huntr

Account Takeover in tooljet/tooljet



✓ Valid) Reported on May 19th 2022

Description

Hi I found a way to takeover user's account

Proof of Concept

- 1. Victim A is a member of a organization orgA
- 2.Attacker create a new account with orgB
- 3.Invite victimA to orgB
- 4. Since an admin can access invitation link attacker copy this link and set new password using this link
- 5. Now logging with victimA's email with newly created password

POC Link:-

https://youtu.be/krzkXTly5ww

Impact

This will lead to account takeover of any low privileged user or admin user

Occurrences

TS organization_users.service.ts L27

CVE

Vulnerability Type

Severity

0

Chat with us

Registry

Other

Affected Version

1.13.0

Visibility

Public

Status

Fixed

Found by



This report was seen 712 times.

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

We created a GitHub Issue asking the maintainers to create a SECURITY.md 6 months ago

We have contacted a member of the tooljet team and are waiting to hear back 6 months ago

We have sent a follow up to the tooljet team. We will try again in 7 days. 6 months ago

We have sent a second follow up to the tooljet team. We will try again in 10 days. 6 months ago

A tooljet/tooljet maintainer validated this vulnerability 6 months ago

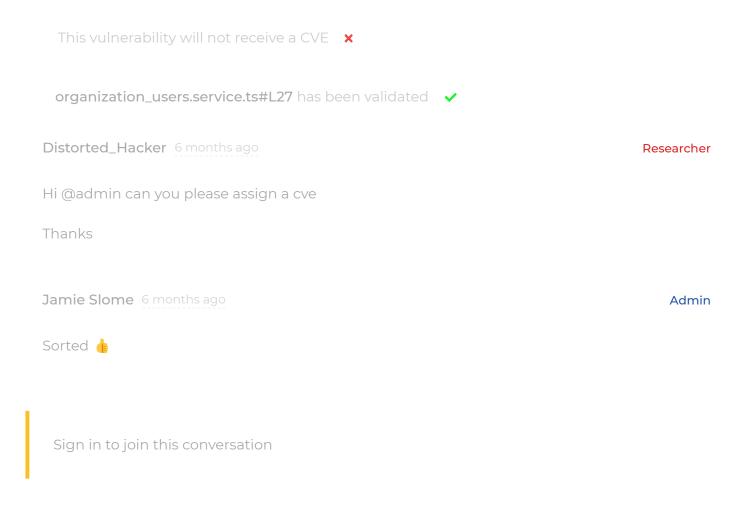
Distorted_Hacker has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A tooljet/tooljet maintainer marked this as fixed in v1.16.0 with commit fac

Chat with us



2022 © 418sec

huntr	part of 418sec
home	company
hacktivity	about
leaderboard	team
FAQ	
contact us	

Chat with us

privacy policy