

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Google Chrome Remote Unspecified Vulnerability in Blink	Use-after-free in Blink in Google Chrome, allows remote attackers to have an unspecified impact via unspecified vectors.	Version(s): prior to 52.0.2743.116	Published - August 03,2016 CVE-2016-5142 CVSS - 7.5 Vendor's Advisory Available at : http://rhn.redhat.com/errata/RHSA-2016-1580.html
Cisco Unified Communications Manager IM and Presence Service Remote DoS via SIM Packets	Cisco Unified Communications Manager IM and Presence Service versions are prone to a denial-of-service vulnerability by a remote unauthenticated attacker, via crafted SIM Packets.	Version(s):9.1(1) SU6, 9.1(1) SU6a, 9.1(1) SU7, 10.5(2) SU2, 10.5(2) SU2a, 11.0(1) SU1, and 11.5(1)	Published - August 03,2016 CVE-2016-1466 CVSS - 7.8 Vendor's Advisory Available at: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-ucm
Cisco IOS DoS Vulnerability in Network Time Protocol Packets Processing	Cisco IOS versions are prone to a denial-of-service vulnerability on devices running these versions. The vulnerability is due to improper clearing of invalid Network Time Protocol Packets (NTP) from the interface queue. An unauthenticated remote attacker could exploit this vulnerability and send crafted packets that could cause an interface wedge and a subsequent denial-of-service, if the device is set to enable NTP operations.	Version(s) 15.5(3)S3, 15.6(1)S2, 15.6(2)S1, 15.6(2)T1	Published - August 04,2016 CVE-2016-1478 CVSS - 7.8 Vendor's Advisory Available at: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160804-wedge
VMWare Multiple Products Remote Code Execution due to DLL Hijacking in VMWare Tools	VMWare ESXi Server version 5.0, 5.1, 5.5, 6.0, VMWare Workstation Pro and Player version 12.1.0, VMWare Fusion version 8.1.0 on Mac OS X and VMWare Tools 10.0.5 are prone to a remote code execution vulnerability due to a DLL hijacking issue. The vulnerability exists in the "Shared Folders" (HGFS) VMWare Tools feature running on Microsoft Windows only.	Version(s) : 5.0, 5.1, 5.5, 6.0	Published - August 04,2016 CVE-2016-5330 CVSS - 6.5 The vendor's advisory is available at: https://www.vmware.com/security/advisories/VMSA-2016-0010.html
Palo Alto Networks PAN-OS Local Privilege Escalation Vulnerability in root_reboot	Palo Alto Networks PAN-OS might allow local users to gain privileges by leveraging improper sanitization of the root_reboot local invocation	Version(s) : before 5.0.19, 5.1.x before 5.1.12, 6.0.x before 6.0.14, 6.1.x before 6.1.12, and 7.0.x before 7.0.8	Published - August 02,2016 CVE-2016-1712 CVSS - 7.2 Vendor's Advisory Available at http://www.securitytracker.com/id/1036326
NUUO NVRmini 2, NVRsolo, Crystal, and Netgear ReadyNAS Remote Code Execution Vulnerability	NUUO NVRmini 2 versions 1.7.5 through 3.0.0, NVRsolo versions 1.0.0 through 3.0.0, Crystal versions 2.2.1 through 3.2.0 and Netgear ReadyNAS versions 1.1.1 through 1.4.1 (both x86 and ARM) are prone to a remote code execution vulnerability. A remote unauthenticated attacker could send a crafted request with a NTPServer parameter to the handle_daylightsaving.php page and gain root access to the system.	Version(s) : NUUO NVRmini 2 versions 1.7.5 through 3.0.0, NVRsolo versions 1.0.0 through 3.0.0, Crystal versions 2.2.1 through 3.2.0 and Netgear ReadyNAS versions 1.1.1 through 1.4.1 (both x86 and ARM)	Published - August 04,2016 CVE-2016-5675 CVSS - 10.0 The vendor's advisory is available at: http://www.kb.cert.org/vuls/id/856152
Mozilla Firefox Remote DoS Vulnerability due to Integer Overflow in WebSockets	Mozilla Firefox is prone to a remote denial-of-service vulnerability due to an integer overflow in Web Sockets during data buffering.	Version(s)Prior to 48	Published - August 02,2016 CVE-2016-5261 CVSS - 7.8 Vendor's Advisory Available at https://www.mozilla.org/en-US/security/advisories/mfsa2016-75/
IBM Qradar Remote Code Execution via Unspecified Vector	IBM Security QRadar SIEM allows remote authenticated users to execute arbitrary OS commands as root via unspecified vectors.	Version(s) :7.1.x and 7.2.x before 7.2.7	Published - August 02,2016 CVE-2016-2875 CVSS - 9.0 Vendor's Advisory Available at http://www-01.ibm.com/support/docview.wss?uid=swg21988094
Linux Kernel Local DoS and Information Disclosure due to a Double Fetch Issue drivers/scsi/aacraid/commctrl.c	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel allows local users to cause a denial of service (out-of-bounds access or system crash), and possibly to obtain sensitive information, by changing a certain size value, aka a "double fetch" vulnerability.	Version(s):Prior to 4.5.x	Published - August 03,2016 CVE-2016-6480 CVSS - 5.6 Vendor's Advisory Available : https://www.freedesktop.org/software/harfbuzz/release/
Apache HTTP Server Remote DoS due to a Dependency Cycle Issue in HTTP/2 Implementation	Apache server HTTP/2 implementation is prone to a remote denial-of-service attack. A remote attacker could exploit this issue by sending a crafted request that will induce a dependency cycle, causing the server to enter an infinite loop.	Version(s): 2.4.18	Published - August 03,2016 SBV-62175 CVSS - 7.8 Vendor's Advisory Available at: http://www.theregister.co.uk/2016/08/03/http2_flaws/
IIS Server Remote DoS due to Slow GET Issue in HTTP/2 Implementation	IIS Server implementation of HTTP/2 is prone to a remote denial-of-service vulnerability, via a slow GET attack.	Version(s): 10	Published - August 03,2016 SBV-62170 CVSS - 7.8 Vendor's Advisory Available: http://www.theregister.co.uk/2016/08/03/http2_flaws/