

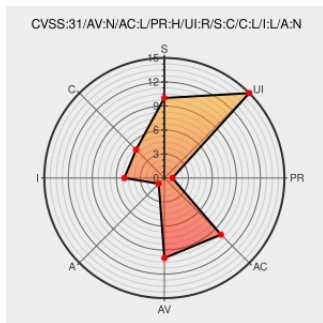


CVE-2022-1558

Published on: Not Yet Published

Last Modified on: 05/30/2022 12:29:00 AM UTC

CVE-2022-1558

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

Certain versions of [Curtain](#) from [Curtain Project](#) contain the following vulnerability:

The Curtain WordPress plugin through 1.0.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed

CVE-2022-1558 has been assigned by [contact@wpscan.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Unknown](#) - **Curtain** version <= 1.0.2

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/0414dad4-e90b-4122-8b77-a8a958ab824d

WordPress Curtain 1.0.2 Cross Site Scripting ≈
Packet Storm

[packetstormsecurity.com](https://packetstormsecurity.com/text/html)
text/html

 [MISC packetstormsecurity.com/files/166839/](https://packetstormsecurity.com/files/166839/)

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	Curtain Project	Curtain	All	All	All	All
cpe:2.3:a:curtain_project:curtain:*:*:*:*:wordpress:*:*						

Discovery Credit

Hassan Khan Yusufzai

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1558 : The Curtain WordPress plugin through 1.0.2 does not sanitise and escape some of its settings, which... twitter.com/i/web/status/1...	2022-05-23 07:24:36
 @Inceptus3	New Vulnerability: CVE-2022-1558 #InceptusSecure #UnderOurProtection	2022-05-23 10:17:58
 @LinInfoSec	Wordpress - CVE-2022-1558: packetstormsecurity.com/files/166839/	2022-05-23 11:00:18
 /r/netcve	CVE-2022-1558	2022-05-23 08:38:32

[← 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](#)