National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: March, 2015

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft Products and they can allow a remote attacker to conduct cross-site scripting attacks, spoofing and gain elevated privileges on the affected systems. Microsoft has released an update that addresses all the vulnerabilities. The vulnerabilities reported are as follows:

Vulnerability	Systems Affected	Description	Workarounds
Microsoft Exchange Server Bugs Permit Cross-Site Scripting and Account Spoofing Attacks **CVE Info:** **CVE-2015-1632** **CVE-2015-1631** **CVE-2015-1630** **CVE-2015-1629** **CVE-2015-1628**	• Microsoft Exchange Server 2013 Service Pack 1 • Microsoft Exchange Server 2013 Cumulative Update 7	Multiple vulnerabilities have been identified in Microsoft Exchange Server and can be exploited by remote attackers to conduct cross-site scripting attacks and spoof meeting organizer accounts.	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/library/security/ms15-026

Windows Kernel Bugs Let Local Users Gain Elevated Privileges **CVE Info:** **CVE-2015-0073** **CVE-2015-0075**	• Windows Server 2003 • 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	Several vulnerabilities have been identified in Windows Kernel and can be exploited by remote attackers to obtain elevated privileges on the vulnerable system. The vulnerabilities reported are as follows: • The first vulnerability exists because Windows Registry Virtualization does not properly restrict user access for virtual store modification. This can allow a local user to run a specially crafted application to execute arbitrary code with the privileges of the target user. • The second vulnerability exists because Windows does not properly validate and enforce impersonation levels, which can be exploited by remote attackers to bypass user account checks to gain elevated privileges.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-025
Microsoft Windows PNG Parsing Flaw Lets Remote Users Obtain Potentially Sensitive Information **CVE Info:** **CVE-2015-0080**	• Windows Server 2003 • 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	A vulnerability has been identified in Microsoft Windows which can be exploited by remote attackers to obtain sensitive information on the vulnerable system. The vulnerability exists because the software does not properly handle uninitialized memory. This can be exploited by remote attackers to create a specially crafted PNG image file that,	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-024

	Windows RT 8.1	when loaded by the target user, will access information on the target user's system.	
Windows Kernel-Mode Driver Bugs Let Local Users Obtain Potentially Sensitive Information and Gain Elevated Privileges **CVE Info:** **CVE-2015-0077** **CVE-2015-0078** **CVE-2015-0094** **CVE-2015-0095**	• Windows Server 2003 • 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	Multiple vulnerabilities have been identified in Windows Kernel-Mode Driver and can be exploited by remote attackers to obtain elevated privileges on the target system. The vulnerabilities reported are as follows: • The vulnerability exists because the kernel-mode driver does not properly initialize function buffers. This vulnerability can allow remote attackers to obtain administrative credentials. • A vulnerability exists because the kernel-mode driver does not properly validate the calling thread's token. This vulnerability can be exploited by remote attackers to obtain administrative credentials. • A vulnerability occurs because the kernel-mode driver discloses private address information during a function call. This can allow remote attackers to use this information in conjunction with a separate vulnerability to bypass Address Space Layout Randomization (ASLR) protections. • A vulnerability exists that	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-023

		can allow a user to trigger a null pointer dereference to obtain kernel memory contents. This vulnerability can allow remote attackers to use information in conjunction with a separate vulnerability to bypass Address Space Layout Randomization (ASLR) protections.	
Microsoft Office Memory Corruption Flaws Let Remote Users Execute Arbitrary Code **CVE Info:** **CVE-2015-0097** **CVE-2015-0086** **CVE-2015-0085**	• Microsoft Office 2007 • Microsoft Office 2010 • Microsoft Office 2013 • Office 2013 RT • Microsoft Word Viewer • Microsoft Excel Viewer • Microsoft Office Compatibility Pack Service Pack 3	Several vulnerabilities have been reported in Microsoft Office, which can be exploited by remote attackers to cause arbitrary code to be executed on the target user's system. These vulnerabilities can allow remote attackers to create a specially crafted Office file that when loaded by the target user, will trigger a use-after-free memory error and execute arbitrary code on the target system The code will run with the privileges of the target user.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-022
Microsoft SharePoint Input Validation Flaws Permit Cross-Site Scripting Attacks **CVE Info:** **CVE-2015-1636** **CVE-2015-1633**	• Microsoft Office 2007 • Microsoft Office 2010 • Microsoft Office 2013 • Office 2013 RT • Microsoft SharePoint Server 2010 • Microsoft SharePoint Server 2013 • Microsoft Office Web Apps 2010 • Microsoft Office Web Apps 2013	Two vulnerabilities have been identified in Microsoft SharePoint and can be exploited by remote attackers to conduct cross-site scripting attacks. The vulnerabilities exist because the software does not properly filter HTML code from user-supplied input before displaying the input. This can be exploited by remote attackers to cause execution of arbitrary scripting	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-022

	• Microsoft SharePoint Server 2007 • Microsoft SharePoint Server 2010 • Microsoft SharePoint Server 2013	code by the target user's browser. The code will originate from the site running the Microsoft SharePoint software and will run in the security context of that site. This will make the code access the target user's cookies, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user.	
Microsoft Windows Photo Decoder Memory Initialization Flaw Lets Remote Users Obtain Potentially Sensitive Information **CVE Info:** **CVE-2015-0076**	• 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	A vulnerability has been identified in Microsoft Windows Photo Decoder and can be exploited by remote attackers to obtain potentially sensitive information on the target system. The vulnerability can allow a remote attacker to create a specially crafted JPEG XR (.JXR) image file that, when loaded by the target user, will obtain potentially sensitive information from the target user's system.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-029
Microsoft Task Scheduler Lets Local Users Gain Elevated Privileges **CVE Info:** **CVE-2015-0084**	• 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	A vulnerability has been identified in Microsoft Task Scheduler which can be exploited by remote attacker to obtain elevated privileges on the target system. The vulnerability exists because the Windows Task Scheduler does not properly validate and enforce impersonation levels. This vulnerability can be exploited by local user with limited privileges to bypass access control list (ACL) settings and run	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-028

		privileged executables.	
Windows Netlogon Service Lets Remote Authenticated Users Spoof Remote Servers **CVE Info:** **CVE-2015-0005**	• Windows Server 2003 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 and Windows Server 2012 R2	A vulnerability was reported in Windows Netlogon Service. A remote authenticated user can spoof remote servers. The vulnerability exists because the Windows Netlogon service does not properly establish secure communication channels. This vulnerability can allow a remote authenticated user on a domain joined system that can monitor network traffic to establish a secure channel connection belonging to a different system and use the channel to obtain session-related information.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/library/security/ms15-027
Microsoft DLL Processing and Windows Text Services Bugs Let Remote Users Execute Arbitrary Code	• Windows Server 2003 • 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	Two vulnerabilities have been identified in Microsoft Windows and can be exploited by remote attackers to cause execution of arbitrary code on the target user's system. • A vulnerability exist that can allow remote attackers to create a specially crafted file that when loaded by the target user, will trigger an object memory handling flaw in Windows Text Services and execute arbitrary code on the target system. The code will run with the privileges of the target user. • Another vulnerability exist that can allow a remote attacker to create a specially crafted DLL. When the	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-020

		target user opens a file from the same working directory as the DLL file, the DLL will be loaded and execute arbitrary code.	
Microsoft Windows Adobe Font Driver Bugs Let Remote Users Execute Arbitrary Code, Deny Service, and Obtain Potentially Sensitive Information **CVE-2015-0093** **CVE-2015-0092** **CVE-2015-0091** **CVE-2015-0090** **CVE-2015-0089** **CVE-2015-0088** **CVE-2015-0087** **CVE-2015-0074**	• Windows Server 2003 • 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	Multiple vulnerabilities have been reported in Microsoft Windows Adobe Font Driver which can be exploited by remote attackers to cause arbitrary code to be executed on the target user's system, cause denial of service conditions on the target system and obtain potentially sensitive information. The vulnerabilities reported are as follows: • A vulnerability exists that can allow a remote user to create a specially crafted file or HTML that, when loaded by the target user will trigger a memory allocation error and cause denial of service conditions on the target user's system. • A vulnerability exists that can allow a remote user to create a specially crafted file or HTML that, when loaded by the target user, will obtain information from system memory. This information can be used in conjunction with a separate vulnerability to bypass Address Space Layout Randomization (ASLR) security features. • A vulnerability exists that	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-021

		can allow a remote user to create a specially crafted file or HTML that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target system. The code will run with kernel-level privileges.	
Microsoft Internet Explorer Multiple Flaws Let Remote Users Execute Arbitrary Code **CVE-2015-1634** **CVE-2015-0032** **CVE-2015-0056** **CVE-2015-0072** **CVE-2015-0099** **CVE-2015-0100** **CVE-2015-1622** **CVE-2015-1623** **CVE-2015-1624** **CVE-2015-1625** **CVE-2015-1626** **CVE-2015-1627**	• Internet Explorer 6 - 11	Multiple vulnerabilities have been identified in Microsoft Internet Explorer and can be exploited by remote attacker to cause execution of arbitrary code on the target user's system. The vulnerabilities reported are as follows: • A vulnerability exists that can allow a remote user to create specially crafted HTML that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code on the target system. The code will run with the privileges of the target user. • Another vulnerability exists which resides in the VBScript engine.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/library/security/ms15-018
Windows VBScript Scripting Engine Memory Corruption	• Windows Server 2003 • Windows Vista • Windows Server 2008	A vulnerability has been identified in Windows VBScript Scripting Engine and can allow a remote attacker to cause execution of arbitrary code on	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/lib

Error Lets Remote Users Execute Arbitrary Code **CVE Info:** **CVE-2015-0032**		the target user's system. This vulnerability can allow a remote user to create specially crafted HTML that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code on the target system. The code will run with the privileges of the target user. An application or Microsoft Office document with an embedded ActiveX control marked "safe for initialization" can also trigger this flaw.	rary/security/ms15-019
Windows Remote Desktop Protocol Object Management Flaw Lets Remote Users Deny Service	• Windows 7 • Windows 8 and Windows 8.1 • Windows Server 2012 and Windows Server 2012 R2	A vulnerability has been identified in Windows Remote Desktop Protocol (RDP) and can be exploited by remote attackers to cause denial of service conditions on the vulnerable system. The vulnerability exists because the system does not properly manage RDP objects in memory. Successful exploitation of the vulnerability can allow a remote user to create multiple RDP session to consume all available system memory and cause the target system to stop responding.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms15-030

Vendor Information

Microsoft
www.microsoft.com

References

Microsoft Security Bulletins

https://technet.microsoft.com/library/security/ms15-030

https://technet.microsoft.com/library/security/ms15-019

http://technet.microsoft.com/library/security/ms15-018

https://technet.microsoft.com/library/security/ms15-021

https://technet.microsoft.com/library/security/ms15-020

http://technet.microsoft.com/library/security/ms15-027

https://technet.microsoft.com/library/security/ms15-028

https://technet.microsoft.com/library/security/ms15-029

https://technet.microsoft.com/library/security/ms15-022

https://technet.microsoft.com/library/security/ms15-023

https://technet.microsoft.com/library/security/ms15-024

https://technet.microsoft.com/library/security/ms15-025

http://technet.microsoft.com/library/security/ms15-026

Security Tracker

http://www.securitytracker.com/id/1031899

http://www.securitytracker.com/id/1031900

http://www.securitytracker.com/id/1031898

http://www.securitytracker.com/id/1031896

http://www.securitytracker.com/id/1031895

http://www.securitytracker.com/id/1031892

http://www.securitytracker.com/id/1031891

http://www.securitytracker.com/id/1031890

http://www.securitytracker.com/id/1031889

http://www.securitytracker.com/id/1031888

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 : info@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu