Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No.: 067 **10-February-2020**

Threat Classification: Authentication Bypass

Name: CISCO Firepower Management Center (FMC) Lightweight Directory Access Protocol (LDAP) Authentication Bypass Vulnerability

Affected Systems:

- Cisco FMC Software configured to authenticate users of web-based management interface through an External LDAP server.

Summary:

The vulnerability is due to improper handling of LDAP authentication responses from an External Authentication server. An attacker could exploit this vulnerability by sending malicious HTTP requests which could allow the attacker to gain administrative access to the web-based management interface of the affected device.

Attack Severity	CRITICAL
Attack Vector	Network
Attack Type	Authentication Bypass

Cisco has released software updates that address this vulnerability. For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-fmc-auth

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 complete upgrade solution.

For detailed information of fixed releases of Cisco FMC software LDAP Authentication Bypass vulnerability, please visit following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-fmc-auth#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.