BuddyForms <= 2.8.9 - Email Verification Bypass due to Insufficient Randomness

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

Summary

CVE	CVE-2024-5149
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-06-05 05:15:50 UTC
Updated	2026-04-08 19:21:51 UTC
Description	The BuddyForms plugin for WordPress is vulnerable to Email Verification Bypass in all versions up to, and including, 2.8.9 v

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from nvd@nist.gov

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

EPSS: 0.003590000 probability, percentile 0.581460000 (date 2026-04-12)

Problem Types: CWE-330 | CWE-330 CWE-330 Use of Insufficiently Random Values

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	security@wordfence.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Themekraft	Buddyforms	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	V
CNA	Themekraft	Post Form Registration Form Profile Form For User Profiles Frontend Content Forms For User Submissions UGC	a
ADP	Themekraft	Post Form Registration Form Profile Form For User Profiles And Content Forms	a

References

Reference	Source	I
plugins.trac.wordpress.org/browser/buddyforms/tags/2.8.9/includes/wp-insert-user.php	af854a3a-2127-422b-91ae-364da2661108	p
www.wordfence.com/threat-intel/vulnerabilities/id/a5c8d361-698b-4abd-bcdd-0361d...	af854a3a-2127-422b-91ae-364da2661108	v
plugins.trac.wordpress.org/changeset/3101478/buddyforms/trunk/includes/wp-insert-user.php	security@wordfence.com	p
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-05-20T00:00:00.000Z	Discovered
CNA	2024-06-04T00:00:00.000Z	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