



# CM Custom Reports <= 1.2.7 - Authenticated (Administrator+) Stored Cross-Site Scripting via Plugin Labels

[MITRE](#)
[NVD](#)
[CVE.ORG](#)
[JSON API](#)
[Print: PDF !\[\]\(666e09182d4cd268646ea700ea60dcdf\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-2432
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-20 09:16:14 UTC
<b>Updated</b>	2026-04-22 21:32:08 UTC
<b>Description</b>	The CM Custom Reports – Flexible reporting to track what matters most plugin for WordPress is vulnerable to Stored Cross

## Risk And Classification

**Primary CVSS:** v3.1 4.4 MEDIUM from security@wordfence.com

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

**EPSS:** 0.000090000 probability, percentile 0.009820000 (date 2026-04-22)

**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Creativemindsolutions	CM Custom Reports Flexible Reporting To Track What Matters Most	affected 1.2.7 semver	Not specifi

### References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/e642b5e1-62c1-4aa9-b579-6b233...	security@wordfence.com	<a href="http://www.wordfence.com/threat-intel/vulnerabilities/id/e642b5e1-62c1-4aa9-b579-6b233...">www.wordfence.com/threat-intel/vulnerabilities/id/e642b5e1-62c1-4aa9-b579-6b233...</a>
plugins.trac.wordpress.org/browser/cm-custom-reports/trunk/backend/classes/modules/Graph...	security@wordfence.com	<a href="http://plugins.trac.wordpress.org/browser/cm-custom-reports/trunk/backend/classes/modules/Graph...">plugins.trac.wordpress.org/browser/cm-custom-reports/trunk/backend/classes/modules/Graph...</a>
plugins.trac.wordpress.org/changeset	security@wordfence.com	<a href="http://plugins.trac.wordpress.org/changeset">plugins.trac.wordpress.org/changeset</a>
plugins.trac.wordpress.org/browser/cm-custom-reports/tags/1.2.7/backend/classes/modules/...	security@wordfence.com	<a href="http://plugins.trac.wordpress.org/browser/cm-custom-reports/tags/1.2.7/backend/classes/modules/...">plugins.trac.wordpress.org/browser/cm-custom-reports/tags/1.2.7/backend/classes/modules/...</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:** san6051 (en)

### Additional Advisory Data

Source	Time	Event
CNA	2026-02-12T21:33:02.000Z	Vendor Notified
CNA	2026-03-19T19:57:41.000Z	Disclosed

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

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)