Product	Description	Affected Versions	Other Information
Adobe Acrobat/Reader Multiple Flaws Let Remote Users 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 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 [CVE-2016-0932, CVE-2016-0934, CVE-2016-0937, CVE-2016-0940, CVE-2016-0941]. A double-free memory error may occur [CVE-2016-0935]. A memory corruption error may occur [CVE-2016-0931, CVE-2016-0933, CVE-2016-0936, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, CVE-2016-0946]. A directory search path flaw in the Adobe Download Manager may occur [CVE-2016-0947]. A remote user can bypass security controls on Javascript API execution [CVE-2016-0943].	Version(s):prior 11	Published - Jan 12 2016 CVE-2016-0931, CVE-2016-0932, CVE-2016-0933, CVE-2016-0934, CVE-2016-0935, CVE-2016-0936, CVE-2016-0937, CVE-2016-0938, CVE-2016-0939, CVE-2016-0940, CVE-2016-0941, CVE-2016-0942, CVE-2016-0943, CVE-2016-0944, CVE-2016-0945, CVE-2016-0946, CVE-2016-0947 CVSS - 9.3 Vendor's Advisory Available at : https://helpx.adobe.com/security/products/acrobat/apsb16-02.html
Windows JScript/VBScript Engine Flaw Lets Remote Users Execute Arbitrary Code	A vulnerability was reported in Windows JScript/VBScript Engine. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create specially crafted HTML or an ActiveX control marked "safe for initialization" embedded in an application or Office document that, when loaded by the target user, will trigger a flaw in the VBScript engine and execute arbitrary code on the target user's system. An anonymous contributor (via VeriSign iDefense Labs) reported this vulnerability.	Version(s):	Published - Jan 12 2016 CVE-2016-0002 CVSS - 9.6 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms16-003
DHCP UDP Length Processing Flaw Lets Remote Users Cause the Target Service to Crash	A vulnerability was reported in DHCP. A remote user on the local network can cause the target service to crash. A remote user on the local network can send a packet with a specially crafted IPv4 UDP length value and cause the target service to crash. Clients, relays, and servers are affected.	Version(s) : 4.0.x, 4.1.x, 4.2.x, 4.1-ESV - 4.1-ESV-R12, 4.3.0 - 4.3.3	Published - Jan 13 2016 CVE-2015-8605 CVSS - 6.5 Vendor's Advisory Available at Ubuntu has issued a fix for Ubuntu Linux 12.04 LTS, 14.04 LTS, 15.04, and 15.10.
Microsoft SharePoint Server Bugs Let Remote Users Conduct Cross-Site Scripting Attacks and Execute Arbitrary Code	Several vulnerabilities were reported in Microsoft SharePoint. 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 a specially crafted file that, when loaded by the target user with Office, will execute arbitrary code on the target system [CVE-2016-0022, CVE-2016-0052, CVE-2016-0053]. The software does not properly filter HTML code from user-supplied input before displaying the input [CVE-2016-0039]. 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.	Version(s):2013 SP1, Foundation 2013 SP1	Published - Feb 9 2016 CVE-2016-0022, CVE-2016-0039, CVE-2016-0052, CVE-2016-0053 CVSS - 9.3 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms16-015
IBM Tivoli Monitoring Flaw Lets Remote Authenticated Users Execute Arbitrary Commands on the Target System	A vulnerability was reported in IBM Tivoli Monitoring. A remote authenticated user can execute arbitrary commands on the target system. A remote authenticated user that has view authority permissions for Take Action commands can send specially crafted data to execute commands on the target system.	Version(s) :6.2.2, 6.2.3, 6.3.0	Published -Feb 4 2016 CVE-2015-5003 CVSS - 8.5 Vendor's Advisory Available at http://www-01.ibm.com/support/docview.wss?uid=swg21970361
Kerberos kadmind Server Stub Memory Leaks Let Remote Authenticated Users Consume Excessive Memory Resources	A vulnerability was reported in Kerberos. A remote authenticated user can consume excessive memory on the target system. A remote authenticated user can send specially crafted data to cause krb5_unparse_name() to fail and leak the client and server name. This can be exploited repeatedly to consume all available memory on the target system.	Version(s) :	Published - Feb 2 2016 CVE-2015-8631 CVSS - 6.8 The vendor's advisory is available at: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151125-asr5000
