Junos OS: SRX Series, MX Series: When a specifically malformed first ISAKMP packet is received kmd/iked crashes

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

Summary

CVE	CVE-2026-33778
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:26 UTC
Updated	2026-04-17 17:23:59 UTC
Description	An Improper Validation of Syntactic Correctness of Input vulnerability in the IPsec library used by kmd and iked of Juniper N

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from sirt@juniper.net

CVSS:4.0/AV:N/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: 0.001360000 probability, percentile 0.332790000 (date 2026-04-20)

Problem Types: CWE-1286 | CWE-1286 CWE-1286 Improper Validation of Syntactic Correctness of Input

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	8.7	HIGH	CVSS:4.0/AV:N/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	8.7	HIGH	CVSS:4.0/AV:N/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	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

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:N/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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/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

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	All	All	All	All
Operating System	Juniper	Junos	22.4	-	All	All
Operating System	Juniper	Junos	22.4	r1	All	All
Operating System	Juniper	Junos	22.4	r1-s1	All	All
Operating System	Juniper	Junos	22.4	r1-s2	All	All
Operating System	Juniper	Junos	22.4	r2	All	All
Operating System	Juniper	Junos	22.4	r2-s1	All	All
Operating System	Juniper	Junos	22.4	r2-s2	All	All
Operating System	Juniper	Junos	22.4	r3	All	All
Operating System	Juniper	Junos	22.4	r3-s1	All	All
Operating System	Juniper	Junos	22.4	r3-s2	All	All
Operating System	Juniper	Junos	22.4	r3-s3	All	All
Operating System	Juniper	Junos	22.4	r3-s4	All	All
Operating System	Juniper	Junos	22.4	r3-s5	All	All
Operating System	Juniper	Junos	22.4	r3-s6	All	All
Operating System	Juniper	Junos	22.4	r3-s7	All	All
Operating System	Juniper	Junos	22.4	r3-s8	All	All
Operating System	Juniper	Junos	23.2	-	All	All
Operating System	Juniper	Junos	23.2	r1	All	All
Operating System	Juniper	Junos	23.2	r1-s1	All	All
Operating System	Juniper	Junos	23.2	r1-s2	All	All
Operating System	Juniper	Junos	23.2	r2	All	All
Operating System	Juniper	Junos	23.2	r2-s1	All	All
Operating System	Juniper	Junos	23.2	r2-s2	All	All
Operating System	Juniper	Junos	23.2	r2-s3	All	All
Operating System	Juniper	Junos	23.2	r2-s4	All	All
Operating System	Juniper	Junos	23.2	r2-s5	All	All
Operating System	Juniper	Junos	23.4	-	All	All
Operating System	Juniper	Junos	23.4	r1	All	All
Operating System	Juniper	Junos	23.4	r1-s1	All	All
Operating System	Juniper	Junos	23.4	r1-s2	All	All
Operating System	Juniper	Junos	23.4	r2	All	All
Operating System	Juniper	Junos	23.4	r2-s1	All	All
Operating System	Juniper	Junos	23.4	r2-s2	All	All
Operating System	Juniper	Junos	23.4	r2-s3	All	All

Operating System	Juniper	Junos	23.4	r2-s4	All	All
Operating System	Juniper	Junos	23.4	r2-s5	All	All
Operating System	Juniper	Junos	23.4	r2-s6	All	All
Operating System	Juniper	Junos	24.2	-	All	All
Operating System	Juniper	Junos	24.2	r1	All	All
Operating System	Juniper	Junos	24.2	r1-s1	All	All
Operating System	Juniper	Junos	24.2	r1-s2	All	All
Operating System	Juniper	Junos	24.2	r2	All	All
Operating System	Juniper	Junos	24.2	r2-s1	All	All
Operating System	Juniper	Junos	24.2	r2-s2	All	All
Operating System	Juniper	Junos	24.2	r2-s3	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	24.4	r2	All	All
Operating System	Juniper	Junos	24.4	r2-s1	All	All
Operating System	Juniper	Junos	24.4	r2-s2	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	r1-s1	All	All
Operating System	Juniper	Junos	25.2	r2	All	All
Hardware	Juniper	Mx10004	-	All	All	All
Hardware	Juniper	Mx10008	-	All	All	All
Hardware	Juniper	Mx2008	-	All	All	All
Hardware	Juniper	Mx2010	-	All	All	All
Hardware	Juniper	Mx2020	-	All	All	All
Hardware	Juniper	Mx204	-	All	All	All
Hardware	Juniper	Mx240	-	All	All	All
Hardware	Juniper	Mx301	-	All	All	All
Hardware	Juniper	Mx304	-	All	All	All
Hardware	Juniper	Mx480	-	All	All	All
Hardware	Juniper	Mx960	-	All	All	All
Hardware	Juniper	Srx1500	-	All	All	All
Hardware	Juniper	Srx1600	-	All	All	All

Hardware	Juniper	Srx2300	-	All	All	All
Hardware	Juniper	Srx300	-	All	All	All
Hardware	Juniper	Srx320	-	All	All	All
Hardware	Juniper	Srx340	-	All	All	All
Hardware	Juniper	Srx345	-	All	All	All
Hardware	Juniper	Srx380	-	All	All	All
Hardware	Juniper	Srx4100	-	All	All	All
Hardware	Juniper	Srx4120	-	All	All	All
Hardware	Juniper	Srx4200	-	All	All	All
Hardware	Juniper	Srx4300	-	All	All	All
Hardware	Juniper	Srx4600	-	All	All	All
Hardware	Juniper	Srx4700	-	All	All	All
Hardware	Juniper	Srx5400	-	All	All	All
Hardware	Juniper	Srx5600	-	All	All	All
Hardware	Juniper	Srx5800	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 22.4R3-S9 semver	SRX Series, MX Series
CNA	Juniper Networks	Junos OS	affected 23.2 23.2R2-S6 semver	SRX Series, MX Series
CNA	Juniper Networks	Junos OS	affected 23.4 23.4R2-S7 semver	SRX Series, MX Series
CNA	Juniper Networks	Junos OS	affected 24.2 24.2R2-S4 semver	SRX Series, MX Series
CNA	Juniper Networks	Junos OS	affected 24.4 24.4R2-S3 semver	SRX Series, MX Series
CNA	Juniper Networks	Junos OS	affected 25.2 25.2R1-S2, 25.2R2 semver	SRX Series, MX Series

References

Reference	Source	Link	Tags
kb.juniper.net/JSA107868	sirt@juniper.net	kb.juniper.net	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: 22.4R3-S9, 23.2R2-S6, 23.4R2-S7, 24.2R2-S4, 24.4R2-S3, 25.2R1-S2, 25.2R2, 25.4R1, 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.