



# CVE-2022-4747

Published on: Not Yet Published

Last Modified on: 02/14/2023 05:16:00 PM UTC

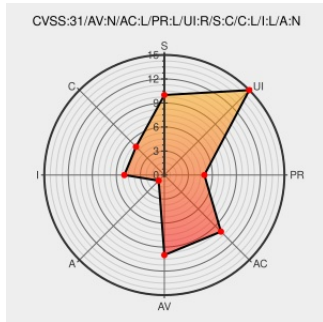
## CVE-2022-4747

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Download Post Category Image With Grid And Slider](#) from [Essentialplugin](#) contain the following vulnerability:

The Post Category Image With Grid and Slider WordPress plugin before 1.4.8 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.

CVE-2022-4747 has been assigned by [contact@wpscan.com](mailto:contact@wpscan.com) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - Post Category Image With Grid and Slider** version = 0

CVSS3 Score: **5.4 - MEDIUM**

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

## CVE References

Description	Tags	Link
Post Category Image With Grid and Slider < 1.4.8 - Contributor+ Stored XSS via Shortcode WordPress Security Vulnerability	<a href="#">web.archive.org</a> <a href="#">text/html</a> <span>Inactive Link</span> <span>Not Archived</span>	<b>MISC</b> <a href="https://wpscan.com/vulnerability/004f1872-1576-447f-8837-f29fa319cbdc">wpscan.com/vulnerability/004f1872-1576-447f-8837-f29fa319cbdc</a>

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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Exploit/POC from Github

The Post Category Image With Grid and Slider WordPress plugin before 1.4.8 does not validate and escape some of its s...


#### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Essentialplugin</a>	<a href="#">Download Post Category Image With Grid And Slider</a>	All	All	All	All

cpe:2.3:a:essentialplugin:download\_post\_category\_image\_with\_grid\_and\_slider:\*:\*:\*:\*:wordpress:\*:\*:

No vendor comments have been submitted for this CVE

#### Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-4747 : The Post Category Image With Grid and Slider WordPress plugin before 1.4.8 does not validate and es... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2023-02-06 20:09:09

[← 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](https://status.cve.report)