



# Perl versions from 5.9.4 before 5.40.4-RC1, from 5.41.0 before 5.42.2-RC1, from 5.43.0 before 5.43.9 contain a vulnerable version of Compress::Raw::Zlib

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-4176
<b>State</b>	PUBLISHED
<b>Assigner</b>	CPANSec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-29 21:16:15 UTC
<b>Updated</b>	2026-03-30 16:16:08 UTC
<b>Description</b>	Perl versions from 5.9.4 before 5.40.4-RC1, from 5.41.0 before 5.42.2-RC1, from 5.43.0 before 5.43.9 contain a vulnerable

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from ADP

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

**EPSS:** 0.000190000 probability, percentile 0.050730000 (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	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## 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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SHAY	Perl	affected 5.9.4 5.40.4-RC1 custom	Not specified
CNA	SHAY	Perl	affected 5.41.0 5.42.2-RC1 custom	Not specified
CNA	SHAY	Perl	affected 5.43.0 5.43.9 custom	Not specified

### References

Reference	Source	Link
www.cve.org/CVERecord	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://www.cve.org">www.cve.org</a>
metacpan.org/release/SHAY/perl-5.40.4/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://metacpan.org">metacpan.org</a>
metacpan.org/release/SHAY/perl-5.42.2/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://metacpan.org">metacpan.org</a>
www.openwall.com/lists/oss-security/2026/03/30/2	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>
github.com/Perl/perl5/commit/c75ae9cc164205e1b6d6dbd57bd2c65c8593fe94	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://github.com">github.com</a>
metacpan.org/release/PMQS/Compress-Raw-Zlib-2.221/source/Changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://metacpan.org">metacpan.org</a>
lists.security.metacpan.org/cve-announce/msg/37638919	9b29abf9-4ab0-4765-b253-1875cd9b441e	<a href="http://lists.security.metacpan.org">lists.security.m</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Bernhard Schmalhofer (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-02-27T00:00:00.000Z	Compress::Raw::Zlib 2.221 committed to Perl bleed.
CNA	2026-03-07T00:00:00.000Z	CVE-2026-3381 published for Compress::Raw::Zlib.
CNA	2026-03-14T00:00:00.000Z	CVE-2026-4176 reserved.
CNA	2026-03-29T00:00:00.000Z	Perl 5.40.4 and 5.42.2 released.

## Solutions

**CNA:** Update to Perl stable release 5.40.4 or 5.42.2 or later, which include Compress::Raw::Zlib 2.222.

## Workarounds

**CNA:** Install Compress::Raw::Zlib 2.220 or later into your @INC include path, so it takes precedence over the vulnerable core module shipped with Perl. Some OS distributions patch their perl package to build Compress::Raw::Zlib against the system zlib rather than the vendored copy. Users of these distributions may not be affected if their system zlib has been updated to 1.3.2 or later, or includes backported patches for the relevant vulnerabilities.

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](#)