



# Junos OS Evolved: QFX5000 Series and PTX Series: An attacker sending crafted multicast packets will cause evo-aftmand / evo-pfemand to crash and restart

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

## Summary

<b>CVE</b>	CVE-2025-59969
<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 22:16:24 UTC
<b>Updated</b>	2026-04-13 15:02:27 UTC
<b>Description</b>	A Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in the advanced forwarding toolkit (evo-

## 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:U/V:C/RE:M/U:Amber

**EPSS:** 0.000190000 probability, percentile 0.047580000 (date 2026-04-15)

**Problem Types:** CWE-120 | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

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	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/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:U/V:C/RE:M/U:Amber

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 22.4R3-S8-EVO semver	PTX Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 23.2 23.2R2-S5-EVO semver	PTX Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 23.4 23.4R2-EVO semver	PTX Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 24.2 24.2R2-EVO semver	PTX Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 24.4 24.4R2-EVO semver	PTX Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 22.2 22.2R3-S7-EVO semver	QFX5000 Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 22.4 22.4R3-S7-EVO semver	QFX5000 Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 23.2 23.2R2-S4-EVO semver	QFX5000 Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 23.4 23.4R2-S5-EVO semver	QFX5000 Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 24.2 24.2R2-S1-EVO semver	QFX5000 Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 24.4 24.4R1-S3-EVO, 24.4R2-EVO semver	QFX5000 Series

## References

Reference	Source	Link	Tags
<a href="https://kb.juniper.net/JSA103159">kb.juniper.net/JSA103159</a>	<a href="mailto:sirt@juniper.net">sirt@juniper.net</a>	<a href="https://kb.juniper.net">kb.juniper.net</a>	
CVE Program record	<a href="https://www.cve.org">CVE.ORG</a>	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	<a href="https://nvd.nist.gov">NVD</a>	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

Source	Time	Event
CNA	2026-01-14T17:00:00.000Z	Initial Publication

### Solutions

**CNA:** 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.

### 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)