WPScan

WordPress Plugin Vulnerabilities

Popup Maker < 1.16.11 - Admin+ Stored Cross Site Scripting

Description

The plugin does not sanitise and escape some of its Popup options, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)

Proof of Concept

```
Create a New popup
Insert pop-up name, title, and body text.
Add a new trigger with default settings, choose "Click Open" and under "On Popup
Close" then click add.
Click add new cookie and in the cookie name add the payload as cookie name:
<script>alert("XSS")</script>
The XSS will be triggered when editing a trigger
```

Affects Plugins

popup-maker

Fixed in version 1.16.11 ✓

References

CVE

CVE-2022-3690

Classification

Type
XSS

OWASP top 10
A7: Cross-Site Scripting (XSS)

CWE
CWE-79

Miscellaneous

Original Researcher
c3p0d4y

Submitter
c3p0d4y

Submitter twitter
https://twitter.com/c3p01337

Verified
Yes

WPVDB ID
725f6ae4-7ec5-4d7c-9533-c9b61b59cc2b

Timeline

Publicly Published

2022-10-31 (about 25 days ago)

Added

2022-10-31 (about 25 days ago)

Last Updated

2022-10-31 (about 25 days ago)

Our Other Services

WPScan WordPress Security Plugin

Vulnerabilities

WordPress

Plugins

Themes

Our Stats

Submit vulnerabilities

About

How it works

Pricing

WPScan

WordPress plugin

News

Contact

For Developers

Status

API details

CLI scanner

Other

Privacy

Terms of service

Submission terms

Disclosure policy

In partnership with Jetpack

An endeavor

Work With Us