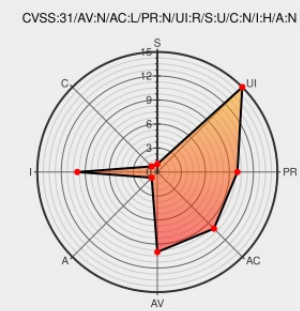
CVE-2015-9434

Published on: 09/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9434

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



Certain versions of Kiwi-logo-carousel from Kiwi-logo-carousel Project contain the following vulnerability:

The kiwi-logo-carousel plugin before 1.7.2 for WordPress has CSRF with resultant XSS via the wp-admin/edit.php?post_type=kwlogos&page=kwlogos_settings tab or tab_flags_order parameter.

CVE-2015-9434 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	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
Kiwi Logo Carousel <= 1.7.1 - Authenticated Cross-Site Scripting (XSS)	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC wpvulndb.com/vulnerabilities/8290

WordPress › Kiwi Logo Carousel « WordPress Plugins	Product Third Party Advisory wordpress.org text/html	MISC wordpress.org/plugins/kiwi-logo-carousel/#developers
No Description Provided	Exploit Third Party Advisory cinu.pl text/html	MISC cinu.pl/research/wp-plugins/mail_3764bb40db5ed12aac2c7812d7544730.html

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	Kiwi-logo-carousel Project	Kiwi-logo-carousel	All	All	All	All
Application	Kiwi-logo-carousel Project	Kiwi-logo-carousel	All	All	All	All

cpe:2.3:a:kiwi-logo-carousel_project:kiwi-logo-carousel:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:kiwi-logo-carousel_project:kiwi-logo-carousel:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→