Tonga National Computer
Emergency Response Team

Cert.to Advisory

Dear Constituents,

Security updates has been released by Microsoft Windows to address vulnerabilities within Windows system that could be exploited to course harm. Multiple vulnerabilities has been reported which could be exploited by a remote attacker to cause DoS, and potentially obtaining information and execute code on targeted system.

This month's Security Updates cover vulnerabilities in Microsoft's Windows operating systems, Internet Explorer, Microsoft Edge, Microsoft SharePoint, Adobe Flash Player, Windows Hyper-V and Microsoft SQL

This month's Security Updates include critical updates for the following vulnerabilities:
(*You can also visit https://portal.msrc.microsoft.com/en-us/security-guidance for the complete list of vulnerabilities that the updates addresses.*)

CVE-2017-8620 Windows Search Remote Code Execution Vulnerability

The most serious vulnerability exists when Windows Search handles objects in memory. An attacker who successfully exploited this vulnerability could take control of the affected system. An attacker could then install programs and allow arbitrary code and compromise the system completely.

CVE-2017-8633: Windows Error Reporting Elevation of Privilege Vulnerability

This vulnerability resides in Windows Error Reporting, that could allow an attacker to run a specially created application to gain access to administrator privileges on the targeted system to steal sensitive information.

CVE-2017-8627: Windows Subsystem for Linux DoS Vulnerability

This vulnerability has been identified in Windows Subsystem for Linux that could allow an attacker to execute code with elevated permissions. Eventually it could allow denial of service, and may lead to targeted system unresponsive.

Solution

For installing **security updates**, simply head on to:

Settings → Update & security → Windows Update → Check for updates, or install the updates manually.

Apply appropriate software fixes as available on vendors website

- https://portal.msrc.microsoft.com/en-us/security-guidance
- https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/b3d96835-f651-e711-80dd-000d3a32fc99

Reminders

(1) Use genuine Windows installation

(2) Use of updated anti-virus programs

(3) Regular back up of data

(4) Take caution when opening emails even when it seem like it's from a known source.

Reference

http://thehackernews.com/2017/08/microsoft-security-patch.html

https://portal.msrc.microsoft.com/en-us/security-guidance

http://cve.mitre.org/

https://nvd.nist.gov/vuln/full-listing/2017/8

Contact Detail

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378
email: cert@cert.to
Website:www.cert.to