Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No.: 62 20-December-2019

Threat Classification: Remote Code Execution

Name: CISCO Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software Remote Code Execution Vulnerability (CVE-2019-15992)

Affected Systems: Affects the following products of CISCO:

- CISCO Adaptive Security Appliance (ASA) software
- CISCO Firepower Threat Defense (FTD) Software

Attack Severity	HIGH
Attack Vector	Network
Attack Type	Remote Code Execution

Summary:

Due to insufficient restrictions implemented in the interpreter Lua, integrated in the Cisco ASA and FTD Software, an authenticated remote attacker may be allowed to execute the arbitrary code with '*root*' privileges on the underlying Linux OS of the affected device resulting in the remote code execution attack.

Cisco has confirmed that the following products are not affected by this vulnerability:

- Adaptive Security Device Manager
- Cisco Security Manager
- Firepower Management Center
- Firepower Management Center 1000

Cisco has released software updates that address this vulnerability. For more information, please find below link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191112-asa-ftd-lua-rce

Fixed Releases:

When considering software upgrades, it is recommended to consult Cisco advisories available on the Cisco Security Advisories and Alerts page for determining the exposure and a complete upgrade solution.

For detailed information of fixed releases for Cisco ASA and FTD software, please visit following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191112-asa-ftd-lua-rce#fs

Recommendations:

- 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.