Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 070 **13-March-2020**

Threat Classification: Remote Code Execution

Name: Microsoft Windows SMBv3 Client/Server Remote Code Execution Vulnerability (CVE-2020-0796)

Affected Systems: Affects the following Microsoft products:

i. **Windows Server**

ii. **Windows 10**

Severity	**CRITICAL**
Exploitation	**More Likely**
Attack Vector	Network
Attack Type	Remote Code Execution

Summary:

A vulnerability exists in **Microsoft Server Message Block 3.1.1 (SMBv3)** protocol when it handles certain requests. An attacker, successfully exploiting this vulnerability, could gain the ability to take control on the target server or client.

- To exploit the vulnerability against a Server, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv3 server.

- To exploit the vulnerability against a Client, an unauthenticated attacker would need to configure a malicious SMBv3 server and convince the user to connect to it.

The security update addresses the vulnerability by correcting how the SMBv3 protocol handles these specially crafted requests. For further details, please visit following official link: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

Recommendations:

- **Block TCP port 445 at the Enterprise Perimeter Firewall**: Blocking this port at the network perimeter firewall will help protect networks from the attacks that originate outside the enterprise perimeter.
- **Follow Microsoft guidelines to prevent SMB traffic from lateral connections and entering/ leaving the Network:** Please visit following official link for guidelines: https://support.microsoft.com/en-us/help/3185535/preventing-smb-traffic-from-lateral-connections
- 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.