Security Advisory

Volume 2016-145-1

CautelaLabs

Product	Description	Affected Versions	Other Information
Symantec Anti Virus Engine Heap Overflow in Processing Files Lets Remote Users Execute Arbitrary Code	A vulnerability was reported in Symantec Anti Virus Engine. A remote user can cause arbitrary code to be executed on the target system. A remote user can create a specially crafted file that, when processed by the target application, will trigger a heap overflow in the processing of PE headers and execute arbitrary code on the target system. The code will run with root privileges on Linux/UNIX/OS X based systems and kernel-level privileges on the target system. Norton and Symantec Enterprise products that ship with the Anti Virus Engine (AVE) are affected.	Version(s): AVE 20151.1.0.32 and prior	Published - May 17 2016 CVE-2016-2208 CVSS - 9.1 Vendor's Advisory Available at : https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160516_00
Cisco Industrial Ethernet Switch Packet Processing Flaw Lets Remote Users Corrupt Queued Data on the Target System	A vulnerability was reported in Cisco Industrial Ethernet Switch. A remote user can corrupt queued data on the target system. A remote user can send specially crafted ICMP packets via IPv4 to the target device to cause the subsequently received packet to be corrupted when enqueued. Control traffic (i.e., ARP) and transit traffic is affected. 4000 Series Switches running IOS 15.2(2)EA, 15.2(2)EA1, 15.2(2)EA2, or 15.2(4)EA are affected. 5000 Series Switches when running IOS 15.2(2)EB or 15.2(2)EB1 are affected.	Version(s):4000 Series, 5000 Series	Published - May 17 2016 CVE-2016-1399 CVSS - 7.5 Vendor's Advisory Available at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160513-ies
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service and Let Remote and Local Users 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 cause the target system to crash. A remote or local user can obtain potentially sensitive information. A remote user can gain elevated privileges. An application can trigger a buffer overflow in the Accessibility function and determine kernel memory layout [CVE-2016-1790]. A remote user in a privileged network position can trigger a URL handling flaw in CFNetwork Proxies to obtain potentially sensitive user information [CVE-2016-1801]. An application can trigger a key processing flaw in CCCrypt to obtain potentially sensitive information [CVE-2016-1802]. An application can trigger a null pointer dereference in CoreCapture to execute arbitrary code with kernel-level privileges [CVE-2016-1803]. A local user can exploit a locking race condition in Disk Images to read kernel memory [CVE-2016-1807]. An application can trigger a memory corruption error in Disk Images to execute arbitrary code with kernel-level privileges [CVE-2016-1808]. An application can trigger a null pointer dereference in IOAcceleratorFamily to cause denial of service condition [CVE-2016-1814]. An application can trigger a null pointer dereference in IOAcceleratorFamily to execute arbitrary code with kernel-level privileges [CVE-2016-1813]. A remote user can create a specially crafted image that, when loaded by the target user, will trigger a null pointer dereference in ImageIO and cause denial of service conditions [CVE-2016-1811]. A local user can trigger a memory corruption error in libc to cause an application to terminate or execute arbitrary code [CVE-2016-1832]. A remote user can create specially crafted XML data that, when loaded by the target user, will trigger a memory corruption error in libxml2 and execute arbitrary code on the target user's system [CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840]. A remote user can create a specially crafted website that, when loaded by the target user, will trigger a memory corruption error in libxslt and execute arbitrary code on the target user's system [CVE-2016-1841]. A remote user in a privileged network position can trigger an error in the processing of shared links in MapKit to obtain potentially sensitive user information [CVE-2016-1842]. A remote user can create specially crafted web content that, when loaded by the target user, will trigger a memory corruption error in OpenGL and execute arbitrary code on the target user's system [CVE-2016-1847]. A physically local user can trigger a flaw in Siri in the processing of Twitter data to access contacts and photos from the lock screen [CVE-2016-1852].	Version(s) : prior to 9.3.2	Published - May 17 2016 CVE Reference: CVE-2016-1790, CVE-2016-1801, CVE-2016-1802, CVE-2016-1803, CVE-2016-1807, CVE-2016-1808, CVE-2016-1811, CVE-2016-1813, CVE-2016-1814, CVE-2016-1817, CVE-2016-1818, CVE-2016-1819, CVE-2016-1823, CVE-2016-1824, CVE-2016-1827, CVE-2016-1828, CVE-2016-1829, CVE-2016-1830, CVE-2016-1831, CVE-2016-1832, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-1841, CVE-2016-1842, CVE-2016-1847, CVE-2016-1852 CVSS - 8.8 Vendor's Advisory Available at: https://support.apple.com/en-us/HT206568
Windows Volume Manager Driver Remote RDP Drive Redirection Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target System	A vulnerability was reported in Windows Volume Manager Driver. A remote user can obtain potentially sensitive information on the target system. A remote user can exploit a session access flaw in the Windows volume manager driver when a USB disk is mounted over Remote Desktop Protocol (RDP) via Microsoft RemoteFX to obtain access to file and directory information on the target mounting user's USB disk.	Version(s) :8.1, RT 8.1, 2012 R2, 10	Published - May 10 2016 CVE-2016-0190 CVSS - 5.5 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms16-067
Microsoft .NET TLS/SSL Implementation Flaw Lets Remote Users Obtain Potentially Sensitive Information	A vulnerability was reported in Microsoft .NET. A remote user can obtain potentially sensitive information on the target system. A remote user that can conduct a man-in-the-middle attack can inject specially crafted non-encrypted data into the security channel and then conduct a man-in-the-middle attack between the target client and target server to obtain potentially sensitive information.	Version(s) : 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1	Published - May 10 2016 CVE-2016-0149 CVSS - 5.9 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms16-065 https://support.microsoft.com/en-us/kb/3155464
Microsoft Windows RPC Memory Free Error Lets Remote Users Gain Elevated Privileges	A vulnerability was reported in Microsoft Windows RPC. A remote user can gain elevated privileges. A remote user can send specially crafted Remote Procedure Call (RPC) requests to trigger a memory free error in the RPC Network Data Representation (NDR) Engine and execute arbitrary code on the target system	Version(s) :Vista SP2, 2008 SP2, 7 SP1, 2008 R2 SP1, 8.1, 2012, 2012 R2, RT 8.1, 10, 10 Version 1511; and prior service packs	Published - May 10 2016 CVE-2016-0178 CVSS - 8.8 The vendor's advisory is available at: https://technet.microsoft.com/library/security/ms16-061
Windows Kernel Symbolic Link Processing Flaw Lets Local Users Gain Elevated Privileges	A vulnerability was reported in the Windows Kernel. A local user can obtain elevated privileges on the target system. The kernel does not properly handle symbolic links. A local user can create specially crafted symbolic links to access privileged registry keys and gain elevated privileges.	Version(s):Vista SP2, 2008 SP2, 7 SP1, 2008 R2 SP1, 8.1, 2012, 2012 R2, RT 8.1, 10, 10 Version 1511; and prior service packs	Published - May 10 2016 CVE-2016-0180 CVSS - 8.2 Vendor's Advisory Available at https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160418_00
Apple iTunes Lets Local Users Gain Elevated Privileges	A vulnerability was reported in Apple iTunes. A local user can obtain elevated privileges on the target system. A local user can place a specially crafted dynamic link library (DLL) on the target system. When the target user subsequently runs the iTunes installer from an untrusted directori, arbitrary code will be executed on the target system.	Version(s) :prior to 12.4	Published - May 17 2016 CVE-2016-1742 CVSS - 7.8 Vendor's Advisory Available at https://support.apple.com/en-us/HT206379

