Exposure of Sensitive Information to an Unauthorized Actor in microweber/microweber

0

✓ Valid Reported on Jan 2nd 2022

Description

Any unauthorized/unauthenticated actor can find the PII data of all the users registered in the application. PII - Personally Identifiable Information leaked by this application is `first name` , `last name` , `email id` , `picture` , `username` , `is_admin` status

Proof of Concept

1 Visit

```
https://demo.microweber.org/demo/api/users/search_authors
```

It shows you details of all the users

Impact

Attacker can grab this PII data and use it for any malicious purpose.

Occurrences

api_user.php L66-L95

Only admins should have access to this endpoint

CVE
CVE-2022-0281
(Published)

Vulnerability Type

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity

High (7.5)

Visibility

Public

Status

Fixed

Found by

Rohan Sharma

@r0hansh

unranked

Fixed by

Peter Ivanov

@peter-mw

maintainer

This report was seen 469 times.

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

Rohan Sharma submitted a patch a year ago

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

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

We have sent a second follow up to the **microweber** team. We will try again in 10 days. 10 months ago

Bozhidar 10 months ago Maintainer

its fixed

Chat with us

Bozhidar 10 months ago Maintainer

https://github.com/microweber/microweber/commit/e680e134a4215c979bfd2eaf58336be34c8fc6e6

Peter Ivanov validated this vulnerability 10 months ago

Rohan Sharma 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 **e680e1** 10 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

api_user.php#L66-L95 has been validated ✓

Sign in to join this conversation