



CMB2 <= 2.10.1 - Authenticated (Contributor+) PHP Object Injection

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

Summary

CVE	CVE-2024-1792
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-09 19:15:19 UTC
Updated	2026-04-08 19:20:51 UTC

Description The CMB2 plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.10.1 via deseriali

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security@wordfence.com

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

EPSS: 0.006890000 probability, percentile 0.717760000 (date 2026-04-12)

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Jtsternberg	CMB2	affected 2.10.1 semver	Not specified
ADP	Cmb2	Cmb2	affected 2.11.0 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/3062907/cmb2/trunk	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wordpress.org/changeset/3062907/cmb2/trunk
www.wordfence.com/threat-intel/vulnerabilities/id/c3f37ef5-ddf5-4bd5-b6aa-121dd...	af854a3a-2127-422b-91ae-364da2661108	www.wordfence.com/threat-intel/vulnerabilities/id/c3f37ef5-ddf5-4bd5-b6aa-121dd...
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Francesco Carlucci (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-03T00:00:00.000Z	Disclosed

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report