WPScan

Themes Vulnerabilities

Ask Me < 6.8.7 - Post Deletion via CSRF

Description

The plugin has a CSRF vulnerability that allows the deletion of a post without using a nonce or prompting for confirmation.

Proof of Concept

```
An attacker can log in to their own account, grab the link structure of the post-deletion request, and then forge it to the victim's post ID and send it to the victim. As soon as the victim accesses the link, the post will be deleted without asking for confirmation or using a nonce.
```

Affects Themes

ask-me
Fixed in version 6.8.7 ✓

References

CVE
CVE-2022-3750

Classification

WPScan

Type
CSRF

OWASP top 10
A2: Broken Authentication and Session Management

CWE
CWE-352

Miscellaneous

Original Researcher
Srijan Adhikari

Submitter
Srijan Adhikari

Submitter twitter
srijanadk

Verified
Yes

WPVDB ID
5019db80-0356-497d-b488-a26a5de78676

Timeline

Publicly Published
2022-10-28 (about 28 days ago)

Added
2022-10-28 (about 28 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

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