CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: 10 August, 2016

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft products and they can be exploited by 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 Info:** CVE-2016-3288 CVE-2016-3289 CVE-2016-3290 CVE-2016-3293 CVE-2016-3321 CVE-2016-3322 CVE-2016-3326 CVE-2016-3327 CVE-2016-3329	Multiple vulnerabilities have been identified in Internet Explorer and could be exploited to cause execution of arbitrary code. These vulnerabilities can allow attackers to view specially crafted webpage using Internet Explorer. Successful exploitation of the vulnerabilities could allow attackers to gain the same user rights as the current user.	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/MS16-095
Multiple Vulnerabilities in Microsoft Edge **CVE Info:** CVE-2016-3289 CVE-2016-3293 CVE-2016-3296	Multiple vulnerabilities have been identified in Microsoft Edge and could allow remote attackers to cause code execution if a user views a specially crafted webpage using Microsoft Edge. Successful exploitation of the vulnerabilities	Microsoft Edge	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS

CVE-2016-3319 CVE-2016-3322 CVE-2016-3326 CVE-2016-3327 CVE-2016-3329	could gain the same user rights as the current user.		16-096
Multiple Vulnerabilities in Microsoft Graphic Components **CVE Info:** CVE-2016-3301 CVE-2016-3303 CVE-2016-3304	Multiple vulnerabilities have been reported in Microsoft Graphic Components. These vulnerabilities could allow remote code execution if a user visits a specially crafted website or open specially crafted documents. Successful exploitation of the vulnerability could allow attackers to execute arbitrary code on the target user's system.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 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/MS16-097
Vulnerability in Windows Kernel Mode Drivers **CVE Info:** CVE-2016-3308 CVE-2016-3309 CVE-2016-3310 CVE-2016-3311	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 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/MS16-098
Multiple Vulnerabilities in Microsoft Office **CVE Info:** CVE-2016-3315 CVE-2016-3313 CVE-2016-3316	Multiple Vulnerabilities have been identified in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. Successful exploitation of the vulnerabilities	Microsoft Office 2007 Microsoft Office 2010 Microsoft Office 2013 Microsoft Office 2013 RT	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-099

CVE-2016-3317 CVE-2016-3318	could allow remote attackers to run arbitrary code in context of the current user.	Microsoft Office 2016 Microsoft Office for Mac 2011 Microsoft Office 2016 for Mac	
Vulnerability in Secure Boot **CVE Info:** CVE-2016-3320	A vulnerability has been reported in Secure Boot. The vulnerability could allow Secure Boot security features to be bypassed if an attacker installs an affected boot manager on a target device. Successful exploitation of this vulnerability could result in, test-signed executable code and drivers to be loaded on the target system.	Windows 8.1 Windows Server 2012 Windows Server 2012 R2 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/MS16-100
Vulnerabilities in Windows Authentication Methods **CVE Info:** CVE-2016-3300 CVE-2016-3237	This security update resolves vulnerabilities in Microsoft Windows. These vulnerabilities could allow elevation of privilege if an attacker runs a specially crafted application on a domain-joined system.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 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/MS16-101
Vulnerability in Microsoft Windows PDF Library **CVE Info:** CVE-2016-3319	This security update resolves vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user views specially crafted PDF content online or opens a specially crafted PDF document. Successful exploitation of the vulnerability could allow the	Windows 8.1 Windows Server 2012 Windows Server 2012 R2 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/MS16-102

	attacker to gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker 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.		
Vulnerability in ActiveSyncProvider **CVE Info:** CVE-2016-3312	This security update resolves vulnerability in Microsoft Windows. The vulnerability could allow information disclosure when Universal Outlook fails to establish a secure connection.	Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-103

Source:

Microsoft Security Bulletin

https://technet.microsoft.com/en-us/library/security/ms16-aug.aspx

https://technet.microsoft.com/library/security/ms16-aug.aspx

Security Tracker

http://securitytracker.com/id/1036577

http://securitytracker.com/id/1036576

http://securitytracker.com/id/1036573

http://securitytracker.com/id/1036572

http://securitytracker.com/id/1036569

http://securitytracker.com/id/1036568

http://securitytracker.com/id/1036564

http://securitytracker.com/id/1036565

http://securitytracker.com/id/1036566

http://securitytracker.com/id/1036562

http://securitytracker.com/id/1036561

http://securitytracker.com/id/1036559

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