**Government of India**
**National Critical Information Infrastructure Protection Centre**
**(A Unit of NTRO)**

**Date: 10 Feb 2020**

# Cyber Security Advisory: Denial-of-Service & Remote Code Execution vulnerability in Cisco Discovery Protocol(CDP)

This data is to be considered as **TLP:AMBER**

As per reports, Denial-of-Service(DoS) and Remote Code Execution(RCE) vulnerability in Cisco Discovery Protocol (CDP) enabled devices have been found. CDP is a proprietary layer-2 networking protocol that Cisco devices use to gather information about devices connected to the network. These vulnerabilities could allow an attacker on the local network to execute DoS & RCE :

| CVE IDs | Description | Impact |
|---|---|---|
| **CVE-2020-3110** | Cisco's Video Surveillance 8000 Series IP cameras with CDP enabled are vulnerable to a heap overflow in the parsing of DeviceID type-length-value (TLV). The CVSS score reflected is in regards to this vulnerability. | These vulnerabilities could allow a remote attacker on the local network to cause a denial of service by rebooting the affected device running CDP.<br><br>A remote attacker could also execute code by sending a malicious unauthenticated CDP packet to the affected device. |
| **CVE-2020-3111** | Cisco Voice over Internet Protocol (VoIP) phones with CDP enabled are vulnerable to a stack overflow in the parsing of PortID type-length-value (TLV). | |
| **CVE-2020-3118** | Cisco's CDP subsystem of devices running, or based on, Cisco IOS XR Software are vulnerable to improper validation of string input from certain fields within a CDP message that could lead to a stack overflow. | |
| **CVE-2020-3119** | Cisco's CDP subsystem of devices running, based on, Cisco NX-OS Software is vulnerable to a stack buffer overflow and arbitrary write in | |

| | | |
|---|---|---|
| | the parsing of Power over Ethernet (PoE) type-length-value (TLV). | |
| **CVE-2020-3120** | Cisco's CDP subsystem of devices running, or based on, Cisco NX-OS, IOS XR, and FXOS Software are vulnerable to a resource exhaustion denial-of-service condition. | This vulnerability could allow a remote attacker on the local network to cause a denial of service by rebooting the affected device running CDP. |

**Reference:**

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-nxos-cdp-rce https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-voip-phones-rce-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-ipcameras-rce-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-ipcameras-rce-dos

## Recommendation:

Users are requested to visit OEM site for latest updates / patches for remediation.

**Disclaimer:**

This document is distributed as TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

**With Best Regards,**
**Knowledge Management System**
**National Critical Information Infrastructure Protection Centre**
**Block-III, Old JNU Campus, New Delhi - 110067**
**Website: www.nciipc.gov.in**
**Toll Free: 1800-11-4430**