Security Advisory 2024-031

High Severity Vulnerabilities in Cisco Products

March 29, 2024 — v1.0

TLP:CLEAR

History:

- *29/03/2024 — v1.0 – Initial publication*

Summary

On March 27, 2024, Cisco released security updates for fourteen (14) vulnerabilities affecting IOS, IOS XE and Cisco Access Point software. Six (6) high severity vulnerabilities with a CVSS score of 8.6, could allow an unauthenticated, remote attacker to cause denial of service on an affected device [1].

Technical details

- `CVE-2024-20311`, an attacker could exploit this vulnerability by sending a crafted LISP packet to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition [2].
- `CVE-2024-20314`, an attacker could exploit this vulnerability by sending certain IPv4 packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust CPU resources and stop processing traffic, resulting in a DoS condition [3].
- `CVE-2024-20307` and `CVE-2024-20308`, an attacker could exploit this vulnerability by sending crafted UDP packets to an affected system. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition [4].
- `CVE-2024-20259`, an attacker could exploit this vulnerability by sending a crafted DHCP request through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition [5].
- `CVE-2024-20271`, an attacker could exploit this vulnerability by sending a crafted IPv4 packet either to or through an affected device. A successful exploit could allow the attacker to cause an affected device to reload unexpectedly, resulting in a DoS condition. To successfully exploit this vulnerability, the attacker does not need to be associated with the affected AP. This vulnerability cannot be exploited by sending IPv6 packets [6].

Affected Products

The complete list of affected products can be found on the vendor's website [1].

Cisco has released workarounds for the vulnerabilities `CVE-2024-20307` and `CVE-2024-20308` [4].

Recommendations

CERT-EU recommends updating to the latest version of the affected product as soon as possible to mitigate this vulnerability.

References

[1] https://sec.cloudapps.cisco.com/security/center/publicationListing.x

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lisp-3gYXs3qP

[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-sda-edge-dos-qZWuWXWG

[4] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev1-NO2ccFWz

[5] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dhcp-dos-T3CXPO9z

[6] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-dos-h9TGGX6W