Product	Description	Affected Versions	Other Information
Windows Task Manager Bugs Let Local Users Obtain System Privileges	several vulnerabilities were reported in Windows Task Manager. A local user can gain system privileges on the target system. A local user can run a specially crafted application to bypass impersonation-level security checks and gain elevated privileges on the target system [CVE-2015-2524, CVE-2015-2528]. A local user can run a specially crafted application to exploit a flaw in Task Scheduler in the verification of file system interactions to execute arbitrary code with Local System privileges [CVE-2015-2525].	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 - September 8 2015 CVE-2015-2524, CVE-2015-2525, CVE-2015-2528 CVSS - 7.8 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms15-102
Microsoft Internet Explorer Multiple Bugs Let Remote Users Obtain Potentially Sensitive Information, Gain Elevated Privileges, Delete Files, 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 delete files on the target system. A remote user can gain elevated privileges. 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 trigger a memory corruption error and execute arbitrary code on the target user's system [CVE-2015-2485, CVE-2015-2486, CVE-2015-2487, CVE-2015-2490, CVE-2015-2491, CVE-2015-2492, CVE-2015-2494, CVE-2015-2498, CVE-2015-2499, CVE-2015-2500, CVE-2015-2501, CVE-2015-2541, CVE-2015-2542]. A remote user that can exploit a separate script execution vulnerability can trigger a flaw in the validation of permissions to cause the script to be run with elevated privileges on the target system [CVE-2015-2489]. Internet Explorer 11 is affected. A remote user can exploit a memory object handling flaw to view potentially sensitive application memory contents [CVE-2015-2483]. Internet Explorer 10 and 11 are affected. A remote user that can exploit a separate vulnerability can exploit a file operation permissions flaw to delete arbitrary files on the target system [CVE-2015-2484]. Internet Explorer 10 and 11 are affected. A remote user can create specially crafted content that, when loaded by the target user, will trigger a memory object handling flaw in the VBScript and JScript engines to execute arbitrary code [CVE-2015-2493]. This can also be exploited via an application or Microsoft Office document that contains an embedded ActiveX control marked "safe for initialization". Internet Explorer 8 is affected.	Version(s):7, 8, 9, 10, 11	Published - September 8 2015 CVE-2015-2483, CVE-2015-2484, CVE-2015-2485, CVE-2015-2486, CVE-2015-2487, CVE-2015-2489, CVE-2015-2490, CVE-2015-2491, CVE-2015-2492, CVE-2015-2493, CVE-2015-2494, CVE-2015-2498, CVE-2015-2499, CVE-2015-2500, CVE-2015-2501, CVE-2015-2541, CVE-2015-2542 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms15-094
Microsoft Office Memory Corruption Flaws Lets 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 file that, when loaded by the target user via Microsoft Office, will trigger a memory corruption error and execute arbitrary code on the target user's system [CVE-2015-2520, CVE-2015-2521, CVE-2015-2523]. Microsoft Office Compatibility Pack is also affected. A remote user can create a specially crafted EPS file that, when loaded by the target user via Microsoft Office or pasted into an Office document by the target user, will execute arbitrary code on the target user's system [CVE-2015-2545].	Version(s): 2007 SP3, 2010 SP2; 2013 SP1, 2013 RT SP1; Office for Mac 2011, 2016; Office Compatibility Pack SP3	Published - September 8 2015 CVE-2015-2520, CVE-2015-2521, CVE-2015-2523, CVE-2015-2545 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-099
Microsoft Hyper-V ACL Flaw Lets Local Users Bypass Security Restrictions	A vulnerability was reported in Microsoft Hyper-V. A local user can bypass security restrictions. Hyper-V does not properly apply access control list (ACL) configuration settings. A local user can run a specially crafted application to cause Hyper-V to permit unintended network traffic. Systems with the Hyper-V role enabled are affected.	Version(s):	Published - September 8 2015 CVE-2015-2534 CVSS - 10.0 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms15-105
Microsoft Lync Input Validation Flaws Let Remote Conduct Cross-Site Scripting Attacks	Several vulnerabilities were reported in Microsoft Lync. A remote user can conduct cross-site scripting attacks. The software does not properly filter HTML code from user-supplied input before displaying the input. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Microsoft Lync 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. Information disclosure may occur [CVE-2015-2531, CVE-2015-2532]. Arbitrary code execution may occur [CVE-2015-2536].	Version(s):2013	Published - September 8 2015 CVE-2015-2531, CVE-2015-2532, CVE-2015-2536 CVSS - 6.5 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-104
Linux Kernel SCSI Generic Driver Integer Overflow Lets Local Users Obtain Root Privileges	A vulnerability was reported in the Linux Kernel. A local user can obtain elevated privileges on the target system. A local user with write permissions on a SCSI generic device can trigger an integer overflow in the start_req() function in 'drivers/scsi/sg.c' to execute arbitrary code with kernel level privileges	Version(s):2.6.28 and later	Published - September 9 2015 CVE-2015-5707 CVSS - 5.0 The vendor's advisory is available at: http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=451a2886b6bf90e2fb378f7c46c655450fb96e81 http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=fdc81f45e9f57858da6351836507fbcf1b7583ee
Adobe Shockwave Player Memory Corruption Flaws Let Remote Users Execute Arbitrary Code	Two vulnerabilities were reported in Adobe Shockwave 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 memory corruption error and execute arbitrary code on the target user's system [CVE-2015-6680, CVE-2015-6681].	Version(s):12.1.9.160 and prior	Published - Sep 8 2015 CVE-2015-6680, CVE-2015-6681 CVSS - 10.0 Vendor's Advisory Available at https://helpx.adobe.com/security/products/shockwave/apsb15-22.html
