6	105731	Security and Quality Rollup for .NET Framework (January 2018)
HIGH	7.5	3.6	100056	Security and Quality Rollup for .NET Framework (May 2017)
HIGH	7.3	6.7	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.3	8.9	92021	MS16-090: Security Update for Windows Kernel-Mode Drivers (3171481)
HIGH	7.3	3.4	10547	Microsoft Windows LAN Manager SNMP LanMan Services Disclosure
HIGH	7.3	5.9	66584	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.3	6.7	71426	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
HIGH	7.3	5.9	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.1	4.2	106097	MySQL 5.5.x < 5.5.59 Multiple Vulnerabilities (January 2018 CPU)
HIGH	7.0	5.9	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
HIGH	7.0	4.7	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
HIGH	9.3*	5.9	59044	MS 2695962: Update Rollup for ActiveX Kill Bits (2695962)
HIGH	9.3*	5.9	62045	MS 2736233: Update Rollup for ActiveX Kill Bits (2736233)
HIGH	9.3*	-	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
HIGH	9.3*	9.7	51903	MS11-003: Cumulative Security Update for Internet Explorer (2482017)
HIGH	9.3*	5.9	51907	MS11-007: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)
HIGH	7.2*	5.9	51912	MS11-012: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)

HIGH	9.3*	9.0	53375	MS11-018: Cumulative Security Update for Internet Explorer (2497640)
HIGH	9.3*	8.9	53376	MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)
HIGH	7.6*	8.9	53381	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)
HIGH	9.3*	5.9	53385	MS11-028: Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015)
HIGH	7.5*	7.3	53387	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)
HIGH	9.3*	5.9	53388	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666)
HIGH	9.3*	8.9	53389	MS11-032: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618)
HIGH	7.2*	8.9	53391	MS11-034: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)
HIGH	9.3*	8.9	55118	MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490)
HIGH	9.3*	5.9	55119	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)
HIGH	9.3*	7.4	55121	MS11-041: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)
HIGH	7.6*	6.7	55123	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution (2536276)
HIGH	9.3*	6.7	55124	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)
HIGH	7.2*	9.5	55126	MS11-046: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665)
HIGH	7.8*	5.1	55128	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275)
HIGH	9.3*	9.2	55130	MS11-050: Cumulative Security Update for Internet Explorer (2530548)

HIGH	7.2*	8.9	55570	MS11-054: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)
HIGH	9.3*	6.7	55787	MS11-057: Critical Cumulative Security Update for Internet Explorer (2559049)
HIGH	7.2*	5.9	55793	MS11-063: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)
HIGH	7.8*	4.9	55794	MS11-064: Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)
HIGH	9.3*	7.4	56174	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)
HIGH	9.3*	5.9	56449	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)
HIGH	9.3*	8.9	56451	MS11-077: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)
HIGH	9.3*	5.9	56452	MS11-078: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)
HIGH	9.3*	8.9	56455	MS11-081: Critical Cumulative Security Update for Internet Explorer (2586448)
HIGH	7.1*	3.6	56737	MS11-084: Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)
HIGH	9.3*	7.4	56738	MS11-085: Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)
HIGH	9.3*	9.7	57273	MS11-087: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)
HIGH	9.3*	9.1	57276	MS11-090: Cumulative Security Update of ActiveX Kill Bits (2618451)
HIGH	9.3*	5.9	57285	MS11-099: Cumulative Security Update for Internet Explorer (2618444)
HIGH	9.3*	7.2	57414	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)
HIGH	9.3*	5.9	57469	MS12-001: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)
HIGH	9.3*	9.0	57473	MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)

