Security Advisory | Volume 2017-172-1

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Windows Kernel-Mode Driver Cursor Elevation of Privilege Vulnerability - CVE-2017-8466	Microsoft Windows 10, Windows 10 1511, Windows 10 1607, Windows 8.1, Windows RT 8.1, Windows Server 2012 R2, and Windows Server 2016 are prone to remote elevation of privileges vulnerability in the kernel-mode driver cursor which enables an attacker to run processes in an elevated context. To exploit the flaw an attacker could entice a user to run a crafted application.	Version(s): <=Microsoft Windows 10, 10-1511, 10-1607, 8.1, Windows RT 8.1, Windows Server 2012 R2, and Windows Server 2016.	Published - June 13, 2017 CVE-2017-8466 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8466 https://portal.msrc.microsoft.com/en-us/security-guidance
Microsoft Windows Uniscribe Remote Code Execution Vulnerability - CVE-2017-8528	Multiple Microsoft products are prone to a remote code execution vulnerability due to Uniscribe mishandling objects in memory. A remote attacker can take control of the affected system by enticing a user to visit a malicious website or to open a specially crafted file.	Version(s): <=Microsoft Office 2007 SP3,2010 SP2, Windows 7 SP1,8.1, Windows Server 2008 SP2, 2008 R2 SP1, Windows Server 2012, and 2012 R2.	Published - June 13, 2017 CVE-2017-8528 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8528
Microsoft Windows Uniscribe Remote Code Execution Vulnerability - CVE-2017-0283	Multiple Microsoft products are prone to a remote code execution vulnerability due to Uniscribe mishandling objects in memory. A remote attacker can take control of the affected system by enticing a user to visit a malicious website or to open a specially crafted file (in certain Office products the Preview Pane is an attack vector for this vulnerability).	Version(s): <=Microsoft Live Meeting 2007 Add-in, Live Meeting 2007 Console, Lync 2010 and 2013, Lync 2010 Attendee, Office 2007 SP 3, Office 2010 SP2, Office Word Viewer, Silverlight 5 Developer Runtime when installed on Windows, Silverlight 5 when installed on Windows, Skype for Business 2016, Windows 10, 10 1511, 10 1607, and 10 1703, Windows 7 SP1, Windows 8.1, Windows Server 2008 SP2, 2008 R2 SP1, Windows Server 2012, 2012 R2, and Windows Server 2016.	Published - June 13, 2017 CVE-2017-0283 CVSS - 9.3 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0283 https://portal.msrc.microsoft.com/en-us/security-guidance
Mozilla Firefox <54 Remote Code Execution Vulnerability - CVE-2017-5471	Mozilla Firefox before 54 is prone to an code execution vulnerability due to a memory corruption issue.	Version(s): <54	Published - June 13,2017 09, 2017 CVE-2017-5471 CVSS - 9.3 Vendor's Advisory - https://www.mozilla.org/en-US/security/advisories/mfsa2017-15/
Microsoft WINS Server Remote Code Execution Vulnerability	Microsoft Windows Server 2008, 2012, 2016 is vulnerable to a remote code execution vulnerability in WINS Server. A remote attacker can execute arbitrary code by forcing the affected system to process malformed WINS packets. Microsoft has stated they would not fix this issue.	Version(s): <=Microsoft Windows Server 2008, 2012, 2016.	Published - June 14, 2017 SBV-72782 CVSS - 10.0 Vendor's Advisory - https://blog.fortinet.com/2017/06/14/wins-server-remote-memory-corruption-vulnerability-in-microsoft-windows-server
Microsoft Malware Protection Engine Remote Code Execution Vulnerability	Microsoft Malware Protection Engine versions 1.1.13804.0 and earlier, as used in multiple Microsoft antimalware products, is prone to a remote code execution vulnerability due to type confusion issues. A remote attacker could exploit this issue via a specially crafted file that would be scanned by the Malware Protection Engine.	Version(s): <= 1.1.13804.0	Published - June 15, 2017 SBV-72781 CVSS - 9.3 Vendor's Advisory - http://www.theregister.co.uk/2017/06/15/microsoft_how_about_sandboxing_windows_defenders_engine/
Linux kernel <=4.11.5 Local Information Disclosure Vulnerability - CVE-2017-1000380	Sound/core/timer.c in the Linux kernel 4.11.5 and earlier is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time.	Version(s): <= 4.11.5	Published - June 17, 2017 CVE-2017-1000380 CVSS - 2.1 Vendor's Advisory - http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ba3021b2c79b2fa9114f92790a99deb27a65b728
Adobe Flash Player Remote Code Execution - CVE-2017-3084	Flash Player Desktop Runtime 25.0.0.171 and earlier on Windows, Macintosh and Linux, Flash Player for Google Chrome 25.0.0.171 and earlier on Windows, Macintosh, Linux and Chrome OS, Flash Player for Microsoft Edge and Internet Explorer 11 25.0.0.171 and earlier on Windows 10 and 8.1 allow attackers to execute arbitrary code due to a use-after-free vulnerability.	Version(s): <= 25.0.0.171	Published - June 13, 2017 CVE-2017-3084 CVSS - 9.3 Vendor's Advisory - https://helpx.adobe.com/security/products/flash-player/apsb17-17.html
Microsoft PowerPoint Remote Code Execution Vulnerability - CVE-2017-8513	Microsoft PowerPoint 2007 and SharePoint Server 2007 x86 are prone to a remote code execution vulnerability. An attacker can exploit this issue to execute arbitrary code on the affected system using a specially crafted file.	Version(s): <= Microsoft PowerPoint 2007 and SharePoint Server 2007 x86 .	Published - June 13, 2017 CVE-2017-8513 CVSS - 9.3 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8513
Microsoft Edge Remote Code Execution Vulnerability due to Scripting Engine Memory Corruption Issue - CVE-2017-8499	The JavaScript Scripting Engine in Microsoft Edge on Windows 10 1703 does not handle objects in memory correctly, making it prone to a remote code execution vulnerability. A remote attacker who could entice the victim to visit a maliciously crafted website could exploit this issue to execute arbitrary code in the context of the current user.	Version(s): <= Microsoft Edge any.	Published - June 13, 2017 CVE-2017-8499 CVSS - 9.3 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8499
Microsoft Windows PDF Library Remote Code Execution Vulnerability - CVE-2017-0291	Microsoft Windows 8, 10, Server 2012, Server 2012 R2 and Server 2016 are prone to a remote code execution vulnerability due to how Windows parses PDF files. A remote attacker can cause arbitrary code to execute in the context of the current user on the affected system by enticing a user to open a specially crafted PDF file.	Version(s): <= Microsoft Windows 8, 10, Server 2012, Server 2012 R2 and Server 2016 .	Published - June 13, 2017 CVE-2017-0291 CVSS - 9.3 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0291 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0291

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Windows Remote Code Execution in Adobe Flash Player - CVE-2017-3076	Memory corruption in Adobe Flash Player 25.0.0.171 and earlier on Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016 allows a remote attacker to execute arbitrary code due to a memory corruption vulnerability.	Version(s): <= Flash Player any	Published - June 13, 2017 CVE-2017-3076 CVSS - 9.3 Vendor's Advisory - https://helpx.adobe.com/security/products/flash-player/apsb17-17.html https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170007