UX Flat <= 4.4 - Authenticated(Contributor+) Stored Cross-Site Scripting via Shortcode

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

Summary

CVE	CVE-2024-2459
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-20 07:15:11 UTC
Updated	2026-04-08 17:18:34 UTC
Description	The UX Flat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'button' shortcode in all versic

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from security@wordfence.com

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

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	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
3.1	CNA	DECLARED	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Changed

Confidentiality
Low

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wpvncom	UX Flat	affected 4.4 semver	Not specified

References

Reference	Source	Link
wordpress.org/plugins/ux-flat	af854a3a-2127-422b-91ae-364da2661108	wordpres
plugins.trac.wordpress.org/changeset/3064741	security@wordfence.com	plugins.t
www.wordfence.com/threat-intel/vulnerabilities/id/1d93db2c-7baf-42d8-9b4a-be91b...	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	2024-03-19T00:00:00.000Z	Disclosed

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