# Pakistan Telecom Authority, Islamabad

**PTA Cyber Security Advisory No: 069** **09-March-2020**

**Threat Classification:** Remote Code Execution

**Name:** Microsoft Internet Connection Sharing (ICS) service Remote code Execution Vulnerability (CVE-2020-0662)

**Affected Systems:** Affects the following Microsoft products:

a. Windows Server 2008 - 2019
b. Windows 7 – Windows 10

**Summary:**

A memory corruption vulnerability exists when an attacker sends specially crafted packets to a server running the Internet Connection Sharing (ICS) service. The successful exploit could allow the attacker to run arbitrary code on the server with elevated privileges.

| | |
|---|---|
| **Attack Severity** | **CRITICAL** |
| **Attack Vector** | Network |
| **Attack Type** | Remote Code Execution |
| **Privileges Required** | Low |

The security update provided by Microsoft addresses the vulnerability by correcting how the Internet Connection Sharing (ICS) service handles the network packets.

For further details, please visit following official website link:
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0662

For Security update guidance and release notes, please visit following link:
https://portal.msrc.microsoft.com/en-us/security-guidance

**Recommendations:**

- Please visit following official website link for the security updates of the aforementioned vulnerability:
  - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-0662
- 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.