Juniper Networks | Support Portal

2026-04 Security Bulletin: Junos OS Evolved: Local, authenticated attackers can gain access to FPCs (CVE-2026-33788)

Article ID JSA107806 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects all versions of Junos OS Evolved.
Affected platforms: PTX Series.

Severity	Severity Assessment (CVSS) Score
High	**CVSS: v3.1:** 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) **CVSS: v4.0:** 8.5 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/AU:Y/R:U/RE:M)

Problem

A Missing Authentication for Critical Function vulnerability in the Flexible PIC Concentrators (FPCs) of Juniper Networks Junos OS Evolved on PTX Series allows a local, authenticated attacker with low privileges to gain direct access to FPCs installed in the device.

A local user with low privileges can gain direct access to the installed FPCs as a high privileged user, which can potentially lead to a full compromise of the affected component.

This issue affects Junos OS Evolved on PTX10004, PTX10008, PTX100016, with JNP10K-LC1201 or JNP10K-LC1202:

- All versions before 21.2R3-S8-EVO,
- 21.4-EVO versions before 21.4R3-S7-EVO,
- 22.2-EVO versions before 22.2R3-S4-EVO,
- 22.3-EVO versions before 22.3R3-S3-EVO,
- 22.4-EVO versions before 22.4R3-S2-EVO,
- 23.2-EVO versions before 23.2R2-EVO.

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

This issue was found during internal product security testing or research.

Solution

The following software releases have been updated to resolve this specific issue: 21.2R3-S8-EVO, 21.4R3-S7-EVO, 22.2R3-S4-EVO, 22.3R3-S3-EVO, 22.4R3-S2-EVO, 23.2R2-EVO, 23.4R1-EVO, and all subsequent releases.

This issue is being tracked as 1621525 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

Use access lists or firewall filters to limit access to the CLI only from trusted hosts and administrators.

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

AFFECTED PRODUCT SERIES / FEATURES