Overall Rating - Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of multiple vulnerabilities in Cisco Intersight Private Virtual Appliance could allow an authenticated, remote attacker to execute arbitrary commands using root-level privileges. The attacker would need to have Administrator privileges on the affected device to exploit these vulnerabilities.

Technical Details

These vulnerabilities are due to insufficient input validation when extracting uploaded software packages. An attacker could exploit these vulnerabilities by authenticating to an affected device and uploading a crafted software package. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges.

These vulnerabilities are rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-20013, CVE-2023-20017
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ivpa-cmdinj-C5XRbbOy