EmbedPress <= 3.8.2 - Missing Authorization to Authenticated (Subscriber+) Plugin Settings Delete via admin_post_remove and remove_private_data

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-4282
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-10 12:15:12 UTC
Updated	2026-04-08 18:18:13 UTC
Description	The EmbedPress plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the '

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	security@wordfence.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpdeveloper	Embedpress	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Wpdevteam	EmbedPress PDF Embedder Embed YouTube Videos 3D FlipBook Social Feeds Docs More	affected 3.8.2 semver

References

Reference
403 Forbidden
403 Forbidden
EmbedPress <= 3.8.2 - Missing Authorization to Authenticated (Subscriber+) Plugin Settings Delete via admin_post_remove and remove_priv
403 Forbidden
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-08-02T00:00:00.000Z	Discovered
CNA	2023-08-02T00:00:00.000Z	Vendor Notified
CNA	2023-08-09T00:00:00.000Z	Disclosed

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

Free CVE JSON API cve.report/api

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