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

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: June 11, 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-2015-1687 CVE-2015-1730 CVE-2015-1731 CVE-2015-1732 CVE-2015-1735 CVE-2015-1736 CVE-2015-1737 CVE-2015-1739 CVE-2015-1740 **Other CVE Info is available on:** https://technet.microsoft.com/library/security/MS15-056	Multiple vulnerabilities have been identified in Internet Explorer. These vulnerabilities can be exploited by remote attackers to cause execution of arbitrary code if a user views a specially crafted webpage using Internet Explorer. Successful exploitation of the vulnerabilities could allow remote attackers to gain the same user rights as the current user.	Microsoft Windows, Internet Explorer versions 6-11	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-056
Vulnerability in Windows Media Player Could Allow Remote Code Execution **CVE Info:** CVE-2015-1728	A vulnerability has been reported in Microsoft Windows and can be exploited to cause execution of arbitrary code. This vulnerability could allow remote code execution if Windows Media Player opens specially crafted media content that is hosted on a malicious website. Successful exploitation of the vulnerability can allow complete control of an affected system remotely.	Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-057

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution **CVE Info:** CVE-2015-1759 CVE-2015-1760 CVE-2015-1770	Multiple vulnerabilities have been identified in Microsoft Office and could be exploited by remote attackers to cause execution of arbitrary code if a user opens a specially crafted Microsoft Office file. Successful exploitation of the vulnerabilities could allow an attacker to run arbitrary code in the context of the current user.		Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-059
Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution **CVE Info:** CVE-2015-1756	A vulnerability has been reported in Microsoft Windows and could allow remote attackers to cause execution of arbitrary code if a user clicks a specially link or a link to specially crafted content, and then invokes F12 Developer Tools in Internet Explorer.	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/MS15-060
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1719 CVE-2015-1720 CVE-2015-1721 CVE-2015-1722 CVE-2015-1723	Multiple vulnerabilities have been identified in Microsoft Windows. These vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. Successful exploitation of the vulnerabilities can 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 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/MS15-061
Vulnerability in Active Directory Federation Services Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1757	A vulnerability has been identified in Microsoft Active Directory Federation Services (AD FS). The vulnerability could allow elevation of privilege if an attacker submits a specially crafted URL to a target site. Due to the vulnerability, in specific situations specially crafted script is not properly sanitized, which subsequently could lead to an attacker-supplied script being run in the security context of a user who views the malicious content.	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-062
Vulnerability in Windows	A vulnerability has been identified in Microsoft	Windows Vista	Users are advised to

Kernel Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1758	Windows and could be exploited by remote attackers to gain elevation of privilege if an attacker places a malicious .dll file in a local directory on the machine or on a network share.	Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 Windows Server 2012 Windows RT	apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-063
Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1764 CVE-2015-1771 CVE-2015-2359	Multiple vulnerabilities have been identified in Microsoft Exchange Server and could allow elevation of privilege if an authenticated user clicks a link to a specially crafted webpage. Successful exploitation of the vulnerabilities requires the attacker to convince users to click a link, typically by way of an enticement in an email or Instant Messenger message.	Microsoft Exchange Server 2013 Service Pack 1 Microsoft Exchange Server 2013 Cumulative Update 8	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-064

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins
https://technet.microsoft.com/library/security/MS15-056

https://technet.microsoft.com/library/security/MS15-057

https://technet.microsoft.com/library/security/MS15-059

https://technet.microsoft.com/library/security/MS15-060

https://technet.microsoft.com/library/security/MS15-061

https://technet.microsoft.com/library/security/MS15-062

https://technet.microsoft.com/library/security/MS15-063

https://technet.microsoft.com/library/security/MS15-064

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