Microsoft .NET Bugs Let Remote Users Obtain Potentially Sensitive Information and Deny Service	Two vulnerabilities were reported in Microsoft .NET. A remote user can consume excessive CPU resources on the target system. A remote user can obtain potentially sensitive information on the target system. A remote user can supply specially crafted Extensible Stylesheet Language Transformations (XSLT) data to cause the target system to recursively compile XSLT transforms and disrupt server availability [CVE-2016-0033]. A remote user can upload a specially crafted icon file to trigger a flaw in Windows Forms (WinForms) in the processing of icon data to view potentially sensitive information on the target system [CVE-2016-0047].	Version(s): 2.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1	Published - Feb 9 2016 CVE-2016-0033, CVE-2016-0047 CVSS - 7.5 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms16-019
Red Hat JBoss XML External Entity Processing Flaw Lets Remote Users Obtain Potentially Sensitive Information	A vulnerability was reported in Red Hat JBoss. A remote user can conduct XML external entity attacks to obtain files on the target system. A remote user can supply specially crafted XML External Entity (XXE) data to the target interface to read files on the target system with the privileges of the target service. The vulnerability resides in the Java Standard Tag Library (JSTL) component. The Apache Software Foundation and David Jorm of IIX reported this vulnerability.	Version(s):8.0.7-142, 8.5.1-021	Published - Feb 4 2016 CVE-2015-0254 CVSS - 7.5 Vendor's Advisory Available at https://rhn.redhat.com/errata/RHSA-2016-0121.html https://rhn.redhat.com/errata/RHSA-2016-0122.html https://rhn.redhat.com/errata/RHSA-2016-0123.html https://rhn.redhat.com/errata/RHSA-2016-0124.html https://rhn.redhat.com/errata/RHSA-2016-0125.html
Microsoft Windows Bugs Let Remote Users Bypass Security, Remote Authenticated Users Execute Arbitrary Code, and Local Users Gain Elevated Privileges	Multiple vulnerabilities were reported in Microsoft Windows. A local user can gain elevated privileges. A remote user can bypass authentication. A remote authenticated user can execute arbitrary code on the target system. A local user can run a specially crafted program to trigger a memory object handling flaw and execute arbitrary code with kernel-level privileges [CVE-2016-0040]. A remote authenticated user can create a specially crafted dynamic link library (DLL) file and then run a specially crafted program on the target system to execute arbitrary code with elevated privileges [CVE-2016-0041, CVE-2016-0042]. A remote authenticated user can send a specially-crafted network packet to the target SyncShareSvc service to trigger an input validation flaw in the Microsoft Sync Framework to cause the target service to stop responding [CVE-2016-0044]. A remote user can connect the target workstation to a specially crafted Kerberos Key Distribution Center (KDC) and bypass a changed password check to decrypt drives protected by BitLocker [CVE-2016-0049].	Version(s):Vista SP2, 2008 SP2, 7 SP1, 2008 R2 SP1, 8.1, 2012, 2012 R2, RT 8.1, 10; and prior service packs	Published - Feb 10 2016 CVE-2016-0040, CVE-2016-0041, CVE-2016-0042, CVE-2016-0044, CVE-2016-0049 CVSS - 7.8 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms16-014
Windows Remote Desktop Unspecified Flaw Lets Remote Authenticated Users Gain Elevated Privileges	vulnerability was reported in Windows Remote Desktop. A remote authenticated user can gain elevated privileges. A remote authenticated user can connect to the target system via the Remote Desktop Protocol (RDP) and run a specially crafted program to gain elevated privileges on the target system.	Version(s)	Published - Feb 9 2016 CVE-2016-0036 CVSS - 8.3 Vendor's Advisory Available https://technet.microsoft.com/library/security/ms16-017
Microsoft Internet Explorer Multiple Bugs Let Remote Users Spoof Web Sites, Obtain Potentially Sensitive Information, Gain Elevated Privileges, 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 gain elevated privileges. A remote user can obtain potentially sensitive information on the target system. A remote user can spoof web sites. A remote user can create a specially crafted DLL file to execute arbitrary code [CVE-2016-0041]. A remote user can create a specially crafted link that, when loaded by the target user, will exploit a flaw in the Hyperlink Object Library and view potentially sensitive information on the target system [CVE-2016-0059]. 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-2016-0060, CVE-2016-0061, CVE-2016-0062, CVE-2016-0063, CVE-2016-0064, CVE-2016-0067, CVE-2016-0071, CVE-2016-0072]. A remote user can send specially crafted HTTP responses to spoof arbitrary web sites [CVE-2016-0077]. A remote user that can exploit a separate vulnerability can bypass cross-domain restrictions to gain elevated privileges on the target system [CVE-2016-0068, CVE-2016-0069].	Version:9, 10, 11	Published -Feb 9 2016 CVE-2016-0041, CVE-2016-0059, CVE-2016-0060, CVE-2016-0061, CVE-2016-0062, CVE-2016-0063, CVE-2016-0064, CVE-2016-0067, CVE-2016-0068, CVE-2016-0069, CVE-2016-0071, CVE-2016-0072, CVE-2016-0077 CVSS - 9.3 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms16-009
