huntr

Cross-site Scripting (XSS) - Stored in microweber/microweber

0

✓ Valid Reported on Feb 8th 2022

Description

There is a reflected XSS in creating and searching tag function . where any user can execute any malicious code results in the cookie stealing or Account takeover vulnerability

Steps to Produce:

Go to this particular URL URL
Click on live edit , Now In the tag section and select the exsisting tag and click on manage tags
Now , Click on the global tags tab and create a tag with the name as the following payload **"><img src=x onerror=confirm(document.domain)>**
Now , whoever using thebparticular tag the Malicious code will get executed
Proof of concept: Video-Proot-of-Concept

CVE
CVE-2022-0558
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Critical (9.8)

Visibility
Public

Status
Fixed

Found by

Nithissh12
@nithissh200

Chat with us

master

Fixed by

Peter Ivanov

@peter-mw

maintainer

This report was seen 375 times.

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

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

Bozhidar 10 months ago Maintainer

https://github.com/microweber/microweber/commit/14a1bb971bcb8b5456c2bf0020c3018907a2704d

Peter Ivanov validated this vulnerability 10 months ago

Nithissh12 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 **14a1bb** 10 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us