Account Takeover in tooljet/tooljet

Valid Reported on May 19th 2022

0

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/krzkXTIy5ww

Impact

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

Occurrences

TS organization_users.service.ts L27

CVE
CVE-2022-2037
(Published)

Vulnerability Type
CWE-1125: Excessive Attack Surface

Severity
Critical (9.8)

Registry
Other

Affected Version
1.13.0

Visibility
Public

Status
Fixed

Found by

Distorted_Hacker
@gaurav-g2
pro

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

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

organization_users.service.ts#L27 has been validated ✔

Distorted_Hacker 6 months ago Researcher

Hi @admin can you please assign a cve

Thanks

Jamie Slome 6 months ago Admin

Sorted 👍

Sign in to join this conversation