Product	Description	Affected Versions	Other Information
Cisco IOS RADIUS Packet Processing Bug Lets Remote Authenticated Users Cause the Target System to Reload	A vulnerability was reported in Cisco IOS. A remote authenticated user can cause the target system to reload. A remote authenticated RADIUS server can return specially crafted RADIUS packets in response to the RADIUS client on the target device to cause the target device to reload. The vendor has assigned bug ID CSCuu59324 to this vulnerability.	Version(s):15.4(3)M2.2	Published - Oct 6 2015 CVE-2015-6263 CVSS - 6.9 Vendor's Advisory Available at : http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151005-ios-radius
Cisco VPN Client Weak 'vpnclient.ini' File Permissions Lets Local Users Gain Elevated Privileges	A vulnerability was reported in Cisco VPN Client. A local user can obtain elevated privileges on the target system. The application installs the 'vpnclient.ini' file with weak access control list permissions. A local user can modify the file to include an arbitrary program name in the Application Launcher section 'Command' field to cause arbitrary code to be executed on the target system with the privileges of the target user.	Version(s):ASR 9000 Series; 5.2.0 (Base)	Published - Oct 7 2015 CVE-2015-7600 CVSS - 7.2 The vendor's advisory is available at: www.cisco.com/
Rails Bugs Let Remote Users Deny Service and Conduct Cross-Site Scripting Attacks	Multiple vulnerabilities were reported in Adobe Flash Player. A remote user can cause arbitrary code to be executed on the target user's Two vulnerabilities were reported in Rails. A remote user can cause denial of service conditions on the target system. A remote user can conduct cross-site scripting attacks. The ActiveSupport::JSON.encode() method does not properly filter HTML code from user-supplied input before displaying the input [CVE-2015-3226]. A remote user can cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Rails software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. Version 4.0.x is not affected. Vector length corruptions may occur [CVE-2015-5568]. The impact was not specified.	Version(s):	Published - September 22, 2015 CVE-2015-3226, CVE-2015-3227 CVSS - 4.3 Vendor's Advisory Available at https://helpx.adobe.com/security/products/flash-player/apsb15-23.html
Adobe Flash Player Multiple Bugs Let Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, and Execute Arbitrary Code	Multiple vulnerabilities were reported in Adobe Flash Player. A remote user can cause arbitrary code to be executed on the target user's 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 create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target user's system. Several use-after-free memory errors can cause code execution [CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, CVE-2015-7644]. A buffer overflow can cause code execution [CVE-2015-7632]. Several memory corruption errors can cause code execution [CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, CVE-2015-7634]. A remote user can bypass the same-origin-policy obtain potentially sensitive information [CVE-2015-7628]	Version(s):19.0.0.185 and prior	Published - Oct 17 2015 CVE-2015-5569, CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7628, CVE-2015-7629, CVE-2015-7630, CVE-2015-7631, CVE-2015-7632, CVE-2015-7633, CVE-2015-7634, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, CVE-2015-7644 CVSS - 5.0 The vendor's advisory is available at: https://helpx.adobe.com/content/help/en/security/products/flash-player/apsb15-25.html
