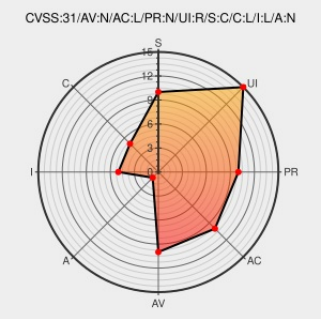
CVE-2021-38348

Published on: 09/10/2021 12:00:00 AM UTC

Last Modified on: 09/21/2021 02:17:00 PM UTC

CVE-2021-38348

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Advance Search from Advance Search Project contain the following vulnerability:

The Advance Search WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the wpas_id parameter found in the ~/inc/admin/views/html-advance-search-admin-options.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.1.2.

CVE-2021-38348 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Advance Search** - **Advance Search** version **<= 1.1.2**

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
Vulnerability Advisories -	www.wordfence.com	MISC www.wordfence.com/vulnerability-advisories/#CVE-2021-38348

Wordfence	text/html	
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/advance-search/trunk/inc/admin/views/html-advance-search-admin-options.php#L88

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	Advance Search Project	Advance Search	All	All	All	All

cpe:2.3:a:advance_search_project:advance_search:*:*:*:*:*:wordpress:*:*:

Discovery Credit

p7e4

Social Mentions

Source	Title	Posted (UTC)
@threatmeter	CVE-2021-38348 The Advance Search WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the wpas_id… twitter.com/i/web/status/1…	2021-09-11 07:09:40

← Previous ID

Next ID→