JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: Junos OS Evolved: QFX5000 Series and PTX Series: An attacker sending crafted multicast packets will cause evo-aftmand / evo-pfemand to crash and restart (CVE-2025-59969)

Article ID JSA103159 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects Junos OS Evolved 22.4, 23.2, 23.4, 24.2, 24.4. Affected platforms: PTX Series. This issue affects Junos OS Evolved 22.2, 22.4, 23.2, 23.4, 24.2, 24.4. Affected platforms: QFX5000 Series.

Severity
High

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) **SEVERITY:**MEDIUM **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/R:U/V:C/RE:M/U:Amber) **SEVERITY:**HIGH

Problem

A Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in the advanced forwarding toolkit (evo-aftmand/evo-pfemand) of Juniper Networks Junos OS Evolved on PTX Series or QFX5000 Series allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS).
An attacker sending crafted multicast packets will cause line cards running evo-aftmand/evo-pfemand to crash and restart or non-line card devices to crash and restart. Continued receipt and processing of these packets will sustain the Denial of Service (DoS) condition.
This issue affects Junos OS Evolved PTX Series:

- All versions before 22.4R3-S8-EVO,
- from 23.2 before 23.2R2-S5-EVO,
- from 23.4 before 23.4R2-EVO,
- from 24.2 before 24.2R2-EVO,
- from 24.4 before 24.4R2-EVO.

This issue affects Junos OS Evolved on QFX5000 Series:

- 22.2-EVO version before 22.2R3-S7-EVO,
- 22.4-EVO version before 22.4R3-S7-EVO,
- 23.2-EVO versions before 23.2R2-S4-EVO,

- 23.4-EVO versions before 23.4R2-S5-EVO,
- 24.2-EVO versions before 24.2R2-S1-EVO,
- 24.4-EVO versions before 24.4R1-S3-EVO, 24.4R2-EVO.

This issue does not affect Junos OS Evolved on QFX5000 Series versions before: 21.2R2-S1-EVO, 21.2R3-EVO, 21.3R2-EVO, 21.4R1-EVO, and 22.1R1-EVO.

Required configuration for exposure:

```
  [ protocols mld ]
```
or
```
  [ protocols pim ]
```

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:
For PTX Series: 22.4R3-S8-EVO, 23.2R2-S5-EVO, 23.4R2-EVO, 24.2R2-EVO, 24.4R2-EVO, 25.2R1-EVO, and all subsequent releases.
For QFX5000 Series: 22.2R3-S7-EVO, 22.4R3-S7-EVO, 23.2R2-S4-EVO, 23.4R2-S5-EVO, 24.2R2-S1-EVO, 24.4R1-S3-EVO, 24.4R2-EVO, 25.2R1-EVO, and all subsequent releases.
This issue is being tracked as 1808638 and 1869606 which are 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