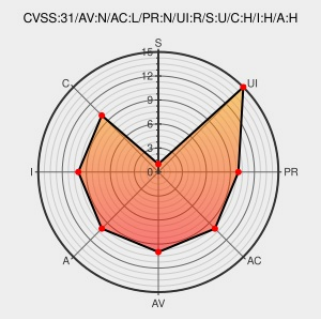
CVE-2022-2233

Published on: Not Yet Published

Last Modified on: 10/24/2023 08:43:00 PM UTC

CVE-2022-2233

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



Certain versions of Banner Cycler from Banner Cycler Project contain the following vulnerability:

The Banner Cycler plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including 1.4. This is due to missing nonce protection on the pabc_admin_slides_postback() function found in the ~/admin/admin.php file. This makes it possible for unauthenticated attackers to inject malicious web scripts into the page, granted they can trick a site's administrator into performing an action such as clicking on a link

CVE-2022-2233 has been assigned by security@wordfence.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **jkriddle** - **Banner Cycler** version **<= 1.4**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/banner-cycler/trunk/admin/admin.php#L131
Banner Cycler <= 1.4 - Cross-Site Request Forgery to Cross-Site Scripting	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/6cc1d7f2-053d-42d4-afb7-6fb69fd71b91?source=cve
Vulnerability Advisories - Wordfence	www.wordfence.com text/html	MISC www.wordfence.com/vulnerability-advisories/#CVE-2022-2233

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	Banner Cycler Project	Banner Cycler	All	All	All	All

cpe:2.3:a:banner_cycler_project:banner_cycler:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-2233 : The Banner Cycler plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up t… twitter.com/i/web/status/1…	2022-09-06 18:04:20
@LinInfoSec	Wordpress - CVE-2022-2233: wordfence.com/vulnerability-…	2022-09-06 21:01:01

← Previous ID

Next ID→