August 30, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware that Juniper Networks has released an ***"out-of-cycle"*** security update to address multiple flaws in the J-Web component of Junos OS that could be combined to achieve remote code execution on susceptible installations. Proof-of-concept (PoC) exploit code has been released for multiple security flaws in Juniper SRX firewalls that, when chained, can allow unauthenticated attackers to gain remote code execution on unpatched devices. The vulnerabilities have been addressed in the below versions -

- EX Series - Junos OS versions 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S4, 22.1R3-S3, 22.2R3-S1, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3, and 23.2R1

- SRX Series - Junos OS versions 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S5, 22.1R3-S3, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3, and 23.2R1

Technical Details

Multiple vulnerabilities in the J-Web component of Juniper Networks Junos OS on SRX Series and EX Series have been resolved through the application of specific fixes to address each vulnerability.

By chaining exploitation of these vulnerabilities, an unauthenticated, network-based attacker may be able to remotely execute code on the devices.

Two PHP external variable modification vulnerabilities in J-Web of Juniper Networks Junos OS on EX Series and SRX Series allows an unauthenticated, network-based attacker to control certain, important environments variables.

Two missing authentications for critical function vulnerabilities in Juniper Networks Junos OS on EX Series and SRX Series allow an unauthenticated, network-based attacker to cause limited impact to the file system integrity.

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

This vulnerability is rated as a **CRITICAL** risk. A software patch 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.

References

- CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, CVE-2023-36847
- 2023-08 Out-of-Cycle Security Bulletin: Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here:
https://bcgov.sharepoint.com/sites/CITZ-ISB/SitePages/vulnerability-reports.aspx

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca