



Junos OS: EX Series, QFX Series: If the same egress filter is configured on both an IRB and a physical interface one of those is not applied

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

Summary

CVE	CVE-2026-33773
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:25 UTC
Updated	2026-04-17 17:56:54 UTC
Description	An Incorrect Initialization of Resource vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on s

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from sirt@juniper.net

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/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:X/RE:M/U:X

EPSS: 0.000470000 probability, percentile 0.141410000 (date 2026-04-20)

Problem Types: NVD-CWE-Other | CWE-1419 CWE-1419 Incorrect Initialization of Resource

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/C...
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/AU:Y/...
3.1	sirt@juniper.net	Primary	5.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N
3.1	CNA	CVSS	5.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/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:MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:M/U:X



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

None

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



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Hardware	Juniper	Ex2300	-	All	All	All
Hardware	Juniper	Ex2300-c	-	All	All	All
Hardware	Juniper	Ex3400	-	All	All	All
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
Hardware	Juniper	Ex9204	-	All	All	All
Hardware	Juniper	Ex9208	-	All	All	All
Hardware	Juniper	Ex9214	-	All	All	All
Operating System	Juniper	Junos	23.4	r2-s6	All	All
Operating System	Juniper	Junos	24.2	r2-s3	All	All
Hardware	Juniper	Qfx10008	-	All	All	All
Hardware	Juniper	Qfx10016	-	All	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 23.4R2-S6 23.4R2-S7 semver	EX Series, QFX Series
CNA	Juniper Networks	Junos OS	affected 24.2R2-S3 24.2R2-S4 semver	EX Series, QFX Series

References

Reference	Source	Link	Tags
CVE-2024-47015	cve@juniper.net	Link	Mitigation, Vendor Advisory

kb.juniper.net/JSA107815	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: 23.4R2-S7, 24.2R2-S4.

Workarounds

CNA: Two different workarounds are available: 1. create the same filter but under a different name and apply that to one of the interfaces, so that each interface has a unique copy of the filter in question as shown in the following example: `user@host# copy ... <filter> to ... <filter2>`
`user@host# set interfaces irb unit <unit2> family inet/inet6 filter output <filter2>` 2. configure the filter as "interface specific" by adding the keyword to the filter definition: `[firewall family inet/inet6 filter <filter> interface-specific]` which implicitly creates a copy of the original filter per applied interface.

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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

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