huntr

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

1

✓ Valid Reported on Aug 21st 2022

Hello there! Hope you are doing great!

Description

While digging into your app's source code, I noticed that the `getComment()` function, that can be found on CommentController, had an IDOR, but when I went to an actual instance of Tooljet and tested it, I noticed that it's way worse than that! 😱

This function returns not only the comment's data, but it also `returns sensitive data about the user who created the comment`. This includes their passwords' hash and `their "forgot password" token, which allows an attacker to simply just change a victim password and log into their account`.

How to Reproduce

1 => Create two different accounts. It works whether they are from the same tenant or not, but if so, you will be able to find the comment in the UI;
2 => While logged in as the victim, go to one of your apps and make a comment in it. Then, store the id of this comment for later;
3 => Now, unauthenticated, but impersonating the attacker, go to the forgot password functionality and put the e-mail of the victim, so that the forgot password token can be generated;
4 => Login as the attacker, and make a GET request to `/api/comments/id-of-victim-comment-here`. It will return some data about the user, such as their email, hashed password, and also their forgot password token!
5 => Log out and go to `/reset-password/forgot-password-token-here`. Define the new password you want for the victim account, and boom! Now you got access :)

Impact

The forgot password token basically just makes us capable of taking over the account of whoever comment in an app that we can see (bruteforcing comment id's might also be an option but I wouldn't count on it, since it would take a long time to find a valid one).

CVE
CVE-2022-3019
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (7.1)

Registry
Other

Affected Version
<=1.22.0

Visibility
Public

Status
Fixed

Found by

Breno Vitório
@brenu
legend

Fixed by

Midhun G S
@gsmithun4
maintainer

This report was seen 631 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. 3 months ago

Midhun G S validated this vulnerability 3 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

Midhun G S marked this as fixed in **1.23.0** with commit **45e0d3** 3 months ago

Midhun G S has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us