July 12, 2024

Overall Rating: Medium

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in the boot process of Cisco IOS XR Software. The vulnerability affects Cisco IOS XR release 24.2.1.

Technical Details

A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker with high privileges to bypass the Cisco Secure Boot functionality and load unverified software on an affected device. To exploit this successfully, the attacker must have root-system privileges on the affected device.

This vulnerability is due to an error in the software build process. An attacker could exploit this vulnerability by manipulating the system's configuration options to bypass some of the integrity checks that are performed during the booting process. A successful exploit could allow the attacker to control the boot configuration, which could enable them to bypass of the requirement to run Cisco signed images or alter the security properties of the running system.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: Low
Privileges Required: High
User Interaction: None

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-2024-20456
- Cisco IOS XR Software Secure Boot Bypass Vulnerability
- VRM Vulnerability Reports