

## Account Takeover in tooljet/tooljet

3

✓ Valid

Reported on Aug 28th 2022

### Description

hacker can invite any user to team and with the bug i report it before can accept the invitation ..... hacker can add user in group to give them new permission in team..... when hacker visit the team can see private info for victim as and the hash password many token and more information.....

### Proof of Concept

<https://drive.google.com/file/d/1fKZ-T0peu2h9yIHnqqsteKn50nbpRCLZ/view?usp=sharing>

### Impact

Account Takeover :: when see the info i can see the hash pass i can creaked it ..... Account Takeover :: when see the info i can see the forgot\_password\_token the hacker can send the request and changed the pass

CVE

CVE-2022-3422

(Published)

Vulnerability Type

CWE-269: Improper Privilege Management

Severity

Critical (9.8)

Registry

Npm

Affected Version

v1.22.0

Visibility

Public

Chat with us

Status  
Fixed

Found by



ahmed8magdy

@ahmed8magdy

pro ▼

This report was seen 1,271 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 back 3 months ago

We have sent a follow up to the **tooljet** team. We will try again in 7 days. 3 months ago

We have sent a second follow up to the **tooljet** team. We will try again in 10 days. 3 months ago

ahmed8magdy 3 months ago

Researcher

hiiii

ahmed8magdy 3 months ago

Researcher

any update @admin  
by reports is Critical

Jamie Slome 3 months ago

Admin

We will still follow up with another nudge to the maintainer. Thank you for your patience, and I am sure we will hear from them soon 👍

We have sent a third and final follow up to the **tooljet** team. This report is now considered stale.  
2 months ago

ahmed8magdy 2 months ago

Chat with us

this is anther bug

ahmed8magdy 2 months ago

Researcher

<https://drive.google.com/file/d/1fKZ-T0peu2h9yIHNqqsteKn50nbpRCLZ/view?usp=sharing>  
my bug not same

ahmed8magdy 2 months ago

Researcher

@admin  
you make my report duplicate  
it is not duplicate it is anther bug  
it is anther account takeover  
can you see the POC video You should hurry because the report has become public  
anyone can see the report and the bug

Jamie Slome 2 months ago

Admin

Hello, we do side with the judgement of the maintainer on their assessment of the report. We do not take specific positions on the reports but believe the maintainers are best placed to qualify the report.

If you still do not agree, I would recommend politely getting in touch with the maintainer to discuss further :)

Shubham Gupta 2 months ago

Maintainer

@admin - It has been a mistake from our end. It is not a duplicate issue. Is it a way to revert the duplicate tag?

ahmed8magdy 2 months ago

Researcher

i can report this bug agine and you shoud fex it in asap

ahmed8magdy 2 months ago

Researcher

@admin hi  
can you solve this mistake

Chat with us

Pavlos [2 months ago](#)

Admin

We're on it :)

Ben Harvie [2 months ago](#)

Admin

This report has now been reset to its previous state as requested :)

Shubham Gupta validated this vulnerability 2 months ago

ahmed8magdy has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Shubham Gupta marked this as fixed in v1.26.1 with commit 7879d8 2 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

♥ Shubham Gupta gave praise 2 months ago

Thanks @ahmed8magdy for raising this.

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

ahmed8magdy [2 months ago](#)

Researcher

thx proo @Shubham Gupta  
now can add this report as cve

ahmed8magdy [2 months ago](#)

Researcher

@admin can add the bug as cve now thx

Chat with us

The CVE has already been published @ahmed8magdy what do you want to do?

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