



WP Directory Kit <= 1.1.9 - Cross-Site Request Forgery to Stored Cross-Site Scripting via wdk_resultitem

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-2277
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-13 02:15:09 UTC
Updated	2026-04-08 18:17:59 UTC
Description	The WP Directory Kit plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1

Risk And Classification

Primary CVSS: v3.1 4.7 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N
3.1	security@wordfence.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

None

Integrity

Low

Availability

None

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

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	WP Directory Kit	affected 1.1.9 semver	Not specified

References

Reference	Source
403 Forbidden	af854a3a-2127-422b-91ae-364da
WP Directory Kit <= 1.1.9 - Cross-Site Request Forgery to Stored Cross-Site Scripting via wdk_resultitem	af854a3a-2127-422b-91ae-364da
403 Forbidden	af854a3a-2127-422b-91ae-364da
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-04-24T00:00:00.000Z	Discovered
CNA	2023-04-25T00:00:00.000Z	Vendor Notified
CNA	2023-04-28T00:00:00.000Z	Disclosed

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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