National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: February, 2014

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft Products and they can allow a remote attacker 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 Internet Explorer Multiple Vulnerabilities **CVE Info:** **CVE-2014-0293** **CVE-2014-0288** **CVE-2014-0286** **CVE-2014-0283** **CVE-2014-0281** **CVE-2014-0280** **More CVE info:** **http://www.securitytracker.com/id/1029741**	• Microsoft Internet Explorer versions 8,9,10,11	Multiple vulnerabilities have been identified in Microsoft Internet Explorer. The vulnerabilities reported are as follows: • A vulnerability exists that can allow a remote user to create specially crafted HTML that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code Successful exploitation of the vulnerability can allow remote attackers to cause execution of arbitrary code on the vulnerable system. • Another vulnerability occurs that can allow remote	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/en-us/security/bulletin/ms14-010

		attackers to create specially crafted HTML that, when loaded by the target user, will trigger a flaw in the VBScript engine and cause execution of arbitrary code on the target system. The code will run with the privileges of the target user. • A vulnerability exists that can allow remote attackers to create specially crafted HTML that, when loaded by the target user, will access potentially sensitive information from a different domain. • A vulnerability exists that can allow remote attackers to leverage other vulnerabilities and exploit a permission validation flaw to run scripting code with elevated privileges.	
Microsoft Windows Direct2D Bug Lets Remote Users Execute Arbitrary Code **CVE Info:** **CVE-2014-0263**	• Microsoft Windows Direct2D versions 7 SP1, 2008 R2 SP1, 8, 8.1, 2012 R2, RT, RT 8.1	A vulnerability has been identified in Microsoft Windows Direct2D that can allow remote attackers to cause execution of arbitrary code on the target user's system. The vulnerability can allow remote attackers to create a file containing specially crafted specially crafted 2D geometric figures that when loaded by the target user will cause execution of 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: http://technet.microsoft.com/en-us/security/bulletin/ms14-007

Microsoft Forefront Protection for Exchange Scanning Parsing Flaw Lets Remote Users Execute Arbitrary Code **CVE Info:** **CVE-2014-0294**	• Microsoft Forefront Protection 2010 for Exchange Server	A vulnerability has been identified in Microsoft Forefront Protection for Exchange. The vulnerability can allow a remote attacker to send a specially crafted email message to a target system that is monitored by Microsoft Forefront Protection 2010 for Exchange to trigger a parsing flaw. Successful exploitation of the vulnerability can allow execution of arbitrary code on the target system when the email message is scanned. The code will run with the privileges of the configured service account.	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/en-us/security/bulletin/ms14-008
Microsoft .NET Bugs Lets Remote Users Execute Arbitrary Code and Deny Service **CVE Info** **CVE-2014-0253** **CVE-2014-0257** **CVE-2014-0295**	• Microsoft .NET versions 1.0 SP3, 2.0 SP2, 3.5, 3.5.1, 4.0, 4.5, 4.5.1	Three vulnerabilities has been identified in Microsoft .NET and they can be exploited by remote attackers to cause execution of arbitrary code by the user's system, cause a denial of service condition and bypass security features. The vulnerabilities reported are as follows: A vulnerability occurs that can allow remote attackers to send specially crafted HTTP POST requests to cause the target ASP.NET server to stop responding to client requests. Two vulnerabilities exist that can allow remote attackers to create specially crafted HTML or a Windows .NET application that when loaded by the target user will cause execution of arbitrary code on the target system. The code will run with	Users are advised to apply updates. More information is available on: http://technet.microsoft.com/en-us/security/bulletin/ms14-009

		the privileges of the target user.	
Microsoft XML Core Services (MSXML) Bug Lets Remote Users Obtain Potentially Sensitive Information **CVE Info:** **CVE-2014-0266**	• Microsoft XML Core Services (MSXML)	A vulnerability has been identified in Microsoft XML Core Services (MSXML) and this can be exploited by remote user to obtain potentially sensitive information. The vulnerability can allow remote attackers to create specially crafted HTML that when loaded by the user via Internet Explorer will read files on the target user's local system or read content of web domains with the privileges of the target user.	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/en-us/security/bulletin/ms14-005
Microsoft Windows IPv6 Stack Flaw Lets Remote Users Deny Service **CVE Info:** **CVE-2014-0254**	• Windows IPv6 Stack	A vulnerability has been identified in the Windows IPv6 Stack and this can be exploited by remote user to cause denial of service conditions. The vulnerability can allow remote attackers to send specially crafted IPv6 router advertisement packets via a target subnet to cause systems on the target subnet to stop responding.	Users are advised to apply updates. More information about the updates is available on: http://technet.microsoft.com/en-us/security/bulletin/ms14-006

Vendor Information

Microsoft

www.microsoft.com

References

Microsoft Security Bulletins

http://technet.microsoft.com/en-us/security/bulletin/ms14-010

http://technet.microsoft.com/en-us/security/bulletin/ms14-007

http://technet.microsoft.com/en-us/security/bulletin/ms14-008

http://technet.microsoft.com/en-us/security/bulletin/ms14-009

http://technet.microsoft.com/en-us/security/bulletin/ms14-005

http://technet.microsoft.com/en-us/security/bulletin/ms14-006

Security Tracker

http://www.securitytracker.com/id/1029741

http://www.securitytracker.com/id/1029743

http://www.securitytracker.com/id/1029744

http://www.securitytracker.com/id/1029745

http://www.securitytracker.com/id/1029746

http://www.securitytracker.com/id/1029747

Secunia

http://secunia.com/advisories/56771/

http://secunia.com/advisories/56793/

http://secunia.com/advisories/56796/

http://secunia.com/advisories/56781/

http://secunia.com/advisories/56788/

http://secunia.com/advisories/56814/

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-mu.gov.mu.

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info : info@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: www.cert-mu.org.mu