

Overall rating: Critical



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 critical vulnerabilities in the following product:

This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory.

This issue affects Juniper Networks Junos OS SRX Series and EX Series:

Junos OS versions earlier than 20.4R3-S9;
Junos OS 21.2 versions earlier than 21.2R3-S7;
Junos OS 21.3 versions earlier than 21.3R3-S5;
Junos OS 21.4 versions earlier than 21.4R3-S5;
Junos OS 22.1 versions earlier than 22.1R3-S4;
Junos OS 22.2 versions earlier than 22.2R3-S3;
Junos OS 22.3 versions earlier than 22.3R3-S2;
Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3.

Technical Details

An Out-of-bounds Write vulnerability in J-Web of Juniper Networks Junos OS SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device.

The following software releases have been updated to resolve this specific issue:

Junos OS: 20.4R3-S9, 21.2R3-S7, 21.3R3-S5, 21.4R3-S5, 22.1R3-S4, 22.2R3-S3, 22.3R3-S2, 22.4R2-S2, 22.4R3, 23.2R1-S1, 23.2R2, 23.4R1, and all subsequent releases.

This issue is being tracked as PR [1747984](#) which is visible on the Customer Support website.

Exploitability Metrics

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

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

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-2024-21591](#)

- [2024-01 Security Bulletin: Junos OS: SRX Series and EX Series: Security Vulnerability in J-web allows a preAuth Remote Code Execution \(CVE-2024-21591\) \(juniper.net\)](#)