PTA Security Advisory-No: 58

30-October-2019

Threat Classification: Remote Code Execution Vulnerability

Name: CISCO Firepower Management Center (FMC) Remote Code Execution Vulnerability (CVE-2019-12688)

Affected Systems: Affects the following product of CISCO:

- **Cisco FMC Software**

Attack Severity	HIGH
Attack Vector	Network
Attack Type	Remote Code Execution
Privileges Required	None

Summary:

Due to insufficient input validation, a vulnerability in the web UI of the Cisco FMC could allow an authenticated remote attacker to execute arbitrary commands on the affected device by sending crafted input to the web UI resulting in Remote Code Execution Attack.

- **Fixed Releases**

Please use following link for fixed releases:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce#fs

Recommendations:

- Update or upgrade from following official Cisco website link for FMC Software Releases to fix the aforementioned vulnerabilities:

  https://software.cisco.com/download/home/286259687/type/286271056/release

- In all cases, ensure that the 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.