Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:097 **19-Aug-2020**

Threat Classification: Authentication Bypass

Name: CISCO Data Center Network Manager (DCNM) Authentication Bypass Vulnerability (CVE-2020-3382)

Affected Systems:

i. Affects all deployment modes of all DCNM appliances that were installed using .ova or .iso installers.

ii. Affects the following CISCO DCNM software releases:

- DCNM 11.0(1), 11.1(1), 11.2(1), and 11.3(1)

Summary:

The vulnerability in the REST API of Cisco Data Center Network Manager could allow an unauthenticated attacker to bypass the authentication by using the static encryption key to craft a valid session token and execute arbitrary actions with administrative privileges on the affected device.

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

For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-bypass-dyEejUMs

Recommendations:

- For detailed information of the fixed releases of CISCO Data Center Network Manager software for the aforementioned vulnerability, please visit following link:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-bypass-dyEejUMs#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.