



CVE-2021-24600

Published on: 09/20/2021 12:00:00 AM UTC

Last Modified on: 10/01/2021 04:16:00 PM UTC

CVE-2021-24600

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Wp Dialog** from **Wp Dialog Project** contain the following vulnerability:

The WP Dialog WordPress plugin through 1.2.5.5 does not sanitise and escape some of its settings before outputting them in pages, allowing high privilege users to perform Cross-Site Scripting attacks even when the `unfiltered_html` capability is disallowed.

CVE-2021-24600 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - WP Dialog** version **<= 1.2.5.5**

CVSS3 Score: **4.8 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link
Attention Required! Cloudflare	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/413b3a2e-1c05-45ec-b00f-1c137a1ae33e

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

Exploit/POC from Github

PoC for exploiting CVE-2021-24600 : The WP Dialog WordPress plugin through 1.2.5.5 does not sanitise and escape some ...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp Dialog Project	Wp Dialog	All	All	All	All
cpe:2.3:a:wp_dialog_project:wp_dialog:*:*:*:*:wordpress:*:*:						

Discovery Credit

liaoja@webray.com.cn inc

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-24600 : The WP Dialog WordPress plugin through 1.2.5.5 does not sanitise and escape some of its settings b... twitter.com/i/web/status/1...	2021-09-20 10:17:25

[← 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](#)