National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: November 2014

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 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 Windows OLE Automation Array Bug Lets Remote Users Execute Arbitrary Code **CVE Info:** **CVE-2014-6332**	• 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 to cause execution of arbitrary code. This vulnerability can allow remote attackers to create specially crafted content that, when loaded by the target user, will and execute arbitrary code on the target system. The code will run with the privileges of the target user.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms14-064
Microsoft Internet Explorer Multiple Memory Corruption Flaws	• Internet Explorer versions 6, 7,8,9,10	Multiple vulnerabilities have been identified in Microsoft Internet Explorer and they can be exploited by remote attacker to cause	Users are advised to apply updates. More information is available on:

Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass ASLR Security Protection **CVE Info:** **CVE-2014-6353** **CVE-2014-6351** **CVE-2014-6350** **CVE-2014-6349** **CVE-2014-6348** **CVE-2014-6347** **CVE-2014-6345** **List of other CVE Information is available on:** **http://www.securitytracker.com/id/1031185**		arbitrary code to be executed on the target user's system and determine the installation path. The vulnerabilities reported are as follows: • A vulnerability exists and this can allow a remote attacker to create specially crafted content that when loaded by the target user will trigger a memory corruption error and execute arbitrary code on the target system. The code will run with the privileges of the target user. • A vulnerability occurs that can allow a remote attacker to cause execution of scripts with elevated privileges. • A vulnerability exists that can allow remote attackers to obtain potentially sensitive information from another domain. • A vulnerability occurs that can allow remote attackers to obtain potentially sensitive information from the target user's clipboard. • A vulnerability exists that can allow remote attackers to bypass	https://technet.microsoft.com/library/security/ms14-065

		Address Space Layout Randomization (ASLR) security protection features.	
Windows Schannel Unspecified Flaw Lets Remote Users Execute Arbitrary Code **CVE Info:** **CVE-2014-6321**	• 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 Windows Schannel and this can be exploited by remote attackers to cause execution of arbitrary code on the target system. This vulnerability can allow remote attackers to send specially crafted packets to execute arbitrary code on the affected system.	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/library/security/ms14-066
Microsoft Windows Remote Desktop Protocol (RDP) Security Audit Bypass Weakness **CVE Info:** **CVE-2014-6318**	• Microsoft Windows 7 • Microsoft Windows 8 • Microsoft Windows 8.1 • Microsoft Windows RT • Microsoft Windows RT 8.1 • Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Microsoft Windows Vista	A vulnerability has been identified in Microsoft Windows, which can be exploited by malicious people to bypass certain security restrictions. The vulnerability exists because Remote Desktop Protocol (RDP) fails to properly log audit events.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms14-074
Microsoft .NET Framework TypeFilterLevel Bypass Vulnerability **CVE Info:** **CVE-2014-4149**	• Microsoft .NET Framework 1.x • Microsoft .NET Framework 2.x • Microsoft .NET Framework 3.x • Microsoft .NET Framework 4.x	A vulnerability has been reported in Microsoft .NET Framework and it can be exploited by malicious users to bypass certain security restrictions. The vulnerability is caused due to an error within the .NET Remoting feature, which can be exploited to bypass TypeFilterLevel checks via	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/MS14-072

		specially crafted objects.	
Microsoft SharePoint Foundation Script Insertion Vulnerability **CVE Info:** **CVE-2014-4116**	• Microsoft SharePoint Foundation 2010	A vulnerability has been reported in Microsoft SharePoint Foundation and this can be exploited by malicious users to conduct script insertion attacks. This vulnerability exists because certain input related to page content in SharePoint lists is not properly sanitised before being used. This can be exploited to insert arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when the malicious data is being viewed.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/MS14-073
Microsoft Internet Information Services (IIS) IP and Domain Restrictions Bypass Security **CVE Info:** **CVE-2014-4078**	• Microsoft Windows 8.1 • Microsoft Windows Server 2012 • Microsoft Windows 8	A security issue has been reported in Microsoft Windows, which can be exploited by remote attackers to bypass certain security restrictions. The security issue is caused due to an error within the Microsoft Internet Information Services (IIS) component. This vulnerability can be exploited to bypass the "IP and domain restrictions" security feature and access otherwise restricted resources.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/ms14-076

Microsoft Windows TCP/IP IOCTL Handling Privilege Escalation Vulnerability **CVE Info:** **CVE-2014-4076**	• Microsoft Windows Server 2003 Datacenter Edition • Microsoft Windows Server 2003 Enterprise Edition • Microsoft Windows Server 2003 Standard Edition • Microsoft Windows Server 2003 Web Edition • Microsoft Windows Storage Server 2003	A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to an unspecified error in the tcpip.sys and tcpip6.sys drivers when processing certain IOCTL and can be exploited to execute arbitrary code with the privileges of an affected application.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/MS14-070
Microsoft XML Core Services XML Content Parsing Vulnerability **CVE Info:** **CVE-2014-4118**	• Microsoft XML Core Services (MSXML) 3.x	A vulnerability has been reported in Microsoft XML Core Services and this can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified error when parsing XML content and can be exploited to execute arbitrary code.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/MS14-067

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins

https://technet.microsoft.com/library/security/ms14-064

https://technet.microsoft.com/library/security/MS14-070

https://technet.microsoft.com/library/security/ms14-076

https://technet.microsoft.com/library/security/ms14-065

http://technet.microsoft.com/library/security/ms14-066

https://technet.microsoft.com/library/security/MS14-072

https://technet.microsoft.com/library/security/MS14-067

Secunia

http://secunia.com/advisories/60089/

http://secunia.com/advisories/59805/

http://secunia.com/advisories/59881/

http://secunia.com/advisories/60009/

http://secunia.com/advisories/60354/

Security Tracker

http://www.securitytracker.com/id/1031193

http://www.securitytracker.com/id/1031192

http://www.securitytracker.com/id/1031190

http://www.securitytracker.com/id/1031188

http://www.securitytracker.com/id/1031186

http://www.securitytracker.com/id/1031185

http://www.securitytracker.com/id/1031184

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