



WordPress embed-code plugin <= 2.3.6 - Denial of Service Attack vulnerability

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

Summary

CVE	CVE-2023-49837
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-21 17:15:07 UTC
Updated	2026-04-28 19:22:28 UTC
Description	Uncontrolled Resource Consumption vulnerability in David Artiss Code Embed.This issue affects Code Embed: from n/a thr

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

EPSS: 0.002530000 probability, percentile 0.486060000 (date 2026-04-28)

Problem Types: CWE-400 | CWE-400 CWE-400 Uncontrolled Resource Consumption

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	audit@patchstack.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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



NVD Known Affected Configurations (CPE 2.3)

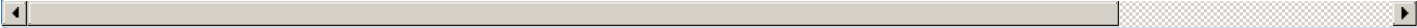
Type	Vendor	Product	Version	Update	Edition	Language
Application	Davidartiss	Code Embed	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	David Artiss	Code Embed	affected n/a 2.3.6 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/simple-embed-code/wordpress-embed-code...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/Wordpress/Plugin/simple-embed-code/vulnerability/wor...	MITRE	patchstack.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



Vendor Comments And Credit

Discovery Credit

CNA: Universe (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.3.7 or a higher version.

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

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](#).

Free CVE JSON API cve.report/api

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