



CVE-2022-4211

Published on: Not Yet Published

Last Modified on: 12/05/2022 08:40:00 PM UTC

CVE-2022-4211

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Chained Quiz](#) from [Kibokolabs](#) contain the following vulnerability:

The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'emailf' parameter on the 'chainedquiz_list' page in versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.

CVE-2022-4211 has been assigned by security@wordfence.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **prasunsen** - **Chained Quiz** version = *

CVSS3 Score: **6.1 - MEDIUM**

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

CVE References

Description	Tags	Link
Vulnerability Advisories Continued - Wordfence	www.wordfence.com text/html	MISC www.wordfence.com/vulnerability-advisories-continued/#CVE-2022-4211
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/changeset?sfp_email=&sfp_mail=&reponame=&old=2824193%40chainedquiz&new=2824193%40chained-quiz&sfp_email=&sfp_mail=
WP plugin Chained Quiz multiple vulnerabilities · GitHub	gist.github.com text/html	MISC gist.github.com/Xib3rR4dAr/417a11bcb9b8da28cfe5ba1c17c44d0e

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	Kibokolabs	Chained Quiz	All	All	All	All

cpe:2.3:a:kibokolabs:chained_quiz:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @sidfm_jp	Liferay Portal CE の Portal Search モジュールの処理にクロスサイトスクリプティングの問題 (CVE-2022-4211 [43739] sid.softtek.jp/content/show/4... #SIDfm #脆弱性情報	2022-10-25 04:30:10
 @CVEreport	CVE-2022-4211 : The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'email...' twitter.com/i/web/status/1...	2022-12-02 21:05:02
 @threatmeter	CVE-2022-4211 Chained Quiz Plugin up to 1.3.2 on WordPress chainedquiz_list emailf cross site scripting A vulnera... twitter.com/i/web/status/1...	2022-12-03 08:51:16
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-4211 - The Chained Quiz plugin for WordPress is vulnerable to Reflected Cross... twitter.com/i/web/status/1...	2022-12-03 08:51:22
 /r/netcve	CVE-2022-4211	2022-12-02 21:53:03

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)