July 4, 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 of an Out-of-Cycle Juniper Networks Junos OS vulnerability. The vulnerability affects Junos OS on SRX Series: 21.4 versions before 21.4R3-S7.9, 22.1 versions before 22.1R3-S5.3, 22.2 versions before 22.2R3-S4.11, 22.3 versions before 22.3R3, and 22.4 versions before 22.4R3.

Technical Details

An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS).

If an SRX Series device receives specific valid traffic destined to the device, it will cause the PFE to crash and restart. Continued receipt and processing of this traffic will create a sustained DoS condition.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-21586
- 2024-07 Out-of-Cycle Security Bulletin: Junos OS: SRX Series: Specific valid traffic leads to a PFE crash (CVE-2024-21586)
- KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process
- KB16765: In which releases are vulnerabilities fixed?
- VRM Vulnerability Reports