

WordPress 3D Tag Cloud Plugin <= 3.8 is vulnerable to Cross Site Request Forgery (CSRF)

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2022-41990
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-17 17:15:09 UTC
Updated	2026-04-28 19:18:51 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in Vinoj Cardoza 3D Tag Cloud allows Stored XSS.This issue affects 3D Tag Cloud 3.8 and below

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cardozatechnologies	Cardoza-3d-tag-cloud	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Vinoj Cardoza	3D Tag Cloud	affected n/a 3.8 custom	Not specified

References

Reference

WordPress 3D Tag Cloud plugin <= 3.8 - Stored Cross-Site Scripting (XSS) via Cross-Site Request Forgery (CSRF) vulnerability - Patchstack

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (Patchstack Alliance) (en)

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