JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: Junos OS: SRX Series, MX Series: When a specifically malformed first ISAKMP packet is received kmd/iked crashes (CVE-2026-33778)

Article ID JSA107868 **Created** 2026-04-08 **Last Updated** 2026-04-08

Product Affected

This issue affects all versions of Junos OS. Affected platforms: SRX Series, MX 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/RE:M)

Problem

An Improper Validation of Syntactic Correctness of Input vulnerability in the IPsec library used by kmd and iked of Juniper Networks Junos OS on SRX Series and MX Series allows an unauthenticated, network-based attacker to cause a complete Denial-of-Service (DoS).

If an affected device receives a specifically malformed first ISAKMP packet from the initiator, the kmd/iked process will crash and restart, which momentarily prevents new security associations (SAs) for from being established. Repeated exploitation of this vulnerability causes a complete inability to establish new VPN connections.

This issue affects Junos OS on SRX Series and MX Series:

- all versions before 22.4R3-S9,
- 23.2 version before 23.2R2-S6,
- 23.4 version before 23.4R2-S7,
- 24.2 versions before 24.2R2-S4,
- 24.4 versions before 24.4R2-S3,
- 25.2 versions before 25.2R1-S2, 25.2R2.

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, 23.2R2-S6, 23.4R2-S7, 24.2R2-S4, 24.4R2-S3, 25.2R1-S2, 25.2R2, 25.4R1, and all subsequent releases.

This issue is being tracked as 1909025 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