New issue

Jump to bottom

Severe Security Issue in Version 4: E-Mail Leak #3600

Closed **okybr** opened this issue on Jun 28, 2021 · 2 comments

Labels bug

okybr commented on Jun 28, 2021

I already contacted some maintainers privately about this, but they did not respond. That's why I'm now making this public.

In Talk version 4, it is very easy to query the e-mail addresses of users without any authentication; thus, possibly revealing their true identities behind their pseudonyms.

This is possible although the documentation states:

> The primary email address of the user. Only accessible to Administrators or the current user.

But in order to find out the e-mail address of a user, you can e.g. simply send a `query Q1 { user(id: "XXXX") { email }}` GraphQL-query to the GraphQL-endpoint of the talk-server -- without any authentication. You can also query all e-mail addresses with `query Q2 { users(query: {}) { nodes { email }}`.

I demand the maintainers (**@wyattjoh** , **@cvle**, **@kgardnr**) to merge the pull-request as soon as possible, and release version 4.13.0 in the version-4-branch.

1

okybr added the bug label on Jun 28, 2021

wyattjoh closed this as completed on Jun 29, 2021

munishsinghal commented on Aug 5, 2021

Even after these changes, it seems user with role ADMIN & MODERATOR can still see the email address in postman with below graphql query
query Q1 { user(id: "XXXX") { email }}
query Q2 { users(query: {}) { nodes { email }}

but user with role Staff, Commentor cannot see email address.

wyattjoh commented on Aug 9, 2021 Member

Those roles still need to see the email address to facilitate communication with the affected users for moderation.

Assignees
No one assigned

Labels
bug

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants