WordPress Clone plugin <= 2.3.7 - Broken Access Control vulnerability

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

Summary

CVE	CVE-2023-25486
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-09 13:15:23 UTC
Updated	2026-04-28 19:19:48 UTC
Description	Missing Authorization vulnerability in Migrate Clone allows Exploiting Incorrectly Configured Access Control Security Levels

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.001730000 probability, percentile 0.384000000 (date 2026-04-28)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Migrate	Clone	affected n/a 2.3.7 custom	Not specified

References

Reference
patchstack.com/database/wordpress/plugin/wp-clone-by-wp-academy/vulnerabilit...
https://patchstack.com/database/wordpress/plugin/wp-clone-by-wp-academy/vulnerability/wordpress-clone-plugin-2-3-7-broken-access-contro
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Mika (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress Clone plugin to the latest available version (at least 2.3.8).

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