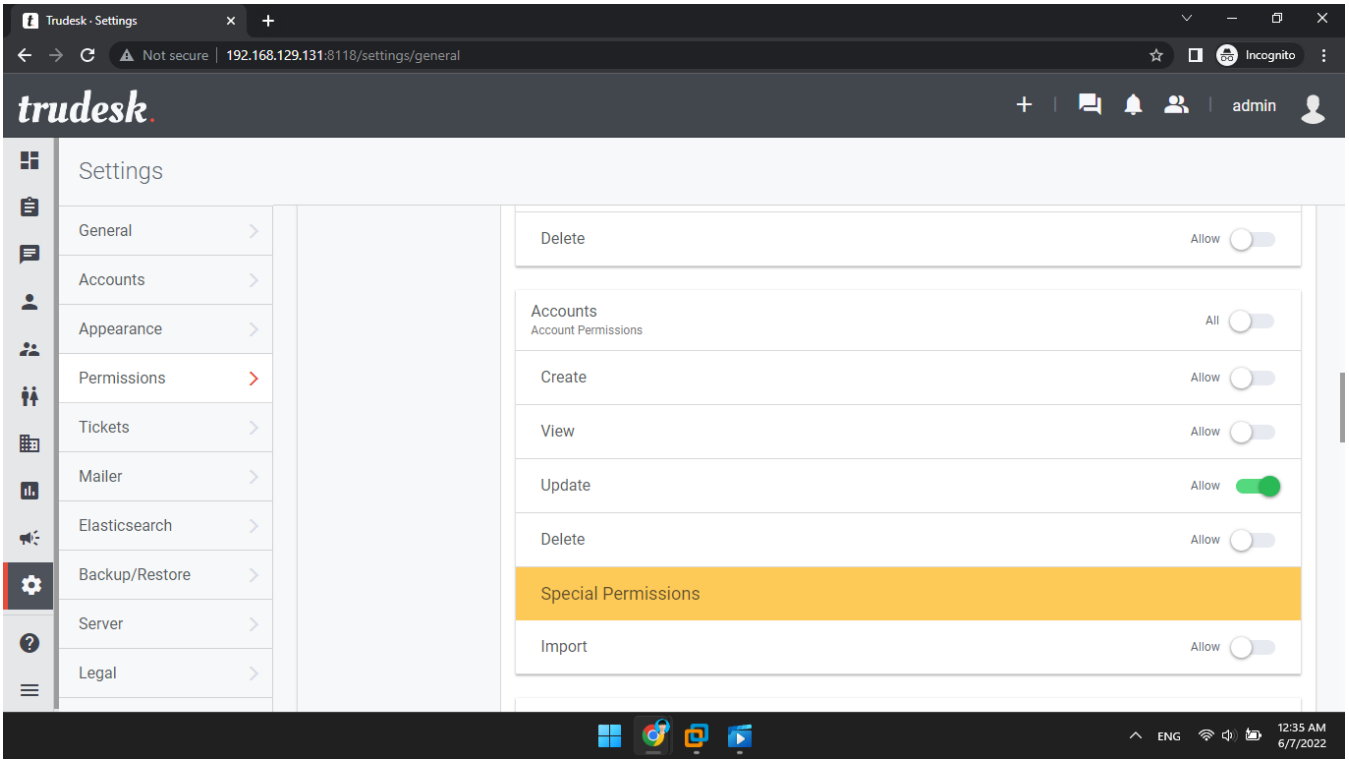
Incorrect use of privileged APIs to steal victim's account in polonel/trudesk 1

Valid Reported on Jun 6th 2022

Description

When user can edit their profile --> Incorrect use of privileged APIs to steal victim's account



Proof of Concept

1. Login with hacker's account, get the request when edit profile
2. Replace the endpoint and email with victim's one
3. Send the request.

POC video:

https://drive.google.com/file/d/1fhauDTJ0sbDSMoAuRydHE-60wC8

Impact

Hacker can access all accounts that he know the mail (leak in message page)
Dangerous for all users
Hacker can steal an admin's account --> get the highest permission

Occurrences

JS users.js L416-L571 JS users.js L598-L631

CVE
CVE-2022-2023
(Published)

Vulnerability Type
CWE-648: Incorrect Use of Privileged APIs

Severity
Critical (10)

Registry
Other

Affected Version
<=1.2.3

Visibility
Public

Status
Fixed

Found by

Lê Ngọc Hoa
@lengochoa7112000
master

Fixed by

Chris Brame
@polonel
unranked

This report was seen 812 times.

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

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

A **polonel/trudesk** maintainer has acknowledged this report 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 in v1.2.4. I will update this report once released.

Chris Brame 6 months ago — Maintainer

Please note that if the user has the `accounts update` permission they can update any user account as per design. This is usually reserved for **Admin** or **Support** roles that may need the user's password reset.

Although your report was indeed valid, it only worked if the "hacker" user had permission to update accounts anyway. It did however lead to an issue where the permissions were needed to update your own profile which in itself was a vulnerability. This is what has been fixed.

Lê Ngọc Hoa 6 months ago — Researcher

I got that! Thank you @maintainer!

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

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

Chris Brame marked this as fixed in **1.2.4** with commit **83fd5a** 5 months ago

Chris Brame has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

users.js#L598-L631 has been validated ✔

users.js#L416-L571 has been validated ✔

Sign in to join this conversation