Junos OS and Junos OS Evolved: Execution of crafted CLI commands allows for arbitrary shell injection as root

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

Summary

CVE	CVE-2026-33791
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:29 UTC
Updated	2026-04-09 22:16:29 UTC
Description	An OS Command Injection vulnerability in the CLI processing of Juniper Networks Junos OS and Junos OS Evolved allows

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from sirt@juniper.net

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/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:A/V:C/RE:M/U:Amber

EPSS: 0.000410000 probability, percentile 0.126860000 (date 2026-04-10)

Problem Types: CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/E:X/C...
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/AU:Y/...
3.1	sirt@juniper.net	Primary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

Low

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/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:A/V:C/RE:M/U:Amber

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 22.4R3-S8 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 23.2 23.2R2-S5 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 23.4 23.4R2-S7 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.2 24.2R2-S2 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.4 24.4R2 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 25.2 25.2R2 semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 22.4R3-S8-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 23.2 23.2R2-S5-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 23.4 23.4R2-S7-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 24.2 24.2R2-S2-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 24.4 24.4R2-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 25.2 25.2R1-S1-EVO, 25.2R2-EVO semver	Not specified

References

Reference	Source	Link	Tags
kb.juniper.net/JSA107875	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

Solutions

CNA: The following software releases have been updated to resolve this specific issue: Junos OS 22.4R3-S8, 23.2R2-S5, 23.4R2-S7, 24.2R2-S2, 24.4R2, 25.2R2, 25.4R1, and all subsequent releases. Junos OS Evolved 22.4R3-S8-EVO, 23.2R2-S5-EVO, 23.4R2-S7-EVO, 24.2R2-S2-EVO, 24.4R2-EVO, 25.2R1-S1-EVO, 25.2R2-EVO, 25.4R1-EVO, and all subsequent releases.

Workarounds

CNA: One of the following mitigations will reduce the risk of malicious exploitation: * Use access lists or firewall filters to limit access to the CLI only from trusted hosts and administrators. * Avoid configuring access to any part of the 'set system' stanza for non-privileged users.

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**