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

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: September, 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 Internet Explorer CVE-2015-2542 CVE-2015-2541 CVE-2015-2501 CVE-2015-2500 CVE-2015-2499 **Other CVE Info is available on:** https://technet.microsoft.com/library/security/ms15-094	Multiple vulnerabilities have been identified in Internet Explorer and can be exploited to cause remote code execution if a user views a specially crafted webpage using Internet Explorer. Successful exploitation of the vulnerabilities could gain the same user rights as the current user.	Internet Explorer 7, 8,9,10,11	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms15-094
Microsoft Edge Multiple Vulnerabilities **CVE Info:** CVE-2015-2485 CVE-2015-2486 CVE-2015-2542	Multiple vulnerabilities have been identified in Microsoft Edge and could be exploited by remote attackers to allow remote code execution if a user views a specially crafted webpage using Microsoft Edge. Successful exploitation of the vulnerability can allow an attacker 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/ms15-095

Vulnerability in Active Directory Service Could Allow Denial of Service **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 Active Directory. The vulnerability could allow denial of service if an authenticated attacker creates multiple machine accounts.	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 in: https://technet.microsoft.com/library/security/ms15-096
Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution **CVE Info:** CVE-2015-2506 CVE-2015-2507 CVE-2015-2508 CVE-2015-2510 CVE-2015-2511	Multiple vulnerabilities have been identified in Microsoft Windows, Microsoft Office, and Microsoft Lync and could be exploited by remote attackers to allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded OpenType fonts.	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/ms15-097
Vulnerabilities in Windows Journal Could Allow Remote Code Execution **CVE Info:** CVE-2015-2513 CVE-2015-2514 CVE-2015-2516 CVE-2015-2519 CVE-2015-2530	Multiple vulnerabilities have been identified in Microsoft Windows and could be exploited by remote attackers to cause execution of remote code if a user opens a specially crafted Journal file.	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/ms15-098
Vulnerabilities in Microsoft Office Could Allow Remote Code Execution **CVE Info:** CVE-2015-2520 CVE-2015-2521	Several vulnerabilities have been identified in Microsoft Office and can be exploited by remote attackers to cause execution of arbitrary code 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	Microsoft Office 2007 Microsoft Office 2010 Microsoft Office 2013 Microsoft Office	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms1

CVE-2015-2523 CVE-2015-2545	user.	2013 RT Microsoft Excel for Mac 2011 Microsoft Excel for Mac 2016 Microsoft SharePoint Foundation 2013 Microsoft SharePoint Server 2013	5-099
Vulnerability in Windows Media Center Could Allow Remote Code Execution **CVE Info:** CVE-2015-2509	A vulnerability has been reported in Microsoft Windows and can be exploited by remote attackers to cause execution of arbitrary code. The vulnerability can be exploited if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. Successful exploitation of the vulnerability can allow an attacker to gain the same user rights as the current user.	Windows Vista Windows 7 Windows 8	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms15-100
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2504 CVE-2015-2526	Multiple vulnerabilities have been identified in Microsoft .NET Framework and can allow elevation of privilege if a user runs a specially crafted .NET application.	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/ms15-101
Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2524 CVE-2015-2525 CVE-2015-2528	Multiple vulnerabilities have been identified in Microsoft Windows and this could be exploited by remote attackers to gain elevation of privilege if an attacker logs on to a system and runs a specially crafted application.	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/ms15-102

		Windows 10	
Vulnerabilities in Microsoft Exchange Server Could Allow Information Disclosure **CVE Info:** CVE-2015-2505 CVE-2015-2543 CVE-2015-2544	Multiple vulnerabilities have been identified in Microsoft Exchange Server and could allow information disclosure if Outlook Web Access (OWA) fails to properly handle web requests, and sanitize user input and email content.	Microsoft Windows Server 2013	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms15-103
Vulnerabilities in Skype for Business Server and Lync Server Could Allow Elevation of Privilege **CVE Info:** CVE-2015-2531 CVE-2015-2532 CVE-2015-2536	Multiple vulnerabilities have been identified in Skype for Business Server and Microsoft Lync Server. These vulnerabilities could allow elevation of privilege if a user clicks a specially crafted URL. Successful exploitation of the vulnerabilities would allow an attacker to convince users to click a link in an instant messenger or email message that directs them to an affected website by way of a specially crafted URL.	Microsoft Lync Server 2013 Skype for Business Server 2015	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms15-104
Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass **CVE Info:** CVE-2015-1681	A vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if an attacker runs a specially crafted application that could cause Windows Hyper-V to incorrectly apply access control list (ACL) configuration settings.	Windows 8.1 Windows Server 2012 R2 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/ms15-105

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins
https://technet.microsoft.com/library/security/ms15-105
https://technet.microsoft.com/library/security/ms15-104
https://technet.microsoft.com/library/security/ms15-103
https://technet.microsoft.com/library/security/ms15-102
https://technet.microsoft.com/library/security/ms15-101
https://technet.microsoft.com/library/security/ms15-101
https://technet.microsoft.com/library/security/ms15-100

https://technet.microsoft.com/library/security/ms15-099
https://technet.microsoft.com/library/security/ms15-098
https://technet.microsoft.com/library/security/ms15-094

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