



# CVE-2021-20846

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

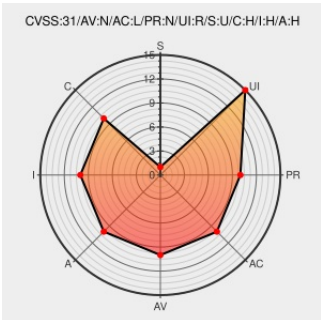
Last Modified on: 11/29/2021 05:10:00 PM UTC

## 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
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>PARTIAL</b>	<b>PARTIAL</b>	<b>PARTIAL</b>

## CVE References

Description	Tags	Link
Push Notifications for WordPress (Lite) – WordPress plugin   WordPress.org	<a href="#">wordpress.org</a> <a href="#">text/html</a>	<a href="#">MISC</a> <a href="#">wordpress.org/plugins/push-notifications-for-wp/</a>

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](mailto: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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-11-24 10:45:16

← Previous ID

Next ID →

© CVE.report 2021 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**