huntr

Incorrect Behavior Make Crash and Can not Access Account in polonel/trudesk

1

✓ Valid Reported on May 25th 2022

Description

Incorrect Behavior Make Crash and Can not Access Account

Proof of Concept

```
1. Send a test message and get the request, send it to Repeater

2. Replace the value of owner and cId with the id of two victims

3. Send the request
```

Impact

Make victim's account crash
Victim can not access the account after although clear the browsing data
Dangerous to all users
Update: The admin account also crashed !

Occurrences

JS messages.js L0

References

- new POC video

CVE

CVE-2022-1947
(Published)

Vulnerability Type

CWE-480: Use of Incorrect Operator

Severity
Critical (9.1)

Registry
Other

Affected Version
<=1.2.2

Visibility
Public

Status
Fixed

Found by

Lê Ngọc Hoa
@lengochoa7112000
master

Fixed by

Chris Brame
@polonel
unranked

This report was seen 548 times.

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

Chris Brame 6 months ago Maintainer

You marked the affected version as "the last version" but in your POC it is using docker.trudesk.io which is using a different codebase.

Please test on version 1.2.2 as the demo version is being decommissioned at the end of the month. You will need to download and run the software locally. Please refer to the documentation.

A **polonel/trudesk** maintainer has acknowledged this report 6 months ago

Lê Ngọc Hoa 6 months ago Researcher

Hi! I am sorry for my bad! I tested on the version 1.2.2, this vulnerability still occurring! This is my new POC video: https://drive.google.com/file/d/1Hx2ZNXqGD6yVYGmH8nDBs7sG0iERGbbx/view?usp=sharing Thank you so much !!!

Lê Ngọc Hoa modified the report 6 months ago

Lê Ngọc Hoa modified the report 6 months ago

Chris Brame 6 months ago Maintainer

I'm not able to reproduce. I'm getting a 400 Bad Request error when changing the `cId` to a user's id. This is because it cannot find a conversation with that ID.

In the POC you do not show that the IDs you have stored in the notepad are actual user IDs.

If you change the `owner` field in the payload and the conversation id is valid it just shows that another user was part of the conversation.

Can you please show where the IDs you have in notepad came from so I can try to reproduce with the same steps?

Chris Brame 6 months ago Maintainer

@researcher I also want to confirm if you see ALL the user IDs when logged into a non-admin account and verify if you can reproduce the vulnerability with a regular user as the attacker instead of an admin as the attacker.

Lê Ngọc Hoa 6 months ago Researcher

Hi Chris Brame, I get the ID of user victim from the URL in message page of Attacker's account you can see it in this **full POC video**

https://drive.google.com/file/d/1IwuRvyEC9-2x5I7ayTAoMS_eLfSOtPaR/view?usp=sharing

Thank you!

Lê Ngọc Hoa 6 months ago Researcher

confirm: see ALL the user IDs when logged into a non-admin account:

https://drive.google.com/file/d/1zMfd94dehdI-zpJsbCeKvhXpBPP1QwMn/view?usp=sharing

Chris Brame 6 months ago Maintainer

Those IDs in the last video and the IDs in the URL are the conversations IDs, NOT the user IDs.

I think that is the cause of the crash is the user ID is missing validation when you replace it with a conversation ID.

But this did help me, I will try to reproduce and update this report when I can.

Chris Brame 6 months ago Maintainer

Can you update using the `develop` branch and see if the exploit is still working? I can not reproduce but I did change some other things with messages which may have fixed this at the same time.

If it is fixed on the `develop` branch I will stash my code and test again on `master`

Lê Ngọc Hoa 6 months ago Researcher

Hi @Chris Brame, I updated using the `develop` branch with docker-compose:

```
wget https://raw.githubusercontent.com/polonel/trudesk/develop/docker-compose.yml
docker-compose up -d
```

I tested again. The exploit is still working.
Is there something wrong?

Chris Brame 6 months ago Maintainer

That would have not been updated as I didn't update the docker images.

Chris Brame 6 months ago Maintainer

I have updated the docker image for the `next` tag. You will need to change the `docker-compose` file to use the `trudesk:next` image.

Lê Ngọc Hoa 6 months ago Researcher

Hi @maintainer ! I tested again using the `develop` branch. The vulnerability fixed! You can watch this video: https://drive.google.com/file/d/1G4j0_XcVn8LY2ft1R0geNZMm0y_hZ3Rx/view?usp=sharing

Chris Brame assigned a CVE to this report 6 months ago

Chris Brame validated this vulnerability 6 months ago

I have marked this as valid as I believe it was fixed in a commit that will release in v1.2.3

@researcher Thanks for your assistance and multiple testing of the application.

Lê Ngọc Hoa 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 Maintainer

@admin Can you change the affected version of this report to be `<=1.2.2`

Chris Brame marked this as fixed in **1.2.3** with commit **a9e38f** 6 months ago

Chris Brame has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

messages.js#L0 has been validated ✓

Jamie Slome 6 months ago Admin

Sorted :)

Sign in to join this conversation

Chat with us