huntr

Insecure Storage of Sensitive Information in microweber/microweber

0

✓ Valid Reported on Feb 19th 2022

Description:-

When the user uploads his profile picture, the uploaded image’s EXIF Geolocation Data does not get stripped. As a result, anyone can get sensitive information of microweber users like their Geolocation, their Device information like Device Name, Version, Software & Software version used, etc.

Proof of Concept:-

1.Browse this link:- https://github.com/ianare/exif-samples/blob/master/jpg/gps/DSCN0012.jpg
2.Download the image Upload the picture on your profile and click on save.
3.Now see the path of the uploaded image (Either by right click on image then copy image address OR right-click, inspect the image, the URL will come in the inspect, edit it as HTML)
4.Then open:- http://exif.regex.info/exif.cgi
5.Paste the URL (https://demo.microweber.org/demo/userfiles/media/default/dscn0012.jpg) of the profile image path now you can see the EXIF data.

Image PoC:-

https://drive.google.com/file/d/154yIOLwwVKmG7RWdqD25rwpaOUZH-X1X/view?usp=sharing

Impact:-

This vulnerability impacts all users on microweber. This vulnerability violates the privacy of a User and shares sensitive information of the user who uploads their profile picture on microweber.

References

- mitre 1
- mitre 2
- Hackerone 1
- Hackerone 2
- consumerreports
- Medium

CVE
CVE-2022-0724
(Published)

Vulnerability Type
CWE-922: Insecure Storage of Sensitive Information

Severity
Critical (9.1)

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 694 times.

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

SAMPRIT DAS modified the report 9 months ago

Chat with us

SAMPRIT DAS modified the report 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

SAMPRIT DAS 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 **b592c8** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Bozhidar 9 months ago Maintainer

here is a new picture uploaded with no data info about it
https://demo.microweber.org/demo/userfiles/media/default/dscn0012-ddaa_1.jpg

SAMPRIT DAS 9 months ago Researcher

Hello @bobimicroweber,

I have confirmed that the vulnerability has been fixed and I want to know when are the Description and References going to be updated on https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0724 ?

Regards,
@sampritdas8

Sign in to join this conversation

Chat with us