Product	Description	Affected Versions	Other Information
Microsoft Graphics Component Bugs Let Remote Users Execute Arbitrary Code and Remote Authenticated Users Bypass Security Features and Gain Elevated Privileges	Multiple vulnerabilities were reported in Microsoft Graphics Component. A remote user can cause arbitrary code to be executed on the target user's system. A remote authenticated user can gain elevated privileges. A remote user can bypass security features on the target system. A remote user can create a specially crafted OpenType font file that, when loaded by the target user, will execute arbitrary code on the target system [CVE-2015-2432, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462]. A remote user can create a specially crafted TrueType font file that, when loaded by the target user, will execute arbitrary code on the target system [CVE-2015-2435, CVE-2015-2455, CVE-2015-2456, CVE-2015-2463, CVE-2015-2464]. A remote user can bypass Address Space Layout Randomization (ASLR) security features on the target system [CVE-2015-2433]. A remote authenticated user can bypass security controls to gain elevated privileges on the target system [CVE-2015-2453, CVE-2015-2454, CVE-2015-2465]. A remote user can create a specially crafted Office Graphics Library (OGL) font that, when loaded by the target user, will execute arbitrary code on the target system [CVE-2015-2431].	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 - Aug 11 2015 CVE-2015-2431, CVE-2015-2432, CVE-2015-2433, CVE-2015-2435, CVE-2015-2453, CVE-2015-2454, CVE-2015-2455, CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms15-080
Microsoft .NET Lets Remote Users Gain Elevated Privileges	Several vulnerabilities were reported in Microsoft .NET. A remote user can obtain elevated privileges on the target system. A user can create a specially crafted .NET application that, when run by the target user, will trigger a flaw in the RyuJIT compiler and execute arbitrary code on the target user's system.	Version(s):4.6	Published - Aug 11 2015 CVE-2015-2479, CVE-2015-2480, CVE-2015-2481 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms15-092
Belkin N300 Dual-Band Wi-Fi Range Extender Flaw Lets Remote Authenticated Users Execute Arbitrary Commands on the Target System	Several vulnerabilities were reported in the Belkin N300 Dual-Band Wi-Fi Range Extender. A remote authenticated user can execute arbitrary commands on the target system. A remote authenticated user can send a specially crafted request to execute arbitrary commands on the target system. The formUSBStorage, formWpsStart, formiNICWpsStart, formWlanSetupWPS, formWlanMP, formBSSetSitesurvey, formHwSet, and formConnectionSetting requests are affected.	Version(s)Model N300; firmware prior to 1.04.10	Published - Aug 14 2015 CVE-2015-5536 CVSS - 9.0 Vendor's Advisory Available at http://www.belkin.com/us/support-article?articleNum=4975
Windows Remote Desktop Protocol (RDP) Flaws Let Remote Users Impersonate Client Sessions and Execute Arbitrary Code	Two vulnerabilities were reported in Windows Remote Desktop Protocol (RDP). A remote user can cause arbitrary code to be executed on the target user's system. A remote user can impersonate client sessions. The Remote Desktop Session Host (RDSH) does not properly validate RDSH certificates during authentication. A remote user that can conduct a man-in-the-middle attack can impersonate the client session [CVE-2015-2472]. A remote user can create a specially crafted DLL that, when placed in the target user's working directory and when an RDP file is then opened by the target user, will execute arbitrary code on the target system. The code will run with the privileges of the target user.	Version(s):	Published - Aug 11 2015 CVE-2015-2472, CVE-2015-2473 CVSS - 9.0 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms15-082
