Product	Description	Affected Versions	Other Information
Microsoft Windows DNS Use-After-Free Memory Error Lets Remote Users Execute Arbitrary Code on the Target System	A vulnerability was reported in Microsoft DNS Server. A remote user can execute arbitrary code on the target system. A remote user can send specially crafted DNS requests to trigger a user-after-free memory error and execute arbitrary code on the target system. The code will run with Local System privileges. Windows servers configured as DNS servers are affected.	Version(s):	Published - Dec 8 2015 CVE-2015-6125 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms15-127
Microsoft Office File Processing Flaws Lets Remote Users Execute Arbitrary C ode	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 create a specially crafted file that, when loaded by the target user via Office, will trigger a memory corruption error and execute arbitrary code on the target system. The code will run with the privileges of the target user. Microsoft Office Compatibility Pack Service Pack 3 and Microsoft Excel Viewer are also affected.	Version(s):2007, 2010, 2013, 2013 RT; Office for Mac 2011, Office 2016 for Mac	Published - Dec 8 2015 CVE-2015-6040, CVE-2015-6118, CVE-2015-6122, CVE-2015-6124, CVE-2015-6177 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms15-131
Microsoft Outlook Email Processing Flaw Lets Remote Users Execute Arbitrary Code	Multiple vulnerabilities were reported in Microsoft Outlook. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create a specially crafted email message that, when loaded by the target user, will execute arbitrary code on the target user's system. Microsoft Office Compatibility Pack SP3 is also affected.	Version(s):2007 SP3, 2010 SP2, 2013, 2013 RT, 2016	Published - Dec 8 2015 CVE-2015-6172 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-131
Microsoft .NET Font File Processing Flaw Lets Remote Users Execute Arbitrary C ode	A vulnerability was reported in Microsoft .NET. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create a specially crafted font file that, when loaded 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):3.0 SP2, 3.5, 3.5.1, 4.0, 4.5, 4.5.1, 4.5.2, 4.6	Published - Dec 8 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/ms15-128
Microsoft Lync Font File Processing Flaws Let Remote Users Execute Arbitrary Code	Several vulnerabilities were reported in Microsoft Lync. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create a specially crafted font file that, when loaded 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) :2010, 2010 Attendee, 2013 SP1	Published -Dec 8 2015 CVE-2015-6106, CVE-2015-6107, CVE-2015-6108 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-128
Microsoft Office Font File Processing Flaws Let Remote Users Execute Arbitrary Code	Several 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 create a specially crafted font file that, when loaded by the target user, will execute arbitrary code on the target system. The code will run with the privileges of the target user. Microsoft Word Viewer is also affected.	Version(s) : 2007 SP3, 2010 SP2	Published - Dec 8 2015 CVE-2015-6106, CVE-2015-6107, CVE-2015-6108 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms15-128
Windows Kernel-Mode Drivers Object Memory Handling Bugs Let Local Users Gain Elevated Privileges	Several vulnerabilities were reported in Windows Kernel-Mode Drivers. A local user can obtain elevated privileges on the target system. A local user can run a specially crafted program to trigger an object handling memory error execute arbitrary commands on the target system with kernel-mode privileges.	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 - Dec 8 2015 CVE-2015-6171, CVE-2015-6173, CVE-2015-6174, CVE-2015-6175 CVSS - 7.5 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-135
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Same-Origin Policy, and Cause Denial of Service Conditions	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 gain elevated privileges. A remote user can bypass cross-origin policy. A remote user can obtain potentially sensitive information on the target system. A remote user can cause denial of service conditions. 