Subway – Private Site Option <= 2.1.4 - Improper Access Control to Sensitive Information Exposure via REST API

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

Summary

CVE	CVE-2024-1678
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-02 17:15:12 UTC
Updated	2026-04-08 18:20:45 UTC
Description	The Subway – Private Site Option plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from security@wordfence.com

CVSS:3.1/AV:N/AC:L/PR:N/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	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

vailability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Dunhakdis	Subway Private Site Option	affected 2.1.4 semver	Not specified
ADP	Dunhakdis	Subway-private Site Option	affected 2.1.4 semver	Not specified

References

Reference	Source	Link
wordpress.org/plugins/subway	af854a3a-2127-422b-91ae-364da2661108	wordpre
www.wordfence.com/threat-intel/vulnerabilities/id/5b80638b-4dd1-47f5-9a70-6bd62...	af854a3a-2127-422b-91ae-364da2661108	www.wo
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

CNA: Francesco Carlucci (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-29T00:00:00.000Z	Disclosed

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