Product	Description	Affected Versions	Other Information
Cisco ASR 1000 Series Router L2TP/IPv4/IPv6/SIP/H.323 Processing Bugs Let Remote Users Cause the Target System to Crash	Multiple vulnerabilities were reported in Cisco ASR 1000 Series Routers. A remote user can cause the target system to crash. A remote user can send a specially crafted packet to cause the target Embedded Services Processor (ESP) to crash and the target device to reload. Layer 2 Tunneling Protocol (L2TP) processing is affected [CVE-2015-6267]. The vendor has assigned bug IDs CSCsw95722 and CSCsw95496 to this vulnerability. IPv4 and IPv6 processing is affected [CVE-2015-6269]. The vendor has assigned bug ID CSCsw69990 to this vulnerability. IPv6 processing is affected [CVE-2015-6270]. The vendor has assigned bug ID CSCsv98555 to this vulnerability. SIP processing on systems configured with Network Address Translation Application Layer Gateway (NAT ALG) are affected [CVE-2015-6271]. The vendor has assigned bug IDs CSCta74749 and CSCta77008 to this vulnerability. H.323 processing on systems configured with NAT ALG or the Firewall feature are affected [CVE-2015-6272].	Version(s):	Published - Aug 28 2015 CVE-2015-6267, CVE-2015-6269, CVE-2015-6270, CVE-2015-6271, CVE-2015-6272 CVSS - 7.8 Vendor's Advisory Available at : http://tools.cisco.com/security/center/viewAlert.x?alertId=40684 http://tools.cisco.com/security/center/viewAlert.x?alertId=40686 http://tools.cisco.com/security/center/viewAlert.x?alertId=40687 http://tools.cisco.com/security/center/viewAlert.x?alertId=40688 http://tools.cisco.com/security/center/viewAlert.x?alertId=40689
Cisco ASR 1000 Series Router UDP Packet Processing Flaw Lets Remote Users Cause the Target Service to Crash	A vulnerability was reported in Cisco ASR 1000 Series Routers. A remote user can cause the target service to crash. A remote user can send a specially crafted UDP packet via IPv4 to the target device to cause the Embedded Services Processor (ESP) processing the packet to crash and the device to reload.	Version(s):	Published - Aug 28 2015 CVE-2015-6268 CVSS - 7.8 The vendor's advisory is available at: http://tools.cisco.com/security/center/viewAlert.x?alertId=40685
Cisco ASR 1000 Series Router IOS XE VFR Bug Lets Remote Users Cause the Target System to Reload	A vulnerability was reported in Cisco ASR 1000 Series Routers. A remote user can cause the target system to reload. A remote user can send specially crafted transit IP packets to the target device to exploit a flaw in the Virtual Fragment Reassembly (VFR) feature and cause the target Embedded Services Processor (ESP) to crash	Version(s)	Published - Aug 28 2015 CVE-2015-6273 CVSS - 7.8 Vendor's Advisory Available at http://tools.cisco.com/security/center/viewAlert.x?alertId=40690
Mozilla Firefox Use-After-Free in nsIPresShell Lets Remote Users Execute Arbitrary Code	A vulnerability was reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create specially crafted content that triggers a resize event where the referenced '<canvas>' element undergoes a style change that deletes the original canvas reference. When the content is loaded by the target user, a use-after-free memory error will occur in nsIPresShell and arbitrary code will be executed on the target user's system.	Version(s):prior to 40.0.3	Published - Aug 27 2015 CVE-2015-4497 CVSS - 10.0 The vendor's advisory is available at: https://www.mozilla.org/en-US/security/advisories/mfsa2015-94/
Mozilla Firefox Lets Remote Users Bypass the Add-on Installation Prompt on the Target System	Multiple vulnerabilities were reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can cause the target application to crash. A remote user can modify files on the target system. A remote user can bypass security controls on the target system. A remote user can obtain potentially sensitive information on the target system. A remote user can conduct cross-site scripting attacks. A remote user can create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target system. Some memory corruption errors may occur [CVE-2015-4473, CVE-2015-4474]. A use-after-free may occur in the processing of audio via the Web A vulnerability was reported in Mozilla Firefox. A remote user can bypass security controls on the target system. A remote user can create specially crafted HTML containing a 'data:' URL that, when loaded by the target user, will bypass the add-on installation permission prompt. As a result, the target user may install an add-on from an untrusted location.	Version(s):prior to 40.0.3	Published - Aug 27 2015 CVE-2015-4498 CVSS - 7.5 Vendor's Advisory Available at https://www.mozilla.org/en-US/security/advisories/mfsa2015-95/
Adobe LiveCycle Data Services XML Processing Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System	A vulnerability was reported in Adobe LiveCycle Data Services. A remote user can obtain potentially sensitive information on the target system. A remote user can send specially crafted XML data to obtain potentially sensitive information from the target system.	Version(s): 4.7, 4.6.2, 4.5, 3.0.x/	Published - Aug 20 2015 CVE-2015-3269 CVSS - 5.0 The vendor's advisory is available at: https://helpx.adobe.com/security/products/livecycleds/apsb15-20.html
