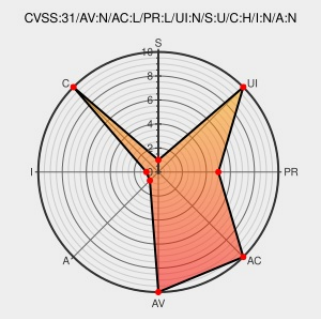
CVE-2023-5429

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:23:00 AM UTC

CVE-2023-5429

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



Certain versions of Information Reel from Gopiplus contain the following vulnerability:

The Information Reel plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with subscriber-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

CVE-2023-5429 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **gopiplus** - **Information Reel** version **<= 10.0**

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
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/changeset/2985373/information-reel#file1
Information Reel <= 10.0 - Authenticated (Subscriber+) SQL Injection via Shortcode	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/64db63e5-ff76-494a-be4f-d820f0cc9ab0?source=cve
403 Forbidden	plugins.trac.wordpress.org text/html	MISC plugins.trac.wordpress.org/browser/information-reel/trunk/information-reel.php?rev=2827123#L134

Inactive Link Not Archived

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	Gopiplus	Information Reel	All	All	All	All

cpe:2.3:a:gopiplus:information_reel:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→