PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Palo Alto PAN-OS Remote Code Execution Vulnerability - CVE-2017-15944	Palo alto PAN-OS 6.1 before 6.1.19, 7.0 before 7.0.19, 7.1 before 7.1.13 and 8.0 before 8.0.6 allows a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): <= 6.1-6.1.19, 8.0-8.0.5, 7.1-7.1.12, 7.0-7.0.18	Published - December 05, 2017 CVE-2017-15944 CVSS - 9.8 Vendor's Advisory - http://www.securityfocus.com/bid/102079 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15944 https://securityadvisories.paloaltonetworks.com/Home/Detail/102
vBulletin <=5.3.x on Windows Remote Code Execution Vulnerability	vBulletin through 5.3.x on Windows allows remote PHP code execution because a require_once call is reachable with an unauthenticated request that can include directory traversal sequences to specify an arbitrary pathname, and because ../ traversal is blocked but ..\ traversal is not blocked. For example, an attacker can make an invalid HTTP request containing PHP code, and then make an index.php?routestring= request with enough instances of ".." to reach an Apache HTTP Server log file.	Version(s): <= 5.3, 5.3.*	Published - December 14, 2017 CVE-2017-17671 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17671 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-17671 https://blogs.securiteam.com/index.php/archives/3569
Linux Kernel <=4.14.3 Local Privilege Elevation or DoS Vulnerability - CVE-2017-8824	The dccp_disconnect function in net/dccp/proto.c in the Linux kernel through 4.14.3 allows local users to gain privileges or cause a denial of service (use-after-free) via an AF_UNSPEC connect system call during the DCCP_LISTEN state.	Version(s): <= 4.14.3	Published - December 05, 2017 CVE-2017-8824 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8824 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8824 http://lists.openwall.net/netdev/2017/12/04/224
Google Chrome <63.0.3239.84 Remote Out of Bounds Write Vulnerability - CVE-2017-15407	Google Chrome before 63.0.3239.84 is prone to an unspecified vulnerability due to out of bounds write in QUIC.	Version(s): = 6	Published - December 06, 2017 CVE-2017-15407 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15407 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15407 https://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed:+blogspot/dbusP+(Google+Chrome+Releases)
Apple MacOS X <10.13.2 Remote Code Execution Vulnerability in Intel Graphics Driver - CVE-2017-13883	Apple MacOS X before 10.13.2 is prone to a remote code execution vulnerability in Intel Graphics Driver due to a memory corruption issue. A remote attacker could exploit this issue to execute arbitrary code with kernel privileges on the affected system via a crafted application.	Version(s): <= 10.13.2	Published - December 06, 2017 CVE-2017-13883 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13883 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13883 https://support.apple.com/en-il/HT208331
[MS17-DEC] Microsoft Malware Protection Engine Remote Code Execution Vulnerability - CVE-2017-11937	The Microsoft Malware Protection Engine version 1.1.14306.0 and earlier, as used in multiple Microsoft antimalware products, does not properly scan a specially crafted file leading to memory corruption which could allow remote code execution in the security context of the LocalSystem account. Microsoft has released a fix for this issue in the automatically updated malware definitions for the affected products. The products vulnerable to this issue are: Microsoft Exchange Server 2013 and 2016; Microsoft Endpoint Protection; Forefront Endpoint Protection 2010; Forefront Endpoint Protection; Security Essentials; Windows Defender for Windows 10, Windows 10 1511, Windows 10 1607, Windows 10 1703, Windows 10 1709, Windows 7 SP1, Windows Server 2016, Windows RT 8.1, Windows 8.1.	Version(s): <= 1.1.14306.0	Published - December 07, 2017 CVE-2017-11937 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11937 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11937
Mozilla Firefox < 57.0.2, Firefox ESR <52.5.2 Buffer Overflow Vulnerability - CVE-2017-7845	Mozilla Firefox before 57.0.2, and Firefox ESR before 52.5.2 are prone to a buffer overflow vulnerability when drawing and validating elements using Direct 3D 9 with the ANGLE graphics library. The flaw could be exploited to cause a potentially exploitable crash. The issue is relevant for Firefox running on Windows OS only.	Version(s): <= 57.0.2, ESR 52.5.2	Published - December 07, 2017 CVE-2017-7845 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7845 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7845 https://www.mozilla.org/en-US/security/advisories/mfsa2017-29/
MS17-DEC] Microsoft Scripting Engine Memory Corruption Vulnerability - CVE-2017-11890	Microsoft Windows 7 SP1, Windows Server 2008 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allow an attacker to execute arbitrary code in the context of the current user, due to how Internet Explorer handles objects in memory, aka "Scripting Engine Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11886, CVE-2017-11889, CVE-2017-11893, CVE-2017-11894, CVE-2017-11895, CVE-2017-11901, CVE-2017-11903, CVE-2017-11905, CVE-2017-11907, CVE-2017-11908, CVE-2017-11909, CVE-2017-11910, CVE-2017-11911, CVE-2017-11912, CVE-2017-11913, CVE-2017-11914, CVE-2017-11916, CVE-2017-11918, and CVE-2017-11930.	Version(s): <= 9, 10, 11	Published - December 12, 2017 SBV-79193 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11890 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11890
[MS17-DEC] Microsoft Edge Memory Corruption Vulnerability - CVE-2017-11888	Microsoft Edge in Microsoft Windows 10 Gold, 1511, 1607, 1703, 1709, and Windows Server 2016 allows an attacker to execute arbitrary code in the context of the current user, due to how Microsoft Edge handles objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability".	Version(s): <= Windows 10 & Windows Server 2016.	Published - December 12, 2017 CVE-2017-11888 CVSS - 7.5 Vendor's Advisory - http://www.securityfocus.com/bid/102065 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11888 https://qualysguard.qualys.com/fo/common/vuln_info.php?allow_modify=1&id=91416
Keeper Password Manager Remote Code Execution Vulnerability	Keeper Password Manager 11 before 11.4.4 as used in Microsoft Windows 10 allows remote attackers to conduct clickjacking attacks, leading to code execution. This issue exists due to improper handling of untrusted webpages.	Version(s): <= 11-11.4.3	Published - December 15, 2017 SBV-79331 CVSS - 8.8 Vendor's Advisory - https://thehackernews.com/2017/12/windows-10-password-manager.html https://blog.keepersecurity.com/2017/12/15/update-for-keeper-browser-extension-v11-4/