WPScan

WordPress Plugin Vulnerabilities

Spacer < 3.0.7 - Admin+ Stored XSS

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

```
Add new Spacers and add payload "><h1 onclick=alert(document.domain)>Gem</h1> to
Settings » Spacer » Add Spacers » New Spacer » Space Title and submit.
```

Affects Plugins

spacer

Fixed in version 3.0.7 ✓

References

CVE

CVE-2022-3618

Classification

Type

XSS

OWASP top 10

A7: Cross-Site Scripting (XSS)

CWE

CWE-79

Miscellaneous

Original Researcher

gem

Submitter

gem

Verified

Yes

WPVDB ID

2011dc7b-8e8c-4190-ab34-de288e14685b

Timeline

Publicly Published

2022-10-28 (about 28 days ago)

Added

2022-10-28 (about 28 days ago)

Last Updated

2022-10-28 (about 28 days ago)

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