WPScan

WordPress Plugin Vulnerabilities

Evaluate <= 1.0 - Admin+ Stored Cross-Site Scripting

Description

The plugin does not sanitize and escapes some of its settings, 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

1. Go to Settings » Evaluate » Add New.
2. Add the payload: <script>alert(1)</script>, and the payload trigger.

Affects Plugins

evaluate

No known fix - plugin closed ×

References

CVE

CVE-2022-3753

WPScan

Classification

Type
XSS

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

CWE
CWE-79

Miscellaneous

Original Researcher
Mariah Almotlag

Submitter
Mariah Almotlag

Verified
Yes

WPVDB ID
8e88a5b9-6f1d-40de-99fc-8e1e66646c2b

Timeline

Publicly Published
2022-10-29 (about 27 days ago)

Added
2022-10-29 (about 27 days ago)

Last Updated

2022-10-29 (about 27 days ago)

WPScan

Our Other Services

WPScan WordPress Security Plugin

Vulnerabilities

WordPress

Plugins

Themes

Our Stats

Submit vulnerabilities

About

How it works

Pricing

WordPress plugin

News

Contact

For Developers

WPScan

Status

API details

CLI scanner

Other

Privacy

Terms of service

Submission terms

Disclosure policy

In partnership with Jetpack

An endeavor

Work With Us