huntr

Open Redirect in microweber/microweber

3

✓ Valid Reported on Feb 13th 2022

Description

An Open Redirect vulnerability enables attacker to redirect the victims/users to malicious websites. The bug exists due to improper fix of https://huntr.dev/bounties/c9d586e7-0fa1-47ab-a2b3-b890e8dc9b25/. By adding an extra slash `/` the previous fix can be bypassed.

Proof of Concept

Visit https://demo.microweber.org/demo/api/logout?redirect_to=https:///evil.com
The above url will redirect you to evil.com

Impact

This issue can be leveraged to phishing attacks.

Occurrences

UserManager.php L258-L277

References

- https://portswigger.net/kb/issues/00500100_open-redirection-reflected

CVE
CVE-2022-0597
(Published)

Vulnerability Type
CWE-601: Open Redirect

Severity
Medium (4.3)

Chat with us

Visibility
Public

Status
Fixed

Found by

Kushagra Sarathe
@kushagrasarathe
unranked

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 420 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 9 months ago — Maintainer

https://github.com/microweber/microweber/commit/99cab88b5a139486db5246112dd8a2635639ce1b

Peter Ivanov validated this vulnerability 9 months ago

Kushagra Sarathe has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in **1.2.11** with commit **acfc6a** 9 months ago

Chat with us

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

UserManager.php#L258-L277 has been validated ✓

0x2374 9 months ago

No bounty?

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