Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:106 **30-September-2020**

Name: Microsoft Domain Controller Netlogon Vulnerability (CVE-2020-1472)

Threat Classification: Elevation of Privilege

Affected Systems: Affects the following Microsoft products:

- Windows Server 2008, 2012, 2016, 2019

Summary:

An attacker can establish a vulnerable Netlogon secure channel connection to a Domain controller using the Netlogon Remote Protocol (MS-NRPC) which may result in gaining the domain administrator access (Critical security breach).

Attack Severity	CRITICAL
Attack Vector	Network
Attack Type	Elevation of Privilege
Privileges Required	None

For further details, please visit following official website link:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

Please visit following Microsoft link for guidance and necessary changes required to address the forementioned vulnerability:

https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

Recommendations:

- Please visit 'Security Updates' section of the following relevant Microsoft official link for the security updates of the aforementioned vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

- It is strongly recommended to patch all Domain Controllers immediately.

- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.

- In all cases, also ensure that devices to be upgraded to new release 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.