



Junos OS: Privileged local user can gain access to a Linux-based FPC as root

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-30650 |
| State | PUBLISHED |
| Assigner | juniper |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-08 19:24:00 UTC |
| Updated | 2026-04-13 22:16:26 UTC |

Description A Missing Authentication for Critical Function vulnerability in command processing of Juniper Networks Junos OS allows a

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from sirt@juniper.net

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/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:N/R:A/V:C/RE:M/U:Amber

EPSS: 0.000180000 probability, percentile 0.046330000 (date 2026-04-13)

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------|-----------|-------|----------|--|
| 4.0 | sirt@juniper.net | Secondary | 8.4 | HIGH | CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/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:N/R:A/V:C/RE:M/U:Amber |
| 4.0 | CNA | CVSS | 8.4 | HIGH | CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/AU:N/R:A/V:C/RE:M/U:Amber |
| 3.1 | sirt@juniper.net | Secondary | 6.7 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 6.7 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H |

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/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:N/R:A/V:C/RE:M/U:Amber



CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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



Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------------|----------|--------------------------------|---------------|
| CNA | Juniper Networks | Junos OS | affected 22.4R3-S8 semver | Not specified |
| CNA | Juniper Networks | Junos OS | affected 23.2 23.2R2-S6 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 semver | Not specified |
| CNA | Juniper Networks | Junos OS | affected 25.2 25.2R2 semver | Not specified |

References

| Reference | Source | Link | Tags |
|---|------------------|---|---------------------|
| kb.juniper.net/JSA107863 | sirt@juniper.net | kb.juniper.net | |
| github.com/orangecertcc/security-research/security/advisories/GHSA-fwhc-... | sirt@juniper.net | github.com | |
| supportportal.juniper.net/JSA107863 | MITRE | supportportal.juniper.net | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

CNA: Juniper SIRT would like to acknowledge and thank Pierre EMERIAUD & Orange CERT-CC from Orange group for responsibly reporting this vulnerability. (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|--|
| CNA | 2026-04-08T16:00:00.000Z | Initial Publication |
| CNA | 2026-04-13T16:00:00.000Z | Removed reference to EVO. Issue is specific to Junos OS with Linux-based line cards. |

Solutions

CNA: The following software releases have been updated to resolve this specific issue: 22.4R3-S8, 23.2R2-S6, 23.4R2-S6, 24.2R2-S3, 24.4R2, 25.2R2, 25.4R1, and all subsequent releases.

Workarounds

CNA: There are no known workarounds for this issue.

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.

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

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