PTA CERT for Telecom Sector

Security Advisory-No: 23

25, Sep 2018

Threat Classification: Vulnerability

Name:

- Cisco IOS XE Software Static Credential Vulnerability (CVE:2018-0150)

Source: Affect following products of Cisco:

- Cisco IOS XE Software

Distribution: The vulnerabilities can be exploited in following versions of Cisco products:

a) Cisco IOS XE release range between 16.x to 16.51
b) Cisco IOS XE release Everest range between 16.x to 16.51
c) Cisco 4400 Series Integrated Services Router 4431 16.5.1
d) Cisco 4400 Series Integrated Services Router 4431 Everest-16.5.1

Exploited Vulnerabilities: Above Cisco vulnerabilities could allow remote attackers to log into a device running an affected release of Cisco IOS XE using hardcoded, the unauthenticated user could gain previliege level 15 access on affected device through the default username and password that are used at initial boot.

Recommendations:

a) Use following Cisco "IOS Software Checker" to verify the specific IOS and IOS XE.
   - https://tools.cisco.com/security/center/softwarechecker.x
   - Update current IOS XE released after March 28 2018

b) Device Administrators should disable the hardcoded user accounts by using command "**no username cisco**" in CLI mode.
c) Configuring proper ACLs and Control Plane Policing (CoPP) on all devices.
d) Designate a PoC for your network users for seeking assistance and reporting security issues.
e) In case of any incident, please report to this office.