22 Oct 2019

MINISTRY OF DEFENCE
CYBER CELL

SECURITY ADVISORY 10/2019
MULTIPLE VULNERABILITIES IN MICROSOFT INTERNET EXPLORER

1. It is learnt from a reliable official source that multiple vulnerabilities are observed in Microsoft Internet Explorer which could be used by a remote attacker to spoof web content or execute arbitrary code on a targeted system. The details of the OS affected are as follows:-

(a) Windows 7 (32/64 bit) Service Pack I.
(b) Windows RT 8.1 and Windows 8.1 (32/64 bit)
(c) Windows Server 2008 R2 64 bit Service Pack I
(d) Windows Server 2008 (32/64 bit) Service Pack II
(e) Windows Server 2012 & Windows Server 2012 R2
(f) Windows Server 2016 & 2019
(g) Windows 10 (32/ 64 bit) version 1703,1709,1803,1809 & 1903

2. The list of vulnerabilities include the following:-
(a) Memory Corruption Vulnerabilities (CVE-2019-1367 CVE-2019-1371)
(b) Spoofing Vulnerabilities (CVE-2019-0608 CVE-2019-1357)
(c) VBScript Engine Remote Execution Vulnerabilities (CVE-2019-1238 CVE-2019-1239)

3. **Solution**. It is requested that appropriate patches as mentioned in the Microsoft Security Bulletin (*https://portal.msrc.microsoft.com/en-US/security-guidance*) may be downloaded and the same may be used for patching the Operating Systems as listed above. The advisory may be disseminated to all the concerned in the MoD. IT / EDP sections are advised to undertake patch management of affected systems accordingly.