July 2, 2024

Overall Rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Cisco NX-OS Software vulnerability. The vulnerability affects MDS 9000 Series Multilayer Switches (CSCwj97007), Nexus 3000 Series Switches (CSCwj97009)1, Nexus 5500 Platform Switches (CSCwj97011), Nexus 5600 Platform Switches (CSCwj97011), Nexus 6000 Series Switches (CSCwj97011), Nexus 7000 Series Switches (CSCwj94682)2, and Nexus 9000 Series Switches in standalone NX-OS mode (CSCwj97009)1.

Technical Details

A vulnerability in the CLI of Cisco NX-OS Software may allow an authenticated, local attacker to execute arbitrary commands as root on the underlying operating system of an affected device.

This vulnerability is due to insufficient validation of arguments that are passed to specific configuration CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected configuration CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.

Please Note: To successfully exploit this vulnerability on a Cisco NX-OS device, an attacker must have Administrator credentials.

This vulnerability is rated as a **MEDIUM** 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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-20399
- Cisco NX-OS Software CLI Command Injection Vulnerability
- VRM Vulnerability Reports