Junos OS and Junos OS Evolved: A high frequency of connecting and disconnecting NETCONF sessions causes management unavailability

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

Summary

CVE	CVE-2026-21919
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 18:04:47 UTC
Description	An Incorrect Synchronization vulnerability in the management daemon (mgd) of Juniper Networks Junos OS and Junos OS

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from sirt@juniper.net

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

EPSS: 0.000450000 probability, percentile 0.136250000 (date 2026-04-21)

Problem Types: CWE-821 | CWE-821 CWE-821 Incorrect Synchronization

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/AU:Y/...
3.1	sirt@juniper.net	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/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

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/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/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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

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	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	24.4	-	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	r2	All	All
Operating System	Juniper	Junos Os Evolved	23.4	-	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r2-s3	All	All
Operating System	Juniper	Junos Os Evolved	23.4	r2-s4	All	All
Operating System	Juniper	Junos Os Evolved	24.2	-	All	All
Operating System	Juniper	Junos Os Evolved	24.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	24.2	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	24.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	24.4	-	All	All
Operating System	Juniper	Junos Os Evolved	24.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	24.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	24.4	r2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 23.4 23.4R2-S4 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.2 24.2R2-S1 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.4 24.4R1-S3, 24.4R2 semver	Not specified
CNA	Juniper Networks	Junos OS	unaffected all version prior to 23.4R1 semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 23.4 23.4R2-S5-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 24.2 24.2R2-S1-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 24.4 24.4R1-S3-EVO, 24.4R2-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	unaffected all version prior to 23.4R1-EVO semver	Not specified

References

Reference	Source	Link	Tags
kb.juniper.net/JSA106019	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: Junos OS Evolved: 23.4R2-S5-EVO, 24.2R2-S1-EVO, 24.4R1-S3-EVO, 24.4R2-EVO, 25.2R1-EVO, and all subsequent releases; Junos OS: 23.4R2-S4, 24.2R2-S1, 24.4R1-S3, 24.4R2, 25.2R1, and all subsequent releases.

Workarounds

CNA: Use access lists or firewall filters to limit access to the device only from trusted hosts and administrators. To further reduce the risk of exploitation you can set values as low as needed for your normal operations for: [system services netconf ssh connection-limit <max_connections>] [system services netconf ssh rate-limit <connections_per_minute>]

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