Security Advisory
Volume 2015-322-1

Product	Description	Affected Versions	Other Information
Linux Kernel ipc_addid() Race Condition Lets Local Users Gain Elevated Privileges	A vulnerability was reported in the Linux kernel. A local user can obtain elevated privileges on the target system. A local user can invoke an ipc_addid() call to trigger an IPC object state race condition and gain root privileges on the target system.	Version(s):	Published - Nov 6 2015 CVE-2015-7613 CVSS - 6.9 Vendor's Advisory Available at : https://github.com/torvalds/linux/commit/b9a532277938
IBM WebSphere Application Server Lets Remote Users Conduct HTTP Response Splitting Attacks	A vulnerability was reported in IBM WebSphere Application Server. A remote user can conduct HTTP response splitting attacks. A remote user can submit a specially crafted URL to cause the target server to return a split response. A remote user can exploit this to spoof content on the target server, attempt to poison any intermediate web caches, or conduct cross-site scripting attacks.	Version(s):6.1, 7.0, 8.0, 8.5, 8.5.5	Published - Nov 9 2015 CVE-2015-2017 CVSS - 4.3 http://www-01.ibm.com/support/docview.wss?uid=swg21966837
Microsoft Internet Explorer Multiple Bugs Let Remote Users Bypass ASLR, Obtain Potentially Sensitive Information, and Execute Arbitrary Code	Multiple vulnerabilities were reported in Microsoft Internet Explorer. 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 obtain potentially sensitive information on the target system [CVE-2015-6086]. A remote user can bypass address space layout randomization (ASLR) on the target system [CVE-2015-6088]. 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-2015-2427, CVE-2015-6064, CVE-2015-6065, CVE-2015-6066, CVE-2015-6068, CVE-2015-6069, CVE-2015-6070, CVE-2015-6071, CVE-2015-6072, CVE-2015-6073, CVE-2015-6074, CVE-2015-6075, CVE-2015-6076, CVE-2015-6077, CVE-2015-6078, CVE-2015-6079, CVE-2015-6080, CVE-2015-6081, CVE-2015-6082, CVE-2015-6084, CVE-2015-6085, CVE-2015-6087]. A remote user can create specially crafted content that, when loaded by the target user, will trigger a memory corruption error in the JScript and VBScript engines and execute arbitrary code on the target user's system [CVE-2015-6089]. 0011 (via HP's Zero Day Initiative), 0016EECD9D7159A949DAD3BC17E0A939 (via HP's Zero Day Initiative), Anonymous (via HP's Zero Day Initiative), Ashfaq Ansari (via HP's Zero Day Initiative), B6BEB4D5E828CF0CCB47BB24AAC22515 (via HP's Zero Day Initiative), Bo Qu of Palo Alto Networks, Jason Kratzer (via VeriSign iDefense Labs), Simon Zuckerbraun (via HP's Zero Day Initiative), Yuki Chen of Qihoo 360Vulcan Team, and Zheng Huang of the Baidu Scloud XTeam reported these vulnerabilities.	Version(s):7, 8, 9, 10, 11	Published - Nov 10 2015 CVE-2015-2427, CVE-2015-6064, CVE-2015-6065, CVE-2015-6066, CVE-2015-6068, CVE-2015-6069, CVE-2015-6070, CVE-2015-6071, CVE-2015-6072, CVE-2015-6073, CVE-2015-6074, CVE-2015-6075, CVE-2015-6076, CVE-2015-6077, CVE-2015-6078, CVE-2015-6079, CVE-2015-6080, CVE-2015-6081, CVE-2015-6082, CVE-2015-6084, CVE-2015-6085, CVE-2015-6086, CVE-2015-6087, CVE-2015-6088, CVE-2015-6089 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-112
Microsoft Edge Lets Remote Users Bypass ASLR and Execute Arbitrary Code	Several vulnerabilities were reported in Microsoft Edge. 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 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-2015-6064, CVE-2015-6073, CVE-2015-6078]. A remote user can bypass address space layout randomization (ASLR) on the target system [CVE-2015-6088].	Version(s):	Published - Nov 10 2015 CVE-2015-6064, CVE-2015-6073, CVE-2015-6078, CVE-2015-6088 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms15-113
Microsoft Windows Kernel Bugs Let Remote Users Execute Arbitrary Code and Local Users Bypass ASLR Restrictions and Gain Elevated Privileges	Multiple vulnerabilities were reported in the Windows Kernel. A remote user can cause arbitrary code to be executed on the target user's system. A local user can obtain potentially sensitive information. A local user can obtain elevated privileges on the target system. A local user can bypass security restrictions. A local user can obtain potentially sensitive information from the kernel and bypass address space layout randomization (ASLR) controls on the target system [CVE-2015-6102, CVE-2015-6109]. A local user can run a specially crafted program to execute arbitrary code on the target system with kernel-level privileges [CVE-2015-6100, CVE-2015-6101]. A remote or local user can create a specially crafted font file that, when loaded by the target user, will trigger an error in the Adobe Type Manager Library and execute arbitrary code on the target user's system [CVE-2015-6103, CVE-2015-6104]. A local user can run a specially crafted program at a low integrity level to exploit a permission validation flaw and modify files outside of the low integrity level restrictions [CVE-2015-6113].	Version(s) :	Published -Nov 10 2015 CVE-2015-6100, CVE-2015-6101, CVE-2015-6102, CVE-2015-6103, CVE-2015-6104, CVE-2015-6109, CVE-2015-6113 CVSS - 5.0 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-115
Microsoft Lync Lets Remote Users Bypass Sandbox Restrictions on the Target System	A vulnerability was reported in Microsoft Lync. A remote user can bypass security controls on the target system. A remote user can create a specially crafted application that, when loaded by the target user, will trigger a flaw in the instantiation of Office applications via COM controls to gain elevated privileges and bypass of the Internet Explorer sandbox].	Version(s) : 2013	Published - Nov 10 2015 CVE-2015-2503 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms15-116
Microsoft Skype for Business Input Validation Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System	A vulnerability was reported in Microsoft Skype for Business. A remote user can obtain potentially sensitive information on the target system. A remote user can send a message containing specially crafted JavaScript that, when received by the connected target instant message user, will execute the script on the target user's system. The script will run in the context of the Skype for Business application and can open web pages, open other messaging sessions, or load URIs on the target user's system to obtain potentially sensitive information.	Version(s): 2016	Published - Nov 10 2015 CVE-2015-6061 CVSS - 4.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-123
Google Chrome PDF.js Plugin Flaw Lets Remote Users Obtain Potentially Sensitive Information From Other Domains	A vulnerability was reported in Google Chrome. A remote user can obtain potentially sensitive information from other domains. A remote user can exploit a flaw in the PDF viewer (pdf.js) to bypass same-origin policy and access potentially sensitive information from other domains.	Version(s):prior to 46.0.2490.86	Published -Nov 12 2015 CVE-2015-1302 CVSS - 7.5 Vendor's Advisory Available at: http://googlechromereleases.blogspot.com/2015/11/stable-channel-update.html
Cisco IOS Lets Remote Users Bypass Tunnel Interface Access Control Lists	A vulnerability was reported in Cisco IOS. A remote user can bypass access controls on the target system. A remote user connected to a tunnel interface can bypass the access control lists (ACLs) when the physical interface ACLs permit the traffic to pass. The vendor has assigned bug ID CSCur01042 to this vulnerability.	Version(s):prior to 15.2(04)M6, 15.4(03)S	Published - Nov 13 2015 CVE-2015-6366 CVSS - 5.0 Vendor's Advisory Available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151112-ios2
Microsoft Office Bugs Let Remote Users Bypass Sandbox Restrictions, Spoof Web Sites, and Execute Arbitrary Code	Multiple 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 bypass security controls on the target system. A remote user can spoof web sites. A remote user can create a specially crafted application that, when loaded by the target user, will trigger a flaw in the instantiation of Office applications via COM controls to gain elevated privileges and bypass of the Internet Explorer sandbox [CVE-2015-2503]. A remote user can create a specially crafted file that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code on the target system [CVE-2015-6038, CVE-2015-6091, CVE-2015-6092, CVE-2015-6093, CVE-2015-6094]. The code will run with the privileges of the target user. A remote user can spoof web sites and cause the target user's client to be redirected to an arbitrary site [CVE-2015-6123]. Outlook for Mac is affected.	Version(s):2007, 2010, 2013, 2016; Office for Mac 2010, Office 2016 for Mac; Office Web Apps 2010, 2013	Published - Nov 10 2015 CVE-2015-2503, CVE-2015-6038, CVE-2015-6091, CVE-2015-6092, CVE-2015-6093, CVE-2015-6094, CVE-2015-6123 CVSS - 9.3 Vendor's Advisory Available https://technet.microsoft.com/library/security/ms15-116
Cisco ASA Bug in DNS Processing Lets Remote Users Cause the Target System to Crash	A vulnerability was reported in Cisco ASA. A remote user can cause the target system to reload. A remote user can issue a request to the target system and then spoof a specially crafted response to the DNS request packet subsequently issued by the target system to cause the target system to reload. Systems configured in routed or transparent firewall mode and single or multiple context mode are affected. Systems with at least one DNS server IP address configured under a DNS server group are affected.	Version: Cisco ASA 1000V Cloud Firewall Cisco ASA 5500 Series Adaptive Security Appliances Cisco ASA 5500-X Series Next-Generation Firewalls Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers Cisco Adaptive Security Virtual Appliance (ASAv) Cisco FirePOWER 9300 ASA Security Module	Published -Nov 14 2015 CVE-2015-6326 CVSS - 7.8 Vendor's Advisory Available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns2