National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: July 9, 2013

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, cause a denial of service condition and gain elevated privileges. Microsoft has released an update that addresses all the vulnerabilities. The vulnerabilities reported are as follows:

Vulnerability	Systems Affected	Description	Workarounds
.NET Framework and Silverlight Multiple vulnerabilities **CVE Info:** CVE-2013-3129 CVE-2013-3131 CVE-2013-3132 CVE-2013-3133 CVE-2013-3171 CVE-2013-3178	• Microsoft .NET Framework 1.0 Service Pack 3 • Microsoft .NET Framework 1.1 Service Pack 1and .NET Framework 3.5 Service Pack 1 • Microsoft .NET Framework 2.0 Service Pack 2 • Microsoft .NET Framework 3.0 Service Pack 2 • Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5.1 • Microsoft .NET Framework 4, and Microsoft .NET Framework 4.5	Multiple vulnerabilities have been identified in Microsoft .NET Framework and Silverlight and they can be exploited by remote attackers to cause execution of arbitrary code on the affected system. Successful exploitation of this vulnerability can allow the remote attackers have same user right as the logged-on user users who operate with administrator rights will be highly impacted.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-052

Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution **CVE Info:** CVE-2013-1300 CVE-2013-1340 CVE-2013-1345 CVE-2013-3129 CVE-2013-3167 CVE-2013-3172 CVE-2013-3173	• Windows XP • Windows Server 2003 • Windows Vista • Windows Server 2008 • Windows 7 • Windows Server 2008 R2 • Windows 8 • Windows Server 2012 • Windows RT	Multiple vulnerabilities have been identified in Windows Kernel-Mode Drivers. These vulnerabilities can be exploited by remote attackers to take complete control of an affected system.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-053
Vulnerability in GDI+ Could Allow Remote Code Execution **CVE Info:** **CVE-2013-3129**	• Windows XP • Windows Server 2003 • Windows Vista • Windows Server 2008 • Windows 7 • Windows Server 2008 R2 • Windows 8 • Windows Server 2012 • Microsoft Communications Platforms	A vulnerability has been identified in Microsoft Windows, Microsoft Office, Microsoft Lync, and Microsoft Visual Studio. It can be exploited by remote attackers to execute code if a user views shared content that embeds TrueType font files.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-054
Cumulative Security Update for Internet Explorer **CVE Info** CVE-2013-3115 CVE-2013-3143 CVE-2013-3144 CVE-2013-3145 CVE-2013-3146 CVE-2013-3164 CVE-2013-3166	Internet Explorer 6 , 7, 8, 9, 10	Multiple vulnerabilities have been identified in Microsoft Internet Explorer that can allow remote code execution if a user views a specially crafted web page using Internet Explorer. Moreover, they can also gain same user rights as the current user.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-055

Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution **CVE Info:** CVE-2013-3174	• Windows XP • Windows Server 2003 • Windows Vista • Windows Server 2008 • Windows 7 • Windows Server 2008 R2 • Windows 8 • Windows Server 2012	This vulnerability could allow remote code execution if a user opens a specially crafted image file. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-056
Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution **CVE Info:** CVE-2013-3127	• Windows XP • Windows Server 2003 • Windows Vista • Windows Server 2008 • Windows 7 • Windows Server 2008 R2 • Windows 8 • Windows Server 2012 • Windows RT	Windows Media Format Runtime has a flaw which could allow remote code execution if a user opens a specially crafted media file. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-057
Vulnerability in Windows Defender Could Allow Elevation of Privilege **CVE Info:** CVE-2013-3154	Windows Defender for Windows 7 and Windows Server 2008 R2	A vulnerability exists in Windows Defender that could allow elevation of privilege. This vulnerability occurs because of the pathnames used by Windows Defender. Successful exploitation of this vulnerability could cause execution of arbitrary code and take complete control of an affected system. The attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. However the latter needs valid logon credentials to exploit this vulnerability.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/en-us/security/bulletin/ms13-058

Vendor Information

Microsoft

www.microsoft.com

References

Microsoft Security Bulletins

https://technet.microsoft.com/en-us/security/bulletin/ms13-052

https://technet.microsoft.com/en-us/security/bulletin/ms13-053

https://technet.microsoft.com/en-us/security/bulletin/ms13-054

https://technet.microsoft.com/en-us/security/bulletin/ms13-055

https://technet.microsoft.com/en-us/security/bulletin/ms13-056

https://technet.microsoft.com/en-us/security/bulletin/ms13-057

https://technet.microsoft.com/en-us/security/bulletin/ms13-058

Symantec - Blog

http://www.symantec.com/connect/blogs/microsoft-patch-tuesday-july-2013

Cisco - Event Response

http://www.cisco.com/web/about/security/intelligence/ERP_jul13.html

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