Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No 20) Apr 18**

1. **Introduction.** A critical vulnerability in **Windows Remote Assistance XXE** feature has been discovered which affects all versions of Windows. Windows Remote Assistance (Quick Assist) is a built-in tool that allows anyone to take remote control and resolve system issues over the web. Attacker can simply send crafted invitation containing malicious payload tricking the targeted computer.

2. **Affected Products.** Vulnerability affects following versions of Microsoft Operating System as under:-

a. Microsoft Windows Server 2016.

b. Windows Server 2012 and R2.

c. Windows Server 2008 SP2 and R2SP1.

d. Windows 10 (32- and 64-bit).

e. Windows 8.1 (32- and 64-bit) and RT 8.1.

f. Windows 7 (32- and 64-bit).

3. **Technical analysis**

a. Vulnerability details are as under:-

(1) CVE Number-CVE-2018-0878.

(2) Vulnerability Impact: Remote Access.

b. Exploit involves how Windows Remote Assistance processes XML External Entities (XXE) where attacker can access sensitive documents.

c. Exploit resides in MSXML3 parser where attacker uses "Out-of-Band Data Retrieval" attack by offering victim access to his own system.

d. Stolen information could be submitted as part of the URL in HTTP request(s) to the attacker where attacker can target specific log/ config files containing username/ passwords.

e. This XXE vulnerability can be used in mass scale phishing attacks targeting individuals believing they are helping another individual with an IT problem.

4. Recommendations

a. Install and update well reputed antiviruses such as Kaspersky,

Avira, Avast etc.

b. Install latest update for VVindows Remote Assistance.

c. Deploy intrusion detection systems to monitor network traffic for any malicious activity.

d. Don't download attachments from emails unless you are sure about the source.

e. It is advised to vigilant while surfing social media and avoid downloading any file or image from unreliable source.