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-2015-7201, CVE-2015-7202]. A remote user can create specially crafted JavaScript that, when loaded by the target user, will trigger an error and potentially execute arbitrary code [CVE-2015-7204]. A remote user can exploit a flaw when a redirect is followed and a redirect is used via perfomance.getEntries() to view content from the target user's browser cache [CVE-2015-7207]. A remote server can set an ASCII control character (i.e., vertical tab) in a cookie, which may adversely affect some servers [CVE-2015-7208]. A remote user can exploit a timing bug in WebFTC to trigger a use-after-free memory error in WebRTC and potentially execute arbitrary code [CVE-2015-7210]. A remote user can trigger an integer overflow in mozilla::layers::BufferTextureClient::AllocateForSurface() to potentially execute arbitrary code [CVE-2015-7212]. A remote user can trigger a flaw in the processing of error events in Web Workers to bypass same-origin policy and obtain potentially sensitive information [CVE-2015-7215]. A remote user can create a specially crafted data: URI that, when loaded by the target user, will display a different URI [CVE-2015-7211]. A remote user can send a specially crafted HTTP2 header to trigger an integer underflow and cause denial of service conditions [CVE-2015-7218, CVE-2015-7219]. The browser uses a vulnerable library (Jasper) that is no longer maintained [CVE-2015-7216]. Linux systems running Gnome are affected. A remote user can create a specially crafted TGA file that, when loaded by the target user, will trigger a heap overflow in gdk-pixbuf and cause denial of service conditions [CVE-2015-7217]. A remote user can trigger a buffer overflow in DirectWriteFontInfo::LoadFontFamilyData() to execute arbitrary code on the target user's system [CVE-2015-7203]. A remote user can trigger a buffer overflow in XDRBuffer::grow() to execute arbitrary code on the target user's system [CVE-2015-7220]. A remote user can trigger a buffer overflow in nsDeque::GrowCapacity() to execute arbitrary code on the target user's system [CVE-2015-7221]. A remote user may be able to trigger an integer underflow in RTPReceiverVideo::ParseRtpPacket() and potentially execute arbitrary code or obtain sensitive information [CVE-2015-7205]. A remote user can create a specially crafted MP4 format file that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code [CVE-2015-7213]. A remote user can create a specially crafted MP4 format file that, when loaded by the target user, will trigger an integer underflow in 'covr' and execute arbitrary code [CVE-2015-7222]. A remote user can exploit a flaw in WebExtension APIs to execute code with the privileges of a certain WebExtension to obtain potentially sensitive information or conduct cross-site scripting attacks [CVE-2015-7223]. A remote user can bypass cross-origin restrictions using data: and view-source: Uri schemes and read data from URLs in other domains and from local files [CVE-2015-7214].	Version(s):prior to 43.0	Published -Dec 16 2015 CVE-2015-7201, CVE-2015-7202, CVE-2015-7203, CVE-2015-7204, CVE-2015-7205, CVE-2015-7207, CVE-2015-7208, CVE-2015-7210, CVE-2015-7211, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7215, CVE-2015-7216, CVE-2015-7217, CVE-2015-7218, CVE-2015-7219, CVE-2015-7220, CVE-2015-7221, CVE-2015-7222, CVE-2015-7223 CVSS - 10.0 Vendor's Advisory Available at: https://www.mozilla.org/en-US/security/advisories/mfsa2015-134/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-135/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-136/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-137/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-138/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-139/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-140/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-141/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-142/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-143/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-144/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-145/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-146/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-147/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-148/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-149/
Apple iOS Multiple Flaws Let Remote Users Spoof URLs and Access Files, Apps Gain Elevated Privileges, and Local Users Obtain Potentially Sensitive Information	Multiple vulnerabilities were reported in Apple iOS. A physically local user can obtain potentially sensitive information. An application can gain elevated privileges. A remote user can obtain files on the target system. A remote user can spoof URLs. A remote user with access to the backup system can trigger a path validation flaw in Mobile Backup to access restricted areas of the file system [CVE-2015-7037]. An application can exploit a timing bug in the loading of the trust cache to execute arbitrary code with system privileges [CVE-2015-7051]. An application can exploit an access control flaw to execute arbitrary code with system privileges [CVE-2015-7055]. An application can exploit a path validation flaw in Mobile Replayer to execute arbitrary code with system privileges [CVE-2015-7069, CVE-2015-7070]. An application can exploit a segment validation flaw in dyld to execute arbitrary code with system privileges [CVE-2015-7072, CVE-2015-7079]. A physically local user can exploit a flaw in Siri to read notifications of content that is configured to not be displayed on the lock screen [CVE-2015-7080]. A remote user can create a specially crafted web site that, when loaded by the target user, will spoof the displayed URL [CVE-2015-7093]. An application can trigger a memory corruption flaw in the processing of plists to execute arbitrary code with system privileges [CVE-2015-7113].	Version(s):prior to 9.2	Published - Dec 9 2015 CVE-2015-7037, CVE-2015-7051, CVE-2015-7055, CVE-2015-7069, CVE-2015-7070, CVE-2015-7072, CVE-2015-7079, CVE-2015-7080, CVE-2015-7093, CVE-2015-7113 CVSS - 9.3 Vendor's Advisory Available at https://support.apple.com/en-us/HT205635

