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

CERT-MU

Targeted Security Alert

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: May 13, 2015

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 knowledge of sensitive information, take full control of the affected systems and bypass security restrictions. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Multiple Vulnerabilities in Internet Explorer CVE-2015-1686 CVE-2015-1684 CVE-2015-1658 CVE-2015-1688 CVE-2015-1689 CVE-2015-1691 **Other CVE Info is available on:** https://technet.microsoft.com/library/security/MS15-043	Multiple vulnerabilities have been identified in Internet Explorer and can be exploited to cause remote code execution if a user views a specially crafted webpage using Internet Explorer. Successful exploitation of the vulnerabilities could gain the same user rights as the current user.	Microsoft Windows, Internet Explorer	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-043
Multiple Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution **CVE Info:** CVE-2015-1670 CVE-2015-1671	Multiple vulnerabilities have been identified in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Microsoft Lync, and Microsoft Silverlight. The most severe vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded TrueType fonts.	Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Microsoft Lync, Microsoft Silverlight	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-044
Vulnerability in Windows Journal Could Allow	Multiple vulnerabilities have been reported in Microsoft Windows. The vulnerabilities could	Microsoft Windows	Users are advised to apply updates. More

Remote Code Execution **CVE Info:** CVE-2015-1675 CVE-2015-1695 CVE-2015-1696 CVE-2015-1697 CVE-2015-1698 CVE-2015-1699	be exploited by remote attackers to cause remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.		information about the updates is available in: https://technet.microsoft.com/library/security/MS15-045
Vulnerabilities in Microsoft Office Could Allow Remote Code Execution **CVE Info:** CVE-2015-1699 CVE-2015-1683	Multiple vulnerabilities have been reported in Microsoft Office and could be exploited to cause execution of remote code if a user opens a specially crafted Microsoft Office file. Successful exploitation of the vulnerability could allow running arbitrary code in the context of the current user.	Microsoft Office	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-046
Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution **CVE Info:** CVE-2015-1700	Multiple vulnerabilities have been identified in Microsoft Office server software. The vulnerabilities could allow remote code execution if an authenticated attacker sends specially crafted page content to a SharePoint server. Successful exploitation of the vulnerabilities could allow attackers to run arbitrary code in the security context of the W3WP service account on the target SharePoint site.	Microsoft Server Software	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-047
Vulnerabilities in .NET Framework Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1672 CVE-2015-1673	Several vulnerabilities have been identified in Microsoft .NET Framework. The vulnerabilities could be exploited by remote attackers to cause elevation of privilege if a user installs a specially crafted partial trust application.	Microsoft Windows, Microsoft .NET Framework	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-048
Vulnerability in Silverlight Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1715	Multiple vulnerabilities have been identified in Microsoft Silverlight. The vulnerability could be exploited to cause elevation of privilege if a specially crafted Silverlight application is run on an affected system.	Microsoft Silverlight	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-049

Vulnerability in Service Control Manager Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1702	A vulnerability has been identified in Windows Service Control Manager (SCM), which is caused when SCM improperly verifies impersonation levels. The vulnerability could allow elevation of privilege if an attacker first logs on to the system and then runs a specially crafted application designed to increase privileges.	Microsoft Windows	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-050
Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege **CVE Info:** CVE-2015-1676 CVE-2015-1677 CVE-2015-1678 CVE-2015-1679 CVE-2015-1680 CVE-2015-1701	Multiple vulnerabilities have been identified in Microsoft Windows. These vulnerabilities could be exploited by remote attackers to cause elevation of privilege if an attacker logs on locally and runs arbitrary code in kernel mode. Successful exploitation of the vulnerability can allow an attacker to install programs; view, change, or delete data; or create new accounts with full user rights.	Microsoft Windows	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-051
Vulnerability in Windows Kernel Could Allow Security Feature Bypass **CVE Info:** CVE-2015-1674	A vulnerability has been identified in Microsoft Windows and this could be exploited by remote attackers to bypass security feature an attacker logs on to an affected system and runs a specially crafted application.	Microsoft Windows	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-052
Vulnerabilities in JScript and VBScript Scripting Engines Could Allow Security Feature Bypass **CVE Info:** CVE-2015-1684 CVE-2015-1686	Several vulnerabilities have been identified in Jscript and VBScript Engines and they could be exploited by remote attackers to cause execution of arbitrary code. The vulnerability exists because of the ASLR security feature bypasses in the JScript and VBScript scripting engines in Microsoft Windows. An attacker could use one of these ASLR bypasses in conjunction with another vulnerability, such as a remote code execution vulnerability, to more reliably run arbitrary code on a target system.	Microsoft Windows	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-053
Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service **CVE Info:** CVE-2015-1681	A vulnerability has been identified in Microsoft Windows. The vulnerability could allow denial of service if a remote, unauthenticated attacker convinces a user to open a share containing a specially crafted *.msc* file. However, an attacker would have no way of forcing a user to visit the share or view the file.	Microsoft Windows	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-054

Vulnerability in Schannel Could Allow Information Disclosure **CVE Info:** CVE-2015-1716	A vulnerability has been identified in Microsoft Windows and this could allow information disclosure when Secure Channel (Schannel) allows the use of a weak Diffie-Hellman ephemeral (DFE) key length of 512 bits in an encrypted TLS session. Allowing 512-bit DHE keys makes DHE key exchanges weak and vulnerable to various attacks. A server needs to support 512-bit DHE key lengths for an attack to be successful; the minimum allowable DHE key length in default configurations of Windows servers is 1024 bits.	Microsoft Windows	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS15-055

Vendor Information
Microsoft
www.microsoft.com

References

Microsoft Security Bulletins
https://technet.microsoft.com/library/security/MS15-055

https://technet.microsoft.com/library/security/MS15-054

https://technet.microsoft.com/library/security/MS15-053

https://technet.microsoft.com/library/security/MS15-052

https://technet.microsoft.com/library/security/MS15-051

https://technet.microsoft.com/library/security/MS15-050

https://technet.microsoft.com/library/security/MS15-049

https://technet.microsoft.com/library/security/MS15-048

https://technet.microsoft.com/library/security/MS15-047

https://technet.microsoft.com/library/security/MS15-046

https://technet.microsoft.com/library/security/MS15-045

https://technet.microsoft.com/library/security/MS15-044

https://technet.microsoft.com/library/security/MS15-043

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