HIGH	9.3*	8.9	57942	MS12-008: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)
HIGH	7.2*	6.7	57943	MS12-009: Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)
HIGH	9.3*	6.7	57944	MS12-010: Cumulative Security Update for Internet Explorer (2647516)
HIGH	9.3*	5.9	57946	MS12-012: Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)
HIGH	9.3*	5.9	57947	MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)
HIGH	9.3*	8.9	57950	MS12-016: Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)
HIGH	9.3*	9.7	58332	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)
HIGH	9.3*	9.7	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	9.3*	6.7	58655	MS12-023: Cumulative Security Update for Internet Explorer (2675157)
HIGH	9.3*	8.9	58657	MS12-025: Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)
HIGH	9.3*	8.9	59043	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)
HIGH	9.3*	7.4	59454	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)
HIGH	9.3*	9.7	59455	MS12-037: Cumulative Security Update for Internet Explorer (2699988)
HIGH	9.3*	5.9	59456	MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)
HIGH	7.2*	8.9	59459	MS12-041: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)
HIGH	9.3*	9.8	59906	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)

HIGH	9.3*	5.9	59908	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)
HIGH	7.2*	7.4	59910	MS12-047: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)
HIGH	9.3*	5.9	59911	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)
HIGH	9.3*	8.9	61527	MS12-052: Cumulative Security Update for Internet Explorer (2722913)
HIGH	7.2*	6.7	61530	MS12-055: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)
HIGH	9.3*	5.9	61531	MS12-056: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2706045)
HIGH	9.3*	9.7	62223	MS12-063: Cumulative Security Update for Internet Explorer (2744842)
HIGH	9.3*	8.9	62906	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2745030)
HIGH	9.3*	8.9	63224	MS12-077: Cumulative Security Update for Internet Explorer (2761465)
HIGH	9.3*	5.9	63228	MS12-081: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)
HIGH	9.3*	8.9	63229	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution (2770660)
HIGH	9.3*	6.7	63420	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)
HIGH	9.3*	5.9	63422	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324)
HIGH	7.2*	8.4	63423	MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)
HIGH	9.3*	9.7	63522	MS13-008: Security Update for Internet Explorer (2799329)
HIGH	9.3*	9.2	64570	MS13-009: Security Update for Internet Explorer (2792100)
HIGH	7.8*	4.4	64579	MS13-018: Vulnerability in TCP/IP Could Allow Denial of Service (2790655)

HIGH	7.2*	5.9	64580	MS13-019: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)
HIGH	9.3*	8.9	65210	MS13-021: Security Update for Internet Explorer (2809289)
HIGH	7.2*	6.7	65215	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)
HIGH	9.3*	6.7	65875	MS13-028: Security Update for Internet Explorer (2817183)
HIGH	9.3*	8.9	65876	MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2828223)
HIGH	9.3*	9.7	66412	MS13-037: Cumulative Security Update for Internet Explorer (2829530)
HIGH	9.3*	9.7	66413	MS13-038: Security Update for Internet Explorer (2847204)
HIGH	7.5*	5.9	66415	MS13-040: Vulnerabilities in .NET Framework Could Allow Spoofing (2836440)
HIGH	7.2*	8.9	66422	MS13-046: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2840221)
HIGH	9.3*	8.9	66863	MS13-047: Cumulative Security Update for Internet Explorer (2838727)
HIGH	7.1*	3.6	66865	MS13-049: Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (2845690)
HIGH	9.0*	6.7	66866	MS13-050: Vulnerability in Windows Print Spooler Components Could Allow Elevation of Privilege (2839894)
HIGH	9.3*	6.7	67209	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)
HIGH	9.3*	9.7	67210	MS13-053: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (2850851)
HIGH	9.3*	6.7	67211	MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)
HIGH	9.3*	9.4	67212	MS13-055: Cumulative Security Update for Internet Explorer (2846071)
HIGH	9.3*	8.9	69324	MS13-059: Cumulative Security Update for Internet Explorer (2862772)

