1

It is possible to elevate privileges for any authenticated user to view permissions matrix and view Direct messages without appropriate permissions.

Share: ![Facebook] ![Twitter] ![LinkedIn] ![Y] ![o]

Description:

For the user with "View Private Room" permission only it is possible to rewrite permission role (e.g. to admin) in /api/v1/me method response via some proxy tools (e.g. Charles) and get access to server`s permissions matrix and view Direct messages.

Releases Affected:

Tested on 3.3.3

Steps To Reproduce (from initial installation to vulnerability):

Leave existing "Guest" role with only "View Private Room" permission and associate newly created user with it .
Install Charles or another network proxy
Enable local SSL proxy.
Turn on the rewrite tool and edit body response "roles" parameter to admin ("roles": ["admin"]) for /api/v1/me method.
Reload Rocket page.
Now you can get https://your_server/admin/permissions page with current server`s permissions.
Now you can receive Direct Messages even if "View Direct Messages" permissions is disabled for you.

Impact

The user which is not meant to be able to participate in Direct Messaging gains the ability to do so and also gets access to the server`s permissions scheme.

This issue has been fixed in 5.0>

channel, private group or direct message, and can see permission matrix as well, following the steps describe in attached video.

TIMELINE

garretby submitted a report to **Rocket.Chat**.   Jul 7th (2 years ago)

markus-rocketchat posted a comment.   Jul 7th (2 years ago)

garretby posted a comment.   Jul 8th (2 years ago)

markus-rocketchat posted a comment.   Jul 8th (2 years ago)

garretby posted a comment.   Jul 9th (2 years ago)

markus-rocketchat changed the status to ○ **Triaged**.   Jul 9th (2 years ago)

markus-rocketchat posted a comment.   Jul 10th (2 years ago)

garretby posted a comment.   Jul 13th (2 years ago)

markus-rocketchat posted a comment.   Jul 16th (2 years ago)

mrrorschach (Rocket.Chat staff) updated the severity from Low to Medium.   Nov 12th (about 1 year ago)

mrrorschach (Rocket.Chat staff) posted a comment.   Nov 12th (about 1 year ago)

mrrorschach (Rocket.Chat staff) closed the report and changed the status to ○ **Resolved**.   Aug 2nd (4 months ago)

mrrorschach (Rocket.Chat staff) posted a comment.   Aug 2nd (4 months ago)

mrrorschach (Rocket.Chat staff) requested to disclose this report.   Sep 22nd (2 months ago)

mrrorschach (Rocket.Chat staff) disclosed this report.   Sep 22nd (2 months ago)