Execution with Unnecessary Privileges in polonel/trudesk

0

Valid Reported on Jun 15th 2021

BUG

Unprivileged user can subscribs others to a ticket

IMPACT

user with lower level permission can subscribe others to a ticket

STEP TO REPRODUCE

1. First from admin goto `http://localhost:8118/teams` and create a team called `team2` .
Now goto `http://localhost:8118/accounts/agents` and add new user called `user B` with `support` role and assign him to above team2.\
2. Now as a external user goto `http://localhost:8118/newissue` and create a new ticket .

3. Now user B goto his account and here he can see above public ticket .
Here user B can subscribes to this ticket .
When user B subscribe bellow request is sent to server

```
PUT /api/v1/tickets/60c632a56e8507002262a20a/subscribe HTTP/1.1
Host: localhost:8118
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 52
Origin: http://localhost:8118
Connection: close
Referer: http://localhost:8118/tickets/1004
Cookie: PHPSESSID=n3ofevpn16pm9p45ngraltrbtk; SMFCookie600=a
Account: TEST2
```

```
{"user":"60c60643fbb7540012529d1d","subscribe":true}
```

here in this request postdata user-B change `user` parameter value to userid of admin and sent the request .
Now admin will be subscribed to this ticket. user B can get admin user id from `http://localhost:8118/accounts/agents` .
So, using this attack admin has been subscribed to a ticket by user-B .

CVE
CVE-2022-1808
(Published)

Vulnerability Type
CWE-250: Execution with Unnecessary Privileges

Severity
High (8.8)

Affected Version
<=1.2.2

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

Fixed by

Chris Brame
@polonel
unranked

Chat with us

This report was seen 679 times.

ranjit-git 6 months ago Researcher

@maintainer
This report is submitted about a year ago.
I see now you checking those report.
If you are unable to reproduce the bug and need more clear step then you can ask me.
There is not need close the report as not applicable after a years.
Not appliicable status decrease my reputation points here

Chris Brame 6 months ago Maintainer

@researcher
I understand. Maybe @admin can help restore your rep as I had an issue with my dashboard not showing any reports and that was just fixed yesterday. Most of these reports went unseen for some time and are invalid now due to the dashboard not loading any reports.

ranjit-git 6 months ago Researcher

@mainatiner
Yes, I will ask admin to look for your dashboard issue.
When I submiited those bug were version trudesk 1.1.5 .
But now latest version is 1.2.0.
But what would be those report status if those bug are fixed recently or fixed few version ago and mainatiner forgot to update here?

Jamie Slome 6 months ago Admin

I'd say that if the vulnerability is no longer an issue, we can mark this report as `N/A`.

The dashboard issue has been addressed and I believe was only broken for a couple of days.
@maintainer - if this looks like a duplicate, feel free to mark accordingly.

However, ultimately, it is up to you as the maintainer what feels correct here 👍

ranjit-git 6 months ago Researcher

@mainatiner
I will send update about all the report if they are still reproduceble on Friday.
I traveling somewhere, so next two days it won't be possible. Is it ok for you?
Sorry for inconvenience.

ranjit-git 6 months ago Researcher

@maintainer
this bug still works

Chris Brame assigned a CVE to this report 6 months ago

Chris Brame validated this vulnerability 6 months ago

ranjit-git has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

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

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.

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

Chris Brame marked this as fixed in 1.2.3 with commit f739ea 6 months ago

Chris Brame has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Chris Brame 6 months ago Maintainer

@admin Can you update this report to show only version `<=1.2.2` is affected.

Jamie Slome 6 months ago

Chat with us

Sorted :)

Sorted :)

Sign in to join this conversation