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information	Multiple vulnerabilities were reported in Apple iOS. 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 specially crafted HTML that, when loaded by the target user, will trigger a memory corruption error in WebKit and execute arbitrary code on the target system [CVE-2016-1723, CVE-2016-1724, CVE-2016-1725, CVE-2016-1726, CVE-2016-1727]. A remote user can send a specially crafted request to view potentially sensitive information on the target system. A remote user can trigger a flaw in the handling of the "a:visited button" CSS selector to determine if the target user has visited a specified link [CVE-2016-1728]. An anonymous researcher (via Joe Vennix) reported this vulnerability. A remote captive portal may be able to read or write cookies on the target user's system [CVE-2016-1730]. Adi Sharabani and Yair Amit of Skycure reported this vulnerability.	Version(s) : prior to 9.2.1	Published -Jan 20 2016 CVE-2016-1723, CVE-2016-1724, CVE-2016-1725, CVE-2016-1726, CVE-2016-1727, CVE-2016-1728, CVE-2016-1730 CVSS - 9.3 Vendor's Advisory Available https://support.apple.com/en-us/HT205732

Product	Description	Affected Versions	Other Information
Google Chrome Multiple Bugs Let Remote Users Obtain Information, Bypass Security Restrictions, Spoof URLs, and Execute Arbitrary Code	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 URLs. A remote user can bypass same origin controls in Omnibox [CVE-2016-1615]. A remote user can exploit a flaw in Blink to view potentially sensitive information [CVE-2016-1614]. A remote user can spoof URLs [CVE-2016-1616]. An invalid cast may occur in the V8 engine [CVE-2016-1612]. A use-after-free memory error may occur in PDFium [CVE-2016-1613]. A remote user that is monitoring the network can view portions of history with HSTS and CSP [CVE-2016-1617]. The random number generator may generate weak numbers [CVE-2016-1618]. An out-of-bounds memory read may occur in PDFium [CVE-2016-1619]. Other errors may occur in the V8 engine [CVE-2016-2051]. Other errors may occur in HarfBuzz [CVE-2016-2052]. Other errors may occur [CVE-2016-1620].	Version:Prior to 48.0.2564.82	Published -Jan 22 2016 CVE-2016-0041, CVE-2016-0059, CVE-2016-0060, CVE-2016-0061, CVE-2016-0062, CVE-2016-0063, CVE-2016-0064, CVE-2016-0067, CVE-2016-0068, CVE-2016-0069, CVE-2016-0071, CVE-2016-0072, CVE-2016-0077 CVSS - 5.3 Vendor's Advisory Available at http://googlechromereleases.blogspot.com/2016/01/stable-channel-update_20.html
Apple OS X Multiple Memory Corruption Flaws Lets Local Users Obtain Root Privileges	Multiple vulnerabilities were reported in Apple OS X. A local user can obtain root privileges on the target system. A local user can exploit a memory corruption error in AppleGraphicsPowerManagement to execute arbitrary code on the target system with kernel-level privileges [CVE-2016-1716]. A local user can exploit a memory corruption error in Disk Images to execute arbitrary code on the target system with kernel-level privileges [CVE-2016-1717]. A local user can exploit a memory corruption error in IOAcceleratorFamily to execute arbitrary code on the target system with kernel-level privileges [CVE-2016-1718]. A local user can exploit a memory corruption error in IOHIDFamily to execute arbitrary code on the target system with kernel-level privileges [CVE-2016-1719]. A local user can exploit a memory corruption error in IOKit to execute arbitrary code on the target system with kernel-level privileges [CVE-2016-1720]. A local user can exploit a flaw in the kernel to execute arbitrary code on the target system with kernel-level privileges [CVE-2016-1721]. A quarantined application can override OSA script libraries on the target system [CVE-2016-1729]. A local user can exploit a memory corruption error in syslog to execute arbitrary code on the target system with root privileges [CVE-2016-1722]	Version(s) :10.11 to v10.11.2	Published -Jan 20 2016 CVE-2015-7995, CVE-2016-1716, CVE-2016-1717, CVE-2016-1718, CVE-2016-1719, CVE-2016-1720, CVE-2016-1721, CVE-2016-1722, CVE-2016-1729 CVSS - 7.8 https://support.apple.com/en-us/HT205731