CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: 14 September, 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-2016-3247 CVE-2016-3291 CVE-2016-3292 CVE-2016-3295 CVE-2016-3297 CVE-2016-3324 CVE-2016-3351 CVE-2016-3353 CVE-2016-3375	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/MS16-104
Multiple Vulnerabilities in Microsoft Edge **CVE Info:** CVE-2016-3247 CVE-2016-3291 CVE-2016-3294	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 could allow attackers to gain the	Microsoft Edge	Users are advised to apply updates. More information about the updates is available on: https://technet.micr

CVE-2016-3295 CVE-2016-3297 CVE-2016-3325 CVE-2016-3330 CVE-2016-3350 CVE-2016-3351 CVE-2016-3370 CVE-2016-3374 CVE-2016-3377	same user rights as the current user.		osoft.com/library/security/MS16-105
Multiple Vulnerabilities in Microsoft Graphic Components **CVE Info:** CVE-2016-3348 CVE-2016-3349 CVE–2016-3354 CVE–2016-3355 CVE–2016-3356	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 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/MS16-106
Multiple Vulnerabilities in Microsoft Office **CVE Info:** CVE-2016-3357 CVE-2016-3358 CVE-2016-3359 CVE-2016-3360 CVE-2016-3361 CVE-2016-3362 CVE-2016-3363 CVE-2016-3364 CVE-2016-3365 CVE-2016-3366 CVE-2016-3381	Multiple Vulnerabilities have been identified in Microsoft Office. These 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/MS16-107
Multiple Vulnerabilities in Microsoft	Multiple Vulnerabilities have been identified in Microsoft Exchange. These vulnerabilities could allow	Microsoft Exchange Server 2007 Microsoft Exchange	Users are advised to apply updates. More information

Exchange **CVE Info:** CVE-2016-0138 CVE-2016-3378 CVE-2016-3379	remote code execution in some Oracle Outside In libraries that are built into Exchange Server if an attacker sends an email with a specially crafted attachment to a vulnerable Exchange server. Successful exploitation of the vulnerabilities could allow remote attackers to run arbitrary code.	Server 2010 Microsoft Exchange Server 2013 Microsoft Exchange Server 2016	about the updates is available on: https://technet.microsoft.com/library/security/MS16-108
Vulnerability in Microsoft Silverlight **CVE Info:** CVE-2016-3367	A vulnerability has been identified in Microsoft Silverlight. This vulnerability could allow remote code execution if a user visits a compromised website that contains a specially crafted Silverlight application.	Microsoft Silverlight 5	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-109
Multiple Vulnerabilities in Microsoft Windows **CVE Info:** CVE-2016-3346 CVE-2016-3352 CVE-2016-3368 CVE-2016-3369	Multiple Vulnerabilities have been identified in Microsoft Windows. These vulnerabilities could allow remote code execution and elevation of privileges if an attacker creates a specially crafted request and executes arbitrary code with elevated permissions 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/MS16-110
Multiple Vulnerabilities in Windows Kernel **CVE Info:** CVE-2016-3305 CVE-2016-3306 CVE-2016-3372 CVE-2016-3373	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/MS16-111

Vulnerability in Windows Lock Screen **CVE Info:** CVE-2016-3302	A vulnerability has been identified in Windows Lock Screen. This vulnerability could allow elevation of privilege if Windows improperly allows web content to load from the Windows lock screen.	Windows 8.1 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/MS16-112
Vulnerability in Windows Secure Kernel Mode **CVE Info:** CVE-2016-3344	A vulnerability has been identified in Windows Secure Kernel Mode. This vulnerability could allow information disclosure when Windows Secure Kernel Mode improperly handles objects in memory.	Windows 10	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-113
Vulnerability in Windows SMBv1 Server **CVE Info:** CVE-2016-3345	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if an authenticated attacker sends specially crafted packets to an affected Microsoft Server Message Block 1.0 (SMBv1) Server.	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/MS16-114
Multiple vulnerabilities in Microsoft Windows PDF Library **CVE Info:** CVE-2016-3370 CVE-2016-3374	Multiple Vulnerabilities have been identified in Microsoft Windows PDF Library. These vulnerabilities could allow information disclosure if a user views specially crafted PDF content online or opens a specially crafted PDF document.	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/MS16-115

Vulnerability in OLE Automation for VBScript Scripting Engine **CVE Info:** CVE-2016-3375	A vulnerability has been identified in OLE Automation for VBScript Scripting Engine. The vulnerability could allow remote code execution if an attacker successfully convinces a user of an affected system to visit a malicious or compromised website.	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/MS16-116
Multiple Vulnerabilities in Adobe Flash Player **CVE Info:** CVE-2016-4271 CVE-2016-4272 CVE-2016-4274 CVE-2016-4275 CVE-2016-4276 More CVE available on: https://technet.microsoft.com/library/security/MS16-117	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/MS16-117

Source:

Microsoft Security Bulletin

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

Security Tracker

http://securitytracker.com/id/1036803

http://securitytracker.com/id/1036802

http://securitytracker.com/id/1036802

http://securitytracker.com/id/1036800

http://securitytracker.com/id/1036799

http://securitytracker.com/id/1036798

http://securitytracker.com/id/1036795

http://securitytracker.com/id/1036789

http://securitytracker.com/id/1036788

http://securitytracker.com/id/1036786

http://securitytracker.com/id/1036785

http://securitytracker.com/id/1036778

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