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

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: September 2014

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft Products and they can be exploited by remote attackers to cause denial of service conditions, cause execution of arbitrary code, and gain elevation of privilege. An update has been released by Microsoft to address all the issues.

The vulnerabilities reported are as follows:

Vulnerability	Systems Affected	Description	Workarounds
Multiple Vulnerabilities in Internet Explorer **CVE Info:** **CVE-2013-7331** **CVE-2014-2799** **CVE-2014-4059** **CVE-2014-4065** **List of other CVE Info:** https://technet.microsoft.com/library/security/MS14-052	• **Internet Explorer versions 6 to 11**	Multiple vulnerabilities have been identified in Microsoft Internet Explorer. These vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. Successful exploitation of these vulnerabilities could allow gaining the same user rights as the current user.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS14-052

Vulnerability in .NET Framework Could Allow Denial of Service **CVE Info:** **CVE-2014-4072**	• 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 .NET Framework and this could allow a denial of service if a remote attacker sends a small number of specially crafted requests to a vulnerable .NET-enabled website.	Users are advised to apply updates. More information is available on: https://technet.microsoft.com/library/security/MS14-053
Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege **CVE Info:** **CVE-2014-4074**	• 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 and this can be exploited to cause elevation of privilege on vulnerable systems. This vulnerability can allow an attacker to run a specially crafted application and cause elevation of privilege. To successfully exploit this vulnerability valid logon credentials are required.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS14-054
Vulnerabilities in Microsoft Lync Server Could Allow Denial of Service **CVE Info:** **CVE-2014-4068** **CVE-2014-4070** **CVE-2014-4071**	• Microsoft Lync Server 2010 • Microsoft Lync Server 2013	Multiple vulnerabilities have been identified in Microsoft Lync Server and they can be exploited by remote attackers to cause a denial of service condition. These vulnerabilities can allow a remote attacker to send specially crafted request to a vulnerable Lync server and cause denial of service.	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS14-055

Vendor Information

Microsoft
www.microsoft.com

References

Microsoft Security Bulletins

https://technet.microsoft.com/library/security/MS14-055

https://technet.microsoft.com/library/security/MS14-054

https://technet.microsoft.com/library/security/MS14-053

https://technet.microsoft.com/library/security/MS14-052

https://technet.microsoft.com/en-us/library/security/ms14-sep.aspx

Security Tracker

http://www.securitytracker.com/id/1030818

http://www.securitytracker.com/id/1030819

http://www.securitytracker.com/id/1030821

Symantec

http://www.symantec.com/connect/blogs/microsoft-patch-tuesday-september-2014

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. : contact@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: www.cert-mu.org.mu