Support Portal

2026-04 Security Bulletin: Junos OS Evolved: PTX Series: If SRTE tunnels provisioned via PCEP are present and specific gRPC queries are received evo-aftmand crashes (CVE-2026-33783)

Article ID JSA107870 **Created** 2026-04-08 **Last Updated** 2026-04-09

Product Affected

This issue affects all versions of Junos OS Evolved.
Affected platforms: PTX Series.

Severity
Medium

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

Problem

A Function Call With Incorrect Argument Type vulnerability in the sensor interface of Juniper Networks Junos OS Evolved on PTX Series allows a network-based, authenticated attacker with low privileges to cause a complete Denial of Service (DoS).

If colored SRTE policy tunnels are provisioned via PCEP, and gRPC is used to monitor traffic in these tunnels, evo-aftmand crashes and doesn't restart which leads to a complete and persistent service impact. The system has to be manually restarted to recover. The issue is seen only when the Originator ASN field in PCEP contains a value larger than 65,535 (32-bit ASN). The issue is not reproducible when SRTE policy tunnels are statically configured.

This issue affects Junos OS Evolved on PTX Series:

- all versions before 22.4R3-S9-EVO,
- 23.2 versions before 23.2R2-S6-EVO,
- 23.4 versions before 23.4R2-S7-EVO,
- 24.2 versions before 24.2R2-S4-EVO,
- 24.4 versions before 24.4R2-S2-EVO,
- 25.2 versions before 25.2R1-S2-EVO, 25.2R2-EVO.

To be exposed to this issue a device needs to be configured with SR specific telemetry statistics:

```
[ protocols source-packet-routing telemetry statistics per-source per-segment-list
]
```

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: 22.4R3-S9-EVO, 23.2R2-S6-EVO, 23.4R2-S7-EVO, 24.2R2-S4-EVO, 24.4R2-S2-EVO, 25.2R1-S2-EVO, 25.2R2-EVO, 25.4R1-EVO, and all subsequent releases.

This issue is being tracked as 1894533 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

Configure the Originator ASN with a value of less than 65,535 (16-bit ASN).

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