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 a vulnerability in the Simple Network Management Protocol (SNMP) service of Cisco FXOS Software for Firepower 4100 Series and Firepower 9300 Security Appliances and of Cisco UCS 6300 Series Fabric Interconnects could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

Vulnerable Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco FXOS Software or Cisco UCS Software and have the SNMP service enabled:

- Firepower 4100 Series (CSCvi80806)
- Firepower 9300 Security Appliances (CSCvi80806)
- UCS 6300 Series Fabric Interconnects (CSCwd38796, CSCwe12029))

The SNMP service is disabled by default.

Note: Cisco FXOS Software releases 2.4.1 and later are not affected by this vulnerability.

Technical Details

This vulnerability is due to the improper handling of specific SNMP requests. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.

Note: This vulnerability affects all supported SNMP versions. To exploit this vulnerability through SNMPv2c or earlier, an attacker must know the SNMP community string that is configured on an affected device. To exploit this vulnerability through SNMPv3, the attacker must have valid credentials for an SNMP user who is configured on the affected device.

This vulnerability is rated as a **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-2023-20200

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp-ucsfi-snmp-dos-qtv69NAO
- https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75058