Tainacan Interface <= 2.7.2 - Reflected Cross-Site Scripting

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

Summary

CVE	CVE-2024-3867
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-16 10:15:08 UTC
Updated	2026-04-08 18:21:34 UTC
Description	The archive-tainacan-collection theme for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from security@wordfence.com

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

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tainacan	Tainacan Interface	affected 2.7.2 semver	Not specified

References

Reference	Source	L
themes.trac.wordpress.org/changeset/224400/tainacan-interface/2.7.2/archive-tainacan-co...	af854a3a-2127-422b-91ae-364da2661108	th
www.wordfence.com/threat-intel/vulnerabilities/id/3ffd63ca-5ea4-451c-aa97-092a7...	af854a3a-2127-422b-91ae-364da2661108	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

Vendor Comments And Credit

Discovery Credit

CNA: Matheus Nascimento de Camargo (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-15T00:00:00.000Z	Disclosed

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