



CVE-2022-4160

Published on: Not Yet Published

Last Modified on: 01/10/2023 10:09:18 AM UTC

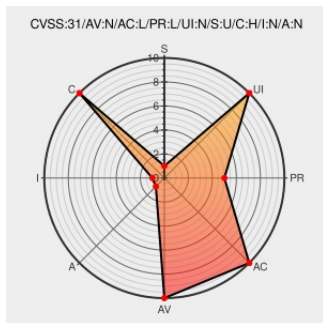
CVE-2022-4160

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Contest Gallery](#) from [Contest-gallery](#) contain the following vulnerability:

The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the `cg_copy_id` POST parameter before concatenating it to an SQL query in `cg-copy-comments.php` and `cg-copy-rating.php`. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.

CVE-2022-4160 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Unknown - Contest Gallery** version = 0

Affected Vendor/Software: **Unknown - Contest Gallery Pro** version = 0

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
Contest Gallery < 19.1.5 - Author+ SQL Injection WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/813de343-4814-42b8-b8df-1695320512cd
Security Bulletin	bulletin.iese.de text/html	MISC bulletin.iese.de/post/contest-gallery_19-1-4-1_14

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	Contest-gallery	Contest Gallery	All	All	All	All
Application	Contest-gallery	Contest Gallery	All	All	All	All
cpe:2.3:a:contest-gallery:contest_gallery:*:*:*:*:wordpress:*:*:						
cpe:2.3:a:contest-gallery:contest_gallery:*:*:*:*:pro:wordpress:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-4160 : The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 1... twitter.com/i/web/status/1...	2022-12-26 13:13:30
 /r/netcve	CVE-2022-4160	2022-12-26 14:38:50

[← Previous ID](#)

[Next ID→](#)