September 11, 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 Crosswork NSO – multiple versions
- Cisco Optical Site Manager – versions prior to 24.3.1
- Cisco RV340 Dual WAN Gigabit VPN Routers – all versions
- Cisco ConfD – multiple versions
- Cisco IOS XR Software – versions 7.7.1 to 7.11.2, 24.1.1 and later
- Cisco IOS XR 64-Bit Software – multiple versions
- Cisco Routed Passive Optical Network (PON) Controller Software – multiple products and models

Technical Details

A vulnerability in the JSON-RPC API feature in ConfD that is used by the web-based management interfaces of Cisco Crosswork Network Services Orchestrator (NSO), Cisco Optical Site Manager, and Cisco RV340 Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to modify the configuration of an affected application or device.

This vulnerability is due to improper authorization checks on the API. An attacker with privileges sufficient to access the affected application or device could exploit this vulnerability by sending malicious requests to the JSON-RPC API. A successful exploit could allow the attacker to make unauthorized modifications to the configuration of the affected application or device, including creating new user accounts or elevating their own privileges on an affected system.

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-2024-20304 CVE-2024-20381 CVE-2024-20317 CVE-2024-20406 CVE-2024-20398 CVE-2024-20483 CVE-2024-20390 CVE-2024-20343
Cisco Security Advisories