JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: vLWC: Default password is not required to be changed which allows unauthorized high-privileged access (CVE-2026-33784)

Article ID JSA107871 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects all versions of JSI vLWC.

Severity
Critical

Severity Assessment (CVSS) Score
CVSS: v3.1: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS: v4.0: 9.3 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/AU:Y/R:U/RE:L)

Problem

A Use of Default Password vulnerability in the Juniper Networks Support Insights (JSI) Virtual Lightweight Collector (vLWC) allows an unauthenticated, network-based attacker to take full control of the device.

vLWC software images ship with an initial password for a high privileged account. A change of this password is not enforced during the provisioning of the software, which can make full access to the system by unauthorized actors possible.

This issue affects all versions of vLWC before 3.0.94.

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: 3.0.94, and all subsequent releases.

This issue is being tracked as JDEF-1032.

Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

Workaround

The password can be changed in the setup menu of the device, which is described at Configure Network Settings through JSI Shell | Juniper Support Insights | Juniper Networks

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