huntr

Static Code Injection in microweber/microweber

0

✓ Valid Reported on Mar 6th 2022

Description

The Microweber application allows HTML tags in the "First name", "Last name" and "Phone number" which can be exploited by Injecting HTML payloads.

Proof of Concept

1.While buying product we need to fill contact information form.
2.Insert your html code in code block. e.g., <code><p>Hurry Up!<a href="evil.com">Go to https://evil.com and get free $1000 in your account now .</a></p></code> (any field except mail)
3.Click on Continue, then your code will be injected into the Personal information section which can be viewed on 'domain/shipping-method' page.

Image & Video POC

https://drive.google.com/drive/folders/1hVdfSQrknQNHOudKPK0ZvqsXkqQxxdtW?usp=sharing

Impact

This vulnerability can be exploit for phishing attack

References

- mitre

CVE
CVE-2022-0895
(Published)

Chat with us

Vulnerability Type
CWE-96: Static Code Injection

CWE-96: Static Code Injection

Severity

High (7.7)

Visibility

Public

Status

Fixed

Found by

crowdoverflow

@crowdoverflow

unranked

Fixed by

Bozhidar Slaveykov

@bobimicroweber

maintainer

This report was seen 615 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

crowdoverflow 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 **b2baab** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Chat with us

Sign in to join this conversation

Chat with us