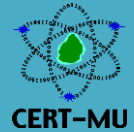




**National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)**



Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: April 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
Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution CVE Info: CVE-2014-1757 CVE-2014-1758 CVE-2014-1761	<ul style="list-style-type: none"> • Microsoft Office 2003 • Microsoft Office 2007 • Microsoft Office 2010 • Microsoft Office 2013 • Microsoft Office 2013 RT • Microsoft Office for Mac • Microsoft SharePoint Server 2010 Service Pack 1 • Microsoft SharePoint Server 2013 • Microsoft Office Web Apps 2010 • Microsoft Office Web Apps 2013 	<p>Multiple vulnerabilities have been identified in Microsoft office. The most severe of these vulnerabilities could allow remote code execution if a specially crafted file is opened or previewed in a vulnerable version of Microsoft Office software. Successful exploitation of these vulnerabilities can allow a remote attacker to gain the same user rights as the current user.</p>	<p>Users are advised to apply updates. More information about the updates is available on:</p> <p>http://technet.microsoft.com/en-us/security/bulletin/ms14-017</p>

<p>Multiple Vulnerabilities in Microsoft Internet Explorer</p> <p>CVE Info:</p> <p>CVE-2014-0235 CVE-2014-1751 CVE-2014-1753 CVE-2014-1755 CVE-2014-1760</p>	<p>Internet Explorer 6, 7,8 for:</p> <ul style="list-style-type: none"> • Windows XP Service Pack 3 • Windows XP Professional x64 Edition Service Pack 2 • 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 	<p>Several vulnerabilities have been reported in Internet Explorer. These vulnerabilities could allow execution of remote code if a user views a specially crafted webpage using Internet Explorer. Successful exploitation of these vulnerabilities could gain the same user rights as the current user.</p>	<p>Users are advised to apply updates. More information is available on:</p> <p>https://technet.microsoft.com/en-us/security/bulletin/ms14-018</p>
<p>Vulnerability in Microsoft Publisher Could Allow Remote Code Execution</p> <p>CVE Info:</p> <p>CVE-2014-1759</p>	<ul style="list-style-type: none"> • Microsoft Office 2003 Service Pack 3 • Microsoft Office 2007 Service Pack 3 	<p>A vulnerability has been identified in Microsoft Office. This vulnerability could allow remote attackers to cause execution of remote code if a user opens a specially crafted file in an affected version of Microsoft Publisher. Successful exploitation of the vulnerability can allow remote attackers to gain the same user rights as the current user.</p>	<p>Users are advised to apply updates. More information about the updates is available on:</p> <p>http://technet.microsoft.com/en-us/security/bulletin/ms14-020</p>

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins

<http://technet.microsoft.com/en-us/security/bulletin/ms14-apr>

<http://technet.microsoft.com/en-us/security/bulletin/ms14-017>

<https://technet.microsoft.com/en-us/security/bulletin/ms14-018>

<http://technet.microsoft.com/en-us/security/bulletin/ms14-020>

Security Tracker

<http://www.securitytracker.com/id/1030034>

<http://www.securitytracker.com/id/1030033>

<http://www.securitytracker.com/id/1030032>

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