Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 068 **13-February-2020**

Threat Classification: Denial of Service

Name: CISCO FXOS, IOS XR and NX-OS Software Cisco Discovery Protocol (CDP) Denial of Service Vulnerability

Affected Systems:

Cisco products having CDP enabled both globally and on at-least one interface and are running a vulnerable release of Cisco FXOS, IOS XR (32-bit or 64-bit), or NX-OS Software are affected by this vulnerability. For a complete list of vulnerable products and details, please visit following link:
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos#vp

Attack Severity	**HIGH**
Attack Vector	Adjacent
Attack Type	Denial of Service
Privileges Required	None

Summary:

A vulnerability in CDP implementation for Cisco FXOS, IOS-XR, and NX-OS software, due to a missing check, when the affected software processes CDP messages, could allow an adjacent attacker to cause a reload of an affected device, resulting in a Denial of Service (DoS) condition. To exploit this vulnerability, an attacker must be in the same broadcast domain. An attacker could exploit this vulnerability by sending a malicious CDP packet to an affected device.

For more information, please visit following official link:
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos

Recommendations:

- Please visit following official link to fix the aforementioned vulnerability: tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos#fs
- 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.