April 16, 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 Juniper published security advisories to address vulnerabilities in multiple products. Included were critical updates for the following:

- cRPD – versions prior to 23.4R1
- Juniper Cloud Native Router – versions prior to 23.4
- Junos OS – versions prior to 23.4R1-S1, 23.4R2 and 2R1
- Junos OS Evolved – multiple versions

Technical Details

An Improper Check for Unusual or Exceptional Conditions vulnerability in Routing Protocol Daemon (RPD) of Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause Denial of Service (DoS).
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-2024-30395 CVE-2024-21598 CVE-2024-30409 CVE-2024-21610
- Juniper Security Bulletins