

Send messenger to another user with any sender account in polonel/trudesk

1



Valid

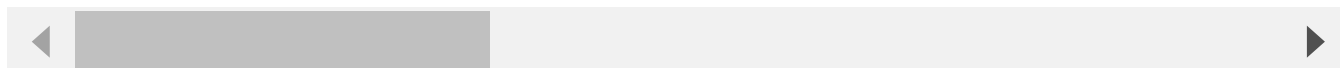
Reported on May 24th 2022

Description

Send messenger to another user with any sender account

Proof of Concept

1. Login with account A.
2. When click to the message box of the user Victim X we have the id of this user.
3. Login with account B. Paste the copied URL and access, send a message, send the message.
4. In the page message of A, we receive a message from victim X with content (X do not send the message, B send the message but A receive the message from X).



Impact

Break the message page of another user

Fake information in message page of another user

References

- [new POC Video](#)
- [IDOR](#)

CVE

CVE-2022-1931

(Published)

Vulnerability Type

CWE-821: Incorrect Synchronization

Chat with us

Severity
Critical (9.1)

Registry
Other

Affected Version
all

Visibility
Public

Status
Fixed

Found by



Lê Ngọc Hoa

@lengochoa7112000

master ▼

Fixed by



Chris Brame

@polonel

unranked ▼

This report was seen 535 times.

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

6 months ago

Lê Ngọc Hoa modified the report 6 months ago

Lê Ngọc Hoa modified the report 6 months ago

Chris Brame 6 months ago

Maintainer

Need to know what version you tested on?

Chat with us

Lê Ngọc Hoa 6 months ago

Researcher

I tested on the demo version

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

Chris Brame [6 months ago](#)

Maintainer

Please test on version 1.2.2 as the demo version is being decommissioned at the end of the month.

Lê Ngọc Hoa [6 months ago](#)

Researcher

I tested on version 1.2.2 and it still got this vulnerability! This is my new POC video:

https://drive.google.com/file/d/1oZwpLdd9sd5OaZsd8qVPJh_lz5g9XsmW/view?usp=sharing

Thank you !!!

Lê Ngọc Hoa modified the report 6 months ago

We have sent a follow up to the **polonel/trudesk** team. We will try again in 7 days. 6 months ago

Chris Brame assigned a CVE to this report 6 months ago

Chris Brame validated this vulnerability 6 months ago

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

This has been fixed and will release with version 1.2.3
I will update this report once released.

[Chat with us](#)

Chris Brame marked this as fixed in 1.2.3 with commit 314540 6 months ago

Chris Brame has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 4l8sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 4l8sec

company

about

team

Chat with us