CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: 16 June, 2016

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 Info:** CVE-2016-0199 CVE-2016-0200 CVE-2016-3202 CVE-2016-3205 CVE-2016-3206 CVE-2016-3207 CVE-2016-3210 CVE-2016-3211 CVE-2016-3212 CVE-2016-3213	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 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/MS16-063
Multiple Vulnerabilities in Microsoft Edge **CVE Info:** CVE-2016-3198	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 on:

CVE-2016-3199 CVE-2016-3201 CVE-2016-3202 CVE-2016-3203 CVE-2016-3214 CVE-2016-3215 CVE-2016-3222	could gain the same user rights as the current user.		https://technet.microsoft.com/library/security/MS16-068
Vulnerability in VBScript and JScript scripting engine in Microsoft Windows **CVE Info:** CVE-2016-3205 CVE-2016-3206 CVE-2016-3207	Vulnerabilities have been reported in the VBScript and JScript scripting engine in Microsoft Windows. These vulnerabilities could allow remote code execution if a user visits a specially crafted website. Successful exploitation of the vulnerability could allow attackers 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.	Windows Vista Windows Server 2008	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-069
Multiple Vulnerabilities in Microsoft Office **CVE Info:** CVE-2016-0025 CVE-2016-3233 CVE-2016-3234	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/MS16-070
Vulnerability in Microsoft Windows	A vulnerability has been reported in Microsoft Windows and could allow	Windows Server 2012	Users are advised to apply updates. More

DNS Server **CVE Info:** CVE-2016-3227	remote code execution if an attacker sends specially crafted requests to a DNS server.	Windows Server 2012 R2	information about the updates is available on: https://technet.microsoft.com/library/security/MS16-071
Vulnerability in Group Policy **CVE Info:** CVE-2016-3223	A vulnerability has been reported in Microsoft Windows and could allow elevation of privilege if an attacker launches a man-in-the-middle (MiTM) attack against the traffic passing between a domain controller and the target machine.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT Windows 10	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-072
Vulnerabilities in Windows Kernel-Mode Drivers **CVE Info:** CVE-2016-3218 CVE-2016-3221 CVE-2016-3232	Multiple Vulnerabilities have been reported in Microsoft Windows. These vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT Windows 10	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-073
Vulnerabilities in Microsoft Graphics Component	Multiple Vulnerabilities have been reported in Microsoft Windows. These vulnerabilities could allow elevation of privilege if a user opens a specially crafted document or visits a specially crafted website.	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:

CVE Info: CVE-2016-3216 CVE-2016-3219 CVE-2016-3220		Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT 8.1 Windows 10	https://technet.microsoft.com/library/security/MS16-074
Vulnerability in Windows SMB Server **CVE Info:** CVE-2016-3225	A vulnerability has been identified in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.	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/MS16-075
Vulnerability in Netlogon **CVE Info:** CVE-2016-3228	A vulnerability has been identified in Microsoft Windows. The vulnerability could allow remote code execution if an attacker with access to a domain controller (DC) on a target network runs a specially crafted application to establish a secure channel to the DC as a replica domain controller.	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-076
Vulnerabilities in Web Proxy Auto Discovery (WPAD) **CVE Info:** CVE-2016-3213 CVE-2016-3236	Multiple vulnerabilities have been identified in Microsoft Windows. These vulnerabilities could allow elevation of privilege if the Web Proxy Auto Discovery (WPAD) protocol falls back to a vulnerable proxy discovery process on a target system.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012 Windows Server	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/secu

		2012 R2 Windows RT 8.1 Windows 10	rity/MS16-077
Vulnerability in Windows Diagnostic Hub **CVE Info:** CVE-2016-3231	A vulnerability has been identified in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.	Windows 10	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-078
Vulnerabilities in Microsoft Exchange Server **CVE Info:** CVE-2016-0028	Multiple vulnerabilities have been identified in Microsoft Exchange Server. These vulnerabilities could allow information disclosure if an attacker sends a specially crafted image URL in an Outlook Web Access (OWA) message that is loaded, without warning or filtering, from the attacker-controlled URL.	Microsoft Exchange Server 2007 Microsoft Exchange Server 2010 Microsoft Exchange Server 2013 Microsoft Exchange Server 2016	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-079
Vulnerabilities in Microsoft Windows PDF **CVE Info:** CVE-2016-3201 CVE-2016-3215 CVE-2016-3203	Multiple vulnerabilities have been identified in Microsoft Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted .pdf file. An attacker who successfully exploited the vulnerabilities could cause arbitrary code to execute in the context of the current user. However, an attacker would have no way to force a user to open a specially crafted .pdf file.	Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows 10	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-080

Vulnerability in Active Directory **CVE Info:** CVE-2016-3226	A vulnerability has been identified in Active Directory. The vulnerability could allow denial of service if an authenticated attacker creates multiple machine accounts.	Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS16-081
Vulnerability in Microsoft Windows Search Component **CVE Info:** CVE-2016-3230	A vulnerability has been reported in Microsoft Windows. The vulnerability could allow denial of service if an attacker logs on to a target system and runs a specially crafted application.	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/MS16-082

Source:

Microsoft Security Bulletin

https://technet.microsoft.com/en-us/library/security/mt733206.aspx

Security Tracker

http://securitytracker.com/id/1036096

http://securitytracker.com/id/1036093

http://securitytracker.com/id/1036095

http://securitytracker.com/id/1036099

http://securitytracker.com/id/1036100

http://securitytracker.com/id/1036101

http://securitytracker.com/id/1036106

http://securitytracker.com/id/1036108

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