JUNIPER NETWORKS | Support Portal

2026-04 Security Bulletin: Junos OS and Junos OS Evolved: An attacker sending a specific genuine BGP packet causes a BGP reset (CVE-2026-33797)

Article ID JSA107850 **Created** 2026-04-08 **Last Updated** 2026-04-23

Product Affected

This issue affects Junos OS 25.2. This issue affects Junos OS Evolved 25.2.

Severity
High

Severity Assessment (CVSS) Score
CVSS: v3.1: 7.4 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H) **SEVERITY:**HIGH **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:A/V:C/RE:M/U:Green) **SEVERITY:**HIGH

Problem

An Improper Input Validation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjacent attacker, sending a specific genuine BGP packet in an already established BGP session to reset only that session causing a Denial of Service (DoS).

An attacker repeatedly sending the packet will sustain the Denial of Service (DoS).
This issue affects Junos OS:

- 25.2 versions before 25.2R2

This issue does not affect Junos OS versions before 25.2R1.

This issue affects Junos OS Evolved:

- 25.2-EVO versions before 25.2R2-EVO

This issue does not affect Junos OS Evolved versions before 25.2R1-EVO.

eBGP and iBGP are affected.
IPv4 and IPv6 are affected.

Required configuration for exposure:

```
[ protocols bgp group <group> neighbor ]
```

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: 25.2R2, 25.4R1, and all subsequent releases.
Junos OS Evolved: 25.2R2-EVO, 25.4R1-EVO, and all subsequent releases.
This issue is being tracked as 1893316 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
2026-04-23: Minor typographical update to Problem Description field from 'doesn't
not' to 'does not'
```

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