Product	Description	Affected Versions	Other Information
Apple OS X Multiple Flaws Let Remote and Local Users Execute Arbitrary Code and Deny Service and Let Local Users Obtain Potentially Sensitive Information and Gain Elevated Privileges	Multiple vulnerabilities were reported in Apple OS X. A remote user can cause arbitrary code to be executed on the target user's system. A remote or local user can cause denial of service conditions on the target system. A local user can obtain potentially sensitive information. A local user or an application can bypass security restrictions. A local user can gain system privileges on the target system. An application can bypass sandbox restrictions and access Contacts after access has been revoked [CVE-2015-7001]. A local user can trigger a memory corruption flaw in the Bluetooth HCI interface to execute arbitrary code with system privileges [CVE-2015-7108]. A remote user in a privileged network position can exploit a URL validation flaw to bypass HSTS [CVE-2015-7094]. A remote user can create a specially crafted web site that, when loaded by the target user, will trigger an uninitialized memory error in zlib and execute arbitrary code [CVE-2015-7054]. A local user can exploit a flaw in the installation of configuration profiles to install a configuration profile without admin privileges [CVE-2015-7062]. A remote user can create a specially crafted font file that, when loaded by the target user, will trigger a memory corruption flaw in CoreGraphics and execute arbitrary code [CVE-2015-7105]. A remote user can create a specially crafted web site that, when loaded by the target user, will trigger a memory corruption flaw in the processing of media files and execute arbitrary code [CVE-2015-7074, CVE-2015-7075]. A local user can load a specially crafted disk image to trigger a memory corruption flaw and execute arbitrary code with kernel privileges [CVE-2015-7110]. A local user can exploit a path validation flaw in the kernel loader to execute arbitrary code with system privileges [CVE-2015-7063]. A sandboxed application can circumvent sandbox restrictions [CVE-2015-7071]. A local user can trigger a use-after-free memory error in the handling of VM objects to execute arbitrary code with system privileges [CVE-2015-7078]. A remote user can create a specially crafted iBooks file that references an external XML entity that, when loaded by the target user, will obtain potentially sensitive user information [CVE-2015-7081]. A remote user can create a specially crafted web image that, when loaded by the target user, will trigger a memory corruption flaw in ImageIO and execute arbitrary code [CVE-2015-7053]. A local user can trigger a null pointer dereference in the Intel Graphics Driver to execute arbitrary code with system privileges [CVE-2015-7076]. A local user can trigger a memory corruption error in the Intel Graphics Driver to execute arbitrary code with system privileges [CVE-2015-7106]. An application can trigger an out-of-bounds memory access error in the Intel Graphics Driver to execute arbitrary code with system privileges [CVE-2015-7077]. An application can trigger a memory corruption flaw in IOAcceleratorFamily to execute arbitrary code with system privileges [CVE-2015-7109]. An application can trigger a memory corruption flaw in IOHIDFamily to execute arbitrary code with system privileges [CVE-2015-7111, CVE-2015-7112]. An application can trigger a null pointer dereference in IOKit to execute arbitrary code with kernel privileges [CVE-2015-7068]. A local user can trigger a null pointer dereference in IOThunderboltFamily to cause denial of service conditions [CVE-2015-7067]. An application cause denial of service conditions [CVE-2015-7040, CVE-2015-7041, CVE-2015-7042, CVE-2015-7043]. A local user can trigger a memory handling flaw to execute arbitrary code with kernel privileges [CVE-2015-7083, CVE-2015-7084]. A local user can trigger a flaw in the parsing of mach messages to execute arbitrary code with kernel privileges [CVE-2015-7047]. A local user can exploit a validation flaw in the loading of kernel extensions to execute arbitrary code with kernel privileges [CVE-2015-7052]. An application can masquerade as the Keychain Server [CVE-2015-7045]. A