huntr

Code Injection in microweber/microweber

0

✓ Valid Reported on Jan 2nd 2022

Description

HTML Injection is a vulnerability in which the attacker can inject malicious html content in the webpage.

Proof of Concept

1 Admin has enabled `Comments` module, so that people can comment on a blog post. 2 Attacker post the following comment:

```
<s><marquee><h1>SOMETHING+SOMETHING
```

Now, observe the changes in the webpage: This html gets executed. The footer of webpage is striked out etc.

Impact

Attackers can change the structure of webpage using different tags like `<marquee>` , `<h1>` , `<center>` , `<s>` etc. Attackers can even hide the `Leave Comment` button This html code also executes in the admin panel when admin checks the comments on a post.

Occurrences

CommentController.php L27-L121

This endpoint only cleans XSS payloads and does not follow any process to clean html tags No use of `clean_html` function which is being used in AdminController@saveCommentEdit in Comments module.

CVE
CVE-2022-0282
(Published)

Vulnerability Type
CWE-94: Code Injection

Severity
Medium (4.3)

Visibility
Public

Status
Fixed

Found by

Rohan Sharma
@r0hansh
unranked

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 399 times.

We are processing your report and will contact the **microweber** team within 24 hours. a year ago

Rohan Sharma modified the report a year ago

Rohan Sharma modified the report a year ago

We have contacted a member of the **microweber** team and are waiting to hear back a year ago

We have sent a follow up to the **microweber** team. We will try again in 7 days. a year ago

We have sent a second follow up to the **microweber** team. We will try agai
10 months ago

Chat with us

Bozhidar 10 months ago Maintainer

https://github.com/microweber/microweber/commit/51b5a4e3ef01e587797c0109159a8ad9d2bac77a

Bozhidar 10 months ago Maintainer

https://github.com/microweber/microweber/commit/6e9fcaa043b4211ef21a494f9892dd19ba8a572c

Bozhidar 10 months ago Maintainer

done

Peter Ivanov validated this vulnerability 10 months ago

Rohan Sharma has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in 1.2.11 with commit 51b5a4 10 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

CommentController.php#L27-L121 has been validated ✓

Sign in to join this conversation

Chat with us