National Computer Board
Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: July 16, 2015

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
Vulnerabilities in SQL Server Could Allow Remote Code Execution CVE-2015-1761 CVE-2015-1762 CVE-2015-1763	Multiple vulnerabilities have been identified in Microsoft SQL Server and could be exploited by remote attackers to cause remote execution. These vulnerabilities could allow remote attackers to run a specially crafted query that is designed to execute a virtual function from a wrong address, leading to a function call to uninitialized memory. Successful exploitation of the vulnerabilities would require permissions to create or modify a database.	SQL Server 2008 Service Pack 3 SQL Server 2008 Service Pack 4 SQL Server 2008 R2 Service Pack 2 SQL Server 2008 R2 Service Pack 3 SQL Server 2012 Service Pack 1 SQL Server 2012 Service Pack 2 SQL Server 2014	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-058
Security Update for Internet Explorer **CVE Info:** CVE-2015-1729 CVE-2015-1733 CVE-2015-1738 CVE-2015-1767 **List of other CVE info:** https://technet.microsoft.com/en-us/library/security/MS15-065	Multiple vulnerabilities have been identified in Internet Explorer and could be exploited by remote attackers to cause execution of arbitrary code. Successful exploitation of the vulnerabilities could allow an attacker to gain the same user rights as the current user.	Internet Explorer 6 Internet Explorer 7 Internet Explorer 8 Internet Explorer 9 Internet Explorer 10 Internet Explorer 11	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-065

Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution **CVE Info:** CVE-2015-1675 CVE-2015-1695 CVE-2015-1696 CVE-2015-1697 CVE-2015-1698 CVE-2015-1699	A vulnerability has been identified in the VBScript scripting engine in Microsoft Windows. The vulnerability could allow remote code execution if a user visits a specially crafted website. This vulnerability could allow remote attackers to gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. Successful exploitation of the vulnerability could allow an attacker to install programs; view, change, or delete data; or create new accounts with full user rights.	Windows Server 2003 Windows Vista Windows Server 2008	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-066
Vulnerability in RDP Could Allow Remote Code Execution **CVE Info:** CVE-2015-2373	A vulnerability has been identified in Microsoft Windows and could allow remote attackers to cause execution of arbitrary code. This vulnerability can allow remote attackers to send a specially crafted sequence of packets to a targeted system with the Remote Desktop Protocol (RDP) server service enabled.	Windows 7 Windows 8 Windows Server 2012	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-067
Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution **CVE Info:** CVE-2015-2361 CVE-2015-2362	Multiple vulnerabilities have been identified in Microsoft Windows. The vulnerabilities could allow remote code execution in a host context if a specially crafted application is run by an authenticated and privileged user on a guest virtual machine hosted by Hyper-V. Successful exploitation of the vulnerabilities require valid logon credentials for a guest virtual machine.	Windows Server 2008 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 Windows Server 2012 R2	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-068
Vulnerabilities in Windows Could Allow Remote Code Execution **CVE Info:** CVE-2015-2368 CVE-2015-2369	Multiple vulnerabilities have been identified in Microsoft Windows and could be exploited by remote attackers to cause execution of arbitrary code. The vulnerabilities could allow Remote Code Execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RTF file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. Successful exploitation of the vulnerabilities	Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012 R2 Windows RT 8.1	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-069

	could allow remote attackers to take complete control of an affected system.		
Vulnerabilities in Microsoft Office Could Allow Remote Code Execution **CVE Info:** CVE-2015-2376 CVE-2015-2377 CVE-2015-2379 CVE-2015-2380 CVE-2015-2415 CVE-2015-2424 CVE-2015-2375 CVE-2015-2378	Multiple vulnerabilities have been reported in Microsoft Office and could be exploited by remote attackers to cause execution of arbitrary code. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user.	Microsoft Office 2007 Microsoft Office 2010 Microsoft Office 2013 Microsoft Office 2013 RT Microsoft Office for Mac	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-070
Vulnerability in Netlogon Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2374	A vulnerability has been identified in Microsoft Windows. This vulnerability could be exploited by remote attackers to allow elevation of privilege if an attacker with access to a primary domain controller (PDC) on a target network runs a specially crafted application to establish a secure channel to the PDC as a backup domain controller (BDC).	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 and Windows Server 2012 R2	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-071
Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2364	A vulnerability has been identified in Microsoft Windows and this could be exploited by remote attackers to elevation of privilege if windows graphics component fails to properly process bitmap conversions. Successful exploitation of the vulnerability could allow an attacker to install programs, view, change or delete data or create new accounts with full administrative rights.	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	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-072
Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2363 CVE-2015-2365	Multiple vulnerabilities have been identified in Microsoft Windows. The vulnerabilities could be exploited by remote attackers to cause elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.	Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-

CVE-2015-2366 CVE-2015-2367 CVE-2015-2381 CVE-2015-2382		2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1	us/library/security/MS15-073
Vulnerability in Windows Installer Service Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2371	A vulnerability has been identified in Microsoft Windows and could allow elevation of privilege if the Windows Installer service improperly runs custom action scripts. An attacker must first compromise a user who is logged on to the target system to exploit the vulnerability. Successful exploitation of the vulnerability could allow an attacker to install programs; view, change, or delete data; or create new accounts with full administrative rights.	Windows Server 2003 Windows Vista 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	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-074
Vulnerabilities in OLE Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2416 CVE-2015-2417	Multiple vulnerabilities have been identified in Microsoft Windows. The vulnerabilities could allow elevation of privilege if used in conjunction with another vulnerability that allows arbitrary code to be run.	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	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-075
Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2370	A vulnerability has been identified in Microsoft Windows. The vulnerability, which exists in Windows Remote Procedure Call (RPC) authentication, could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application. An attacker who successfully exploited this vulnerability could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-076

		2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1	
Vulnerability in ATM Font Driver Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2387	A vulnerability has been identified in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a target system and runs a specially crafted application. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete 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 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	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-077

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins

https://technet.microsoft.com/library/security/MS15-058
https://technet.microsoft.com/en-us/library/security/MS15-065
https://technet.microsoft.com/en-us/library/security/MS15-066
https://technet.microsoft.com/en-us/library/security/MS15-067
https://technet.microsoft.com/en-us/library/security/MS15-068
https://technet.microsoft.com/en-us/library/security/MS15-069
https://technet.microsoft.com/en-us/library/security/MS15-070
https://technet.microsoft.com/en-us/library/security/MS15-071
https://technet.microsoft.com/en-us/library/security/MS15-072
https://technet.microsoft.com/en-us/library/security/MS15-073
https://technet.microsoft.com/en-us/library/security/MS15-074
https://technet.microsoft.com/en-us/library/security/MS15-075
https://technet.microsoft.com/en-us/library/security/MS15-076
https://technet.microsoft.com/en-us/library/security/MS15-077

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: www.cert-mu.org.mu