Juniper Networks | Support Portal

2026-04 Security Bulletin: Junos Space: ilpFilter field on nLegacy.jsp is vulnerable to reflected cross-site script injection (CVE-2026-21904)

Article ID JSA106003 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects all versions of Junos Space.

Severity
Medium

Severity Assessment (CVSS) Score
CVSS: v3.1: 6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVSS: v4.0: 5.1 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N)

Problem

An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Juniper Networks Junos Space allows an attacker to inject script tags in the list filter field that, when visited by another user, enables the attacker to execute commands with the target's permissions, including an administrator.

This issue affects all versions of Junos Space before 24.1R5 Patch V3.

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: 24.1R5 Patch V3, and all subsequent releases.

This issue is being tracked as 1837738 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

There are no known workarounds for this issue.

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