remote user A remote user can create a specially crafted package that, when loaded by the target user, will trigger a buffer overflow in libc and execute arbitrary code [CVE-2015-7038, CVE-2015-7039]. Some vulnerabilities exist in expat versions prior to 2.1.0 [CVE-2012-1147, CVE-2012-1148]. A remote user can create a specially crafted web site that, when loaded by the target user, will trigger a memory corruption error in OpenGL and execute arbitrary code [CVE-2015-7064, CVE-2015-7065, CVE-2015-7066]. Some vulnerabilities exist in LibreSSL prior to versions 2.1.8 [CVE-2015-5333, CVE-2015-5334]. A remote user can create a specially crafted iWork file that, when loaded by the target user, will execute arbitrary code on the target user's system [CVE-2015-7107]. An application with root privileges can bypass kernel address space layout randomization protections [CVE-2015-7046]. A remote user can trigger a memory corruption error in the handling of SSL handshakes to execute arbitrary code [CVE-2015-7073]. A remote user can create a specially crafted certificate that, when processed by the target system, will trigger a memory corruption error in the ASN.1 decoder to execute arbitrary code [CVE-2015-7059, CVE-2015-7060, CVE-2015-7061]. An application can gain access to the target user's Keychain items [CVE-2015-7058]. An application with root privileges can exploit a flaw in handling union mounts to execute arbitrary code with system privileges [CVE-2015-7044].	Version(s):2007, 2010, 2013, 2016; Office for Mac 2010, Office 2016 for Mac; Office Web Apps 2010, 2013	Published -Dec 9 2015 CVE-2012-1147, CVE-2012-1148, CVE-2015-5333, CVE-2015-5334, CVE-2015-7001, CVE-2015-7038, CVE-2015-7039, CVE-2015-7040, CVE-2015-7041, CVE-2015-7042, CVE-2015-7043, CVE-2015-7044, CVE-2015-7045, CVE-2015-7046, CVE-2015-7047, CVE-2015-7052, CVE-2015-7053, CVE-2015-7054, CVE-2015-7058, CVE-2015-7059, CVE-2015-7060, CVE-2015-7061, CVE-2015-7062, CVE-2015-7063, CVE-2015-7064, CVE-2015-7065, CVE-2015-7066, CVE-2015-7067, CVE-2015-7068, CVE-2015-7071, CVE-2015-7073, CVE-2015-7074, CVE-2015-7075, CVE-2015-7076, CVE-2015-7077, CVE-2015-7078, CVE-2015-7081, CVE-2015-7083, CVE-2015-7084, CVE-2015-7094, CVE-2015-7105, CVE-2015-7106, CVE-2015-7107, CVE-2015-7108, CVE-2015-7109, CVE-2015-7110, CVE-2015-7111, CVE-2015-7112 CVSS - 6.8 Vendor's Advisory Available https://support.apple.com/en-us/HT205637
Adobe Flash Player Multiple Bugs Let Remote Users Bypass Security Controls and Execute Arbitrary Code on the Target System	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 create specially crafted content that, when loaded by the target user, will execute arbitrary code on the target user's system. A heap buffer overflow may occur [CVE-2015-8438, CVE-2015-8446]. A memory corruption error may occur [CVE-2015-8444, CVE-2015-8443, CVE-2015-8417, CVE-2015-8416, CVE-2015-8451, CVE-2015-8455, CVE-2015-8047, CVE-2015-8045, CVE-2015-8060, CVE-2015-8418, CVE-2015-8419, CVE-2015-8408]. A stack overflow may occur [CVE-2015-8407, CVE-2015-8457]. A type confusion error may occur [CVE-2015-8439, CVE-2015-8456]. An integer overflow may occur [CVE-2015-8445]. A buffer overflow may occur [CVE-2015-8415]. A use-after-free memory error may occur [CVE-2015-8050, CVE-2015-8049, CVE-2015-8437, CVE-2015-8450, CVE-2015-8449, CVE-2015-8448, CVE-2015-8436, CVE-2015-8452, CVE-2015-8048, CVE-2015-8413, CVE-2015-8412, CVE-2015-8410, CVE-2015-8411, CVE-2015-8424, CVE-2015-8422, CVE-2015-8420, CVE-2015-8421, CVE-2015-8423, CVE-2015-8425, CVE-2015-8433, CVE-2015-8432, CVE-2015-8431, CVE-2015-8426, CVE-2015-8430, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8434, CVE-2015-8435, CVE-2015-8414, CVE-2015-8059, CVE-2015-8058, CVE-2015-8055, CVE-2015-8057, CVE-2015-8056, CVE-2015-8061, CVE-2015-8067, CVE-2015-8066, CVE-2015-8062, CVE-2015-8068, CVE-2015-8064, CVE-2015-8065, CVE-2015-8063, CVE-2015-8405, CVE-2015-8404, CVE-2015-8402, CVE-2015-8403, CVE-2015-8071, CVE-2015-8401, CVE-2015-8406, CVE-2015-8069, CVE-2015-8070, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8454]. A remote user can bypass security controls on the target system [CVE-2015-8453, CVE-2015-8440, CVE-2015-8409].	Version:	Published -Dec 8 2015 CVE-2015-8045, CVE-2015-8047, CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8060, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8407, CVE-2015-8408, CVE-2015-8409, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8415, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8438, CVE-2015-8439, CVE-2015-8440, CVE-2015-8441, CVE-2015-8442, CVE-2015-8443, CVE-2015-8444, CVE-2015-8445, CVE-2015-8446, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8451, CVE-2015-8452, CVE-2015-8453, CVE-2015-8454, CVE-2015-8455, CVE-2015-8456, CVE-2015-8457 CVSS - 10.0 Vendor's Advisory Available at https://helpx.adobe.com/security/products/flash-player/apsb15-32.htmlasa-dns2