CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: October, 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 Internet Explorer CVE-2015-2482 CVE-2015-6042 CVE-2015-6044 CVE-2015-6046 CVE-2015-6047 CVE-2015-6048 CVE-2015-6049 CVE-2015-6050 **Other CVE Info is available on:** https://technet.microsoft.com/library/security/MS15-106	Multiple vulnerabilities have been identified in Internet Explorer and can be exploited to cause remote code execution if a user views a specially crafted webpage using Internet Explorer. Successful exploitation of the vulnerabilities could gain the same user rights as the current user.	Internet Explorer 7, 8,9,10,11	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-106
Microsoft Edge Multiple Vulnerabilities **CVE Info:** CVE-2015-6057 CVE-2015-6058	Multiple vulnerabilities have been identified in Microsoft Edge and could be exploited by remote attackers to allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. Successful exploitation of the vulnerability can allow an attacker to gain the same user rights as the current user.	Microsoft Edge	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-107

Multiple Vulnerabilities in JScript and VBScript **CVE Info:** CVE-2015-2482 CVE-2015-6052 CVE-2015-6055 CVE-2015-6059	Multiple vulnerabilities have been identified in the VBScript and JScript scripting engines in Microsoft Windows. These vulnerabilities can be exploited by remote attackers to cause execution of arbitrary code 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. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that uses the IE 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/MS15-108
Security Update for Windows Shell to Address Remote Code Execution **CVE Info:** CVE-2015-2515 CVE-2015-2548	Multiple vulnerabilities have been identified in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or an attacker convinces a user to view specially crafted content online.	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/MS15-109
Multiple Vulnerabilities in Microsoft Office **CVE Info:** CVE-2015-2555 CVE-2015-2557 CVE-2015-2558	Multiple vulnerabilities have been identified in Microsoft Office and could allow remote code execution if a user opens a specially crafted Microsoft Office file. Successful exploitation of the vulnerabilities can allow an attacker to run arbitrary code in the context of the current user.	Microsoft Office 2007 Microsoft Office 2010 Microsoft Office 2013 Microsoft Office 2013 RT Microsoft Office 2016 Microsoft Office for Mac 2011 Microsoft Office 2016 for Mac	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-110
Windows Kernel to Address Elevation of Privilege **CVE Info:** CVE-2015-2520 CVE-2015-2521 CVE-2015-2523	Multiple vulnerabilities have been identified in Microsoft Windows and can be exploited by remote attackers to allow elevation of privilege if an attacker logs on to an affected system and run a specially crafted application.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-111

CVE-2015-2545		Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1 Windows 10	

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins
https://technet.microsoft.com/library/security/MS15-111
https://technet.microsoft.com/library/security/MS15-110
https://technet.microsoft.com/library/security/MS15-109
https://technet.microsoft.com/library/security/MS15-108
https://technet.microsoft.com/library/security/MS15-107
https://technet.microsoft.com/library/security/MS15-106

Security Tracker

http://www.securitytracker.com/id/1033802
http://www.securitytracker.com/id/1033800
http://www.securitytracker.com/id/1033803
http://www.securitytracker.com/id/1033804
http://www.securitytracker.com/id/1033799

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: www.cert-mu.org.mu