Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 63 **16-January-2020**

Threat Classification: Spoofing Digital Certificate

Name: Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)

Affected Systems: Affects the following products of Microsoft:

a. Windows 10
b. Windows Server 2016
c. Windows Server 2019

Summary:

A spoofing vulnerability exists in validation process of Windows CryptoAPI (Crypt32.dll) for Elliptic Curve Cryptography (ECC) certificates.
Attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, pretending the file from a trusted, legitimate source. The user may consider the malicious file as legitimate file, because the digital signature would appear to be from a trusted provider.

Attack Severity	High
Attack Vector	Network
Attack Type	Spoofing
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-2020-0601#ID0EMGAC

- 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.