PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Mozilla Firefox and Firefox ESR <52.0.1 Integer Overflow in createImageBitmap()	Mozilla Firefox before 52.0.1, and Firefox ESR before 52.0.1 are prone to a remote code execution vulnerability due to an integer overflow issue in the createImageBitmap function. This issue was reported through the Pwn2Own contest.	Version(s): Mozilla Firefox before 52.0.1, and Firefox ESR before 52.0.1	Published - March 17, 2017 CVE-2017-5428 CVSS - 9.3 Vendor's Advisory Available at https://www.mozilla.org/en-US/security/advisories/mfsa2017-08/
VMWare Multiple Products Remote Code Execution due to an Issue in Apache Struts	VMWare DaaS 6.x and 7.x, VMware vCenter Server 5.5, 6.0 and 6.5, vRealize Operations Manager 6.x and vRealize Hyperic Server 5.x allow a remote attacker to execute arbitrary code due to an issue in Apache Struts.	Version(s): VMWare DaaS 6.x and 7.x, VMware vCenter Server 5.5, 6.0 and 6.5, vRealize Operations Manager 6.x and vRealize Hyperic Server 5.x	Published - March 13, 2017 CVE-2017-5638 CVSS - 10.0 Vendor's Advisory Available at: http://www.vmware.com/security/advisories/VMSA-2017-0004.html
Cisco Multiple Products Remote Code Execution in Apache Struts	Cisco Identity Services Engine (ISE) 1.3(0.876), 1.4(0.253), 2.0(0.306), 2.0(1.130) and 2.2(0.470), Prime Service Catalog Virtual Appliance 12.0, Emergency Responder 12.0(0.98000.50), Unity Connection 11.5(1.999) and 12.0, Unified SIP Proxy 10.0, Unified Communications Manager (CUCM) 12.0(0.99999.2), Unified Contact Center Enterprise 10.0(2), 10.5(3)ES, 11.0(2)ES, 11.5(1)ES, 11.6(1), 9.0(4)ES allow a remote attacker to execute arbitrary code due to an issue in Apache Struts.	Version(s): Cisco Identity Services Engine (ISE) 1.3(0.876), 1.4(0.253), 2.0(0.306), 2.0(1.130) and 2.2(0.470), Prime Service Catalog Virtual Appliance 12.0, Emergency Responder 12.0(0.98000.50), Unity Connection 11.5(1.999) and 12.0, Unified SIP Proxy 10.0, Unified Communications Manager (CUCM) 12.0(0.99999.2), Unified Contact Center Enterprise 10.0(2), 10.5(3)ES, 11.0(2)ES, 11.5(1)ES, 11.6(1), 9.0(4)ES	Published - March 13, 2017 CVE-2017-5638 CVSS - 10.0 Vendor's Advisory Available at : https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170310-struts2
Cisco IOS and IOS XE Remote Code Execution via the Cluster Management Protocol	A vulnerability in the Cisco Cluster Management Protocol (CMP) processing code in Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a reload of an affected device or remotely execute code with elevated privileges. The Cluster Management Protocol utilizes Telnet internally as a signaling and command protocol between cluster members. The vulnerability is due to the combination of two factors: (1) the failure to restrict the use of CMP-specific Telnet options only to internal, local communications between cluster members and instead accept and process such options over any Telnet connection to an affected device; and (2) the incorrect processing of malformed CMP-specific Telnet options. An attacker could exploit this vulnerability by sending malformed CMP-specific Telnet options while establishing a Telnet session with an affected Cisco device configured to accept Telnet connections. An exploit could allow an attacker to execute arbitrary code and obtain full control of the device or cause a reload of the affected device. This affects Catalyst switches, Embedded Service 2020 switches, Enhanced Layer 2 EtherSwitch Service Module, Enhanced Layer 2/3 EtherSwitch Service Module, Gigabit Ethernet Switch Module (CGESM) for HP, IE Industrial Ethernet switches, ME 4924-10GE switch, RF Gateway 10, and SM-X Layer 2/3 EtherSwitch Service Module. Cisco Bug IDs: CSCvd48893.	Version(s): Cisco IOS and Cisco IOS XE Software	Published - March 17, 2017 CVE-2017-3881 CVSS - 10.0 Vendor's Advisory Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp
Microsoft Windows Remote Code Execution in Adobe Flash Player	Adobe Flash Player versions 24.0.0.221 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016, have an exploitable use after free vulnerability related to an interaction between the privacy user interface and the ActionScript 2 Camera object. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.221 and earlier, running on Windows 8.1, Windows Server 2012, Server 2012 R2, Windows 10 and Windows Server 2016	Published - March 14, 2017 CVE-2017-3003 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/MS17-023
Adobe Flash Player <=24.0.0.221 Remote Code Execution due to a Flaw in the Primetime TVSDK	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK API functionality related to timeline interactions. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.221 and earlier	Published - March 14, 2017 CVE-2017- 2998 CVSS - 9.3 Vendor's Advisory Available at: https://helpx.adobe.com/security/products/flash-player/apsb17-07.html
