CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: 12 October, 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-2016-3267 CVE-2016-3298 CVE-2016-3331 CVE-2016-3382 CVE-2016-3383 CVE-2016-3384 CVE-2016-3385 CVE-2016-3387 CVE-2016-3388 CVE-2016-3390 CVE-2016-3391	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 on: https://technet.microsoft.com/library/security/MS16-118
Multiple Vulnerabilities in Microsoft Edge **CVE Info:**	Multiple vulnerabilities have been identified in Microsoft Edge and could allow remote attackers to cause code execution if a user views a	Microsoft Edge	Users are advised to apply updates. More information about the updates

CVE-2016-3267 CVE-2016-3331 CVE-2016-3382 CVE-2016-3386 CVE-2016-3387 CVE-2016-3388 CVE-2016-3389 CVE-2016-3390 CVE-2016-3391 CVE-2016-3392 CVE-2016-7189 CVE-2016-7190 CVE-2016-7194	specially crafted webpage using Microsoft Edge. Successful exploitation of the vulnerabilities could allow attackers to gain the same user rights as the current user.		is available on: https://technet.microsoft.com/library/security/MS16-119
Multiple Vulnerabilities in Microsoft Graphic Components **CVE Info:** CVE-2016-3393 CVE-2016-3396 CVE-2016-3209 CVE-2016-3262 CVE-2016-3263 CVE-2016-7182 CVE-2016-3270	Multiple vulnerabilities have been reported in Microsoft Graphic Components. These vulnerabilities could allow an attacker to cause execution of arbitrary code and obtain elevated privileges on the target 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 on: https://technet.microsoft.com/library/security/MS16-120
Multiple Vulnerabilities in Microsoft Office **CVE Info:** CVE-2016-7193	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 could allow remote attackers to run arbitrary code in 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 on: https://technet.microsoft.com/library/security/MS16-121
Vulnerability in Microsoft Video	A vulnerability has been identified in Microsoft Windows.	Windows Vista Windows 7	Users are advised to apply updates.

Control **CVE Info:** CVE-2016-0142	The vulnerability could allow remote code execution if Microsoft Video Control fails to properly handle objects in memory. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user.	Windows 8.1 Windows RT 8.1 Windows 10	More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-122
Multiple Vulnerabilities in Windows Kernel **CVE Info:** CVE-2016-3266 CVE-2016-3376 CVE-2016-7185 CVE-2016-7211 CVE-2016-3341	Multiple Vulnerabilities have been identified in Windows Kernel. These vulnerabilities could allow elevation of privilege if an attacker runs a specially crafted application on a target 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 on: https://technet.microsoft.com/library/security/MS16-123
Vulnerability in Windows Diagnostics Hub standard collector service **CVE Info:** CVE-2016-7188	A vulnerability has been identified in window Diagnostics Hub standard collector service. A local user can run a specially crafted application to execute arbitrary commands on the target system with elevated privileges	Windows 10	More information about the updates is available on: https://technet.microsoft.com/library/security/ms16-125
Vulnerability in Windows Microsoft Internet Messaging API **CVE Info:** CVE-2016-3298	A vulnerability has been identified in Windows Microsoft Internet Messaging API. This vulnerability exists when the Microsoft Internet Messaging API improperly handles objects in memory. An attacker who successfully exploited this vulnerability could test for the presence of files on disk.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-126

Multiple Vulnerabilities in Adobe Flash Player **CVE Info:** CVE-2016-4273 CVE-2016-4286 CVE-2016-6981 CVE-2016-6982 CVE-2016-6983 CVE-2016-6984 More CVE information available on: https://technet.microsoft.com/library/security/MS16-127	Multiple vulnerabilities were identified in Adobe Flash Player. These vulnerabilities could allow a remote attacker to cause arbitrary code execution, obtain potentially sensitive information 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 on: https://technet.microsoft.com/library/security/MS16-127

Source:

Microsoft Security Bulletin

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

Security Tracker

http://securitytracker.com/id/1036983

http://securitytracker.com/id/1036984

http://securitytracker.com/id/1036985

http://securitytracker.com/id/1036988

http://securitytracker.com/id/1036992

http://securitytracker.com/id/1036993

http://securitytracker.com/id/1036996

http://securitytracker.com/id/1036997

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