CVE-2021-4362

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

Summary

CVE	CVE-2021-4362
State	PUBLIC
Assigner	security@wordfence.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-07 02:15:00 UTC
Updated	2023-11-07 03:40:00 UTC
Description	The Kiwi Social Share plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the k

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpkube	Kiwi Social Share	2.1.0	All	All	All

References

Reference	Source	Link	Tags
Kiwi Social Sharing 2.1.0 - 2.1.2 - Arbitrary Options Change	MISC	www.wordfence.com	
WordPress Kiwi Social Sharing plugin fixed critical vulnerability. – NinTechNet	MISC	blog.nintechnet.com	
Social Sharing Plugin – Kiwi – WordPress plugin | WordPress.org	MISC	wordpress.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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