Support Portal

2026-04 Security Bulletin: Junos OS: EX Series, QFX Series: In a VXLAN scenario when specific control protocol packets are received, memory leaks and eventually no traffic is passed (CVE-2026-33781)

Article ID JSA107869 **Created** 2026-04-08 **Last Updated** 2026-04-09

Product Affected

This issue affects Junos OS 24.4 and 25.2. Affected platforms: EX Series, QFX Series.

Severity
Medium

Severity Assessment (CVSS) Score
CVSS: v3.1: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **CVSS: v4.0:** 7.1 (CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/AU:Y/RE:M)

Problem

An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX and QFX Series devices allow an unauthenticated, adjacent attacker to cause a complete Denial of Service (DoS).

On EX4k, and QFX5k platforms configured as service-provider edge devices, if L2PT is enabled on the UNI and VSTP is enabled on NNI in VXLAN scenarios, receiving VSTP BPDUs on UNI leads to packet buffer allocation failures, resulting in the device to not pass traffic anymore until it is manually recovered with a restart.
This issue affects Junos OS:

- 24.4 releases before 24.4R2,
- 25.2 releases before 25.2R1-S1, 25.2R2.

This issue does not affect Junos OS releases before 24.4R1.

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: 24.4R2, 25.2R1-S1, 25.2R2, 25.4R1, and all subsequent releases.

This issue is being tracked as 1895370 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

To prevent VSTP BPDUs from being processed on UNI interfaces configure:

```
[ protocols layer2-control bpdu-block interface all drop ]
```

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