1

REST API gets `query` as parameter and executes it

Share:

SUMMARY BY ROCKET.CHAT

Summary: Any user with 'view-d-room' permission can access any (except users.services) data from the `users` collection

Description:

The "users.list" REST endpoint gets a `query` parameter from JSON and runs `Users.find(queryFromClientSide)`. This means virtually any authenticated user can access any data (except password hashes) of any user authenticated. They can list admins and then brute-force their passwords with that information, for example. And all emails get leaked.

This report is only for one specific endpoint, but there are a lot of endpoint that have a `query` parameter, some attach fields to it making it "safer", but it's never a good idea to run queries that came from the users. This always will end-up as a security vulnerability. This is basically a SQL injection in a NOSQL database.

https://github.com/RocketChat/Rocket.Chat/blob/develop/app/api/server/v1/users.js#L232

Although contained to 'view-d-room', most accounts have this permission and even then, this permission does not allow for unfettered access to the entire `users` collection (except the password hash)

Releases Affected:

From 2.5 on.

Steps To Reproduce (from initial installation to vulnerability):

Signup to open.rocket.chat, get the X-Auth-Token and X-User-Id from storage. Fill the data in the query above, and access the list of most metadata of every admin user

```
--header 'X-Requested-With: XMLHttpRequest' \
--header 'X-User-Id: yyy'
```

Suggested mitigation

This endpoint needs to rethinking, why being so generic? It's a breaking change now, but it should never been this generic. So there isn't much hope besides breaking compatibility and making the endpoint simple, into one that does only one thing.

And other REST endpoints should be investigated too. We will do it, but it's such a critical problem that it seems the Rocket.Chat team can explore it more too.

Impact

Any authenticated account can access virtually any data from the `users` collection.

Fix

We have fix this vulnerability in 4.7.5>

TIMELINE

paulocsanz submitted a report to **Rocket.Chat**. Mar 29th (2 years ago)

markus-rocketchat changed the status to ○ **Triaged**. Apr 7th (2 years ago)

paulocsanz posted a comment. Jul 22nd (about 1 year ago)

paulocsanz posted a comment. Jul 22nd (about 1 year ago)

markus-rocketchat posted a comment. Jul 29th (about 1 year ago)

mrrorschach Rocket.Chat staff closed the report and changed the status to ○ **Resolved**. Jul 4th (5 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)