CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: 11 December 2015

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft products and they can be exploited by remote attackers to cause execution of arbitrary code, gain knowledge of sensitive information, take full control of the affected systems and bypass security restrictions. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Multiple Vulnerabilities in Microsoft Internet Explorer CVE-2015-6083 CVE-2015-6134 CVE-2015-6135 CVE-2015-6136 CVE-2015-6138 CVE-2015-6139 CVE-2015-6140 CVE-2015-6141 CVE-2015-6142 **List of other CVE info is available on:** https://technet.microsoft.com/library/security/MS15-124	Multiple vulnerabilities have been identified in Internet Explorer and could be exploited to cause execution of arbitrary code. These vulnerabilities can allow remote attackers to view specially crafted webpage using Internet Explorer. Successful exploitation of the vulnerabilities could allow gaining the same user rights as the current user.	Internet Explorer 7 Internet Explorer 8 Internet Explorer 9 Internet Explorer 10 Internet Explorer 11	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-124
Multiple Vulnerabilities in Microsoft Edge	Multiple vulnerabilities have been identified in Microsoft Edge and could allow remote attackers to cause code execution if a user views	Microsoft Edge	Users are advised to apply updates. More information about

CVE-2015-6139 CVE-2015-6140 CVE-2015-6142 CVE-2015-6148 CVE-2015-6151 **List of other CVE info is available on:** https://technet.microsoft.com/library/security/MS15-125	a specially crafted webpage using Microsoft Edge. Successful exploitation of the vulnerabilities could gain the same user rights as the current user.		the updates is available in: https://technet.microsoft.com/library/security/MS15-125
Vulnerability in JScript and VBScript **CVE Info:** CVE-2015-1642 CVE-2015-2423 CVE-2015-2466 CVE-2015-2467 CVE-2015-2468 CVE-2015-2469 CVE-2015-2470 CVE-2015-2477	Multiple vulnerabilities have been identified in the VBScript scripting engine in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker hosts a specially crafted website that is designed to exploit the vulnerabilities through Internet Explorer and then convinces a user to view the website. Successful exploitation of the vulnerability can also allow an attacker to embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that uses the Internet Explorer rendering engine to direct the user to the specially crafted website.	Windows Vista Windows Server 2008	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-126
Security Update for Microsoft Windows DNS to Address Remote Code Execution **CVE Info:** CVE-2015-6100 CVE-2015-6101 CVE-2015-6102 CVE-2015-6103 CVE-2015-6104	This security update addresses a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an attacker sends specially crafted requests to a DNS server.	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 and Windows Server 2012 R2	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-127

CVE-2015-6109 CVE-2015-6113			
Security Update for Microsoft Graphics Component to Address Remote Code Execution **CVE Info:** CVE-2015-6098	This security update resolves vulnerabilities in Microsoft Windows, .NET Framework, Microsoft Office, Skype for Business, Microsoft Lync, and Silverlight. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-128
Multiple Vulnerabilities in Microsoft Silverlight **CVE Info:** CVE-2015-6096 CVE-2015-6099 CVE-2015-6115	Multiple Vulnerabilities have been identified in Microsoft Silverlight. These vulnerabilities could allow remote code execution if Microsoft Silverlight incorrectly handles certain open and close requests that could result in read- and write-access violations.	Microsoft Silverlight 5 Microsoft Silverlight 5 Developer Runtime when installed on Mac or all supported releases of Microsoft Windows	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-129
Security Update for Microsoft Uniscribe to Address Remote Code Execution **CVE Info:** CVE-2015-2478	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains specially crafted fonts.	Windows 7 Windows Server 2008 R2	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-130
Multiple Vulnerabilities in Microsoft Windows	Multiple Vulnerabilities have been identified in Microsoft Office and could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who	Microsoft Office 2007 Microsoft Office 2010 Microsoft Office	Users are advised to apply updates. More information about the updates is

CVE Info: CVE-2015-6040 CVE-2015-6118 CVE-2015-6122 CVE-2015-6124 CVE-2015-6172 CVE-2015-6177	successfully exploited the vulnerabilities could run arbitrary code in the context of the current user.	2013 Microsoft Office 2016 Microsoft Office 2013 RT Microsoft Office for Mac 2011 Microsoft Office 2016 for Mac	available in: https://technet.microsoft.com/library/security/MS15-131
Security Update for Microsoft Windows to Address Remote Code Execution **CVE:** CVE-2015-6128 CVE-2015-6132 CVE-2015-6133	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-132
Security Update for Windows PGM to Address Elevation of Privilege **CVE Info:** CVE-2015-6126	A vulnerability has been identified in Microsoft Windows which could allow elevation of privilege if an attacker logs on to a target system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-133
Security Update for Windows Media Center to Address Remote Code Execution	This security update addresses multiple vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious	Windows Vista Windows 7 Windows 8 and Windows 8.1	Users are advised to apply updates. More information about the updates is available in: https://technet.micro

CVE Info: CVE-2015-6061	code. Successful exploitation of the vulnerabilities could allow an attacker to gain the same user rights as the current user.		soft.com/library/security/MS15-134
Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege **CVE Info:** CVE-2015-6171 CVE-2015-6173 CVE-2015-6174 CVE-2015-6175	Multiple vulnerabilities have been identified in Microsoft Windows and could allow elevation of privilege if an attacker logs on to a target system and runs a specially crafted application.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-135

Vendor Information

Microsoft
www.microsoft.com

References

Microsoft Security Bulletins

https://technet.microsoft.com/library/security/MS15-124

https://technet.microsoft.com/library/security/MS15-125

https://technet.microsoft.com/library/security/MS15-126

https://technet.microsoft.com/library/security/MS15-127

https://technet.microsoft.com/library/security/MS15-128

https://technet.microsoft.com/library/security/MS15-129

https://technet.microsoft.com/library/security/MS15-130

https://technet.microsoft.com/library/security/MS15-131

https://technet.microsoft.com/library/security/MS15-132

https://technet.microsoft.com/library/security/MS15-133

https://technet.microsoft.com/library/security/MS15-134

https://technet.microsoft.com/library/security/MS15-135

Security Tracker

http://www.securitytracker.com/id/1034338

http://www.securitytracker.com/id/1034337

http://www.securitytracker.com/id/1034336

http://www.securitytracker.com/id/1034335

http://www.securitytracker.com/id/1034334

http://www.securitytracker.com/id/1034333

http://www.securitytracker.com/id/1034332

http://www.securitytracker.com/id/1034331

http://www.securitytracker.com/id/1034330

http://www.securitytracker.com/id/1034329

http://www.securitytracker.com/id/1034325

http://www.securitytracker.com/id/1034324

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu