August 22, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

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

- Cisco Unified CM – versions 12.5(1), 14S and 15
- Cisco Unified CM SME – versions 12.5(1), 14 and 15

Technical Details

A vulnerability in the SIP call processing function of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a crafted SIP message to an affected Cisco Unified CM or Cisco Unified CM SME device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition that interrupts the communications of reliant voice and video devices.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-20375 CVE-2024-20417 CVE-2024-6387 CVE-2024-20466 CVE-2024-20486 CVE-2024-20488
- Cisco Security Advisory – cisco-sa-cucm-dos-kkHq43We
- Cisco Security Advisories