PTA Security Advisory-No: 59

04-November-2019

Threat Classification: Remote Code Execution Vulnerability

Name: Microsoft Operating System BlueKeep RDP Vulnerability (CVE-2019-0708)

Affected Systems: Affects the following products of Microsoft:

a. Windows 2000
b. Windows Vista
c. Windows XP
d. Windows 7
e. Windows Server 2003
f. Windows Server 2003 R2
g. Windows Server 2008
h. Windows Server 2008 R2

Summary:

The above Microsoft products, including both 32-bit and 64-bit as well as all service pack versions with RDP enabled, have a vulnerability which could allow a remote attacker to send specially crafted packets resulting in an unauthorized access. An attacker can exploit this vulnerability to perform remote code execution on an unprotected system.

BlueKeep is considered worm-able because malware exploiting this vulnerability could propagate to other vulnerable systems; thus, spreading in a fashion similar to the WannaCry malware attacks.

Attack Severity	Critical
Attack Vector	Network
Attack Type	BlueKeep
Privileges Required	None

Recommendations:

- Update or upgrade from following official Microsoft website link to fix the aforementioned vulnerabilities:

  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

- In all cases, ensure that devices to be upgraded meet the requirements set by the vendor.

- Whenever required, run software with minimal access rights and privileges.

- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.

- Only use licensed software and avoid download/use of cracked and pirated software.

- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.

- In case of any incident, please report to this office.