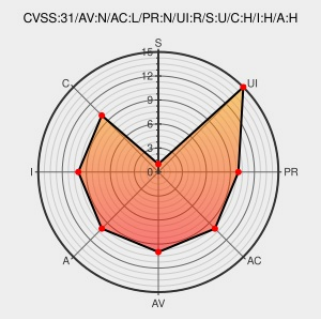
CVE-2022-1749

Published on: Not Yet Published

Last Modified on: 11/07/2023 03:42:00 AM UTC

CVE-2022-1749

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wpmk Ajax Finder from Wpmk Ajax Finder Project contain the following vulnerability:

The WPMK Ajax Finder WordPress plugin is vulnerable to Cross-Site Request Forgery via
the createplugin_atf_admin_setting_page() function found in the ~/inc/config/create-plugin-config.php file due to a missing nonce check which allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.1.

CVE-2022-1749 has been assigned by security@wordfence.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **createplugin** - **WPMK Ajax Finder** version **<= 1.0.1**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Vulnerability Advisories - Wordfence	www.wordfence.com text/html	MISC www.wordfence.com/vulnerability-advisories/#CVE-2022-1749
WPMK Ajax Finder <= 1.0.1 - Cross-Site Request Forgery to Cross-Site Scripting	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/1d063d01-5f67-4c7f-ab71-01708456e82b?source=cve
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/find-any-think/trunk/inc/config/create-plugin-admin.php

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpmk Ajax Finder Project	Wpmk Ajax Finder	All	All	All	All

cpe:2.3:a:wpmk_ajax_finder_project:wpmk_ajax_finder:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-1749 : The WPMK Ajax Finder WordPress plugin is vulnerable to Cross-Site Request Forgery via the createplu… twitter.com/i/web/status/1…	2022-06-13 14:06:32
@LinInfoSec	Php - CVE-2022-1749: wordfence.com/vulnerability-…	2022-06-13 18:00:22
@phpadvisories	CVE-2022-1749 | WPMK Ajax Finder Plugin bis 1.0.1 auf WordPress create-plugin-config.php createplugin_atf_admin_set… twitter.com/i/web/status/1…	2022-06-13 20:10:23
/r/netcve	CVE-2022-1749	2022-06-13 15:38:15

← Previous ID Next ID→