



# 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

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

## 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/MSX/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/MSX/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	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	<a href="#">Juniper Networks</a>	<a href="#">Junos OS</a>	affected 23.2R2-S7 semver	Not specified
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS</a>	affected 23.4 23.4R2-S6 semver	Not specified
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS</a>	affected 24.2 24.2R2-S3 semver	Not specified
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS</a>	affected 24.4 24.4R2-S2 semver	Not specified
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS</a>	affected 25.2 25.2R2 semver	Not specified
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS</a>	unaffected 25.4R1	Not specified

## References

Reference	Source	Link	Tags
<a href="https://kb.juniper.net/JSA107807">kb.juniper.net/JSA107807</a>	<a href="mailto:sirt@juniper.net">sirt@juniper.net</a>	<a href="https://kb.juniper.net">kb.juniper.net</a>	Mitigation, Vendor Advisory
CVE Program record	<a href="https://www.cve.org">CVE.ORG</a>	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	<a href="https://nvd.nist.gov">NVD</a>	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)