huntr

Generation of Error Message Containing Sensitive Information in microweber/microweber

1

✔ Valid   Reported on Feb 13th 2022

Description

Sensitive information as part of the error is getting disclosed while viewing comments from "load_module:comments#search="

Proof of Concept

Login to https://demo.microweber.org
Visit
https://demo.microweber.org/demo/admin/view:modules/load_module:comments#search=
Now enter anything in search= parameter you can see 500 internal error with sensitive information

Impact

This vulnerability is capable of leaking sensitive data of the system where the website is hosted

Occurrences

🐘 search_content.php L38-L53

References

- https://huntr.dev/bounties/285ff8a0-a273-4d62-ba01-3e4b4e18467b/

Chat with us

CWE-209: Generation of Error Message Containing Sensitive Information

Severity
Critical (9.4)

Visibility
Public

Status
Fixed

Found by

0x2374
@0x2374
unranked ⌄

Fixed by

Peter Ivanov
@peter-mw
maintainer

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

0x2374 9 months ago   Researcher

POC Video : https://drive.google.com/file/d/1iOYRykepd6_Knn0HNq5Lk0yW2pQprIiX/view?
usp=sharing

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

0x2374 9 months ago   Researcher

Hello any update?

Chat with us

Bozhidar 9 months ago

https://github.com/microweber/microweber/commit/2417bd2eda2aa2868c1dad1abf62341f22bfc2
0a

We have sent a follow up to the **microweber** team. We will try again in 7 days. 9 months ago

Peter Ivanov validated this vulnerability 9 months ago

0x2374 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 **2417bd** 9 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

search_content.php#L38-L53 has been validated ✔

Sign in to join this conversation

huntr

part of 418sec

home

company

hacktivity

about

leaderboard

team

FAQ

contact us

Chat with us

Chat with us