Microsoft Office Flaws Let Remote Users Execute Arbitrary Code and Conduct Cross-Site Scripting Attacks	Two vulnerabilities were reported in Microsoft Office. A remote user can cause arbitrary code to be executed on the target user's 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 trigger a memory corruption error and execute arbitrary code on the target user's system [CVE-2015-2555, CVE-2015-2557, CVE-2015-2558]. The software does not properly filter HTML code from user-supplied input before displaying the input [CVE-2015-6037]. A remote user can cause arbitrary scripting code to be executed by the target user's browser. The code will run in the security context of an arbitrary site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. The following Microsoft Office components are affected: Microsoft Excel 2007, Microsoft Visio 2007 Microsoft Excel 2010, Microsoft Visio 2010 Microsoft Excel 2013, Microsoft Excel 2013 RT Microsoft Excel 2016 Microsoft Excel for Mac 2011 Microsoft Excel 2016 for Mac Microsoft Excel Viewer, Microsoft Office Compatibility Pack Microsoft Office Web Apps Server 2013	Version(s) : 2007, 2010, 2013, 2013 RT, 2016; Office for Mac 2011, Office 2016 for Mac	Published - Oct 13 2015 CVE-2015-2555, CVE-2015-2557, CVE-2015-2558, CVE-2015-6037 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-110
Adobe Acrobat/Reader Multiple Flaws Let Remote Users Obtain Potentially Sensitive Information, Execute Arbitrary Code, and Bypass Security Restrictions	Multiple vulnerabilities were reported in Adobe Acrobat/Reader. A remote user can cause arbitrary code to be executed on the target user's 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 create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target user's system. A buffer overflow may cause information disclosure [CVE-2015-6692]. Several use-after-free memory errors can cause code execution [CVE-2015-6689, CVE-2015-6688, CVE-2015-6690, CVE-2015-7615, CVE-2015-7617, CVE-2015-6687, CVE-2015-6684, CVE-2015-6691, CVE-2015-7621, CVE-2015-5586, CVE-2015-6683]. Several heap buffer overflows can cause code execution [CVE-2015-6696, CVE-2015-6698]. Several memory corruption errors can cause code execution [CVE-2015-6685, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, CVE-2015-6686, CVE-2015-7622]. Several memory leak flaws have unspecified impact [CVE-2015-6699, CVE-2015-6700, CVE-2015-6701, CVE-2015-6702, CVE-2015-6703, CVE-2015-6704, CVE-2015-6697]. Several security bypass flaws can cause information disclosure [CVE-2015-5583, CVE-2015-6705, CVE-2015-6706, CVE-2015-7624].	Version(s) : 10.1.15 and prior, 11.0.12 and prior	Published - Oct 13 2015 CVE-2015-5583, CVE-2015-5586, CVE-2015-6683, CVE-2015-6684, CVE-2015-6685, CVE-2015-6686, CVE-2015-6687, CVE-2015-6688, CVE-2015-6689, CVE-2015-6690, CVE-2015-6691, CVE-2015-6692, CVE-2015-6693, CVE-2015-6694, CVE-2015-6695, CVE-2015-6696, CVE-2015-6697, CVE-2015-6698, CVE-2015-6699, CVE-2015-6700, CVE-2015-6701, CVE-2015-6702, CVE-2015-6703, CVE-2015-6704, CVE-2015-6705, CVE-2015-6706, CVE-2015-6707, CVE-2015-6708, CVE-2015-6709, CVE-2015-6710, CVE-2015-6711, CVE-2015-6712, CVE-2015-6713, CVE-2015-6714, CVE-2015-6715, CVE-2015-6716, CVE-2015-6717, CVE-2015-6718, CVE-2015-6719, CVE-2015-6720, CVE-2015-6721, CVE-2015-6722, CVE-2015-6723, CVE-2015-6724, CVE-2015-6725, CVE-2015-7614, CVE-2015-7615, CVE-2015-7616, CVE-2015-7617, CVE-2015-7618, CVE-2015-7619, CVE-2015-7620, CVE-2015-7621, CVE-2015-7622, CVE-2015-7623, CVE-2015-7624, CVE-2015-7829 CVSS - 9.3 The vendor's advisory is available at: https://helpx.adobe.com/content/help/en/security/products/acrobat/apsb15-24.html
IBM AIX Unspecified Flaw in netstat Lets Local Users Obtain Root Privileges	A vulnerability was reported in IBM AIX. A local user can obtain root privileges on the target system. A local user can exploit a flaw in netstat when the system has a fiber channel adapter to gain root privileges on the target system.	Version(s): 5.3, 6.1, 7.1	Published - Oct 14 2015 CVE-2015-4948 CVSS - 6.9 Vendor's Advisory Available at http://aix.software.ibm.com/aix/efixes/security/netstat_advisory.asc
