Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:102 **04-Sep-2020**

Threat Classification: Denial of Service (DOS)

Name: CISCO IOS-XR Zero-day Memory Exhaustion Vulnerabilities (CVE-2020-3566, CVE-2020-3569)

Affected Systems:

- Devices running any release of IOS XR software with an active interface configured under Multicast routing and receiving Distance Vector Multicast Routing Protocol (DVMRP) traffic.

Summary:

Due to the incorrect handling of IGMP packets, an attacker could exploit these vulnerabilities by sending crafted IGMP traffic to an affected device resulting in IGMP process crash or memory exhaustion, which may also result in other processes instability including but not limited to, interior and exterior routing protocols.

Attack type	**0-day**
Attack Severity	**HIGH**
Attack Vector	Network
Privileges required	None

For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

Recommendations:

- CISCO has yet not released the software updates to fix the aforementioned vulnerabilities. Please follow below mentioned link for the updates, when made available:
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dvmrp-memexh-dSmpdvfz

- 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.