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restrictions, and Conduct Cross-Site Scripting Attacks	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 Audio API during MediaStream playback [CVE-2015-4477]. Some integer and buffer overflows may occur when processing MPEG4 video [CVE-2015-4479, CVE-2015-4480, CVE-2015-4493]. Some buffer overflows may occur in the Libvpx library in the processing of WebM video [CVE-2015-4485, CVE-2015-4486]. Some memory errors may occur [CVE-2015-4487, CVE-2015-4488, CVE-2015-4489]. A use-after-free memory error may occur in XMLHttpRequest::Open() in a SharedWorker [CVE-2015-4492]. A remote user can create a specially crafted MP3 audio file that, when loaded by the target user, will read portions of system memory [CVE-2015-4475]. A remote user can redefine some non-configurable properties on JavaScript objects when parsing JSON to bypass same-origin policy [CVE-2015-4478]. On Windows-based systems, a local user can trigger a hardlink race condition to cause the Mozilla Maintenance Service to write its log file to a restricted location with an arbitrary file name. This can be exploited to gain elevated privileges on the target system [CVE-2015-4481]. A remote user can create a MAR file with a specially crafted name that, when opened, will trigger an out-of-bounds write and potentially execute arbitrary code [CVE-2015-4482]. A remote user that can conduct a man-in-the-middle attack and modify a 'feed:' protocol URL to cause the mixed content blocker to be disabled for that page [CVE-2015-4483].	Version(s):prior to 40.0	Published - Aug 11 2015 CVE-2015-4473, CVE-2015-4474, CVE-2015-4475, CVE-2015-4477, CVE-2015-4478, CVE-2015-4479, CVE-2015-4480, CVE-2015-4481, CVE-2015-4482, CVE-2015-4483, CVE-2015-4484, CVE-2015-4485, CVE-2015-4486, CVE-2015-4487, CVE-2015-4488, CVE-2015-4489, CVE-2015-4490, CVE-2015-4491, CVE-2015-4492, CVE-2015-4493 CVSS - 7.5 Vendor's Advisory Available at https://www.mozilla.org/en-US/security/advisories/mfsa2015-79/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-80/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-81/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-82/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-83/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-84/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-85/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-86/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-87/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-88/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-89/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-90/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-91/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-92/
Adobe Flash Player Buffer Overflows and Memory Corruption Errors Let Remote Users 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 create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target system. A type confusion flaw may occur [CVE-2015-5128, CVE-2015-5554, CVE-2015-5555, CVE-2015-5558, CVE-2015-5562]. A use-after-free may occur [CVE-2015-5550, CVE-2015-5551, CVE-2015-3107, CVE-2015-5556, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5557, CVE-2015-5559, CVE-2015-5127, CVE-2015-5563, CVE-2015-5561, CVE-2015-5124, CVE-2015-5564, CVE-2015-5565]. A heap overflow may occur [CVE-2015-5129, CVE-2015-5541]. A buffer overflow may occur [CVE-2015-5131, CVE-2015-5132, CVE-2015-5133]. A memory corruption error may occur [CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, CVE-2015-5553]. An integer overflow may occur [CVE-2015-5560]. A vector length corruption flaw may occur [CVE-2015-5125].	Version(s): 18.0.0.209 and prior	Published - Aug 14 2015 CVE-2015-5125, CVE-2015-5127, CVE-2015-5128, CVE-2015-5129, CVE-2015-5130, CVE-2015-5131, CVE-2015-5132, CVE-2015-5133, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5541, CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5550, CVE-2015-5551, CVE-2015-5552, CVE-2015-5553, CVE-2015-5554, CVE-2015-5555, CVE-2015-5556, CVE-2015-5557, CVE-2015-5558, CVE-2015-5559, CVE-2015-5560, CVE-2015-5561, CVE-2015-5562, CVE-2015-5563, CVE-2015-5564, CVE-2015-5565 CVSS - 10.0 The vendor's advisory is available at: https://helpx.adobe.com/security/products/flash-player/apsb15-19.html
Linux ping Use-After-Free Memory Error Lets Local Users Deny Service and Gain Elevated Privileges	A vulnerability was reported in Linux ping. A local user can cause denial of service conditions on the target system. A local user can obtain elevated privileges on the target system. A local user can make a SOCK_DGRAM socket system call for the IPPROTO_ICMP or IPPROTO_ICMPV6 protocols and then make a connect() system call after a disconnect to trigger a use-after-free in the ping_unhash() function to execute arbitrary code or cause the system to crash.	Version(s): prior to 4.0.3	Published - Aug 6 2015 CVE-2015-4291 CVSS - 7.0 Vendor's Advisory Available at http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.0.3
