huntr

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

0

✓ Valid Reported on Feb 20th 2022

Description

There is a Reflected cross site scripting issue chained using these endpoints: [1] /admin/content/0/edit [2] /apiqq</script><script>alert(1)</script>fca4/page

Proof of Concept

Login to https://demo.microweber.org
Now visit https://demo.microweber.org/demo/admin/content/0/edit
Now open this url (in same tab or new):
https://demo.microweber.org/demo/apiqq%3C/script%3E%3Cscript%3Ealert(1)%3C/script%3Efca4/page
The xss payload will be executed in the browser.

Impact

Cross site scripting attacks can lead to cookies stealing (can be chained to account takeover), redirecting users to attackers controlled malicious websites etc

CVE
CVE-2022-0719
(Published)

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

Severity
High (7.6)

Visibility
Public

Status

Fixed

Found by

Damanpreet
@daman-preet-singh
unranked

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 426 times.

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

Damanpreet modified the report 9 months ago

Damanpreet modified the report 9 months ago

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

Bozhidar 9 months ago Maintainer

https://github.com/microweber/microweber/commit/0b6b1eb5ba85ffc8f74e6f5f5be9dc9f9f7e9d8f

Bozhidar Slaveykov validated this vulnerability 9 months ago

Damanpreet has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in **1.3** with commit **a5925f** 9 mont

Chat with us

Bozhidar Slaveykov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation