JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: Junos OS: SRX Series: In a NAT64 configuration, receipt of a specific, malformed ICMPv6 packet will cause the srxpfe process to crash and restart. (CVE-2026-33790)

Article ID JSA107874 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

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

Severity
High

Severity Assessment (CVSS) Score
CVSS: v3.1: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) **CVSS: v4.0:** 8.7 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/AU:Y/R:A/V:C/RE:M/U:Amber)

Problem

An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow daemon (flowd) of Juniper Networks Junos OS on SRX Series allows an attacker sending a specific, malformed ICMPv6 packet to cause the srxpfe process to crash and restart. Continued receipt and processing of these packets will repeatedly crash the srxpfe process and sustain the Denial of Service (DoS) condition.

During NAT64 translation, receipt of a specific, malformed ICMPv6 packet destined to the device will cause the srxpfe process to crash and restart.

This issue cannot be triggered using IPv4 nor other IPv6 traffic.

This issue affects Junos OS on SRX Series:

- all versions before 21.2R3-S10,
- all versions of 21.3,
- from 21.4 before 21.4R3-S12,
- all versions of 22.1,
- from 22.2 before 22.2R3-S8,
- all versions of 22.4,
- from 22.4 before 22.4R3-S9,
- from 23.2 before 23.2R2-S6,
- from 23.4 before 23.4R2-S7,

- from 24.2 before 24.2R2-S3,
- from 24.4 before 24.4R2-S3,
- from 25.2 before 25.2R1-S2, 25.2R2.

This issue requires a NAT IPv6 to IPv4 (NAT64) configuration to be present. For example:

```
[ security nat source pool 1 address <IPv4 address> ]
[ security nat source rule-set 1 from zone <private-zone> ... ]
[ security nat source rule-set 1 to zone <public-zone> ... ]
[ security nat source rule-set 1 rule 1 match source-address <IPv6 subnet> ]
[ security nat source rule-set 1 rule 1 match destination-address 0.0.0.0/0 ]
[ security nat source rule-set 1 rule 1 then source-nat pool 1 ]

[ set security nat static rule-set 1 from zone <pvt-zone> ]
[ set security nat static rule-set 1 rule 1 match destination-address <dest IPv6
subnet / 96 > ]
[ set security nat static rule-set 1 rule 1 then static-nat inet ]
```

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:

Junos OS: 21.2R3-S10, 21.4R3-S12, 22.4R3-S9, 23.2R2-S6, 23.4R2-S7, 24.2R2-S3, 24.4R2-S3, 25.2R1-S2, 25.2R2, 25.4R1, and all subsequent releases.

This issue is being tracked as 1897060 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
- https://www.cve.org/CVERecord?id=CVE-2026-33790

AFFECTED PRODUCT SERIES / FEATURES