Linux Kernel Bug in UDF Filesystem Support 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. On systems built with UDF file system support (CONFIG_UDF_FS), a local user can mount a specially crafted UDF file system to trigger an error in the udf_read_inode() function in 'fs/udf/inode.c' and cause the target system to crash.	Version(s) prior to 3.19.1	Published - Aug 6 2015 CVE-2015-4167 CVSS - 6.5 The Source Code Fix is available at: http://www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.19.1
Microsoft Office Multiple Flaws Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information	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 obtain potentially sensitive information on the target system. A remote user can create a specially crafted file that, when loaded by the target user, will execute arbitrary code on the target system [CVE-2015-1642, CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2477]. A remote user that can exploit a separate vulnerability in Internet Explorer running in Enhanced Protection Mode (EPM) can supply a specially crafted command line parameter to Excel, Notepad, PowerPoint, Visio, or Word to view files at a medium integrity level [CVE-2015-2423]. A remote user can create a specially crafted template that, when loaded by the target user, will execute arbitrary code on the target system [CVE-2015-2466]. A remote user can create a specially crafted file that, when loaded by the target user, will trigger an integer underflow and execute arbitrary code on the target system [CVE-2015-2470]	Version(s): 2007 SP3, 2010 SP2; 2013 SP1, 2013 RT SP1; Office for Mac 2011, 2016; Office Compatibility Pack SP3; Word Viewer	Published - Aug 11 2015 CVE-2015-1642, CVE-2015-2423, CVE-2015-2466, CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2470, CVE-2015-2477 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-081
Windows Server Message Block Flaw in Error Logging Lets Remote Authenticated Users Execute Arbitrary Code on the Target System	A vulnerability reported in Windows Server Message Block. A remote authenticated user can execute arbitrary code on the target system. A remote authenticated user can send specially crafted data to trigger a memory corruption flaw in the Server Message Block (SMB) error logging component and execute arbitrary code on the target system.	Version(s): Vista SP2, 2008 SP2	Published - Jul 15 2015 CVE-2015-2474 CVSS - 9.0 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms15-083

Product	Description	Affected Versions	Other Information
Apache Subversion Bugs Let Remote Users Obtain Potentially Sensitive Information	wo vulnerabilities were reported in Apache Subversion. A remote user can obtain potentially sensitive information on the target system. A remote user can supply a specially crafted path value to exploit a flaw in mod_authz_svn to gain access to potentially sensitive information from an ostensibly hidden repository [CVE-2015-3184]. Repositories configured for anonymous read are affected. [Editor's note: This vulnerability has been assigned CVE-2015-3185 for the Apache httpd.] A remote authenticated user can exploit a flaw in svn_repos_trace_node_locations() to view path names that are ostensibly hidden by authz [CVE-2015-3187].	Version: 1.7.0 to 1.7.20, 1.8.0 to 1.8.13	Published - Aug 7 2015 CVE-2015-3184, CVE-2015-3187 CVSS - 7.5 Vendor's Advisory Available at http://subversion.apache.org/security/CVE-2015-3184-advisory.txt http://subversion.apache.org/security/CVE-2015-3187-advisory.txt
Fortinet FortiGate/FortiOS MAC Authentication Flaw Lets Remote Users Modify Data on the Target System	A vulnerability was reported in Fortinet FortiGate/FortiOS. A remote user can modify data on the target system. The SSL-VPN feature only validates the first byte of the TLS message authentication code. As a result, a remote user that can conduct a man-in-the-middle attack can modify encrypted data without detection by the target system.	Version:4.3.12 and prior	Published - Jul 14 2015 CVE-2015-5965 CVSS - 5.0 Vendor's Advisory Available at http://www.fortiguard.com/advisory/FG-IR-15-016/