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

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: August 13, 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
Multiple Vulnerabilities in Microsoft Internet Explorer CVE-2015-2423 CVE-2015-2441 CVE-2015-2442 CVE-2015-2443 CVE-2015-2444 CVE-2015-2445 CVE-2015-2446 CVE-2015-2447 CVE-2015-2448 CVE-2015-2449 CVE-2015-2450 CVE-2015-2451 CVE-2015-2452	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 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/library/security/ms15-079
Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution CVE-2015-2432 CVE-2015-2458 CVE-2015-2459 CVE-2015-2460 CVE-2015-2461	Multiple vulnerabilities have been identified in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Microsoft Lync, and Microsoft Silverlight. These vulnerabilities could allow remote attackers to cause execution of arbitrary code if a user opens a specially crafted document or visits an untrusted webpage that contains embedded TrueType or OpenType fonts.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 Windows 8.1 Windows Server 2012	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms15-080

CVE-2015-2462		Windows Server 2012 R2 Windows RT and Windows RT 8.1 Windows 10	
Vulnerabilities in Microsoft Office Could Allow Remote Code Execution **CVE Info:** CVE-2015-1642 CVE-2015-2423 CVE-2015-2466 CVE-2015-2467 CVE-2015-2468 CVE-2015-2469 CVE-2015-2470 CVE-2015-2477	Multiple vulnerabilities have been identified in Microsoft Office. These vulnerabilities could be exploited by remote attackers to cause execution of arbitrary code if a user opens a specially crafted Microsoft Office file. Successful exploitation could allow 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 2011 Microsoft Office for Mac 2016	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-081
Vulnerability in RDP Could Allow Remote Code Execution **CVE Info:** CVE-2015-2472 CVE-2015-2473	Multiple vulnerabilities have been identified in Microsoft Window. These vulnerabilities could allow execution of arbitrary code if an attacker places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open a Remote Desktop Protocol (RDP) 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 could allow remote attackers to take full control of the vulnerable systems and make modifications such as install programs, view, and change, delete data or create new accounts.	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/library/security/ms15-082
Vulnerability in Server Message Block Could Allow Remote Code Execution **CVE Info:** CVE-2015-2474	A vulnerability has been identified in Microsoft Windows and can allow execution of arbitrary code if an attacker sends a specially crafted string to the SMB server error logging.	Windows Vista Windows Server 2008	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms15-083
Vulnerabilities in XML Core Services Could Allow Information Disclosure	Multiple vulnerabilities have been reported in Microsoft Windows and Microsoft Office. The vulnerabilities could be exploited by remote attackers to allow information disclosure by	Windows Vista Windows Server 2008 Windows 7	Users are advised to apply updates. More information about the

CVE Info: CVE-2015-2368 CVE-2015-2369	either exposing memory address if a user clicks a specially crafted link or explicitly allowing the use of Secure Sockets Layer (SSL) 2.0. Successful exploitation of the vulnerability requires user interaction such that they have to click on a link by way of an enticement or Instant Messenger message.	Windows Server 2008 R2 Windows 8 and 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1	updates is available in: https://technet.microsoft.com/library/security/ms15-084
Vulnerability in Mount Manager Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1769	A vulnerability has been reported in Microsoft Windows. The vulnerability can allow elevation of privilege if an attacker inserts a malicious USB device into a target system. Successful exploitation of the vulnerability could allow remote attackers to write a malicious binary to disk and execute it.	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 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-085
Vulnerability in System Center Operations Manager Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2420	A vulnerability has been identified in Microsoft System Center Operations Manager. The vulnerability could allow elevation of privilege if a user visits an affected website by way of a specially crafted URL.	Microsoft System Center 2012 Operations Manager Microsoft System Center 2012 Operations Manager R2	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/en-us/library/security/MS15-086
Vulnerability in UDDI Services Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2364	A vulnerability has been identified in Microsoft Windows and can be exploited by remote attackers to allow elevation of privilege if an attacker engineered a cross-site scripting (XSS) scenario by inserting a malicious script into a webpage search parameter. Successful exploitation of the vulnerability requires user interaction such that the user would have to visit a specially crafted webpage where the malicious script would then be executed.	Windows Server 2008 Microsoft BizTalk Server	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-087
Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege	Multiple vulnerabilities have been identified in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application or convinces a user to open	Windows Vista Windows Server 2008 Windows 7 Windows Server	Users are advised to apply updates. More information about the updates is available in:

CVE: CVE-2015-2428 CVE-2015-2429 CVE-2015-2430	a specially crafted file that invokes a vulnerable sandboxed application, allowing an attacker to escape the sandbox.	2008 R2 Windows 8 and Windows 8.1	https://technet.microsoft.com/library/security/MS15-090
Cumulative Security Update for Microsoft Edge **CVE Info:** CVE-2015-2371	Multiple vulnerabilities have been identified in Microsoft Edge. The vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. Successful exploitation of the vulnerabilities can allow remote attackers to gain the same user rights as the current user.	Microsoft Edge	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-091
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2481 CVE-2015-2480 CVE-2015-2479	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 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/library/security/MS15-092

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins
https://technet.microsoft.com/library/security/ms15-079
https://technet.microsoft.com/library/security/ms15-080
https://technet.microsoft.com/library/security/MS15-081
https://technet.microsoft.com/library/security/ms15-082
https://technet.microsoft.com/library/security/ms15-083
https://technet.microsoft.com/library/security/ms15-084
https://technet.microsoft.com/library/security/MS15-085
https://technet.microsoft.com/en-us/library/security/MS15-086
https://technet.microsoft.com/library/security/MS15-087
https://technet.microsoft.com/library/security/MS15-090
https://technet.microsoft.com/library/security/MS15-091
https://technet.microsoft.com/library/security/MS15-092

Security Tracker
http://www.securitytracker.com/id/1033237
http://www.securitytracker.com/id/1033253
http://www.securitytracker.com/id/1033251
http://www.securitytracker.com/id/1033249
http://www.securitytracker.com/id/1033238
http://www.securitytracker.com/id/1033239
http://www.securitytracker.com/id/1033241
http://www.securitytracker.com/id/1033242
http://www.securitytracker.com/id/1033243
http://www.securitytracker.com/id/1033244
http://www.securitytracker.com/id/1033246
http://www.securitytracker.com/id/1033248

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