Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:082 **14-May-2020**

Threat Classification: Denial Of Service (DOS)

Name: CISCO Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software SSL/TLS Denial of Service (DOS) Vulnerability

Affected Systems:

Cisco ASA or FTD Software with following features enabled:

- AnyConnect SSL VPN
- Clientless SSL VPN
- HTTP server used for the management interface

Summary:

Due to improper resource management for inbound SSL/TLS connections, an attacker could exploit this vulnerability by establishing multiple SSL/TLS connections with specific conditions. A successful exploit could allow the attacker to exhaust the memory on the affected device, resulting in a DoS condition for services on the device that process SSL/TLS traffic.

Attack Severity	**HIGH**
Attack Vector	Network
Privileges required	None

For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-vpn-dos-qY7BHpjN

Recommendations:

- For detailed information of fixed releases of Cisco ASA and FTD software for the aforementioned vulnerability, please visit following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-vpn-dos-qY7BHpjN#fs

- When considering software upgrades, CISCO recommends to consult Cisco advisories available on the Cisco Security Advisories and Alerts page for determining the exposure and complete upgrade solution.

- 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.