Insecure Storage of Sensitive Information in chocobozzz/peertube

0

Valid Reported on Feb 27th 2022

Vulnerability name: EXIF Geolocation Data Not Stripped From Uploaded Images (vulnerability)
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://p.lu/lazy-static/avatars/683e95a1-c9d3-4c70-949d-b37a5525f8c2.jpg) of the profile image path now you can see the EXIF data.
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

- https://huntr.dev/bounties/0cdc4a29-dada-4264-b326-8b65b4f11062/
- https://hackerone.com/reports/446238
- https://hackerone.com/reports/446238

CVE
CVE-2022-0881
(Published)

Vulnerability Type
CWE-922: Insecure Storage of Sensitive Information

Severity
High (7.6)

Visibility
Public

Status
Fixed

Found by

tharunavula
@tharunavula
amateur

Fixed by

chocobozzz
@chocobozzz
unranked

This report was seen 644 times.

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

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

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

chocobozzz validated this vulnerability 9 months ago

tharunavula has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

chocobozzz marked this as fixed in **4.1.1** with commit **0c058f** 9 months ago

chocobozzz has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation