Junos OS: EX Series, QFX Series: In a VXLAN scenario when specific control protocol packets are received, memory leaks and eventually no traffic is passed

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-33781
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:27 UTC
Updated	2026-04-17 17:53:32 UTC
Description	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Net

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:X/V:X/RE:M/U:X

EPSS: 0.000200000 probability, percentile 0.051450000 (date 2026-04-20)

Problem Types: CWE-754 | CWE-754 CWE-754 Improper Check for Unusual or Exceptional Conditions

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:X/V:X/RE:M/U:X

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Hardware	Juniper	Ex4000	-	All	All	All
Hardware	Juniper	Ex4100	-	All	All	All
Hardware	Juniper	Ex4100-f	-	All	All	All
Hardware	Juniper	Ex4100-h	-	All	All	All
Hardware	Juniper	Ex4300	-	All	All	All
Hardware	Juniper	Ex4400	-	All	All	All
Hardware	Juniper	Ex4600	-	All	All	All
Hardware	Juniper	Ex4650	-	All	All	All
Operating System	Juniper	Junos	24.4	-	All	All
Operating System	Juniper	Junos	24.4	r1	All	All
Operating System	Juniper	Junos	24.4	r1-s2	All	All
Operating System	Juniper	Junos	24.4	r1-s3	All	All
Operating System	Juniper	Junos	25.2	-	All	All
Operating System	Juniper	Junos	25.2	r1	All	All
Operating System	Juniper	Junos	25.2	r2	All	All
Hardware	Juniper	Qfx5110	-	All	All	All
Hardware	Juniper	Qfx5120	-	All	All	All
Hardware	Juniper	Qfx5130	-	All	All	All
Hardware	Juniper	Qfx5200	-	All	All	All
Hardware	Juniper	Qfx5210	-	All	All	All
Hardware	Juniper	Qfx5220	-	All	All	All
Hardware	Juniper	Qfx5230-64cd	-	All	All	All
Hardware	Juniper	Qfx5240	-	All	All	All
Hardware	Juniper	Qfx5241	-	All	All	All
Hardware	Juniper	Qfx5700	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 24.4 24.4R2 semver	EX Series, QFX Series
CNA	Juniper Networks	Junos OS	affected 25.2 25.2R1-S1, 25.2R2 semver	EX Series, QFX Series
CNA	Juniper Networks	Junos OS	unaffected 24.4R1 semver	EX Series, QFX Series

References

Reference	Source	Link	Tags
kb.juniper.net/JSA107869	sirt@juniper.net	kb.juniper.net	Mitigation, Vendor Advisory
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

Solutions

CNA: The following software releases have been updated to resolve this specific issue: 24.4R2, 25.2R1-S1, 25.2R2, 25.4R1, and all subsequent releases.

Workarounds

CNA: To prevent VSTP BPDUs from being processed on UNI interfaces configure: [protocols layer2-control bpdu-block interface all drop]

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 registred 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**