Junos OS and Junos OS Evolved: When an unsigned Python op script configuration is present, a local low privileged user can compromise the system

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

Summary

CVE	CVE-2026-33793
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 Execution with Unnecessary Privileges vulnerability in the User Interface (UI) of Juniper Networks Junos OS and Junos

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from sirt@juniper.net

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/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:X/R:X/V:X/RE:X/U:X

EPSS: 0.000140000 probability, percentile 0.023930000 (date 2026-04-10)

Problem Types: CWE-250 | CWE-250 CWE-250: Execution with Unnecessary Privileges

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/E:X/C...
4.0	CNA	CVSS	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L
3.1	sirt@juniper.net	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/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

Low

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:L/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:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 22.4R3-S7 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 23.2 23.2R2-S4 semver	Not specified

CNA	Juniper Networks	Junos OS	affected 23.4 23.4R2-S6 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.2 24.2R1-S2, 24.2R2 semver	Not specified
CNA	Juniper Networks	Junos OS	affected 24.4 24.4R1-S2, 24.4R2 semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 22.4R3-S7-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 23.2 23.2R2-S4-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 23.4 23.4R2-S6-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 24.2 24.2R2-EVO semver	Not specified
CNA	Juniper Networks	Junos OS Evolved	affected 24.4 24.4R1-S1-EVO, 24.4R2-EVO semver	Not specified

References

Reference	Source	Link	Tags
kb.juniper.net/JSA103142	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 Evolved: 22.4R3-S7-EVO, 23.2R2-S4-EVO, 23.4R2-S6-EVO, 24.2R2-EVO, 24.4R1-S1-EVO, 24.4R2-EVO, 25.2R1-EVO and all subsequent releases. Junos OS: 22.4R3-S7, 23.2R2-S4, 23.4R2-S6, 24.2R1-S2, 24.2R2, 24.4R1-S2, 24.4R2, 25.2R1 and all subsequent releases.

Workarounds

CNA: Use access lists or firewall filters to limit access to the CLI only from trusted hosts and administrators.

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**