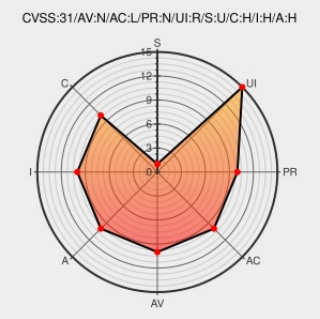
CVE-2021-20846

Published on: 11/24/2021 12:00:00 AM UTC

Last Modified on: 11/29/2021 05:10:00 PM UTC

CVE-2021-20846

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Push Notifications For Wordpress from Delitestudio contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in Push Notifications for WordPress (Lite) versions prior to 6.0.1 allows a remote attacker to hijack the authentication of an administrator and conduct an arbitrary operation via a specially crafted web page.

CVE-2021-20846 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Delite Studio** - **Push Notifications for WordPress (Lite)** version **versions prior to 6.0.1**

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Push Notifications for WordPress (Lite) – WordPress plugin | WordPress.org	wordpress.org text/html	MISC wordpress.org/plugins/push-notifications-for-wp/

JVN#85492429: WordPress Plugin "Push Notifications for WordPress (Lite)" vulnerable to cross-site request forgery	jvn.jp text/xml	MISC jvn.jp/en/jp/JVN85492429/index.html
Delite Studio | We make software.	delitestudio.com text/html	MISC delitestudio.com/en/

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	Delitestudio	Push Notifications For Wordpress	All	All	All	All
Application	Delitestudio	Push Notifications For Wordpress Lite	All	All	All	All

cpe:2.3:a:delitestudio:push_notifications_for_wordpress:*:*:*:*:lite:wordpress:*:*:

cpe:2.3:a:delitestudio:push_notifications_for_wordpress_lite:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-20846 : Cross-site request forgery CSRF vulnerability in Push Notifications for WordPress Lite version… twitter.com/i/web/status/1…	2021-11-24 10:45:16

← Previous ID

Next ID→