Junos OS Evolved: PTX Series: A vulnerability allows a unauthenticated, network-based attacker to execute code as root

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-21902
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-25 18:23:40 UTC
Updated	2026-03-30 15:16:05 UTC
Description	An Incorrect Permission Assignment for Critical Resource vulnerability in the On-Box Anomaly detection framework of Junip

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from sirt@juniper.net

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

EPSS: 0.002880000 probability, percentile 0.521720000 (date 2026-04-01)

Problem Types: CWE-732 | CWE-732 CWE-732 Incorrect Permission Assignment for Critical Resource

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/E:X/C...
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/AU:Y/...
3.1	sirt@juniper.net	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

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: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:U/V:X/RE:M/U:Red

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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 Os Evolved	25.4	r1	All	All
Hardware	Juniper	Ptx10001-36mr	-	All	All	All
Hardware	Juniper	Ptx10002-36qdd	-	All	All	All
Hardware	Juniper	Ptx10003	-	All	All	All
Hardware	Juniper	Ptx10004	-	All	All	All
Hardware	Juniper	Ptx10008	-	All	All	All
Hardware	Juniper	Ptx10016	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS Evolved	affected 25.4 25.4R1-S1-EVO, 25.4R2-EVO semver	PTX Series
CNA	Juniper Networks	Junos OS Evolved	unaffected 25.4R1-EVO semver	PTX Series

References

Reference	Source	Link
kb.juniper.net/JSA107128	sirt@juniper.net	kb.juniper.n
github.com/watchtowrlabs/watchTowr-vs-JunosEvolved-CVE-2026-21902/blob/m...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
supportportal.juniper.net/JSA107128	sirt@juniper.net	supportporta
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

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: 25.4R1-S1-EVO, 25.4R2-EVO*, 26.2R1-EVO*, and all subsequent releases. * Future Release

Workarounds

CNA: To reduce the risk of exploitation of this issue, use access lists or firewall filters to limit access to only trusted networks and hosts. Please ensure such filters only permit explicitly required connections and block all others. Also this service can be disabled by 'request pfe anomalies disable'.

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 and Source URL Uptime Status status.cve.report