RSSN has Arbitrary Code Execution via Unvalidated JIT Instruction Generation in C-FFI Interface

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

Summary

CVE	CVE-2026-30960
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-10 18:18:55 UTC
Updated	2026-04-28 21:11:07 UTC
Description	rssn is a scientific computing library for Rust, combining a high-performance symbolic computation engine with numerical m

Risk And Classification

Primary CVSS: v4.0 9.4 CRITICAL from security-advisories@github.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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: 0.000090000 probability, percentile 0.009670000 (date 2026-04-28)

Problem Types: CWE-94 | CWE-269 | CWE-695 | CWE-754 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection') | CWE-269 CWE-269: Improper Privilege Management | CWE-695 CWE-695: Use of Low-Level Functionality | CWE-754 CWE-754: Improper Check for Unusual or Exceptional Conditions

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	9.4	CRITICAL	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/
4.0	CNA	DECLARED	9.4	CRITICAL	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apich-Organization	Rssn	affected < 0.2.9	Not specified

References

Reference	Source	Link	Tags
github.com/Apich-Organization/rssn/security/advisories/GHSA-9c4h-pwmf-m6fj	security-advisories@github.com	github.com	
github.com/Apich-Organization/rssn/releases/tag/v0.2.9	security-advisories@github.com	github.com	
rustsec.org/advisories/RUSTSEC-2026-0038.html	security-advisories@github.com	rustsec.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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