JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: Junos OS and Junos OS Evolved: Execution of crafted CLI commands allows for arbitrary shell injection as root (CVE-2026-33791)

Article ID JSA107875 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects all versions of Junos OS. This issue affects all versions of Junos OS Evolved.

Severity
Medium

Severity Assessment (CVSS) Score
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:N/SI:N/SA:L/AU:Y/R:A/V:C/RE:M/U:Amber)

Problem

An OS Command Injection vulnerability in the CLI processing of Juniper Networks Junos OS and Junos OS Evolved allows a local, high-privileged attacker executing specific, crafted CLI commands to inject arbitrary shell commands as root, leading to a complete compromise of the system.

Certain 'set system' commands, when executed with crafted arguments, are not properly sanitized, allowing for arbitrary shell injection. These shell commands are executed as root, potentially allowing for complete control of the vulnerable system.

This issue affects:
Junos OS:

- all versions before 22.4R3-S8,
- from 23.2 before 23.2R2-S5,
- from 23.4 before 23.4R2-S7,
- from 24.2 before 24.2R2-S2,
- from 24.4 before 24.4R2,
- from 25.2 before 25.2R2;

Junos OS Evolved:

- all versions before 22.4R3-S8-EVO,
- from 23.2 before 23.2R2-S5-EVO,

- from 23.4 before 23.4R2-S7-EVO,
- from 24.2 before 24.2R2-S2-EVO,
- from 24.4 before 24.4R2-EVO,
- from 25.2 before 25.2R1-S1-EVO, 25.2R2-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:
Junos OS 22.4R3-S8, 23.2R2-S5, 23.4R2-S7, 24.2R2-S2, 24.4R2, 25.2R2, 25.4R1, and all subsequent releases.
Junos OS Evolved 22.4R3-S8-EVO, 23.2R2-S5-EVO, 23.4R2-S7-EVO, 24.2R2-S2-EVO, 24.4R2-EVO, 25.2R1-S1-EVO, 25.2R2-EVO, 25.4R1-EVO, and all subsequent releases.

This issue is being tracked as 1872082 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

One of the following mitigations will reduce the risk of malicious exploitation:

- Use access lists or firewall filters to limit access to the CLI only from trusted hosts and administrators.
- Avoid configuring access to any part of the '`set system`' stanza for non-privileged users.

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-2026-33791

AFFECTED PRODUCT SERIES / FEATURES