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

CVE	CVE-2025-59969
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:24 UTC
Updated	2026-04-13 15:02:27 UTC
Description	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/MSC:X/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/MSC:X/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	Juniper Networks	Junos OS Evolved	affected 22.4R3-S8-EVO semver	PTX Series
CNA	Juniper Networks	Junos OS Evolved	affected 23.2 23.2R2-S5-EVO semver	PTX Series
CNA	Juniper Networks	Junos OS Evolved	affected 23.4 23.4R2-EVO semver	PTX Series
CNA	Juniper Networks	Junos OS Evolved	affected 24.2 24.2R2-EVO semver	PTX Series
CNA	Juniper Networks	Junos OS Evolved	affected 24.4 24.4R2-EVO semver	PTX Series
CNA	Juniper Networks	Junos OS Evolved	affected 22.2 22.2R3-S7-EVO semver	QFX5000 Series
CNA	Juniper Networks	Junos OS Evolved	affected 22.4 22.4R3-S7-EVO semver	QFX5000 Series
CNA	Juniper Networks	Junos OS Evolved	affected 23.2 23.2R2-S4-EVO semver	QFX5000 Series
CNA	Juniper Networks	Junos OS Evolved	affected 23.4 23.4R2-S5-EVO semver	QFX5000 Series
CNA	Juniper Networks	Junos OS Evolved	affected 24.2 24.2R2-S1-EVO semver	QFX5000 Series
CNA	Juniper Networks	Junos OS Evolved	affected 24.4 24.4R1-S3-EVO, 24.4R2-EVO semver	QFX5000 Series

References

Reference	Source	Link	Tags
kb.juniper.net/JSA103159	sirt@juniper.net	kb.juniper.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**