PTA CERT for Telecom Sector

Security Advisory-No: Ext:148-18

12, Sep 2018

Threat Classification: Vulnerability

Name:

1) Scripting Engine Memory Corruption Vulnerability (CVE-2018-8242)
2) Microsoft Edge Memory Corruption Vulnerability (CVE-2018-8262)
3) Chakra Memory Corruption Vulnerability (CVE-2018-8280)
4) Microsoft Edge Memory Corruption Vulnerability (CVE-2018-8301)
5) Microsoft Edge Information Disclosure Vulnerability (CVE-2018-8324)
6) PowerShell Editor Services Remote Code Execution Vulnerability (CVE-2018-8327)

Overview

Cyber Security researchers have discovered critical Vulnerabilities in Microsoft Windows, Microsoft Office, internet explorer (IE), power shell, visual studio and adobe flash player.
These vulnerabilities facilitate a remote attacker to execute malicious code on vulnerable system.

Technical Analysis

a) Critical issues are observed due to memory corruption flaws in Internet explorer, edge browser and chakra scripting engine.
b) A critical flaw (CVE-2018-8327) affects Power Shell editor services that could allow a remote attacker to execute malicious code on vulnerable system.

Affected Products These vulnerabilities affect Microsoft Windows and following software's:

a) Internet Explorer IE
b) ChakraCore
c) Microsoft .NET Framework
d) Power Shell
e) Visual Studio
f) Microsoft Office
g) Adobe Flash Player
h) Microsoft Share Point ASP .NET
i) ASP.NET

Recommendations

a) All vendors have released security patches; it is strongly advised to update against these vulnerabilities.
b) For updating Microsoft Windows, go to Setting ▸ Update & Security ▸ Windows ▸ Updates ▸ Check for updates.
c) Install and update well-reputed antivirus such as Kaspersky, Bitdefender, Nod32 and Avast etc.
d) Regularly update all software's including Windows OS and Microsoft Office.
e) Don't download attachments from unknown emails source.
f) In case of any incident, please report to this office.