January 15, 2024

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Juniper Networks published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- CTPView – versions prior to 9.1R5
- Junos OS – multiple versions
- Junos OS Evolved – multiple versions
- Security Director Insights – versions prior to 23.1R1
- Session Smart Router – versions prior to SSR-6.2.3-r2

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.

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

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-21611, CVE-2024-21596, CVE-2024-21591, CVE-2024-21595, CVE-2024-21616, CVE-2023-36842, CVE-2024-21617, CVE-2024-21604, CVE-2024-21599, CVE-2024-21607, CVE-2024-21585, CVE-2024-21600, CVE-2024-21606, CVE-2024-21603, CVE-2024-21613, CVE-2024-21594, CVE-2024-21612,CVE-2024-21614, CVE-2024-21597, CVE-2024-21589, CVE-2024-21587, CVE-2024-21601, CVE-2024-21602
- Juniper Networks Security Advisories