Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 065 **30-January-2020**

Threat Classification: Remote Code Execution

Name: Microsoft Windows Remote Desktop Gateway (RD Gateway) Remote code Execution Vulnerability (CVE-2020-0609 and CVE-2020-0610)

Affected Systems: Affects all of the supported **Windows Server** versions:

a. Windows Server 2012
b. Windows Server 2012 R2
c. Windows Server 2016
d. Windows Server 2019

Summary:

This vulnerability is pre-authentication and does not requires user interaction. Due to the existence of Remote code execution vulnerability in Windows Remote Desktop Gateway (RD Gateway), an unauthenticated attacker could connect to the target system using RDP and send specially crafted requests. A successful exploitation of this vulnerability could allow the attacker to execute arbitrary code on the target system. An attacker could then install programs; change, or delete sensitive data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems RD Gateway via RDP.

Attack Severity	**Critical**
Attack Vector	Network
Attack Type	Remote Code Execution
Privileges Required	None

Recommendations:

- Please visit following official website link for the mitigation process of the aforementioned vulnerability:
  - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0609
  - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610

- As this vulnerability only **affects UDP transport**, therefore, block inbound UDP traffic.

- Whenever required, access the system 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.