relatedcode/Messenger 7bcd20b - Information Disclosure

Summary

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

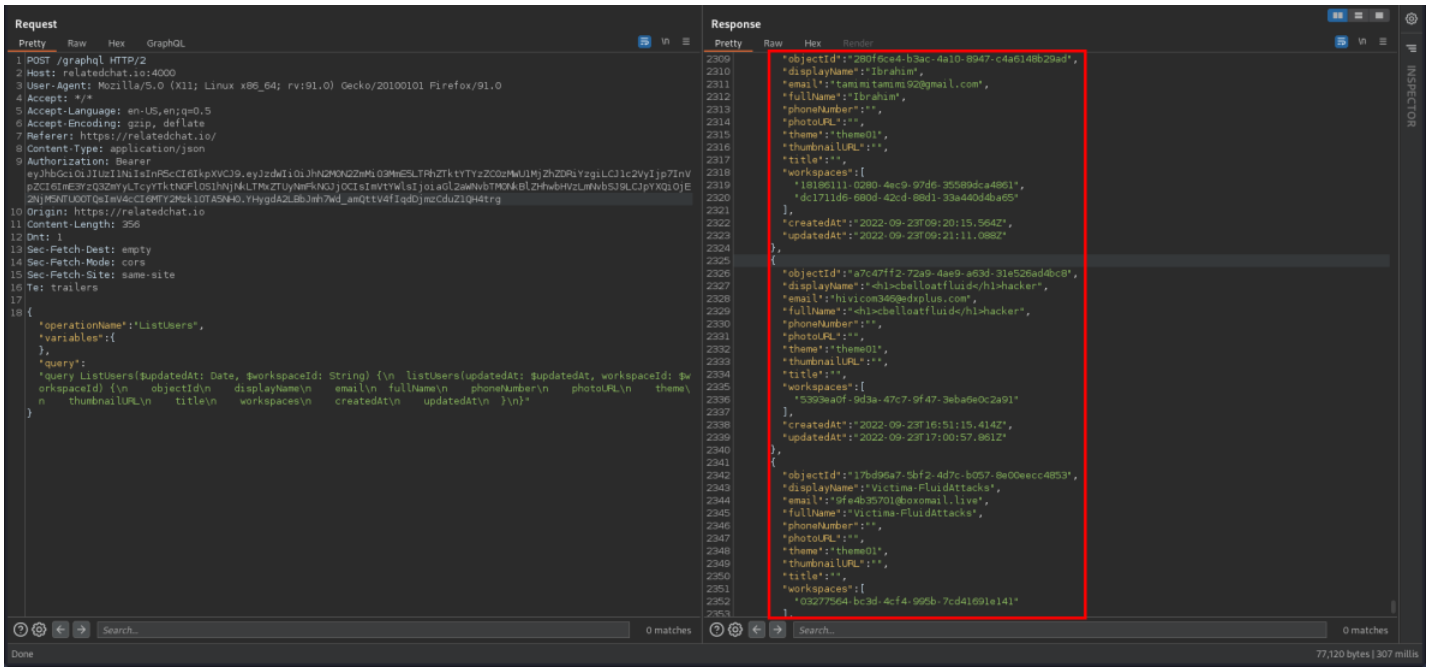
Vulnerability

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



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

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.

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories