PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
[cisco-sa-20170317-cmp] 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): IOS-XE & IOS	Published - March 17, 2017 CVE-2017-3881 CVSS - 10.0 Vendor's Advisory Available at https://www.mozilla.org/en-US/security/advisories/mfsa2017-08/
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): 52.0.1, 52.0.1 ESR 7, AUS7.3 EUS7.3 TUS7.3	Published - March 17, 2017 CVE-2017-5428 CVSS - 9.3 Vendor's Advisory Available at https://www.mozilla.org/en-US/firefox/organizations/all/
VMWare ESXi, Workstation and Fusion Remote Code Execution Vulnerability - CVE-2017-4902	Buffer overflow in VMWare ESXi 6.0 U1, 6.0 U2, 6.0 U3 before ESXi600-201703001 and 6.5 before ESXi650-201703002, Workstation 12.x before 12.5.5 and Fusion 8.x before 8.5.6 allow a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): 6.0 - 6.0 Express Patch 8, 6.5 - 6.5 Patch1 8.0 - 8.5.5	Published - March 28, 2017 CVE-2017-4902 CVSS - 10.0 Vendor's Advisory https://nvd.nist.gov/vuln/detail/CVE-2017-4902
[cisco-sa-20170405-ame] Cisco Aironet Access Points Series 1830 and 1850 Remote Default Credential Vulnerability	Cisco Aironet Access Point platforms series 1830 and 1850 that are running Cisco Mobility Express Software 8.2.x prior to 8.2.111.0 are pre-installed with a hard-coded SSH administration level password. An attacker with layer 3 connectivity to the affected device could exploit this issue taking full control of the platform.	Version(s):8.2 - 8.2.110.0	Published - April 05, 2017 CVE-2017-3834 CVSS - 10.0 Vendor's Advisory http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3834
Linux Kernel <4.5 Remote Code Execution via UDP Traffic	udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.	Version(s):4.5	Published - April 04, 2017 CVE-2017-10229 CVSS - 10.0 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10229
VMWare ESXi, Workstation and Fusion Remote Code Execution Vulnerability - CVE-2017-4902	Buffer overflow in VMWare ESXi 6.0 U1, 6.0 U2, 6.0 U3 before ESXi600-201703001 and 6.5 before ESXi650-201703002, Workstation 12.x before 12.5.5 and Fusion 8.x before 8.5.6 allow a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): 6.0 - 6.0 Express Patch 8, 6.5 - 6.5 Patch1 8.0 - 8.5.5	Published - April 04, 2017 CVE-2017-4902 CVSS - 10.0 Vendor's Advisory https://nvd.nist.gov/vuln/detail/CVE-2017-4902
[APSB17-01] Adobe Acrobat DC, Reader DC, Acrobat XI and Reader XI Code Execution Vulnerability - CVE-2017-3010	Adobe Acrobat Reader versions 15.020.20042 and earlier, 15.006.30244 and earlier, 11.0.18 and earlier have an exploitable memory corruption vulnerability in the rendering engine. Successful exploitation could lead to arbitrary code execution.	Version(s): 11.0.19, 0 15.023.20053 15.006.30279 15.023.20053	Published - April 04, 2017 CVE-2017-3010 CVSS - 9.3 Vendor's Advisory http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3010
VMWare ESXi, Workstation and Fusion Remote Code Execution Vulnerability - CVE-2017-4904	VMWare ESXi 6.0 U1, 6.0 U2, 6.0 U3 before ESXi600-201703001 and 6.5 before ESXi650-201703002, Workstation 12.x before 12.5.5 and Fusion 8.x before 8.5.6 allow a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): 6.0 - 6.0 Express Patch 8, 6.5 - 6.5 Patch1 8.0 - 8.5.5	Published - April 04, 2017 CVE-2017-4904 CVSS - 10.0 Vendor's Advisory https://nvd.nist.gov/vuln/detail/CVE-2017-4904
VMWare ESXi, Workstation and Fusion Remote Code Execution Vulnerability - CVE-2017-4903	Buffer overflow in VMWare ESXi 6.0 U1, 6.0 U2, 6.0 U3 before ESXi600-201703001 and 6.5 before ESXi650-201703002, Workstation 12.x before 12.5.5 and Fusion 8.x before 8.5.6 allow a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): 6.0 - 6.0 Express Patch 8, 6.5 - 6.5 Patch1 8.0 - 8.5.5	Published - April 04, 2017 CVE-2017-4903 CVSS - 10.0 Vendor's Advisory https://nvd.nist.gov/vuln/detail/CVE-2017-4903