Cisco ASR 5000 Series Router OSPF Header Processing Flaw Lets Remote Users Cause the Target OSPF Service to Restart	A vulnerability was reported in Cisco ASR 5000 Series Routers. A remote user can cause the target service to restart. A remote user can send specially crafted Open Shortest Path First (OSPF) protocol packets to the target device to trigger an input validation flaw cause the target OSPF process to restart.	Version(s):ASR 5000 Series; 19.0.M0.60828	Published - Aug 21 2015 CVE-2015-6256 CVSS - 7.0 Vendor's Advisory Available at http://tools.cisco.com/security/center/viewAlert.x?alertId=40585
Cisco Prime Infrastructure Lets Remote Authenticated Users Gain Elevated Privileges	A vulnerability was reported in Cisco Prime Infrastructure. A remote authenticated user can gain elevated privileges. A remote authenticated user can exploit a flaw in the username storage and authentication process to gain elevated privileges on the target system.	Version(s) prior to 1.4(0.45)	Published - Aug 21 2015 CVE-2015-4331 CVSS - 6.5 The Source Code Fix is available at: http://tools.cisco.com/security/center/viewAlert.x?alertId=40553
Microsoft Windows Object Manager/Registry/Filesystem Flaws Let Local Users Gain Elevated Privileges	Several vulnerabilities were reported in Microsoft Windows in the Object Manager, Registry, and Filesystem. A local user can obtain elevated privileges on the target system. A local user can run a specially crafted application to, in conjunction with a separate vulnerability, bypass impersonation level security controls in the Windows Object Manager to gain elevated privileges [CVE-2015-2428]. A local user can create a specially crafted file that, when opened by the target user via an application that has a separate vulnerability, will trigger a flaw in the Windows Registry to bypass the sandbox and gain elevated privileges [CVE-2015-2429].	Version(s):Vista SP2, 2008 SP2, 7 SP1, 2008 R2 SP1, 8, 8.1, 2012, 2012 R2, RT, RT 8.1; and prior service packs	Published - Aug 11 2015 CVE-2015-2428, CVE-2015-2429, CVE-2015-2430 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-090
Openswan Diffie Hellman Parameter Processing Flaw Lets Remote Users Deny Service	A vulnerability was reported in Openswan. A remote user can cause denial of service conditions on the target system. A remote user can send a specially crafted g^x value (of zero) to cause the target pluto IKE daemon to restart.	Version(s):prior to 2.6.45	Published - Aug 29 2015 CVE-2015-3240 CVSS - 9.0 Vendor's Advisory Available at: The vendor has issued a fix (2.6.45).
OpenAFS Multiple Flaws Let Remote Users Spoof Commands and Obtain Potentially Sensitive Information and Local Users Deny Service and Obtain Potentially Sensitive Information	Multiple vulnerabilities were reported in OpenAFS. A local user can cause denial of service conditions on the target system. A local or remote user can obtain potentially sensitive information from system memory. A remote user can spoof commands. The system does not properly clear memory allocated for Volume Location Database (VLDB) entry structures. When VLDB entries are created, a remote user that is monitoring the network can obtain stack data [CVE-2015-3282]. The Basic OverSeer (BOS) server uses clear text for command messages [CVE-2015-3283]. A remote user can spoof commands to modify the server state on systems where restricted mode is not enabled. A local user can supply a specially crafted pioctl command to obtain portions of kernel memory [CVE-2015-3284]. A local user can supply a specially crafted Object Storage Device (OSD) command to trigger a kernel panic [CVE-2015-3285]. A local user can trigger a buffer overflow in the Solaris kernel extension by modifying a grouplist for process authentication groups (PAGs) [CVE-2015-3286]. A local user can supply a specially crafted regular expression to trigger a buffer overflow in the OpenAFS vlserver and cause the service to crash [CVE-2015-3287].	Version: prior to 40.0.3	Published - Aug 12 2015 CVE-2015-3282, CVE-2015-3283, CVE-2015-3284, CVE-2015-3285, CVE-2015-3286, CVE-2015-3287 CVSS - 5.0 Vendor's Advisory Available at http://www.openafs.org/security/OPENAFS-SA-2015-001.txt http://www.openafs.org/security/OPENAFS-SA-2015-002.txt http://www.openafs.org/security/OPENAFS-SA-2015-003.txt http://www.openafs.org/security/OPENAFS-SA-2015-004.txt http://www.openafs.org/security/OPENAFS-SA-2015-005.txt http://www.openafs.org/security/OPENAFS-SA-2015-006.txt
HP Operations Manager for Windows TLS Diffie-Hellman Export Cipher Downgrade Attack Lets Remote Users Decrypt Connections	A vulnerability was reported in HP Operations Manager for Windows. A remote user may be able to decrypt TLS connections in certain situations. A remote user that can conduct a man-in-the-middle attack can cause the target system to downgrade the Diffie-Hellman algorithm to 512-bit export-grade cryptography. The remote user may then be able to decrypt the connection. This vulnerability resides in the TLS protocol and not in the specific TLS implementation, but the vulnerability is exposed because the target system supports export-grade ciphers. This attack is known as the "Logjam" attack.	Versions: 8.10, 8.16, 9.0	Published - August 31 2015 CVE-2015-4000 CVSS - 5.0 Vendor's Advisory Available at https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04773119