Reflected XSS in microweber/microweber

0

Valid Reported on Apr 28th 2022

Description

Bypass XSS filter on /module/

Proof of Concept

```
https://demo.microweber.org/demo/module/?module=admin%2Fmodules%2Fmanage&ic
```

Drag something around to trigger the XSS. Might only work in FireFox.

How to fix

This is still CVE-2022-1439 basically.
I can break out of these html attributes, this time I use another parameter cuz I need a valid ? module= to get some html elements which I need to trigger this event handler, but the core bug is the same.
This affects many parameters on /module/ you can even define your own and they'll be appended as html attribs. You can not allow breaking out of these with quotes.
Maybe you can just replace " and ' here like < and >.

Impact

Executing JavaScript as the victim

CVE
CVE-2022-1584
(Published)

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

Severity
Medium (6.3)

Registry
Other

Affected Version
?

Visibility
Public

Status
Fixed

Found by

Finn Westendorf
@wfinn
legend

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 559 times.

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

Finn Westendorf modified the report 7 months ago

Finn Westendorf 7 months ago Researcher

```
https://demo.microweber.org/demo/module/?module=x%22draggable=%22true%22ondragexit=ale
```

Chat with us

For the record here's the same bypass in the same old "module" parameter, but you have to drag

For the record here's the same bypass in the same old "module" parameter, but you have to drag somethibg else over it, e.g. a bookmark.

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

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

Peter Ivanov validated this vulnerability 7 months ago

Finn Westendorf 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 **1.2.16** with commit **527abd** 7 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation