National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: February, 2015

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft Products and they can allow a remote attacker to cause execution of arbitrary code, gain elevated privileges and gain knowledge of sensitive information. Microsoft has released an update that addresses all the vulnerabilities. The vulnerabilities reported are as follows:

Vulnerability	Systems Affected	Description	Workarounds
Microsoft System Center Virtual Machine Manager Lets Remote Authenticated Users Gain Elevated Privileges **CVE Info:** CVE-2015-0012	• Microsoft System Center Virtual Machine Manager 2012 R2 Update Rollup 4	A vulnerability has been identified in Microsoft System Center Virtual Machine Manager and can be exploited by remote attackers to gain elevated privileges on the vulnerable system. The vulnerability exists because the Virtual Machine Manager (VMM) does not properly validate user roles. Successful exploitation of the vulnerability can allow gaining administrative privileges on the vulnerable VMM server and take control of all of the target VMM server's managed virtual machines.	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/library/security/ms15-017

Microsoft Graphics Component TIFF Processing Flaw Discloses Potentially Sensitive System Information **CVE Info:** **CVE-2015-0061**	• 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	A vulnerability has been identified in Microsoft Graphics Component and this can be exploited by remote attackers to obtain sensitive information. Successful exploitation of the vulnerability can allow a remote attacker to create a specially crafted TIFF image that when it is loaded by the user will disclose portions of the system memory.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/library/security/ms15-016
Microsoft Windows SeAssignPrimaryTokenPrivilege Bug Lets Local Users Gain Elevated Privileges **CVE Info:** **CVE-2015-0062**	• 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 and this can be exploited by remote attackers to obtain elevated privileges on the vulnerable system. The vulnerability exists because the software does not properly validate and enforce impersonation levels. Successful exploitation of the vulnerability can allow remote attackers to exploit a flaw in processes *SeAssignPrimaryTokenPrivilege* to bypass impersonation-level security checks and gain elevated privileges.	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/library/security/ms15-015
Microsoft Internet Explorer Multiple Flaws Let Remote Users Execute Arbitrary Code, Gain Elevated Privileges, and Bypass the ASLR Security	• Internet Explorer versions 6, 7, 8, 9, 10, 11	Multiple vulnerabilities have been identified in Internet Explorer and they can be exploited by remote attackers to cause execution of arbitrary code, bypass same origin policy and bypass ASLR security feature. The vulnerabilities reported are as follows:	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/library/security/ms15-009

Feature **CVE Info** **CVE-2014-8967** **CVE-2015-0017** **CVE-2015-0018** **CVE-2015-0019** **CVE-2015-0020** **CVE-2015-0021** **CVE-2015-0022** **CVE-2015-0023** **CVE-2015-0025** **CVE-2015-0026** **CVE-2015-0027** **CVE-2015-0028** **CVE-2015-0029** **CVE-2015-0030** **CVE-2015-0031** **CVE-2015-0035** **CVE-2015-0036** List of other CVE Information is available on: https://technet.microsoft.com/library/security/ms15-009		• A vulnerability occurs that can allow a remote attacker to create a specially crafted file that when loaded by the user will cause a memory corruption error. This vulnerability can be exploited by remote attackers to cause execution of arbitrary code and run with the privileges of the user. • A vulnerability exists that can allow a remote user can create specially crafted HTML that when it is opened by the user, it bypasses the Address Space Layout Randomisation security feature and obtain information about the stack memory layout, which can be used to facilitate exploitation of separate vulnerabilities. • A vulnerability exists that can allow a remote attacker to scripting code to run with elevated privileges. • A vulnerability occurs that can allow remote attackers to bypass same-origin domain policy in order to get information from another domain or Internet Explorer zone.	

Microsoft Office Object Handling Errors in Excel and Word Let Remote Users Execute Arbitrary Code **CVE-2015-0065** **CVE-2015-0064** **CVE-2015-0063**	• Microsoft Office 2007 • Microsoft Office 2010 • Microsoft Office 2013 • Microsoft SharePoint Server 2010 • Microsoft Office Web Apps 2010	Three vulnerabilities have reported in Microsoft Office and they can be exploited by remote attackers to cause execution of arbitrary code on the vulnerable system. The vulnerabilities reported are: • A vulnerability occurs that can allow remote attackers to create a specially crafted Office file that when loaded by the target user, will trigger an object memory handling flaw in Microsoft Excel and execute arbitrary code on the target system. The code will run with the privileges of the target user. • A vulnerability exists that can allow a remote user to create a specially crafted Office file that when loaded by the user will trigger an object memory handling flaw in OneTableDocumentStream() in Microsoft Word and cause execution of arbitrary code on vulnerable systems. The code will run with the privileges of the user. • A vulnerability exists that can allow a remote attacker to create a specially crafted Office file that, when loaded by the target user will trigger an object memory handling flaw in Microsoft Word and cause execution of arbitrary	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/library/security/ms15-012

		code on the vulnerable system. The code will run with the privileges of the target user.	
Microsoft Windows Group Policy Security Configuration Engine Flaw Lets Remote Users Bypass Policy **CVE Info:** **CVE-2015-0009**	• 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	A vulnerability was reported in the Microsoft Windows Group Policy Security Configuration Engine and this can be exploited by remote attackers to bypass security policy. This vulnerability can allow a remote attacker to conduct a man-in-the-middle attack to modify domain controller responses to client requests to cause Group Policy settings on the target system to revert to their default setting. Successful exploitation of the vulnerability can allow remote attacker to bypass intended security policy.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/ms15-014
Windows Kernel-Mode Driver Flaws Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges **CVE-2015-2010** **CVE-2015-0060** **CVE-2015-0057** **CVE-2015-0058** **CVE-2015-0059**	• Windows Server 2003 • Windows Vista • Windows Server 2008 • Windows 7 • Windows Server 2008 R2 • Windows 8 and Windows 8.1 • Windows RT and Windows RT 8.1	Several vulnerabilities have been identified in the Windows Kernel-Mode Driver and can be exploited by remote attackers to cause execution of arbitrary code and gain elevated privileges on vulnerable systems. The vulnerabilities reported are as follows: • A vulnerability exists and can allow a remote attacker to create a specially crafted TrueType font file that when loaded by the target user, will trigger a flaw in 'Win32k.sys' and cause execution of arbitrary code	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/ms15-010

CVE-2015-0060 **CVE-2015-2010**		on the user's system. • A vulnerability occurs that can allow a remote attacker to create a specially crafted application that when run by user will bypass a security feature in the Cryptography Next Generation (CNG) kernel-mode driver (cng.sys) handling of impersonation levels to gain elevated privileges. • A vulnerability exists that can allow a remote attacker to exploit an object handling flaw in 'Win32k.sys' and gain elevated privileges on the target system. • A vulnerability exists that can allow a remote attacker to create a specially crafted TrueType font file that, when loaded by the target user, will cause execution of arbitrary code on the target system. • A vulnerability exists that can allow a remote attacker to trigger a cursor object double free memory error in 'win32k.sys' to cause execution of arbitrary code with kernel-level privileges.	

Microsoft Windows Group Policy Processing Error Lets Remote Users Execute Arbitrary Code in Certain Cases **CVE Info:** **CVE-2015-0009**	• 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	A vulnerability has been identified in Microsoft Windows and this can be exploited by remote attackers to cause execution of arbitrary code on the user's system in certain cases. Successful exploitation of the vulnerability can allow remote attackers to exploit a flaw in the processing Group Policy data and execute arbitrary code on the target domain-joined system when the target system connects to the remote user's domain controller.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/ms15-011
Microsoft Office Lets Remote Users Bypass Address Space Layout Randomization **CVE Info:** **CVE-2014-0254**	• Microsoft Office 2007 • Microsoft Office 2010 • Microsoft Office 2013	A vulnerability has been identified in Microsoft Office and can allow remote attackers to bypass the Address Space Layout Randomization (ASLR) security feature. This vulnerability can allow a remote user to bypass the ASLR security feature and obtain the information about the stack memory layout. This information can be used to facilitate exploitation of separate vulnerabilities.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/ms15-013

Vendor Information

Microsoft
www.microsoft.com

References

Microsoft Security Bulletins

http://technet.microsoft.com/library/security/ms15-017

http://technet.microsoft.com/library/security/ms15-016

http://technet.microsoft.com/library/security/ms15-015

http://technet.microsoft.com/library/security/ms15-009

http://technet.microsoft.com/library/security/ms15-012

https://technet.microsoft.com/library/security/ms15-014

https://technet.microsoft.com/library/security/ms15-010

https://technet.microsoft.com/library/security/ms15-011

https://technet.microsoft.com/library/security/ms15-013

Security Tracker

http://www.securitytracker.com/id/1031726

http://www.securitytracker.com/id/1031725

http://www.securitytracker.com/id/1031724

http://www.securitytracker.com/id/1031723

http://www.securitytracker.com/id/1031722

http://www.securitytracker.com/id/1031721

http://www.securitytracker.com/id/1031720

http://www.securitytracker.com/id/1031719

http://www.securitytracker.com/id/1031718

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