Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:107 **13-10-2020**

Name: CISCO IOS XE Ethernet Frame Denial of Service Vulnerability (CVE-2020- 3465)

Threat Classification: Denial of Service (DoS)

Affected Systems:

Affects the following Cisco products if they are running the vulnerable release of IOS XE:

- 1000 Series Integrated Services Routers
- 1100 Series Industrial Integrated Services Routers
- 1100 Terminal Services Gateways
- 4221 Integrated Services Routers
- 4300 Series Integrated Services Routers
- Catalyst 9800-L and 9800-CL Wireless Controllers
- Cloud Services Router 1000V Series
- ESR6300 Embedded Series Routers
- Integrated Services Virtual Routers
- VG400 Analog Voice Gateways

Summary:

This vulnerability is due to incorrect handling of certain valid Ethernet frames. An attacker could exploit this vulnerability by sending Ethernet frames onto the Ethernet segment which may allow the attacker to cause the device to reload, resulting in a DoS condition.

Attack Severity	**HIGH**
Attack Vector	Adjacent Network
Privileges required	None

For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-le-drTOB625

Recommendations:

- For detailed information of the fixed releases of CISCO IOS XE software for the aforementioned vulnerability, please visit following official link:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-le-drTOB625#fs

- 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.

- 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.