July 2, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Juniper Networks Session Smart Router or Conductor vulnerability. The vulnerability affects Session Smart Router: All versions before 5.6.15, from 6.0 before 6.1.9-lts, and from 6.2 before 6.2.5-sts; Session Smart Conductor: All versions before 5.6.15, from 6.0 before 6.1.9-lts, and from 6.2 before 6.2.5-sts; WAN Assurance Router: 6.0 versions before 6.1.9-lts, and 6.2 versions before 6.2.5-sts.

Technical Details

An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router or Conductor running with a redundant peer allows a network-based attacker to bypass authentication and take full control of the device.

This vulnerability is rated as a **CRITICAL** 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-2024-2973
- 2024-06: Out-Of-Cycle Security Bulletin: Session Smart Router(SSR): On redundant router deployments API authentication can be bypassed (CVE-2024-2973)
- VRM Vulnerability Reports