Adobe Flash Player <=24.0.0.221 Remote Code Execution due to a Flaw in the ActionScript2 TextField Object	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability in the ActionScript2 TextField object related to the variable property. Successful exploitation could lead to arbitrary code execution.	Version(s): Adobe Flash Player versions 24.0.0.221 and earlier .	Published - March 14, 2017 CVE-2017-3002 CVSS - 9.3 Vendor's Advisory Available at : https://helpx.adobe.com/security/products/flash-player/apsb17-07.html
Microsoft Exchange Outlook Web Access Elevation of Privilege Vulnerability	Microsoft Exchange Outlook Web Access (OWA) in Exchange Server 2013 Cumulative Update 14, 2013 SP1, and 2016 Cumulative Update 3 does not properly handle web requests, making it prone to a remote privilege escalation vulnerability. A remote attacker who could entice the victim to click a malicious link, or open a malicious file, could exploit this issue to execute arbitrary code.	Version(s):Microsoft Exchange Outlook Web Access (OWA) in Exchange Server 2013 Cumulative Update 14, 2013 SP1, and 2016 Cumulative Update 3	Published - March 14, 2017 CVE-2017-0110 CVSS - 9.3 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms17-015
Microsoft Edge Scripting Engine Memory Corruption Vulnerability	The Scripting Engine in Microsoft Edge does not properly access objects in memory 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 0 in microsoft winsows 10 and microsoft windows server 2016	Published - March 14, 2017 CVE-2017-0151 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms17-007
Microsoft Internet Explorer Memory Corruption Vulnerability	Microsoft Internet Explorer 9, 10, and 11 do not properly access objects in memory making them 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. This issue has been exploited in the wild.	Version(s): Microsoft Internet Explorer 9, 10, and 11 .	Published - March 14, 2017 CVE-2017-0149 CVSS - 9.3 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms17-006

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Windows SMB Remote Code Execution Vulnerability	Microsoft Windows Vista, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Windows 7, 8, 10 and Server 2016 are prone to a remote code execution vulnerability in SMB. A remote attacker can exploit this vulnerability by sending a specially crafted packet to the target system.	Version(s): Microsoft Windows Vista, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, Windows 7, 8, 10 and Server 2016 .	Published - March 14, 2017 CVE-2017-0146 CVSS - 10.0 Vendor's Advisory Available at : https://technet.microsoft.com/en-us/library/security/MS17-010
Microsoft iSNS Server Memory Corruption Vulnerability	Microsoft Windows Server 2008, Server 2008 R2, Server 2012, Server 2012 R2 and Server 2016 are prone to a remote code execution vulnerability in iSNS Server due to a memory corruption issue. A remote attacker can exploit this issue to execute arbitrary code via a specially crafted application to connect to the iSNS Server.	Version(s):Microsoft Windows Server 2008, Server 2008 R2, Server 2012, Server 2012 R2 and Server 2016	Published - March 14, 2017 CVE-2017-0104 CVSS - 9.3 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms17-012
Microsoft Windows Uniscribe Remote Code Execution Vulnerability	Microsoft Windows Vista, 7, Server 2008 and Server 2008 R2 are prone to a remote code execution vulnerability in Uniscribe. A remote attacker can take control of the affected system by enticing a user to visit a malicious website or by providing the user a specially crafted file.	Version(s): Microsoft Windows Vista, 7, Server 2008 and Server 2008 R2	Published - March 14, 2017 CVE-2017-0089 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms17-011
Microsoft Windows GDI Elevation of Privilege Vulnerability	The graphics device interface in Windows 10, Windows 10 version 1511, Windows 10 version 1607, Windows 7 SP1, Windows 8.1, Windows Server 2008 SP2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 and Windows Vista SP2 are prone to an elevation of privileges vulnerability due to inadequate memory handling. A logged on attacker could exploit the flaw by running a crafted application and then could potentially run arbitrary code in kernel mode which could enable program installation, modification of data and creation of new accounts.	Version(s): Windows 10, Windows 10 version 1511, Windows 10 version 1607, Windows 7 SP1, Windows 8.1, Windows Server 2008 SP2, Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 and Windows Vista SP2	Published - March 14, 2017 CVE-2017-0025 CVSS - 9.3 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms17-013