huntr

Improper Neutralization of Special Elements Used in a Template Engine in microweber/microweber

0

✔ **Valid**   Reported on Mar 6th 2022

Description

The Microweber application allows HTML tags in the "Blog Comments" which can be exploited by Injecting HTML payloads.

Proof of Concept

1.Open any blog in which comment is allowed.
2.Insert your html code in code block. e.g., <code><p>Hurry Up!Go to https://evil.com and get free $1000 in your account now .</p></code>
3.Post this code as comment

Video & Image PoC

https://drive.google.com/drive/folders/1iitC8a7Pq_GNbOew5tyKoR8O4Z05MM6v?usp=sharing

Impact

This vulnerability can be exploit for phishing attack

References

- mitre

CVE
CVE-2022-0896
(Published)

Vulnerability Type
CWE-1336: Improper Neutralization of Special Elements Used in a Template En

Severity

Chat with us

High (7.1)

Visibility
Public
Status
Fixed

Found by

crowdoverflow
@crowdoverflow

unranked ⌄

Fixed by

Bozhidar Slaveykov
@bobimicroweber

maintainer

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 **e02244** 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

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us