

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Juniper's Critical RCE Vulnerability Shakes Network Security

Date of Publication

January 17, 2024

Admiralty Code

A1

TA Number

TA2024018







Summary

Initial Publication: January 10, 2024

Affected Product: Junos OS Evolved, Junos OS on SRX Series and EX Series

Impact: Juniper Networks has a critical remote code execution (RCE) vulnerability, CVE-2024-21591, which affects SRX Series firewalls and EX Series switches. This flaw enables attackers to trigger a Denial-of-Service condition and potentially execute remote code with root privileges.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-21591	Junos OS J-Web Out-of-bounds Write Vulnerability	Junos OS on SRX Series and EX Series			
CVE-2024-21611	Juniper Networks Junos OS Denial of Service Vulnerability	Junos OS and Junos OS Evolved			

Vulnerability Details

#1

Juniper Networks faces a critical remote code execution (RCE) vulnerability, CVE-2024-21591, within its SRX Series firewalls and EX Series switches. Exploiting this vulnerability allows an assailant to trigger a Denial-of-Service (DoS) condition. The vulnerability stems from an insecure function that enables the unauthorized overwriting of arbitrary memory.

#2

In specific scenarios, successful exploitation can lead to remote code execution, providing the attacker with root privileges on the targeted device. This flaw affects all versions of Junos OS deployed on SRX Series and EX Series.

#3

Juniper Networks has identified a high-severity bug in Junos OS and Junos OS Evolved, marked as CVE-2024-21611. This vulnerability could potentially be weaponized by an unauthenticated, network-based attacker to trigger a DoS condition.

#4

While there is currently no evidence of these vulnerabilities being exploited in the wild, it's noteworthy that various security deficiencies affecting Juniper's SRX firewalls and EX switches were exploited by threat actors in the preceding year. Notably, more than 8,900 Juniper devices have exposed J-Web interfaces on the internet, with concentrations in regions such as South Korea, the United States, Hong Kong, Indonesia, and India.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21591	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.	cpe:2.3:o:juniper:junos:*.~*.~*.~*.~*.~*.~*	CWE-787
CVE-2024-21611	Junos OS: 21.4 versions earlier than 21.4R3; 22.1 versions earlier than 22.1R3; 22.2 versions earlier than 22.2R3. Junos OS Evolved: 21.4-EVO versions earlier than 21.4R3-EVO; 22.1-EVO versions earlier than 22.1R3-EVO; 22.2-EVO versions earlier than 22.2R3-EVO.		CWE-401

Recommendations



Apply Official Fixes Immediately: Prioritize and apply the latest security patches provided by Juniper Networks to address the RCE vulnerability promptly.



Workaround: Until patches for CVE-2024-21591 are deployed, it is advisable to implement a precautionary measure by restricting J-Web access exclusively to trusted network hosts. This temporary restriction enhances security until a comprehensive solution is applied.



Monitor memory utilization: To mitigate potential risks associated with CVE-2024-21611 in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved, it is recommended to proactively monitor memory utilization. If it reaches 85% of the total RE memory, consider restarting the rpd or rebooting the system as a preventive measure.



Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>TA0007</u> Discovery	<u>TA0040</u> Impact	<u>T1588</u> Obtain Capabilities	<u>T1059</u> Command and Scripting Interpreter
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1588.006</u> Vulnerabilities	<u>T1210</u> Exploitation of Remote Services	<u>T1498</u> Network Denial of Service
<u>T1018</u> Remote System Discovery	<u>T1046</u> Network Service Discovery		

Patch Details

The following software releases have been updated to address the specific issue associated with CVE-2024-21591:

Junos OS: 19.1R3-S11, 19.2R3-S8, 19.3R3-S9, 19.4R3-S13, 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, 23.1R2, 23.2R1-S1, 23.2R2, 23.3R1, 23.3R2, 23.4R1, and all subsequent releases.

Link:

<https://supportportal.juniper.net/s/article/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>

The listed software releases have been updated to address the specific issue associated with CVE-2024-21611:

Junos OS Evolved: 21.4R3-EVO, 22.1R3-EVO, 22.2R3-EVO, 22.3R1-EVO, 22.3R2-EVO, 22.4R1-EVO, and all subsequent releases.

Junos OS: 21.3R3-S2, 21.4R3, 22.1R3, 22.2R3, 22.3R1, 22.3R2, 22.4R1, and all subsequent releases.

Link:

<https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-iflow-scenario-continuous-route-churn-will-cause-a-memory-leak-and-eventually-an-rpd-crash-CVE-2024-21611>

References

<https://threatprotect.qualys.com/2024/01/16/juniper-network-operating-system-junos-os-j-web-out-of-bound-write-vulnerability-cve-2024-21591/>

<https://www.cisa.gov/news-events/alerts/2024/01/11/juniper-networks-releases-security-bulletin-junos-os-and-junos-os-evolved>

<https://www.hivepro.com/threat-advisory/juniper-exploited-multiple-critical-vulnerabilities/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

January 17, 2024 • 3:00 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com