July 16, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Juniper published a security advisory to address vulnerabilities in multiple products. Included were updates for the following:

- BBE Cloudsetup (BCS) – versions prior to 2.1.0
- Junos OS – multiple versions
- Juno OS Evolved – multiple versions
- Junos Space – versions prior to 24.1R1

Technical Details

An Uncontrolled Resource Consumption vulnerability in the aftmand process of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to consume memory resources, resulting in a Denial of Service (DoS) condition. The processes do not recover on their own and must be manually restarted.

This vulnerability is rated as a **HIGH** 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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-39565 CVE-2024-39548 CVE-2024-39545 CVE-2024-39549 CVE-2024-39552 CVE-2024-39561 CVE-2024-39536 CVE-2024-39536 CVE-2024-39560 CVE-2024-39562 CVE-2024-39553
- Juniper Security Bulletins