Juniper Junos - Privileged local user can gain access to a Linux-based FPC as root (CVE-2025-30650)

Moderate **orange-cert-cc** published **GHSA-fwhc-gh5m-v8fq** 2 hours ago

Package

Junos (Juniper)

Affected versions

23.4R2-S3.9

Patched versions

23.2R2-S6

Description

Overview

A local attacker with high privileges (`shell` and `maintenance`) is able to escalate to root without the use of the root password.

Details

A local attacker with very little privileges is able to launch a script as root on card (FPC) boot-up and thus gain root access.

Affected products

The issue is confirmed with at least MPC10E, but possibly also LC9600 on MX and FPC3 on PTX. On systems with MPC7E the first vulnerability is not present, and the second one might be different, to be confirmed. In both cases, having root access on the FPC provides full root access to the whole router, with persistence (no veriexec, low to no accounting on LC linuxes, ...).

This was tested on JunOS 23.4R2-S3.9 on MX480 using a FPC10 but other versions might be vulnerable as well.

Juniper confirms it affects also:

- 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.

Not affected products

As MPC2E and MPC3E do not seem to use an (accessible) Linux layer, these cards do not seem impacted.

Mitigation

Security patch

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.

References

https://supportportal.juniper.net/JSA107863
https://nvd.nist.gov/vuln/detail/CVE-2025-20661](https://www.cve.org/cverecord?id=CVE-2025-30650)

Credits

Pierre MERIAUD from Orange group
Orange CERT-CC at Orange group

Timeline

Date reported: March 18, 2025
Date fixed: April 8, 2026

Severity

Moderate 6.7 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

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

CVE ID

CVE-2025-30650

Weaknesses

▶ CWE-306