April 17, 2024

**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 that Cisco published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Cisco Integrated Management Controller (IMC) – multiple versions and platforms

## Technical Details

A vulnerability in the CLI of the Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to *root*. To exploit this vulnerability, the attacker must have *read-only* or higher privileges on an affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to *root*.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ

These vulnerabilities are rated as an overall **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-2024-20356 CVE-2024-20295 CVE-2024-20373
- Cisco Security Advisory – cisco-sa-cimc-cmd-inj-bLuPcb
- Cisco Security Advisory – cisco-sa-cimc-cmd-inj-mUx4c5AJ
- Cisco Security Advisories