BuddyPress <= 12.4.0 - Authenticated (Subscriber+) Stored Cross-Site Scripting

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

Summary

CVE	CVE-2024-3974
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-14 15:42:39 UTC
Updated	2026-04-08 18:21:38 UTC
Description	The BuddyPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'user_name' parameter in versior

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/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	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Buddypress	Buddypress	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Buddypress	BuddyPress	affected 12.4.0 semver	Not specified

References

Reference	Source	Li
plugins.trac.wordpress.org/browser/buddypress/trunk/bp-members/bp-members-blocks.php	af854a3a-2127-422b-91ae-364da2661108	plu
www.wordfence.com/threat-intel/vulnerabilities/id/3657384e-025a-44ad-8b7e-1a2fe...	af854a3a-2127-422b-91ae-364da2661108	ww
plugins.trac.wordpress.org/changeset/3079691/buddypress	af854a3a-2127-422b-91ae-364da2661108	plu
plugins.trac.wordpress.org/browser/buddypress/trunk/bp-members/bp-members-admin.php	af854a3a-2127-422b-91ae-364da2661108	plu
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

CNA: wesley (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-05-03T00:00:00.000Z	Disclosed

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**