



# Junos OS and Junos OS Evolved: An attacker sending a specific genuine BGP packet causes a BGP reset

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-33797
<b>State</b>	PUBLISHED
<b>Assigner</b>	juniper
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-09 22:16:29 UTC
<b>Updated</b>	2026-04-09 22:16:29 UTC
<b>Description</b>	An Improper Input Validation vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated

## Risk And Classification

**Primary CVSS:** v4.0 7.1 HIGH from sirt@juniper.net

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:Y/R:A/V:C/RE:M/U:Green

**EPSS:** 0.000220000 probability, percentile 0.059740000 (date 2026-04-10)

**Problem Types:** CWE-20 | CWE-20 CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	7.1	HIGH	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/E:X/C...
4.0	CNA	CVSS	7.1	HIGH	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/...
3.1	sirt@juniper.net	Primary	7.4	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
3.1	CNA	CVSS	7.4	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

## CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

Low

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:Y/R:A/V:C/RE:M/U:Gr  
een

### CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 25.2 25.2R2 semver	Not specified

CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS</a>	unaffected 25.2R1 semver	Not specified
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 25.2 25.2R2-EVO semver	Not specified
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	unaffected 25.2R1-EVO semver	Not specified

## References

Reference	Source	Link	Tags
<a href="https://kb.juniper.net/JSA107850">kb.juniper.net/JSA107850</a>	<a href="mailto:sirt@juniper.net">sirt@juniper.net</a>	<a href="https://kb.juniper.net">kb.juniper.net</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

### Solutions

**CNA:** 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.

### Workarounds

**CNA:** There are no known workarounds for this issue.

### Exploits

**CNA:** Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)