Juniper Networks | Support Portal

2026-04 Security Bulletin: JSI Virtual Lightweight Collector: Shell escape allows privilege escalation to root (CVE-2026-21915)

Article ID JSA106016 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects all versions of JSI vLWC.

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:N/R:U/RE:M)

Problem

A Permissive List of Allowed Input vulnerability in the CLI of Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) allows a local, high privileged attacker to escalate their privileges to root.

The CLI menu accepts input without carefully validating it, which allows for shell command injection. These shell commands are executed with root permissions and can be used to gain complete control of the system.

This issue affects all JSI vLWC versions before 3.0.94.

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

This issue was seen during production usage.

Solution

The following software releases have been updated to resolve this specific issue: 3.0.94, and all subsequent releases.

This issue is being tracked as JDEF-980.

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