CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Date: 24 January, 2017

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft products and they can be exploited by attackers to cause execution of arbitrary code, bypass security measures, take full control of the affected systems, obtain Elevation of Privilege and cause denial of service condition. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Vulnerability in Microsoft Edge **CVE Info:** CVE-2017-0002	A vulnerability has been identified in Microsoft Edge and could allow remote attackers to cause code execution if a user views a specially crafted webpage using Microsoft Edge. Successful exploitation of this vulnerability could allow the remote attacker to gain elevated privilege on the target system.	Windows 10 Windows Server 2016	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/MS17-001
Vulnerability in Microsoft Office **CVE Info:** CVE-2017-0003	A vulnerability has been identified in Microsoft Office and could allow remote code execution if a user opens a specially crafted Microsoft Office file. Successful exploitation of the vulnerability could allow remote attackers to run arbitrary code in context of the current user.	Microsoft Office 2016 Microsoft SharePoint Enterprise Server 2016	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/ms17-002

Multiple Vulnerabilities in Adobe Flash Player **CVE Info:** CVE-2017-2925 CVE-2017-2926 CVE-2017-2927 More CVE available on: https://technet.microsoft.com/library/security/ms17-003	Multiple vulnerabilities have been identified in Adobe Flash Player. These vulnerabilities could allow a remote attacker to bypass security restrictions, access sensitive information and execute arbitrary code on the target system. Successful exploitation of these vulnerabilities could allow a remote attacker to take control of the affected system	Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT 8.1 Windows 10 Windows Server 2016	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/ms17-003 https://helpx.adobe.com/security/products/flash-player/apsb17-02.html
Vulnerability in Local Security Authority Subsystem Service (LSASS) **CVE Info:** CVE-2017-0004	A denial of service vulnerability exists the Local Security Authority Subsystem Service (LSASS) due to the improper handling of authentication requests. Successful exploitation of the vulnerability would allow an attacker to cause a denial of service on the target system's LSASS service, which triggers an automatic reboot of the system.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2	Users are advised to apply updates. More information about the updates is available on: https://technet.microsoft.com/library/security/ms17-004

Source:

Microsoft Security Bulletin

https://technet.microsoft.com/en-us/library/security/ms17-jan.aspx

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: http://cert-mu.org.mu