PTA CERT for Telecom Sector

Security Advisory-No: Ext-L-64-31 04, Jan 2019

Threat Classification: Vulnerability

Name: IE Zero-day - Scripting Engine Memory Corruption Vulnerability (CVE-2018-8653)

Overview:

Microsoft released an emergency software patch to plug a critical security hole in its Internet Explorer (IE) Web browser that attackers are already using to break into Windows computers.

Description:

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website, for example, by sending an email.

The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.

Affected Version:

a) Internet Explorer 11 from Windows 7 to Windows 10, Windows Server 2012/2016/2019

b) IE 9 on Windows Server 2008

c) IE 10 on Windows Server 2012

Mitigation:

To address the vulnerability Microsoft has released updates could be found on the link below:

- https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8653

Recommendations:

a) Apply windows updated as soon as possible.
b) In case of any incident, please report to this office.