Security Advisory | Volume 2017-220

CautelaLabs

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability - CVE-2017-6764	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.	Version =1.0	Published - Aug 02, 2017 CVE-2017-6764 CVSS-3.0 Vendor's Advisory - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170802-asa
Microsoft Office Outlook Security Feature Bypass Vulnerability	Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016 as packaged in Microsoft Office allows a security feature bypass vulnerability due to the way that it handles input, aka "Microsoft Office Outlook Security Feature Bypass Vulnerability".	Version(s): =Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook	Published - July 26, 2017 CVE-2017-8571 CVSS - 6.8 Vendor's Advisory - https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-8571
Microsoft Office Outlook Information Disclosure Vulnerability	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory. An attacker who exploited the vulnerability could use the information to compromise the user's computer or data.To exploit the vulnerability, an attacker could craft a special document file and then convince the user to open it. An attacker must know the memory address location where the object was created. The update addresses the vulnerability by changing the way certain functions handle objects in memory.	Version(s):= Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016	Published - July 26, 2017 CVE-2017-8572 CVSS -4.3 http://www.cvedetails.com/cve/cve-2017-8572
Microsoft Office Outlook Memory Corruption Vulnerability	A remote code execution vulnerability exists in the way that Microsoft Outlook parses specially crafted email messages. An attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Exploitation of this vulnerability requires that a user open a specially crafted file with an affected version of Microsoft Outlook. In an email attack scenario, an attacker could exploit the vulnerability by sending a specially crafted file to the user and then convincing the user to open the file.The security update addresses the vulnerability by correcting the way that Microsoft Outlook parses specially crafted email message.	Version : Microsoft Outlook 2007 SP3, Outlook 2010 SP2, Outlook 2013 SP1, Outlook 2013 RT SP1, and Outlook 2016	Published - July 26, 2017 CVE-2017-8572 CVSS -4.3 http://www.cvedetails.com/cve/cve-2017-8572
Mozilla Foundation Security	The Developer Tools feature suffers from a XUL injection vulnerability due to improper sanitization of the web page source code. In the worst case, this could allow arbitrary code execution when opening a malicious page with the style editor tool.	Version : Red Hat Enterprise Linux 7 firefox Affected Red Hat Enterprise Linux 6	Published - Aug 08, 2017 CVE-2017-7798 CVSS-8.8 Vendor's Advisory - https://access.redhat.com/security/cve/cve-2017-7798 https://www.mozilla.org/en-US/security/advisories/mfsa2017-18/#CVE-2017-7798.