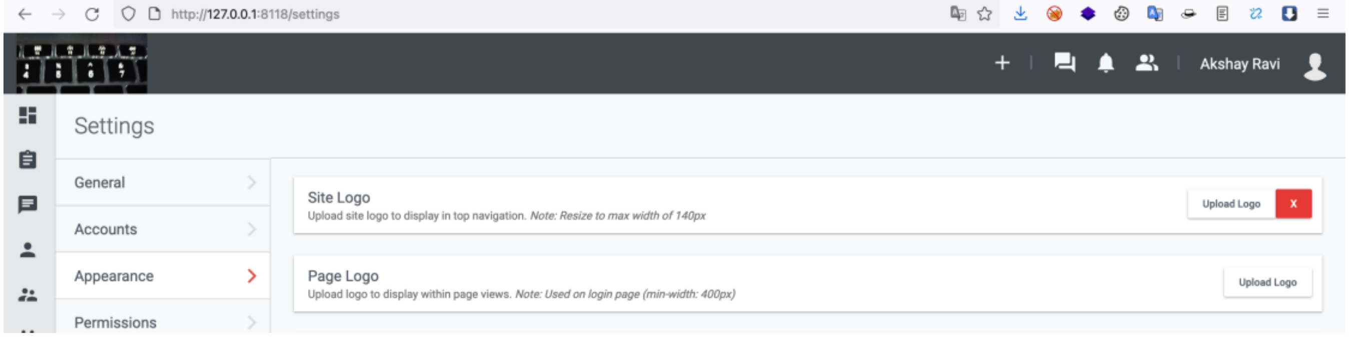
huntr

Meta Data Is Not Stripped From images in polonel/trudesk

0

✓ Valid Reported on May 23rd 2022

Hey team, while uploading `site/page logo` as an administrator, The meta data of the image like `geolocation, device information, version, name` etc is not getting stripped, as a result the attacker can collect all the meta data information of the image by using tools like exif tool, metadata checker etc which is publicly available.



Site Logo

Upload site logo to display in top navigation. *Note: Resize to max width of 140px*

Page Logo

Upload logo to display within page views. *Note: Used on login page (min-width: 400px)*

Steps to reproduce:

Upload site/page logo
copy the image location and save it or check the meta data directly by this site `http://exif-viewer.com`
The all information on the image(meta data) will be publicly disclosed

Patch recommendation:

Remove the meta data from uploaded images

Impact

This vulnerability impacts and violates the privacy of the one who uploads the image, because the meta data will be publicly accessible by third party attackers via the common predictable endpoint `http://127.0.0.1:8118/assets/topLogo.jpg`

References

- https://huntr.dev/bounties/ff878be9-563a-4d0e-99c1-fc3c767f6d3e

CVE

CVE-2022-1893
(Published)

Vulnerability Type

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

Severity

Medium (4.6)

Registry

Other

Affected Version

<=1.2.2

Visibility

Public

Status

Fixed

Found by

Akshay Ravi

@akshayravic09yc47

pro

Fixed by

Chris Brame

@polonel

unranked

This report was seen 525 times.

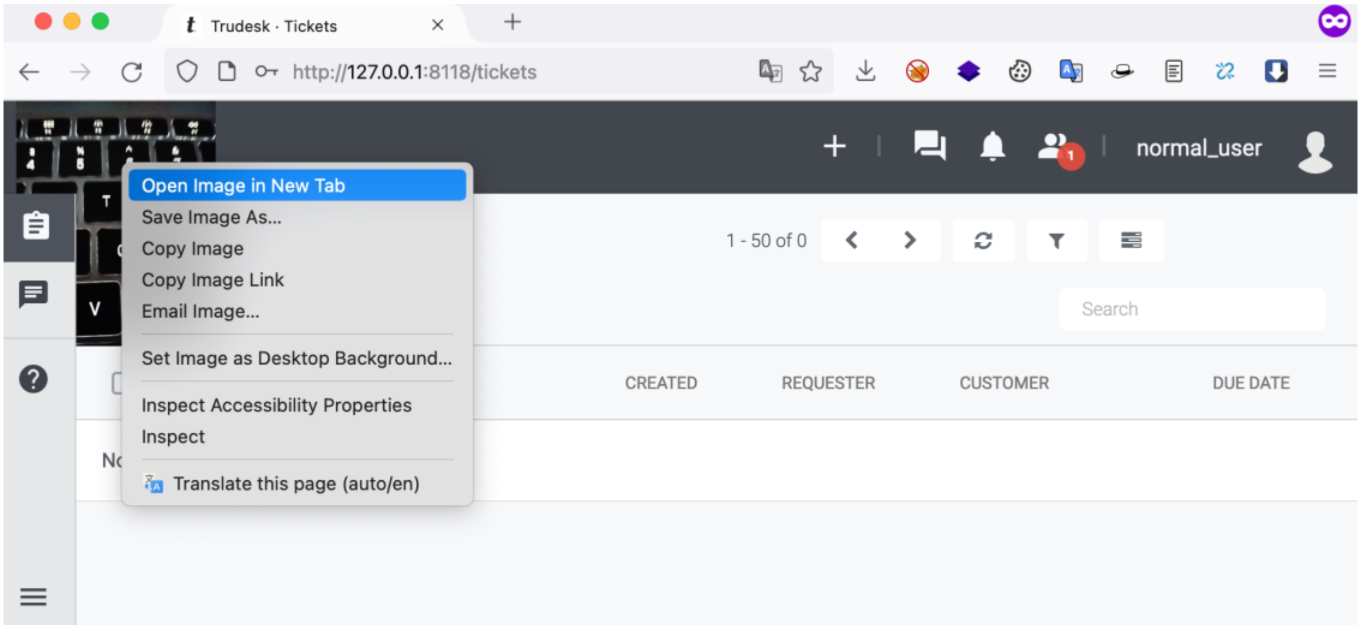
We are processing your report and will contact the **polonel/trudesk** team within 24 hours.
6 months ago

Akshay Ravi 6 months ago

Chat with us

#Note:

Hey @maintainer, As an normal user can also access the image with no privileges, beacuse the site logo is common for all..here is the POC👇:



I was added the CVSS score as low(3.3), feel free to change it to medium or higher than (3.3) if you wish as per these impacts, thanks

We have contacted a member of the **polonel/trudesk** team and are waiting to hear back
6 months ago

Chris Brame modified the Severity from Low (3.3) to Medium (4.6) 6 months ago

Chris Brame assigned a CVE to this report 6 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

Chris Brame validated this vulnerability 6 months ago

Akshay Ravi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chris Brame 6 months ago

This has been fixed and will release with version 1.2.3

I will update this report once released.

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

6 months ago

Chris Brame marked this as fixed in **1.2.3** with commit **ae904d** 6 months ago

Chris Brame has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us