Security Advisory | Volume 2017-108-1

CautelaLabs

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Edge Remote Code Execution Vulnerability due to Memory Corruption	Edge on Microsoft Windows 10 1607 is prone to a code execution vulnerability. An attacker can exploit this issue by enticing a user to visit a malicious webpage.	Version(s): Windows 10 Version 1607 for 32-bit Systems and x64-based Systems	Published - April 11, 2017 CVE-2017-0200 CVSS - 9.3 Vendor's Advisory Available at https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0200
Microsoft LDAP Elevation of Privilege Vulnerability	Microsoft Windows 10, Windows 10 1511, Windows 1607, Windows 1703, Windows 7, Windows 8.1, Windows Server 2008 and 2008 R2, Windows Server 2012 and 2012 R2, Windows Server 2016 and Windows Vista allow a remote attacker to gain privileges via a crafted application. This issue exists due to a flaw in the processing of LDAP request buffer lengths.	Version(s): Microsoft Windows 10, Windows 10 1511, Windows 1607, Windows 1703, Windows 7, Windows 8.1, Windows Server 2008 and 2008 R2, Windows Server 2012 and 2012 R2, Windows Server 2016 and Windows Vista	Published - April 11, 2017 CVE-2017-0166 CVSS - 9.3 Vendor's Advisory Available at https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0166
Microsoft Hyper-V Remote Code Execution Vulnerability	Microsoft Windows 10 1511, 1607 and 1703, and Windows Server 2016 are prone to remote code execution in Hyper-V. an attacker can exploit this vulnerability using a crafted application which could allow him to execute arbitrary code on the affected system.	Version(s): Microsoft Windows 10 1511, 1607 and 1703, and Windows Server 2016	Published - April 11, 2017 CVE-2017-0181 CVSS - 9.3 Vendor's Advisory https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0181
Microsoft Office/WordPad Remote Code Execution Vulnerability	Microsoft Office 2007 SP3, 2010 SP2 x64, 2010 SP2 x86, 2013 SP1 x64, 2013 SP1 x86, 2016 x64, 2016 x86, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2 and Windows Server 2012 are prone to a remote code execution vulnerability via a specially crafted Word Document (RTF files with ".doc" extension name).	Version(s):Microsoft Office 2007 SP3, 2010 SP2 x64, 2010 SP2 x86, 2013 SP1 x64, 2013 SP1 x86, 2016 x64, 2016 x86, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2 and Windows Server 2012	Published - April 10, 2017 CVE-2017-0199 CVSS - 9.3 Vendor's Advisory https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0199
Microsoft Remote Code Execution Vulnerability due to Scripting Engine Memory Corruption Issue	Microsoft Edge on Windows 10, Windows 10 1511, Windows 10 1607 and Windows 10 1703 is prone to a remote code execution vulnerability due to a memory corruption issue during rendering performed by the scripting engine. A remote attacker could either entice the victim to visit a maliciously crafted website or could embed a malicious ActiveX control in a Microsoft application or Office document that uses the scripting engine. Consequently the attacker could leverage the resulting memory corruption to execute arbitrary code with the privileges of the current user.	Version(s):Microsoft Edge on Windows 10, Windows 10 1511, Windows 10 1607 and Windows 10 1703	Published - April 11, 2017 CVE-2017-0093 CVSS - 9.3 Vendor's Advisory - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0093
Microsoft Windows Remote Code Execution in Adobe Flash Player	Use-after-free in Adobe Flash Player 25.0.0.127 and earlier on Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016 allows a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): Adobe Flash Player 25.0.0.127 and earlier on Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016	Published - April 11, 2017 CVE-2017-3058 CVSS - 9.3 Vendor's Advisory http://www.securityfocus.com/bid/97551
Adobe Flash Player <=25.0.0.127 Remote Code Execution Vulnerability	Use-after-free in Adobe Flash Player 25.0.0.127 and earlier allows a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): Adobe Flash Player 25.0.0.127 and earlier	Published - April 11, 2017 CVE-2017-3063 CVSS - 9.3 Vendor's Advisory https://helpx.adobe.com/security/products/flash-player/apsb17-10.html
Microsoft Windows Remote Code Execution in Adobe Flash Player	Memory corruption in Adobe Flash Player 25.0.0.127 and earlier on Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016 allows a remote attacker to execute arbitrary code via unspecified vectors.	Version(s): Adobe Flash Player 25.0.0.127 and earlier on Microsoft Windows 8.1, Server 2012, Server 2012 R2, Windows 10, and Server 2016	Published - April 11, 2017 CVE-2017-3060 CVSS - 9.3 Vendor's Advisory http://www.securityfocus.com/bid/97557
Microsoft Office XSS Elevation of Privilege Vulnerability	Microsoft Excel Web App 2010 SP2, Office Web Apps 2010 SP2 and 2012 SP1, Office Online Server and Excel Services on Microsoft SharePoint Server 2010 SP2 and 2013 SP1 are prone to a cross-site scripting vulnerability due to a improper sanitization of input. An attacker can exploit this issue with a crafted request to an affected Web App server.	Version(s): Microsoft Excel Web App 2010 SP2, Office Web Apps 2010 SP2 and 2012 SP1, Office Online Server and Excel Services on Microsoft SharePoint Server 2010 SP2 and 2013 SP1	Published - April 10, 2017 CVE-2017-0195 CVSS - 9.3 Vendor's Advisory https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0195