New issue

Critical Vulnerability #43

Closed

ghost opened on Aug 26, 2023

I require a means of contact to disclose information concerning the vulnerability.

Closed **Critical Vulnerability** #43

q2apro on Aug 26, 2023 · edited by q2apro

Please be so kind and post it here so we can fix it. Thank you.

I just checked the code, I could find in **q2apro-onsitenotifications-page.php** the following:

```
$activity_url = qa_path_absolute('message').'/'.$event['handle'];
```

The `$event['handle']` should be `qa_html($event['handle']);` . Also on other occurrences.

Same for `$event['message']` it should be printed with qa_html().

`$linkTitle` must also be printed with qa_html();

Note that there are different distributors. Not all the code is from me. :)

👍 1

ghost on Aug 26, 2023

Exactly! There's no filter, you can even steal sessions from any user just by pasting a simple payload or compromise their history by posting an HTML comment.

Just going to someone's wall and putting: "><script>alert(1)</script> will be executed every time they open the notification, anything after the "> will be included on the page.

👍 2

q2apro added a commit that references this issue on Aug 27, 2023

`Update q2apro-onsitenotifications-page.php` … Verified 0ca85ca

q2apro on Aug 27, 2023 · edited by q2apro Edits ▾ Owner …

Updated: https://github.com/q2apro/q2apro-on-site-notifications/blob/master/q2apro-onsitenotifications-page.php

Hope it's fixed now. 👍

ghost on Aug 27, 2023 …

I've checked and the vulnerability has been fixed. Thank you for your prompt attention. :)

❤️ 1

ghost closed this as completed on Aug 27, 2023

Sign up for free **to join this conversation on GitHub.** Already have an account? Sign in to comment

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Participants