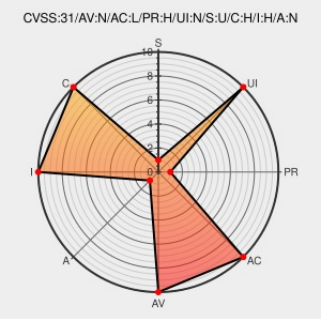
CVE-2021-43408

Published on: Not Yet Published

Last Modified on: 11/24/2021 04:53:00 PM UTC

CVE-2021-43408

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



Certain versions of Duplicate Post from Duplicate Post Project contain the following vulnerability:

The "Duplicate Post" WordPress plugin up to and including version 1.1.9 is vulnerable to SQL Injection. SQL injection vulnerabilities occur when client supplied data is included within an SQL Query insecurely. SQL Injection can typically be exploited to read, modify and delete SQL table data. In many cases it also possible to exploit features of SQL server to execute system commands and/or access the local file system. This particular vulnerability can be exploited by any authenticated user who has been granted access to use the Duplicate Post plugin. By default, this is limited to Administrators, however the plugin presents the option to permit access to the Editor, Author, Contributor and Subscriber roles.

CVE-2021-43408 has been assigned by info@appcheck-ng.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Copy Delete Posts** - **Duplicate Post WordPress Plugin** version **< 1.2.0**

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: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Duplicate Post WordPress Plugin SQL Injection Vulnerability	appcheck-ng.com text/html	MISC appcheck-ng.com/security-advisory-duplicate-post-wordpress-plugin-sql-injection-vulnerability/
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/copy-delete-posts/tags/1.2.0/post/handler.php#L510

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	Duplicate Post Project	Duplicate Post	All	All	All	All

cpe:2.3:a:duplicate_post_project:duplicate_post:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43408 : The Duplicate Post WordPress plugin up to and including version 1.1.9 is vulnerable to SQL Injecti… twitter.com/i/web/status/1…	2021-11-19 16:10:26
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-43408 Description: The Duplicate Post WordPress plugin up to and includ… twitter.com/i/web/status/1…	2021-11-19 17:00:10

← Previous ID Next ID→