

CVE-2023-36845

Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability

Exigent

CISA KEV since Nov 13, 2023

Actively exploited

Public exploit module (Metasploit)

A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series and SRX Series allows an unauthenticated, network-based attacker to remotely execute code. Using a crafted request which sets the variable PHPRC an attacker is able to modify the PHP execution environment allowing the injection und execution of code.

EVRS

86/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.951

99.87th percentile · FIRST

CISA DEADLINE

Nov 17, 2023

KEV since 2023 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.951 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

This issue affects Juniper Networks Junos OS on EX Series and SRX Series: * All versions prior to 20.4R3-S9; * 21.1 versions 21.1R1 and later; * 21.2 versions prior to 21.2R3-S7; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 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.

Affected and fixed versions · 21 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
junos	< 20.4 20.4 21.1 21.2 21.3 21.4 22.1 22.2 22.3 22.4 23.2	20.4	NVD
srx100	—	no fixed version listed	NVD
srx110	—	no fixed version listed	NVD
srx1400	—	no fixed version listed	NVD
srx1500	—	no fixed version listed	NVD
srx210	—	no fixed version listed	NVD



PACKAGE	AFFECTED	FIXED IN	SOURCE
srx220	–	no fixed version listed	NVD
srx240	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-q56g-qr28-qh57	Additional guidance	supportportal.juniper.net/JSA72300
supportportal.juniper.net	supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-JunOS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US	NVD	nvd.nist.gov/vuln/detail/CVE-2023-36845
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-40765
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-36845		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.