WordPress WP Directory Kit plugin <= 1.2.6 - Broken Access Control vulnerability

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

Summary

CVE	CVE-2023-41875
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-13 15:15:25 UTC
Updated	2026-04-28 19:21:21 UTC
Description	Missing Authorization vulnerability in wpdirectorykit.com WP Directory Kit allows Exploiting Incorrectly Configured Access C

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.005460000 probability, percentile 0.679550000 (date 2026-05-09)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpdirectorykit	Wp Directory Kit	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wpdirectorykit.com	WP Directory Kit	affected n/a 1.2.6 custom	Not specified

References

Reference
patchstack.com/database/wordpress/plugin/wpdirectorykit/vulnerability/wordpr...
https://patchstack.com/database/wordpress/plugin/wpdirectorykit/vulnerability/wordpress-wp-directory-kit-plugin-1-2-6-broken-access-control-v
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Debangshu Kundu & Arpeet Rathi (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress WP Directory Kit plugin to the latest available version (at least 1.2.7).

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