



# Sereal::Encoder versions from 4.000 through 4.009\_002 for Perl embeds a vulnerable version of the Zstandard library

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2024-14031
<b>State</b>	PUBLISHED
<b>Assigner</b>	CPANSec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 12:16:26 UTC
<b>Updated</b>	2026-04-01 17:16:56 UTC
<b>Description</b>	Sereal::Encoder versions from 4.000 through 4.009_002 for Perl embeds a vulnerable version of the Zstandard library. Sere

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from ADP

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

**EPSS:** 0.000400000 probability, percentile 0.122640000 (date 2026-04-01)

**Problem Types:** CWE-1395 CWE-1395 Dependency on Vulnerable Third-Party Component

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	YVES	SerealEncoder	affected 4.000 4.009_002 custom	Not specified

### References

Reference	Source	Link	Tags
www.cve.org/CVERecord	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://www.cve.org">www.cve.org</a>	
metacpan.org/release/YVES/Sereal-Encoder-4.010/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://metacpan.org">metacpan.org</a>	
github.com/advisories/GHSA-w77f-wv46-4vcx	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

Source	Time	Event
CNA	2017-02-06T00:00:00.000Z	Sereal::Encoder version 4.001_001 released.
CNA	2018-12-27T00:00:00.000Z	Zstandard 1.3.8 released.
CNA	2019-07-25T00:00:00.000Z	CVE-2019-11922 for Zstandard published
CNA	2020-02-04T00:00:00.000Z	Sereal::Encoder version 4.010 released.
CNA	2023-02-09T00:00:00.000Z	Advisory added to the CPANSA database.
CNA	2024-02-17T00:00:00.000Z	Advisory updated in the CPANSA database.

### Solutions

**CNA:** Upgrade to Sereal::Encoder version 4.010 or later.

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

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](#)**