JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: Junos OS: Privileged local user can gain access to a Linux-based FPC as root (CVE-2025-30650)

Article ID JSA107863 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects all versions of Junos OS.

Severity	Severity Assessment (CVSS) Score
Medium	**CVSS: v3.1:** 6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) **CVSS: v4.0:** 8.4 (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)

Problem

A Missing Authentication for Critical Function vulnerability in command processing of Juniper Networks Junos OS allows a privileged local attacker to gain access to line cards running Junos OS Evolved as root.

This issue affects systems running Junos OS using Linux-based line cards. Affected line cards include:

- MPC7, MPC8, MPC9, MPC10, MPC11
- LC2101, LC2103
- LC480, LC4800, LC9600
- MX304 (built-in FPC)
- MX-SPC3
- SRX5K-SPC3
- EX9200-40XS

- FPC3-PTX-U2, FPC3-PTX-U3
- FPC3-SFF-PTX
- LC1101, LC1102, LC1104, LC1105

This issue affects Junos OS:

- all versions before 22.4R3-S8,
- from 23.2 before 23.2R2-S6,
- from 23.4 before 23.4R2-S6,
- from 24.2 before 24.2R2-S3,

- from 24.4 before 24.4R2,
- from 25.2 before 25.2R2.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.
This issue was discovered during external security research.

Solution

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.

This issue is being tracked as 1872703 which is visible on the Customer Support website.
Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

Workaround

There are no known workarounds for this issue.

Severity Assessment

Information for how Juniper Networks uses CVSS can be found at KB 16446 "Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories."

Modification History

```
2026-04-08: Initial Publication
```

Related Information

- KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process
- KB16765: In which releases are vulnerabilities fixed?
- KB16446: Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories
- Report a Security Vulnerability - How to Contact the Juniper Networks Security Incident Response Team
- https://www.cve.org/CVERecord?id=CVE-2025-30650

Acknowledgements

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

AFFECTED PRODUCT SERIES / FEATURES