Sensitive Data Exposure Due To Insecure Storage Of Profile Image in polonel/trudesk

0

Valid Reported on Mar 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 trudesk 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.Then select the image and click on "View Image Data" now you can see the EXIF data.

Video PoC:-

https://drive.google.com/file/d/1_-lUIFVpC0BrxrviLgO-Kythb-qaBt8a/view?usp=sharing

Impact

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

References

- mitre 1
- hackerone 2
- medium

- hackerone 1
- mitre 2
- consumerreports

CVE
CVE-2022-1044
(Published)

Vulnerability Type
CWE-922: Insecure Storage of Sensitive Information

Severity
High (8.2)

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

Fixed by

Chris Brame
@polonel
unranked

This report was seen 705 times.

We are processing your report and will contact the **polonel/trudesk** team within 24 hours.
8 months ago

Chris Brame modified the report 8 months ago

Chris Brame validated this vulnerability 8 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Chris Brame 8 months ago Maintainer

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

Although the bounty is valid; This project is not microweber.

SAMPRIT DAS 8 months ago Researcher

@maintainer sorry by mistake I have put the microweber name because previously I have reported the same vulnerability to microweber and I use that template to report here forgot to change the name @admin can you edit the name from microweber to trudesk from the description.

SAMPRIT DAS 8 months ago Researcher

@admin Can you register a CVE for this?

SAMPRIT DAS 8 months ago Researcher

@admin

Jamie Slome 8 months ago Admin

Removed microweber references from the report 👍

We can assign a CVE, we just require the GO AHEAD from the maintainer.

@Chris, are you happy for us to assign and publish a CVE for this report?

SAMPRIT DAS 8 months ago Researcher

@Chris @polonel @maintainer can you please reply

Chris Brame 8 months ago Maintainer

Yes, you can assign and publish a CVE for this report.

SAMPRIT DAS 8 months ago Researcher

@admin Maintainer is agree so can you please register a CVE for this report?

Jamie Slome 8 months ago Admin

CVE assigned! 👍

Once you have confirmed the fix @maintainer, we will be able to go ahead and publish the CVE.

We have sent a fix follow up to the **polonel/trudesk** team. We will try again in 7 days. 8 months ago

We have sent a second fix follow up to the **polonel/trudesk** team. We will try again in 10 days. 8 months ago

We have sent a third and final fix follow up to the **polonel/trudesk** team. This report is now considered stale. 8 months ago

SAMPRIT DAS 7 months ago Researcher

@admin Any update on deploying a fix for this report?

Chris Brame marked this as fixed in **v1.2.1** with commit **097b48** 7 months ago

Chris Brame has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

SAMPRIT DAS 7 months ago Researcher

@admin maintainer has confirmed the fix for this report so can you please update the CVE-ID on NVD/mitre

Jamie Slome 6 months ago

Sorted! 👍

Sorted! 🍋

It should be available in the next couple of hours :)

> Sign in to join this conversation