

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Multiple Critical Vulnerabilities in Juniper Exploited in the Wild

Date of Publication

November 14, 2023

Admiralty Code

A1

TA Number

TA2023458
















Summary

First Seen: Aug 17, 2023

Affected Platform: Juniper Junos OS

Impact: Multiple vulnerabilities have been discovered in Juniper Networks Junos OS, with the potential for preAuth Remote Code Execution when chained in Juniper devices. Juniper Networks has confirmed the successful exploitation of these vulnerabilities in the wild, urging customers to upgrade immediately.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-36844	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	Juniper Junos OS			
CVE-2023-36845	Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability	Juniper Junos OS			
CVE-2023-36846	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS			
CVE-2023-36847	Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS			
CVE-2023-36851	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS			

Vulnerability Details

#1

Multiple vulnerabilities in Juniper Networks Junos OS on SRX Series and EX Series, particularly in the J-Web component, have been addressed with specific fixes. These vulnerabilities, discovered during external security research, impact various software versions. Juniper has confirmed successful exploitation in the wild, urging customers to upgrade immediately.

#2

The vulnerabilities in Juniper devices can be chained for remote code execution, and experts recommend updating or disabling the J-Web interface. Researchers published a proof-of-concept exploit, highlighting the simplicity of exploitation, the potential for large-scale attacks, and the identification of approximately 12,000 vulnerable Juniper devices. They also developed an exploit impacting older versions.

#3

A specific vulnerability (CVE-2023-36845) previously required a file upload, but a new variant that operates without this prerequisite has been published, emphasizing the importance of fixing the code execution ability. The listed software releases (20.4R3-S9, 21.2R3-S7*, 21.3R3-S5, 21.4R3-S5*, 22.1R3-S4, 22.2R3-S2, 22.3R2-S2, 22.3R3-S1, 22.4R2-S1, 22.4R3*, 23.2R1-S1, 23.2R2*, 23.4R1*) prevent the code execution vulnerability.

#4

Juniper recommends disabling J-Web or limiting access to trusted hosts as a workaround. Updates to fix the remaining vulnerabilities are pending, but addressing the code execution issue significantly reduces their impact. CISA orders federal agencies to address these vulnerabilities by November 17, 2023, emphasizing the importance of securing these critical network devices.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-36844	All versions prior to 20.4R3-S9;	cpe:2.3:o:juniper:junos:*:*:*:*:*:*	CWE-473
CVE-2023-36845	21.1 version 21.1R1 and later versions;		CWE-473
CVE-2023-36846	21.2 versions prior to 21.2R3-S7;		CWE-306
CVE-2023-36847	21.3 versions prior to 21.3R3-S5;		CWE-306
CVE-2023-36851	21.4 versions prior to 21.4R3-S5;		CWE-306
CVE-2023-36851	22.1 versions prior to 22.1R3-S4; 22.2 versions prior to 22.2R3-S2; 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; 22.4 versions prior to 22.4R2-S1, 22.4R3; 23.2 versions prior to 23.2R1-S1, 23.2R2 15.0.4		CWE-306

Recommendations



Immediate Upgrade: Juniper strongly advises users to upgrade their systems immediately to the [specified software releases](#). This is essential to prevent the code execution vulnerability and secure the affected devices.

Chained Vulnerabilities Mitigation:



Disabling J-Web as a Workaround: As a temporary workaround, consider disabling the J-Web interface or limiting access to trusted hosts. This can provide an additional layer of protection until the necessary updates are applied.



Vulnerability Scanning and Assessment: Conduct regular vulnerability scans and assessments of your IT infrastructure. Identify and address any vulnerabilities promptly to reduce the attack surface.

Potential **MITRE ATT&CK** TTPs

<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0040</u> Impact	<u>TA0042</u> Resource Development
<u>T1059</u> Command and Scripting Interpreter	<u>T1203</u> Exploitation for Client Execution	<u>T1204.002</u> Malicious File	<u>T1204</u> User Execution
<u>T1055</u> Process Injection	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1588</u> Obtain Capabilities

Patch Details

Upgrade J-Web component to the following versions 20.4R3-S9, 21.2R3-S7*, 21.3R3-S5, 21.4R3-S5*, 22.1R3-S4, 22.2R3-S2, 22.3R2-S2, 22.3R3-S1, 22.4R2-S1, 22.4R3*, 23.2R1-S1, 23.2R2*, 23.4R1* or later versions.

Mitigation:

Update or disable the J-Web interface to mitigate the risk of chained vulnerabilities leading to remote code execution.

Link:

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

References

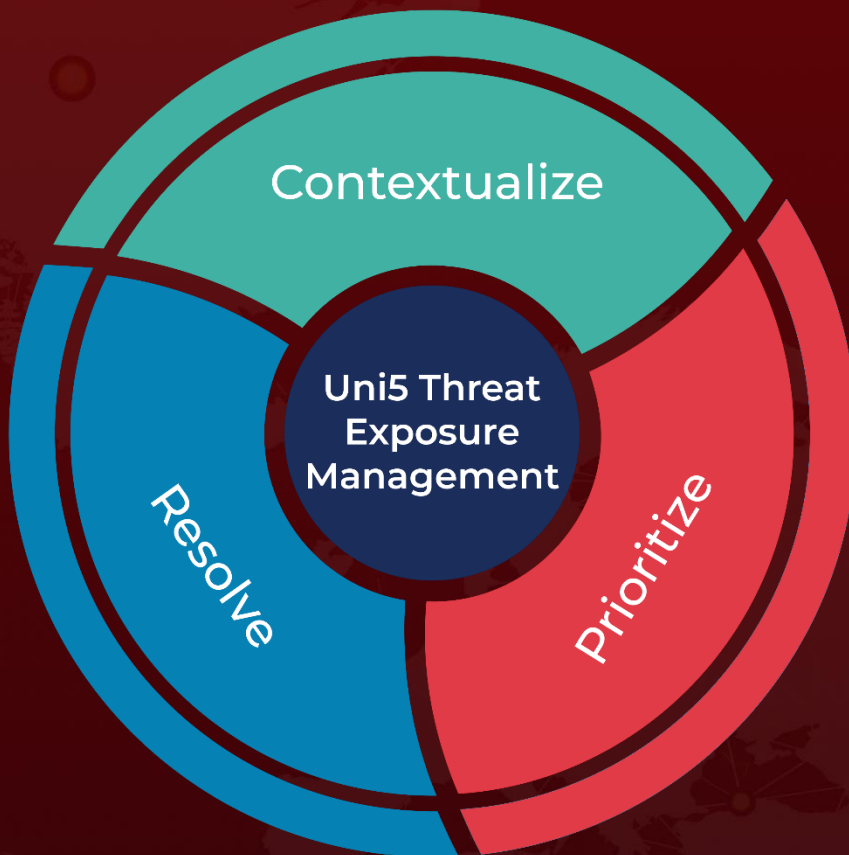
<https://securityaffairs.com/154128/security/cisa-juniper-flaws-known-exploited-vulnerabilities-catalog.html>

<https://www.cisa.gov/news-events/alerts/2023/11/13/cisa-adds-six-known-exploited-vulnerabilities-catalog>

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

November 14, 2023 • 4:30 AM

© 2023 All Rights are Reserved by HivePro®



More at www.hivepro.com