ClickCease Click Fraud Protection <= 3.2.4 - Improper Authorization to sensitive information exposure via get_settings

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

Summary

CVE	CVE-2023-6810
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-07 10:15:06 UTC
Updated	2026-04-08 18:18:42 UTC
Description	The ClickCease Click Fraud Protection plugin for WordPress is vulnerable to unauthorized access of data due to an improp

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from security@wordfence.com

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

Problem Types: CWE-284 | CWE-284 CWE-284 Improper Access Control

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Eranfl	ClickCease Click Fraud Protection	affected 3.2.4 semver	Not specified

References

Reference	Source	Lir
plugins.trac.wordpress.org/changeset/3081436/clickcease-click-fraud-protection/trunk/cla...	af854a3a-2127-422b-91ae-364da2661108	plu
www.wordfence.com/threat-intel/vulnerabilities/id/5d572cac-b8e3-4c52-9b35-80fe5...	af854a3a-2127-422b-91ae-364da2661108	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

Vendor Comments And Credit

Discovery Credit

CNA: Francesco Carlucci (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-05-06T00:00:00.000Z	Disclosed

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