



CVE-2022-1951

Published on: Not Yet Published

Last Modified on: 07/15/2022 08:03:00 PM UTC

CVE-2022-1951

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Core Plugin For Kitestudio Themes](#) from [Kitestudio](#) contain the following vulnerability:

The core plugin for kitestudio WordPress plugin before 2.3.1 does not sanitise and escape some parameters before outputting them back in a response of an AJAX action, available to both unauthenticated and authenticated users when a premium theme from the vendor is active, leading to a Reflected Cross-Site Scripting.

CVE-2022-1951 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - core plugin for kitestudio themes** version < 2.3.1

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Core Plugin for Kitestudio Themes < 2.3.1 - Reflected Cross-Site-	web.archive.org	

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	Kitestudio	Core Plugin For Kitestudio Themes	All	All	All	All
cpe:2.3:a:kitestudio:core_plugin_for_kitestudio_themes:*:*:*:*:wordpress:*:*:						

Discovery Credit

cydave

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1951 : The core plugin for kitestudio WordPress plugin before 2.3.1 does not sanitise and escape some par... twitter.com/i/web/status/1...	2022-07-11 13:08:44
 @LinInfoSec	Wordpress - CVE-2022-1951: wpscan.com/vulnerability/...	2022-07-11 15:00:38
 /r/netcve	CVE-2022-1951	2022-07-11 14:38:54

← Previous ID

Next ID→