HIGH	7.8*	3.6	69330	MS13-065: Vulnerability in ICMPv6 Could Allow Denial of Service (2868623)
HIGH	9.3*	9.0	69829	MS13-069: Cumulative Security Update for Internet Explorer (2870699)
HIGH	7.2*	6.7	69835	MS13-076: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2876315)
HIGH	9.3*	9.6	70332	MS13-080: Cumulative Security Update for Internet Explorer (2879017)
HIGH	9.3*	9.4	70333	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)
HIGH	9.3*	6.6	70334	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2878890)
HIGH	9.3*	8.9	70846	MS13-088: Cumulative Security Update for Internet Explorer (2888505)
HIGH	9.3*	9.4	70847	MS13-089: Critical Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)
HIGH	9.3*	9.2	70848	MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986)
HIGH	9.3*	9.5	71312	MS13-097: Cumulative Security Update for Internet Explorer (2898785)
HIGH	7.6*	8.9	71313	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution (2893294)
HIGH	9.3*	8.9	71314	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution (2909158)
HIGH	7.2*	6.7	71316	MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430)
HIGH	7.2*	5.9	71943	MS14-003: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2913602)
HIGH	7.1*	6.6	72428	MS14-005: Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2916036)
HIGH	9.3*	9.4	72432	MS14-009: Vulnerabilities in .NET Framework Could Allow Privilege Escalation (2916607)
HIGH	9.3*	8.9	72433	MS14-010: Cumulative Security Update for Internet Explorer (2909921)

HIGH	9.3*	5.9	72434	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (2928390)
HIGH	7.2*	6.7	72934	MS14-015: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2930275)
HIGH	9.3*	8.9	73415	MS14-018: Cumulative Security Update for Internet Explorer (2950467)
HIGH	7.2*	7.4	73986	MS14-027: Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege (2962488)
HIGH	9.3*	9.4	73988	MS14-029: Security Update for Internet Explorer (2962482)
HIGH	9.3*	6.7	74428	MS14-036: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (2967487)
HIGH	7.6*	7.4	76408	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege (2975685)
HIGH	7.2*	9.4	76409	MS14-040: Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (2975684)
HIGH	7.2*	5.9	77163	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2984615)
HIGH	7.5*	6.7	77165	MS14-047: Vulnerability in LRPC Could Allow Security Feature Bypass (2978668)
HIGH	7.2*	5.9	77167	MS14-049: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (2962490)
HIGH	9.3*	8.3	77572	MS14-052: Cumulative Security Update for Internet Explorer (2977629)
HIGH	9.3*	8.9	78431	MS14-056: Cumulative Security Update for Internet Explorer (2987107)
HIGH	9.3*	9.7	78433	MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)
HIGH	9.3*	9.8	78435	MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)
HIGH	9.3*	9.8	79125	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)
HIGH	9.3*	9.0	79126	MS14-065: Cumulative Security Update for Internet Explorer (3003057)

HIGH	9.3*	5.9	79128	MS14-067: Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)
HIGH	9.3*	6.7	79132	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)
HIGH	9.3*	7.4	79137	MS14-078: Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)
HIGH	7.1*	3.6	79138	MS14-079: Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (3002885)
HIGH	9.3*	8.9	79828	MS14-080: Cumulative Security Update for Internet Explorer (3008923)
HIGH	9.3*	6.7	79833	MS14-084: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3016711)
HIGH	7.2*	8.9	80492	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (3021674)
HIGH	9.3*	8.9	80493	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege (3025421)
HIGH	7.8*	2.7	80496	MS15-007: Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (3014029)
HIGH	9.3*	9.2	81262	MS15-009: Security Update for Internet Explorer (3034682)
HIGH	7.2*	9.5	81263	MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)
HIGH	9.3*	8.9	81733	MS15-018: Cumulative Security Update for Internet Explorer (3032359)
HIGH	9.3*	6.7	81736	MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (3032323)
HIGH	7.2*	8.9	81737	MS15-023: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (3034344)
HIGH	9.3*	8.9	82770	MS15-032: Cumulative Security Update for Internet Explorer (3038314)
HIGH	9.3*	8.9	82772	MS15-035: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)
HIGH	7.2*	5.9	82793	MS15-037: Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (3046269)

