21Oct 2019

MINISTRY OF DEFENCE
CYBER CELL

SECURITY ADVISORY 08/2019
MICROSOFT DEFENDER DENIAL OF SERVICE VULNERABILITY

1. It is learnt from reliable official source that a denial of service vulnerability has been reported in Microsoft Defender which could allow an attacker to prevent legitimate accounts from executing legitimate system binaries. This vulnerability exists when Microsoft Defender improperly handles files. An attacker could exploit this vulnerability by execution on the affected system. Successful exploitation of this vulnerability could allow an attacker to cause a denial of service on the affected system. The details of the OS affected are as follows:-

(a) Most versions of Windows 10 32 bit systems and x64 based systems
(b) Windows 8.1 32 bit systems and 64 bit systems
(c) Most versions of Windows 2008 serves of 32 bit and x64 bit systems
(d) Windows 7 32 bit and x64 bit systems
(e) Most versions of Windows server 2012
(f) Most versions of Windows server 2016 (Server Core installation) and Windows server 2019 (Server Core installation).
(g) Windows RT 8.1

2. For additional information and to apply appropriate patches for above mentioned vulnerability please visit the URL mentioned below.

https://portal.msrc.microsft.com/en-US/security-guidance.

3. 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.