Subject: **Prevention Against Cyber Attack — Eternalblue Exploit in Windows (Advisory No. 08) August, 2017**

1. **Introduction.** Eternalblue is an exploit developed by National Security Agency (NSA) of USA that is used for hacking any unpatched Windows PC / Servers in a network ***without any user interaction.***

2. **Threats Posed by Eternalblue Vulnerability**

   a. The exploit is available for public use and any computer savvy person can use it to hack PCs / Servers.

   b. The exploit is being used in two cyber-attacks which are **Wannacry & Petya Ransomware Attack.** The attacks have infected millions of computers in more than 150 countries.

   c. The hack is very successful as majority of **end users** and **network administrator don't update Windows OS** and **don't maintain backup of critical data.**

   d. The problem is more pronounced in case of **isolated / offline networks** where OS upgrade on Servers (dedicated and VMs) is difficult.

3. **Recommendations.** *Most important measures to secure against this cyber-attack are to* ***update Windows OS*** *and* ***Data Backup on periodic basis.*** However, detailed recommendations are mentioned below:-

a. **Recommendations for End Users**

(1) Update all Windows OS (Win XP, 7, 8, 8.1, 10, 2003 and 2008) using official update feature.

(2) Maintain regular offline backups or centralized offline backup of critical data.

(3) Disable windows SMB service by adding the following two registry keys.

(a) HKEY_ LOCAL_ MACHINE\SYSTEM\Current Control Set\Services\LanmanServer\Parameters.

i. Smb1
REG_DWORD: 0 = Disabled
REG_ DWORD: 1 = Enabled
Default: 1 = Enabled

ii. Smb2
REG DWORD: 0 = Disabled
REG DWORD: 1 = Enabled
Default: 1 = Enabled

(4) Disable "Turn on fast startup" feature in Windows.

(5) To disable WMIC (Windows Management Instrumentation Command-line), steps given below be followed:-

(a) Go to Administrative Tools -> Computer Management.
(b) Expand 'Services and Applications'
(c) Right click for Properties on 'WMI Control'.
(d) Select the Security tab

(e) Press the Security button

(f) Uncheck Remote Enable

(6) Install and update reputable antivirus like Kaspersky, AVAST, Avira, ESET etc.

(7) Install and regularly update software firewall such as Comodo Firewall or Zonealarm or at least keep windows firewall enabled.

(8) Update all third party applications with the latest patches.

(9) Do not open email attachments from untrusted sources.

(10) Disable macros in all office applications such as Word, PowerPoint, Excel etc.

(11) If a computer has been infected, disconnect it from the network to prevent the malware from spreading and apply the latest decryption tools available online.

b. **Recommendations For System Administrators**

(1) Install official updates in all Windows Server may it be dedicated or VM based server.

(2) Windows OS MUST be updated in isolated / segregated networks as well.

(3) Maintain backups of critical data using central NAS or other storages.

(4) Windows Servers must never be used for personal tasks such as checking emails, surfing web or downloading etc.

(5) Disconnect those systems from network that cannot be updated.

(6) Configure perimeter firewalls (or routers) to block all inbound traffic on Port 445 even for servers hosted in DMZ.

(7) Turn off a windows feature in control panel by unchecking "SMB 1.0/CIFS File Sharing Support" in "Program and Features" tool if not required.

(8) To disable SMBv1 on the SMB server, configure the following registry key:

(a) Registry subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\ParametersRegistry entry: SMB1
REG_DWORD: 0= Disabled
REG_ DWORD: 1 = Enabled
Default: 1 = Enabled

(9) To disable SMBv2 on the SMB server, configure the following registry key:

(a) Registry

subkey:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\ParametersRegistry entry: SMB2
REG_DWORD: 0 = Disabled
REG_DWORD: 1 = Enabled
Default: 1 = Enabled

(10) Restrict users' permissions to install and run unwanted applications.

(11) Actively monitor and validate traffic, going in and out of the network.

(12) Whitelist the WannaCry killswitch domains in network firewalls:-

(a) www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

(b) www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

(13) Educate users on prevention against cyber threats specially phishing email having lucrative offers.

(14) Employ data categorization and network segmentation to mitigate further exposure and damage to data.

(15) Steps mentioned below be followed to disable WMIC, if not required:-

(a) On the target server, go to Administrative Tools -> Computer Management.

(b) Expand 'Services and Applications'

(c) Right click for Properties on 'WMI Control'.

(d) Select the Security tab

(e) Press the Security button

(f) Uncheck Remote Enable