HIGH	7.2*	7.4	82774	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)
HIGH	9.3*	8.9	83358	MS15-043: Cumulative Security Update for Internet Explorer (3049563)
HIGH	9.3*	9.2	83440	MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)
HIGH	9.3*	5.5	83356	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3057134)
HIGH	7.2*	9.8	83370	MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191)
HIGH	9.3*	8.9	84053	MS15-056: Cumulative Security Update for Internet Explorer (3058515)
HIGH	9.3*	6.7	84056	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (3059317)
HIGH	7.2*	8.9	84059	MS15-061: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057839)
HIGH	9.3*	9.7	84761	MS15-065: Cumulative Security Update for Internet Explorer (3076321)
HIGH	7.2*	5.9	84744	MS15-072: Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (3069392)
HIGH	7.2*	6.7	84747	MS15-073: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3070102)
HIGH	7.2*	8.9	84748	MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (3067505)
HIGH	7.2*	9.7	84746	MS15-077: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (3077657)
HIGH	9.3*	9.7	84882	MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904)
HIGH	9.3*	8.9	85333	MS15-079: Cumulative Security Update for Internet Explorer (3082442)
HIGH	9.3*	9.2	85348	MS15-080 : Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)

HIGH	9.3*	5.9	85332	MS15-082: Vulnerability in RDP Could Allow Remote Code Execution (3080348)
HIGH	7.2*	7.4	85330	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege (3082487)
HIGH	9.3*	5.9	85322	MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3060716)
HIGH	9.3*	8.9	85540	MS15-093: Security Update for Internet Explorer (3088903)
HIGH	9.3*	9.0	85877	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)
HIGH	9.3*	5.9	85847	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)
HIGH	7.2*	8.9	85844	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657)
HIGH	9.3*	5.9	86366	MS15-109: Security Update for Windows Shell to Address Remote Code Execution (3096443)
HIGH	7.2*	8.9	86373	MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege (3096447)
HIGH	9.3*	8.9	86819	MS15-112: Cumulative Security Update for Internet Explorer (3104517)
HIGH	9.3*	8.9	86822	MS15-115: Security Update for Microsoft Windows to Address Remote Code Execution (3105864)
HIGH	7.2*	8.9	86824	MS15-117: Security Update for NDIS to Address Elevation of Privilege (3101722)
HIGH	7.2*	5.9	86826	MS15-119: Security Update for Winsock to Address Elevation of Privilege (3104521)
HIGH	9.3*	6.7	87257	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)
HIGH	9.3*	6.7	87259	MS15-130: Security Update for Microsoft Uniscribe to Address Remote Code Execution (3108670)
HIGH	7.2*	8.4	87261	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (3116162)
HIGH	7.2*	5.9	87262	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege (3116130)

HIGH	7.2*	8.9	87264	MS15-135: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3119075)
HIGH	7.5*	7.4	59056	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5*	6.7	59529	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.5*	5.9	64992	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5*	8.9	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	5.2	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.8	6.7	89779	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (3143142)
MEDIUM	6.8	6.0	90440	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock)
MEDIUM	6.6	8.9	105184	Windows 7 and Windows Server 2008 R2 December 2017 Security Updates
MEDIUM	6.5	3.6	177229	Apache Struts 2.0.0 < 6.1.2.1 Denial of Service (S2-063)
MEDIUM	6.5	2.5	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	6.5	8.4	132101	Windows Speculative Execution Configuration Check
MEDIUM	6.1	3.8	97741	MS17-016: Security Update for Windows IIS (4013074)
MEDIUM	6.1	3.0	108752	ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities
MEDIUM	5.9	3.6	91014	MS16-065: Security Update for .NET Framework (3156757)
MEDIUM	5.9	3.6	148960	Oracle Java SE 1.7.0_301 / 1.8.0_291 / 1.11.0_11 / 1.16.0_1 Multiple Vulnerabilities (Apr 2021 CPU)
MEDIUM	5.9	6.7	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported

MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.6	3.4	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.5	6.7	94013	MS16-124: Security Update for Windows Registry (3193227)
MEDIUM	5.5	4.4	94640	MS16-139: Security Update for Windows Kernel (3199720)
MEDIUM	5.5	3.6	95770	MS16-153: Security Update for Common Log File System Driver (3207328)
MEDIUM	5.5	6.5	109166	MySQL 5.5.x < 5.5.60 Multiple Vulnerabilities (April 2018 CPU)
MEDIUM	5.3	6.6	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	3.0	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	1.4	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.3	1.4	129387	Apache Struts 2.3.20 < 2.3.29 / 2.5.x < 2.5.13 Denial of Service Vulnerability (S2-041)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	1.4	62940	MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check)
MEDIUM	5.3	1.4	88653	MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (3133043)
MEDIUM	5.3	6.7	94009	MS16-126: Security Update for Microsoft Internet Messaging API (3196067)
MEDIUM	5.3	3.4	10546	Microsoft Windows LAN Manager SNMP LanMan Users Disclosure
MEDIUM	5.3	3.3	141800	Oracle Java SE 1.7.0_281 / 1.8.0_271 / 1.11.0_9 / 1.15.0_1 Multiple Vulnerabilities (Oct 2020 CPU)
MEDIUM	5.3	2.2	145218	Oracle Java SE 1.7.0_291 / 1.8.0_281 / 1.11.0_10 / 1.15.0_2 Information Disclosure (Windows Jan 2021 CPU)
MEDIUM	5.3	2.9	156887	Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (January 2022 CPU)
MEDIUM	5.3	1.4	170161	Oracle Java SE Multiple Vulnerabilities (January 2023 CPU)
MEDIUM	5.3	2.2	166316	Oracle Java SE Multiple Vulnerabilities (October 2022 CPU)

MEDIUM	5.3	2.2	183295	Oracle Java SE Multiple Vulnerabilities (October 2023 CPU)
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	3.6	91609	MS16-082: Security Update for Microsoft Windows Search Component (3165270)
MEDIUM	5.0	4.2	111153	MySQL 5.5.x < 5.5.61 Multiple Vulnerabilities (July 2018 CPU)
MEDIUM	4.9	3.6	138561	MySQL Denial of Service (Jul 2020 CPU)
MEDIUM	4.8	-	87875	MS KB3123479: Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program
MEDIUM	4.7	4.4	141503	Security Updates for Microsoft .NET Framework (October 2020)
MEDIUM	4.3	1.4	102588	Apache Tomcat 8.0.0.RC1 < 8.0.45 Cache Poisoning
MEDIUM	4.3	2.9	97742	MS17-022: Security Update for Microsoft XML Core Services (4010321)
MEDIUM	4.2	-	73992	MS KB2960358: Update for Disabling RC4 in .NET TLS
MEDIUM	4.0	-	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	5.1*	5.9	55802	MS 2562937: Update Rollup for ActiveX Kill Bits (2562937)
MEDIUM	5.1*	5.9	58335	MS 2647518: Update Rollup for ActiveX Kill Bits (2647518)
MEDIUM	6.8*	6.7	66423	MS KB2820197: Update Rollup for ActiveX Kill Bits
MEDIUM	4.0*	-	69334	MS KB2862973: Update for Deprecation of MD5 Hashing Algorithm for Microsoft Root Certificate Program
MEDIUM	6.8*	-	78446	MS KB2977292: Update for Microsoft EAP Implementation that Enables the Use of TLS
MEDIUM	4.3*	-	84763	MS KB3057154: Update to harden use of DES encryption (3057154)
MEDIUM	4.3*	2.7	51909	MS11-009: Vulnerability in JScript and VBScript Scripting Engine Could Allow Information Disclosure (2475792)
MEDIUM	4.3*	6.2	53383	MS11-026: Vulnerability in MHTML Could Allow Information Disclosure (2503658)

