RAUC: Improper Signing of Plain Bundles Exceeding 2 GiB

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-34155
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 14:16:11 UTC
Updated	2026-04-01 14:24:02 UTC
Description	RAUC controls the update process on embedded Linux systems. Prior to version 1.15.2, RAUC bundles using the 'plain' for

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:H/VA:N/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: 0.000270000 probability, percentile 0.073080000 (date 2026-04-01)

Problem Types: CWE-196 | CWE-347 | CWE-196 CWE-196: Unsigned to Signed Conversion Error | CWE-347 CWE-347: Improper Verification of Cryptographic Signature

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:H/VA:N/SC:H/SI
4.0	CNA	DECLARED	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:H/VA:N/SC:H/SI

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Passive

Confidentiality

Low

Integrity

High

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:L/VI:H/VA:N/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	Rauc	Rauc	affected < 1.15.2	Not specified

References

Reference	Source	Link	Tags
github.com/rauc/rauc/commit/4fb7c798d6ae412344fb8f8d310d773046af3441	security-advisories@github.com	github.com	
github.com/rauc/rauc/security/advisories/GHSA-6hj7-q844-m2hx	security-advisories@github.com	github.com	
github.com/rauc/rauc/releases/tag/v1.15.2	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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