



# 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

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

## 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/MSX/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:M/U:R

**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/MSX/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:M/U:R



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	Location	Language
Operating System	<a href="#">Juniper</a>	<a href="#">Junos Os Evolved</a>	25.4	r1	All	All
Hardware	<a href="#">Juniper</a>	<a href="#">Ptx10001-36mr</a>	-	All	All	All
Hardware	<a href="#">Juniper</a>	<a href="#">Ptx10002-36qdd</a>	-	All	All	All
Hardware	<a href="#">Juniper</a>	<a href="#">Ptx10003</a>	-	All	All	All
Hardware	<a href="#">Juniper</a>	<a href="#">Ptx10004</a>	-	All	All	All
Hardware	<a href="#">Juniper</a>	<a href="#">Ptx10008</a>	-	All	All	All
Hardware	<a href="#">Juniper</a>	<a href="#">Ptx10016</a>	-	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	affected 25.4 25.4R1-S1-EVO, 25.4R2-EVO semver	PTX Series
CNA	<a href="#">Juniper Networks</a>	<a href="#">Junos OS Evolved</a>	unaffected 25.4R1-EVO semver	PTX Series

#### References

Reference	Source	Link
<a href="#">kb.juniper.net/JSA107128</a>	<a href="mailto:sirt@juniper.net">sirt@juniper.net</a>	<a href="#">kb.juniper.net</a>
<a href="#">github.com/watchtowrlabs/watchTower-vs-JunosEvolved-CVE-2026-21902/blob/main/</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="#">github.com</a>
<a href="#">supportportal.juniper.net/JSA107128</a>	<a href="mailto:sirt@juniper.net">sirt@juniper.net</a>	<a href="#">supportportal.juniper.net</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

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](#) 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 registered 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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)