Junos OS: A low privileged user can escalate their privileges so that they can login as root

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-21916
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:24 UTC
Updated	2026-04-17 18:05:52 UTC
Description	A UNIX Symbolic Link (Symlink) Following vulnerability in the CLI of Juniper Networks Junos OS allows a local, authenticat

Risk And Classification

Primary CVSS: v4.0 7 HIGH from sirt@juniper.net

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:M/U:X

EPSS: 0.000120000 probability, percentile 0.017970000 (date 2026-04-21)

Problem Types: CWE-61 | CWE-61 CWE-61 UNIX Symbolic Link (Symlink) Following

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	7	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/E:X/C...
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/AU:Y/...
3.1	sirt@juniper.net	Primary	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

Low

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:M/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	All	All	All	All
Operating System	Juniper	Junos	23.2	-	All	All
Operating System	Juniper	Junos	23.2	r1	All	All
Operating System	Juniper	Junos	23.2	r1-s1	All	All

Operating System	Juniper	Junos	23.2	r1-s1	All	All
Operating System	Juniper	Junos	23.2	r1-s2	All	All
Operating System	Juniper	Junos	23.2	r2	All	All
Operating System	Juniper	Junos	23.2	r2-s1	All	All
Operating System	Juniper	Junos	23.2	r2-s2	All	All
Operating System	Juniper	Junos	23.2	r2-s3	All	All
Operating System	Juniper	Junos	23.2	r2-s4	All	All
Operating System	Juniper	Junos	23.2	r2-s5	All	All
Operating System	Juniper	Junos	23.2	r2-s6	All	All
Operating System	Juniper	Junos	23.4	-	All	All
Operating System	Juniper	Junos	23.4	r1	All	All
Operating System	Juniper	Junos	23.4	r1-s1	All	All
Operating System	Juniper	Junos	23.4	r1-s2	All	All
Operating System	Juniper	Junos	23.4	r2	All	All
Operating System	Juniper	Junos	23.4	r2-s1	All	All
Operating System	Juniper	Junos	23.4	r2-s2	All	All
Operating System	Juniper	Junos	23.4	r2-s3	All	All
Operating System	Juniper	Junos	23.4	r2-s4	All	All
Operating System	Juniper	Junos	23.4	r2-s5	All	All
Operating System	Juniper	Junos	24.2	-	All	All
Operating System	Juniper	Junos	24.2	r1	All	All
Operating System	Juniper	Junos	24.2	r1-s1	All	All
Operating System	Juniper	Junos	24.2	r1-s2	All	All
Operating System	Juniper	Junos	24.2	r2	All	All
Operating System	Juniper	Junos	24.2	r2-s1	All	All
Operating System	Juniper	Junos	24.2	r2-s2	All	All
Operating System	Juniper	Junos	24.4	-	All	All
Operating System	Juniper	Junos	24.4	r1	All	All
Operating System	Juniper	Junos	24.4	r1-s2	All	All
Operating System	Juniper	Junos	24.4	r1-s3	All	All
Operating System	Juniper	Junos	24.4	r2	All	All
Operating System	Juniper	Junos	24.4	r2-s1	All	All
Operating System	Juniper	Junos	25.2	-	All	All
Operating System	Juniper	Junos	25.2	r1	All	All
Operating System	Juniper	Junos	25.2	r1-s1	All	All
Operating System	Juniper	Junos	25.2	r1-s2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 23.2R2-S7 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 23.4 23.4R2-S6 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.2 24.2R2-S3 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.4 24.4R2-S2 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 25.2 25.2R2 semver	Not specified
CNA	Juniper Networks	Junos OS	unaffected 25.4R1	Not specified

References

Reference	Source	Link	Tags
kb.juniper.net/JSA107807	sirt@juniper.net	kb.juniper.net	Mitigation, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: The following software releases have been updated to resolve this specific issue: 23.2R2-S7, 23.4R2-S6, 24.2R2-S3, 24.4R2-S2, 25.2R2, and all subsequent releases.

Workarounds

CNA: To prevent exploitation, use access controls to keep users from performing 'file link' operations.

Exploits

CNA: Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**