Windows Kernel Flaws Let Local Users Gain System Privileges and Bypass Windows Trusted Boot Policy	Multiple vulnerabilities were reported in the Windows Kernel. A local user can bypass security restrictions. A local user can gain system privileges on the target system. The system does not properly validate junctions when mount points are being created. A local user that has exploited a separate flaw to execute arbitrary code in a sandboxed application can exploit this flaw to gain the privileges of the target user running the target application [CVE-2015-2553]. A local user can run a specially crafted application to trigger a object memory handling error and execute arbitrary code with system level privileges on the target system [CVE-2015-2549, CVE-2015-2550, CVE-2015-2554]. A local user can bypass the Windows Trusted Boot policy controls on the target system [CVE-2015-2552]. This can be exploited to disable code integrity checks and bypass Trusted Boot integrity validation for BitLocker and Device Encryption security features.	Version(s): Vista SP2, 2008 SP2, 7 SP1, 2008 R2 SP1, 8, 8.1, 2012, 2012 R2, RT, RT 8.1, 10; and prior service packs	Published - October 2 2015 CVE-2015-2549, CVE-2015-2550, CVE-2015-2552, CVE-2015-2553, CVE-2015-2554 CVSS - 7.2 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms15-111
Linux Kernel SCTP Initialization Race Condition Lets Local Users Cause Denial of Service Conditions on the Target System	A vulnerability was reported in the Linux kernel. A local user can cause denial of service conditions on the target system. A local user can create SCTP sockets when the SCTP module is not loaded to trigger a null pointer dereference and cause the target system to crash.	Version(s):	Published - Oct 14 2015 CVE-2015-5283 CVSS - 6.9 Vendor's Advisory Available at http://patchwork.ozlabs.org/patch/515996/
Juniper Junos 'pam.conf' Corruption May Let Remote Users Access the Target System with Root Privileges	A vulnerability was reported in Juniper Junos. A remote user can gain access to the target system in certain cases. On systems where the 'pam.conf' file has been corrupted in a certain way, a remote user can gain root access to the target system without requiring a password. The corruption may occur inadvertently. The remote user cannot corrupt the file without exploiting a separate vulnerability	Version(s):3.4.0 - 3.4.5	Published - Oct 15 2015 CVE-2015-7751 CVSS - 6.9 Vendor's Advisory Available http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10707

Product	Description	Affected Versions	Other Information
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, and Obtain Potentially Sensitive Information	Multiple vulnerabilities were reported in Google Chrome. A remote user can cause arbitrary code to be executed on the target user's 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 create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target user's system. A use-after-free memory error may occur in PDFium [CVE-2015-6756]. A use-after-free memory error may occur in Service Worker [CVE-2015-6757]. A variable cast error may occur in PDFium [CVE-2015-6758]. An information leak may occur in Local Storage [CVE-2015-6759]. An error handling flaw may occur in libANGLE [CVE-2015-6760]. A memory corruption error may occur in FFmpeg [CVE-2015-6761]. A cross-origin bypass may occur in Blink [CVE-2015-6755]. A remote user can bypass cross-origin resource sharing (CORS) restrictions using specially crafted CSS fonts [CVE-2015-6762]. Various additional vulnerabilities exist [CVE-2015-6763].	Version: prior to 46.0.2490.71	Published - Oct 15 2015 CVE-2015-6755, CVE-2015-6756, CVE-2015-6757, CVE-2015-6758, CVE-2015-6759, CVE-2015-6760, CVE-2015-6761, CVE-2015-6762, CVE-2015-6763 CVSS - 5.0 Vendor's Advisory Available at http://googlechromereleases.blogspot.com/2015/10/stable-channel-update.html
Adobe Flash Player Type Confusion Errors Let Remote Users Execute Arbitrary Code	Several vulnerabilities were reported in Adobe Flash Player. 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, when loaded by the target user, will trigger a type confusion error and execute arbitrary code on the target user's system. One of these vulnerabilities is being actively exploited [CVE-2015-7645].	Versions:19.0.0.207 and prior	Published - Oct 16 2015 CVE-2015-7645, CVE-2015-7647, CVE-2015-7648 CVSS - 10.0 Vendor's Advisory Available at https://helpx.adobe.com/security/products/flash-player/apsb15-27.html