HTML Injection vulnerability in create tag functionality in microweber/microweber

0

✓ Valid Reported on Sep 8th 2022

Vulnerability Details

In the Microweber CMS, While doing a live edit on to the application, we have the option to create a new global tag in the application. While creating a global tag, the "Tag Name" input field doesn't properly get sanitized and it's vulnerable to HTML Injection vulnerability

Steps to Reproduce

First, Go to the shop and live edit the tag field
You will have option to manage new tags
In the manage tags, we can create a global tag
While creating a global tag, In the "Tag Name" field, enter the simple HTML code like "><h2>XSS
After saving the tag you will see a HTML tag got executed

Impact

HTML injection attack is closely related to Cross-site Scripting (XSS). HTML injection uses HTML to deface the page. XSS, as the name implies, injects JavaScript into the page. Both attacks exploit insufficient validation of user input.

References

- html Injection POC

CVE
CVE-2022-3245
(Published)

Vulnerability Type
CWE-94: Code Injection

Severity
Medium (4.3)

Registry
Other

Affected Version
1.3.1

Visibility
Public

Status
Fixed

Found by

Nithissh12
@nithissh200
master

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 732 times.

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

Nithissh12 modified the report 3 months ago

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

We have sent a follow up to the **microweber** team. We will try again in 7 days. 2 months ago

We have sent a second follow up to the **microweber** team. We will try again i
2 months ago

Chat with us

Peter Ivanov 2 months ago Maintainer

Hello, i cant reproduce this. Can you post a video ?

Nithissh12 2 months ago Researcher

Hi Peter I have updated the reference please check

Peter Ivanov modified the Severity from Medium (6.3) to Medium (4.3) 2 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Peter Ivanov validated this vulnerability 2 months ago

Nithissh12 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Peter Ivanov marked this as fixed in 1.3.2 with commit f20abf 2 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Nithissh12 2 months ago Researcher

Thanks man have a great day ahead :-)

Peter Ivanov 2 months ago Maintainer

Thanks too , cheers

Sign in to join this conversation

Chat with us