March 28, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Cisco published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Cisco IOS – multiple versions and platforms
- Cisco IOS XE – multiple versions and platforms
- Cisco Access Points – multiple models and versions
- Cisco Switches – multiple models and versions
- Cisco SD-Access fabric edge node – multiple models and versions

Technical Details

A vulnerability in the Locator ID Separation Protocol (LISP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to the incorrect handling of LISP packets. 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.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-20303 CVE-2024-20311 CVE-2024-20312 CVE-2024-20313 CVE-2024-20314 CVE-2024-20276 CVE-2024-20307 CVE-2024-20308 CVE-2024-20259 CVE-2024-20265 CVE-2024-20271 CVE-2024-20324 CVE-2024-20306 CVE-2024-20278 CVE-2024-20316 CVE-2024-20333 CVE-2024-20309 CVE-2024-20354 CVE-2022-20821
- Cisco Security Advisories