



CVE-2021-24457

Published on: 08/02/2021 12:00:00 AM UTC

Last Modified on: 08/10/2021 01:32:00 AM UTC

CVE-2021-24457

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

Certain versions of [Portfolio Responsive Gallery](#) from [Ays-pro](#) contain the following vulnerability:

The `get_portfolios()` and `get_portfolio_attributes()` functions in the `class-portfolio-responsive-gallery-list-table.php` and `class-portfolio-responsive-gallery-attributes-list-table.php` files of the Portfolio Responsive Gallery WordPress plugin before 1.1.8 did not use whitelist or validate the `orderby` parameter before using it in SQL statements passed to the `get_results()` DB calls, leading to SQL injection issues in the admin dashboard

CVE-2021-24457 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Ays Pro - Portfolio Responsive Gallery** version < 1.1.8

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------



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	Ays-pro	Portfolio Responsive Gallery	All	All	All	All

cpe:2.3:a:ays-pro:portfolio_responsive_gallery:*:*:*:*:wordpress:*:*:

Discovery Credit

To Quang Duong

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-24457 : The get_portfolios and get_portfolio_attributes functions in the class-portfolio-responsive-ga... twitter.com/i/web/status/1...	2021-08-02 10:42:54
@LinInfoSec	Wordpress - CVE-2021-24457: wpscan.com/vulnerability/...	2021-08-02 12:41:53

[← Previous ID](#)

[Next ID →](#)