Microsoft Graphics Component Bugs Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges	Multiple vulnerabilities were reported in Microsoft Graphics Components. A remote user can cause arbitrary code to be executed on the target user's system. A local user can gain system privileges on the target system. A remote user can bypass security controls on the target system. A remote user can cause denial of service conditions. A remote user can create a specially crafted 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. A local user can exploit a object handling flaw in the Windows Adobe Type Manager Library to obtain system level privileges on the target system [CVE-2015-2507, CVE-2015-2508, CVE-2015-2512]. A remote user can create a specially crafted OpenType font that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target user's system [CVE-2015-2510]. A remote user can create a specially crafted OpenType font that, when loaded by the target user, will trigger a processing flaw in the Windows Adobe Type Manager Library and cause the target system to crash [CVE-2015-2506]. A local user can run a specially crafted application to trigger a flaw in the Windows kernel-mode driver (Win32k.sys) and execute arbitrary code with kernel-level privileges [CVE-2015-2511, CVE-2015-2517, CVE-2015-2518, CVE-2015-2546]. A local user can run a specially crafted application to trigger a flaw in the Windows kernel-mode driver (Win32k.sys) in the validation of integrity levels and execute arbitrary code with kernel-level privileges [CVE-2015-2527]|. A local user that can exploit a separate vulnerability can determine the base address of a kernel driver to bypass the Address Space Layout Randomization (ASLR) protections [CVE-2015-25	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 21 2015 CVE-2015-2506, CVE-2015-2507, CVE-2015-2508, CVE-2015-2510, CVE-2015-2511, CVE-2015-2512, CVE-2015-2517, CVE-2015-2518, CVE-2015-2527, CVE-2015-2529, CVE-2015-2546 CVSS - 7.5 The Source Code Fix is available at: https://technet.microsoft.com/library/security/ms15-097
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, Obtain Potentially Sensitive Information, and Spoof Content	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 spoof content. 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 may occur in Skia [CVE-2015-1294]. A use-after-free may occur in Printing [CVE-2015-1295]. A use-after-free may occur in Blink [CVE-2015-1299]. A remote user can bypass same-origin restrictions in DOM [CVE-2015-1291, CVE-2015-1293] and ServiceWorker [CVE-2015-1292]. A remote user can spoof characters in omnibox [CVE-2015-1296]. A permission scoping error may occur in WebRequest [CVE-2015-1297]. The impact was not specified. A URL validation flaw may occur in extensions [CVE-2015-1298]. The impact was not specified. An information leak may occur in Blink [CVE-2015-1300]. Some additional vulnerabilities exist in the V8 engine [CVE-2015-6580]. A double free memory error may occur in the opj_j2k_copy_default_tcp_and_create_tcd() function in 'j2k.c' in OpenJPEG [CVE-2015-6581]. A matrix inversion error may occur in the decompose() function in 'platform/transforms/TransformationMatrix.cpp' in Blink [CVE-2015-6582]. The browser does not display a location bar for a hosted app's window after navigation away from the installation site [CVE-2015-6583]. A remote user may be able to spoof content via a specially crafted app.	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 - September 4 2015 CVE-2015-1291, CVE-2015-1292, CVE-2015-1293, CVE-2015-1294, CVE-2015-1295, CVE-2015-1296, CVE-2015-1297, CVE-2015-1298, CVE-2015-1299, CVE-2015-1300, CVE-2015-1301, CVE-2015-6580, CVE-2015-6581, CVE-2015-6582, CVE-2015-6583 CVSS - 7.5 Vendor's Advisory Available at http://googlechromereleases.blogspot.com/2015/09/stable-channel-update.html

Product	Description	Affected Versions	Other Information
PowerDNS Authoritative Server Packet Processing Flaw Lets Remote Users Cause the Target Service to Crash	A vulnerability was reported in PowerDNS Authoritative Server. A remote user can cause the target service to crash. A remote user can send specially crafted DNS packets to trigger a flaw in the DNS parsing code to cause the target service to crash.	Version(s):3.4.0 - 3.4.5	Published - Sep 4 2015 CVE-2015-5230 CVSS - 9.0 Vendor's Advisory Available at: https://doc.powerdns.com/md/security/powerdns-advisory-2015-02/
Microsoft Office Buffer Overflow in Processing OpenType Fonts Lets Remote Users Execute Arbitrary Code	A vulnerability was 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, will trigger a buffer overflow and execute arbitrary code on the target system.	Version: 2007 SP3, 2010 SP2	Published - Sep 8 2015 CVE-2015-2510 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-097
Microsoft SharePoint Foundation Input Validation Flaw Lets Remote Conduct Cross-Site Scripting Attacks	A vulnerability was reported in Microsoft SharePoint Foundation. A remote user can conduct cross-site scripting attacks. The software does not properly filter HTML code from user-supplied input before displaying the input. 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 Microsoft SharePoint 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.	Versions: Foundation 2013	Published - Sep 8 2015 CVE-2015-2522 CVSS - 5.0 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-099
Microsoft Lync Buffer Overflow in Processing OpenType Fonts Lets Remote Users Execute Arbitrary Code	A vulnerability was 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 OpenType font that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target system.	Versions: 2010, 2013 SP1	Published - Sep 8 2015 CVE-2015-2510 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-097