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

0

Valid Reported on Feb 19th 2022

Description

The endpoint https://demo.microweber.org/demo/admin/post/{id}/edit is vulnerable to cross site scripting. The "Edit source" field is affected.

Proof of Concept

Login into https://demo.microweber.org
Navigate to https://demo.microweber.org/demo/admin/post/25/edit
click EditSource, and put this payload:
<img src=x onerror=alert(1)>
and click Ok
The xss payload will be executed.

Impact

Cross site scripting attacks can lead to account takeover via cookie stealing, temporary webpage deface, redirections etc.

CVE
CVE-2022-0723
(Published)

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

Severity
High (8)

Visibility
Public

Status

Fixed

Found by

Damanpreet

@daman-preet-singh

unranked

Fixed by

Bozhidar Slaveykov

@bobimicroweber

maintainer

This report was seen 486 times.

We are processing your report and will contact the **microweber** team within 24 hours. 9 months ago

We have contacted a member of the **microweber** team and are waiting to hear back 9 months ago

Bozhidar Slaveykov validated this vulnerability 9 months ago

Damanpreet has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

We have sent a fix follow up to the **microweber** team. We will try again in 7 days. 9 months ago

Bozhidar Slaveykov marked this as fixed in **1.2.11** with commit **15e519** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

Bozhidar 9 months ago Maintainer

We clean this xss on a backend

Sign in to join this conversation