huntr

Exposure of "Forgot Password" Token on Threads Controller Leads to Account Takeover in tooljet/tooljet

1

✓ Valid Reported on Sep 10th 2022

Description

Hello there! Hope you are doing great!

I kept looking for issues that are similar to CVE-2022-3019, and ended up finding one more, it's in the Thread entity, and I found it by looking at the `/api/threads/:app_id/all` endpoint. It retrieves sensitive information about every user that's in an app's thread, including these users' "forgot password" token, which means that a different user involved in the same project as you can steal your account, leading to both horizontal and vertical (admin as victim) privilege escalation.

Steps to Reproduce

1 => Create two different accounts. As this is a more specific issue, they need to be able to edit the same app. So you can create an "admin" and invite the second user after that;
2 => As the "admin", go to the app editor and make a comment;
3 => Now, as the second user and the attacker, access the app editor and click on the "comments" button so the browser will try to load all the threads;
4 => Look at the request that's being sent to `/api/threads/:app_id/all` , it retrieves sensitive information about the comment owner within its "user" attribute. With this data, you could takeover the admin account, just like we did in the previous report;

Impact

Just like in the previous report, an attacker could steal the account of different users. But in this case, it's a little bit more specific, because it is needed to be an editor in the same app as the victim.

Occurrences

TS thread.entity.ts L33

TS thread.entity.ts L32

CVE
CVE-2022-3348
(Published)

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

Severity
Medium (6.5)

Registry
Other

Affected Version
<=1.24.3

Visibility
Public

Status
Fixed

Found by

Breno Vitório
@brenu
legend

Fixed by

Gandharv
@gondar00
maintainer

This report was seen 745 times.

We are processing your report and will contact the **tooljet** team within 24 hours. 3 months ago

We have contacted a member of the **tooljet** team and are waiting to hear b

Chat with us

We have sent a follow up to the **tooljet** team. We will try again in 7 days. 2 months ago

We have sent a second follow up to the **tooljet** team. We will try again in 10 days. 2 months ago

Gandharv validated this vulnerability 2 months ago

Breno Vitório has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Gandharv marked this as fixed in **v1.26.0** with commit **37bf6d** 2 months ago

Gandharv has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

thread.entity.ts#L32 has been validated ✓

Sign in to join this conversation

2022 © 418sec