MEDIUM	5.1*	9.5	53384	MS11-027: Cumulative Security Update of ActiveX Kill Bits (2508272)
MEDIUM	4.3*	6.2	55117	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure (2544893)
MEDIUM	6.2*	7.4	55572	MS11-056: Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)
MEDIUM	6.4*	3.4	55799	MS11-069: Vulnerability in .NET Framework Could Allow Information Disclosure (2567951)
MEDIUM	6.6*	5.9	58330	MS12-018: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)
MEDIUM	6.9*	5.8	59040	MS12-032: Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338)
MEDIUM	6.9*	5.9	59041	MS12-033: Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege (2690533)
MEDIUM	5.0*	4.0	62905	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure (2733829)
MEDIUM	5.8*	3.7	63230	MS12-083: Vulnerability in IP-HTTPS Component Could Allow Security Feature Bypass (2765809)
MEDIUM	4.9*	3.6	64577	MS13-016: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778344)
MEDIUM	6.9*	6.7	65883	MS13-036: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2829996)
MEDIUM	6.9*	5.9	69836	MS13-077: Vulnerability in Windows Service Control Manager Could Allow Elevation of Privilege (2872339)
MEDIUM	4.9*	4.2	70851	MS13-093: Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)
MEDIUM	6.9*	5.9	73416	MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2922229)
MEDIUM	5.0*	5.1	74423	MS14-031: Vulnerability in TCP Protocol Could Allow Denial of Service (2962478)
MEDIUM	4.3*	2.7	74425	MS14-033: Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2966061)
MEDIUM	4.3*	2.5	77164	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass (2984625)

MEDIUM	5.0*	3.6	77573	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service (2990931)
MEDIUM	5.0*	6.2	79834	MS14-085: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3013126)
MEDIUM	6.1*	3.5	80494	MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (3022777)
MEDIUM	4.3*	3.4	81269	MS15-016: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3029944)
MEDIUM	4.3*	3.5	81738	MS15-024: Vulnerability in PNG Processing Could Allow Information Disclosure (3035132)
MEDIUM	4.3*	5.7	81743	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (3035126)
MEDIUM	4.3*	4.4	81745	MS15-031: Vulnerability in Schannel Could Allow Security Feature Bypass (3046049) (FREAK)
MEDIUM	4.3*	3.4	82775	MS15-039: Vulnerability in XML Core Services Could Allow Security Feature Bypass (3046482)
MEDIUM	6.9*	5.9	83355	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege (3055642)
MEDIUM	5.0*	4.2	83360	MS15-055: Vulnerability in Schannel Could Allow Information Disclosure (3061518)
MEDIUM	6.9*	5.9	84057	MS15-063: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (3063858)
MEDIUM	6.9*	5.9	84745	MS15-074: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (3072630)
MEDIUM	5.0*	4.4	84741	MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege (3072633)
MEDIUM	4.3*	3.6	85335	MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure (3080129)
MEDIUM	4.3*	4.2	85334	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)
MEDIUM	4.0*	3.6	85846	MS15-096: Vulnerability in Active Directory Service Could Allow Denial of Service (3072595)

MEDIUM	4.3*	3.8	86825	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege (3104507)
MEDIUM	5.8*	4.0	86827	MS15-121: Security Update for Schannel to Address Spoofing (3081320)
MEDIUM	4.9*	4.0	86828	MS15-122: Security Update for Kerberos to Address Security Feature Bypass (3105256)
MEDIUM	5.0*	3.6	66842	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	6.8*	5.9	67259	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	4.3*	-	57690	Terminal Services Encryption Level is Medium or Low
LOW	3.7	4.4	106976	Apache Tomcat 8.0.0.RC1 < 8.0.50 Security Constraint Weakness
LOW	3.7	1.4	159462	Apache Tomcat 8.x < 8.5.78 Spring4Shell (CVE-2022-22965) Mitigations
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.4	5.1	78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)
LOW	3.1	4.4	134204	MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (3125869)
LOW	3.1	1.4	97736	MS17-021: Security Update for Windows DirectShow (4010318)
LOW	3.3*	4.4	81267	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass (3004361)
LOW	2.1*	3.6	81742	MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (3030377)
LOW	2.6*	3.4	82777	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure (3048010)
LOW	1.9*	3.6	83363	MS15-054: Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service (3051768)

LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	-	91231	7-Zip Installed
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	73943	Apache Struts Detection
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	92415	Application Compatibility Cache
INFO	N/A	-	34096	BIOS Info (WMI)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	24270	Computer Manufacturer Information (WMI)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	139785	DISM Package List (Windows)
INFO	N/A	-	55472	Device Hostname
INFO	N/A	-	54615	Device Type
INFO	N/A	-	72684	Enumerate Users via WMI
INFO	N/A	-	168980	Enumerate the PATH Variables
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information

INFO	N/A	-	179947	Intel CPUID detection
INFO	N/A	-	92421	Internet Explorer Typed URLs
INFO	N/A	-	148499	Java Detection and Identification (Windows)
INFO	N/A	-	160301	Link-Local Multicast Name Resolution (LLMNR) Service Detection
INFO	N/A	-	69333	MS KB2861855: Updates to Improve Remote Desktop Protocol Network-Level Authentication
INFO	N/A	-	73990	MS KB2871997: Update to Improve Credentials Protection and Management
INFO	N/A	-	83359	MS KB3042058: Update to Default Cipher Suite Priority Order
INFO	N/A	-	85880	MS KB3083992: Update to Improve AppLocker Publisher Rule Enforcement
INFO	N/A	-	92424	MUICache Program Execution History
INFO	N/A	-	71216	ManageEngine Endpoint Central Detection
INFO	N/A	-	148037	ManageEngine Endpoint Central Installed
INFO	N/A	-	51351	Microsoft .NET Framework Detection
INFO	N/A	-	72879	Microsoft Internet Explorer Enhanced Security Configuration Detection
INFO	N/A	-	162560	Microsoft Internet Explorer Installed
INFO	N/A	-	72367	Microsoft Internet Explorer Version Detection
INFO	N/A	-	139615	Microsoft Internet Information Services (IIS) Installed
INFO	N/A	-	140655	Microsoft Internet Information Services (IIS) Sites Enumeration
INFO	N/A	-	57033	Microsoft Patch Bulletin Feasibility Check
INFO	N/A	-	125835	Microsoft Remote Desktop Connection Installed
INFO	N/A	-	56954	Microsoft Revoked Digital Certificates Enumeration
INFO	N/A	-	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	-	10904	Microsoft Windows 'Backup Operators' Group User List
INFO	N/A	-	48763	Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

INFO	N/A	-	10905	Microsoft Windows 'Print Operators' Group User List
INFO	N/A	-	10906	Microsoft Windows 'Replicator' Group User List
INFO	N/A	-	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	-	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
INFO	N/A	-	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	-	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	-	92370	Microsoft Windows ARP Table
INFO	N/A	-	92371	Microsoft Windows DNS Cache
INFO	N/A	-	92364	Microsoft Windows Environment Variables
INFO	N/A	-	92365	Microsoft Windows Hosts File
INFO	N/A	-	187318	Microsoft Windows Installed
INFO	N/A	-	20811	Microsoft Windows Installed Software Enumeration (credentialed check)
INFO	N/A	-	178102	Microsoft Windows Installed Software Version Enumeration
INFO	N/A	-	92366	Microsoft Windows Last Boot Time
INFO	N/A	-	161502	Microsoft Windows Logged On Users
INFO	N/A	-	63080	Microsoft Windows Mounted Devices
INFO	N/A	-	92372	Microsoft Windows NetBIOS over TCP/IP Info
INFO	N/A	-	103871	Microsoft Windows Network Adapters
INFO	N/A	-	92367	Microsoft Windows PowerShell Execution Policy
INFO	N/A	-	151440	Microsoft Windows Print Spooler Service Enabled
INFO	N/A	-	34252	Microsoft Windows Remote Listeners Enumeration (WMI)
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	38689	Microsoft Windows SMB Last Logged On User Disclosure

INFO	N/A	-	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	46742	Microsoft Windows SMB Registry : Enumerate the list of SNMP communities
INFO	N/A	-	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	-	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
INFO	N/A	-	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
INFO	N/A	-	10400	Microsoft Windows SMB Registry Remotely Accessible
INFO	N/A	-	44401	Microsoft Windows SMB Service Config Enumeration
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	10456	Microsoft Windows SMB Service Enumeration
INFO	N/A	-	92373	Microsoft Windows SMB Sessions
INFO	N/A	-	23974	Microsoft Windows SMB Share Hosting Office Files
INFO	N/A	-	10396	Microsoft Windows SMB Shares Access
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	92368	Microsoft Windows Scripting Host Settings
INFO	N/A	-	58452	Microsoft Windows Startup Software Enumeration
INFO	N/A	-	38153	Microsoft Windows Summary of Missing Patches
INFO	N/A	-	92369	Microsoft Windows Time Zone Information

INFO	N/A	-	10719	MySQL Server Detection
INFO	N/A	-	147021	MySQL Server Installed (Windows)
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	34220	Netstat Portscanner (WMI)
INFO	N/A	-	24272	Network Interfaces Enumeration (WMI)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117887	OS Security Patch Assessment Available
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	55930	Oracle GlassFish HTTP Server Version
INFO	N/A	-	55929	Oracle GlassFish Server Administration Console
INFO	N/A	-	65743	Oracle Java JRE Enabled (Internet Explorer)
INFO	N/A	-	71462	Oracle Java JRE Premier Support and Extended Support Version Detection
INFO	N/A	-	65739	Oracle Java JRE Universally Enabled
INFO	N/A	-	33545	Oracle Java Runtime Environment (JRE) Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	66173	RDP Screenshot
INFO	N/A	-	92429	Recycle Bin Files
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	62042	SMB QuickFixEngineering (QFE) Enumeration
INFO	N/A	-	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	-	35296	SNMP Protocol Version Detection

INFO	N/A	-	19763	SNMP Query Installed Software Disclosure
INFO	N/A	-	34022	SNMP Query Routing Information Disclosure
INFO	N/A	-	10550	SNMP Query Running Process List Disclosure
INFO	N/A	-	10800	SNMP Query System Information Disclosure
INFO	N/A	-	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	185519	SNMP Server Detection
INFO	N/A	-	40448	SNMP Supported Protocols Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	35297	SSL Service Requests Client Certificate
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	97086	Server Message Block (SMB) Protocol Version 1 Enabled
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	160486	Server Message Block (SMB) Protocol Version Detection

INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	14773	Service Detection: 3 ASCII Digit Code Responses
INFO	N/A	-	91459	SolarWinds Server & Application Monitor (SAM) Detection
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	117885	Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure
INFO	N/A	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	56468	Time of Last System Startup
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	92434	User Download Folder Files
INFO	N/A	-	92431	User Shell Folders Settings
INFO	N/A	-	92435	UserAssist Execution History
INFO	N/A	-	24269	WMI Available
INFO	N/A	-	44871	WMI Windows Feature Enumeration
INFO	N/A	-	33139	WS-Management Server Detection
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	162174	Windows Always Installed Elevated Status

INFO	N/A	-	48337	Windows ComputerSystemProduct Enumeration (WMI)
INFO	N/A	-	159817	Windows Credential Guard Status
INFO	N/A	-	58181	Windows DNS Server Enumeration
INFO	N/A	-	164690	Windows Disabled Command Prompt Enumeration
INFO	N/A	-	72482	Windows Display Driver Enumeration
INFO	N/A	-	171956	Windows Enumerate Accounts
INFO	N/A	-	159929	Windows LSA Protection Status
INFO	N/A	-	148541	Windows Language Settings Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	155963	Windows Printer Driver Enumeration
INFO	N/A	-	63620	Windows Product Key Retrieval
INFO	N/A	-	160576	Windows Services Registry ACL

* indicates the v3.0 score was not available; the v2.0 score is shown