Product	Description	Affected Versions	Other Information
Adobe Acrobat/Reader Multiple Flaws Let Remote Users Execute Arbitrary Code Bypass Security Restrictions, and Obtain Potentially Sensitive Information	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 obtain potentially sensitive information 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-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1075, CVE-2016-1094, CVE-2016-1121, CVE-2016-1122, CVE-2016-4102, CVE-2016-4107]. A heap buffer overflow may occur [CVE-2016-4091, CVE-2016-4092]. A memory corruption error may occur [CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, CVE-2016-4105]. An integer overflow may occur [CVE-2016-1043]. A memory leak may occur [CVE-2016-1079, CVE-2016-1092]. A remote user can obtain potentially sensitive information [CVE-2016-1112]. A remote user can bypass restrictions on Javascript API execution [CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1044, CVE-2016-1062, CVE-2016-1117]. A directory search path error may allow code execution [CVE-2016-1087, CVE-2016-1090, CVE-2016-4106].	Version(s):	Published - May 10 2016 CVE-2016-1037, CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1043, CVE-2016-1044, CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1062, CVE-2016-1063, CVE-2016-1064, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1075, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1079, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1087, CVE-2016-1088, CVE-2016-1090, CVE-2016-1092, CVE-2016-1093, CVE-2016-1094, CVE-2016-1095, CVE-2016-1112, CVE-2016-1116, CVE-2016-1117, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1121, CVE-2016-1122, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4091, CVE-2016-4092, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4102, CVE-2016-4103, CVE-2016-4104, CVE-2016-4105, CVE-2016-4106, CVE-2016-4107 CVSS - 9.8 Vendor's Advisory Available https://www.mozilla.org/en- https://helpx.adobe.com/security/products/acrobat/apsb16-14.html