



relatedcode/Messenger 7bcd20b - Information Disclosure

Summary



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](#)

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

Vulnerability

Kind	Business information leak – Personal Information
Rule	<u>226. Business information leak – Personal Information</u>
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)	<u>CVE-2022-41707</u>



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.

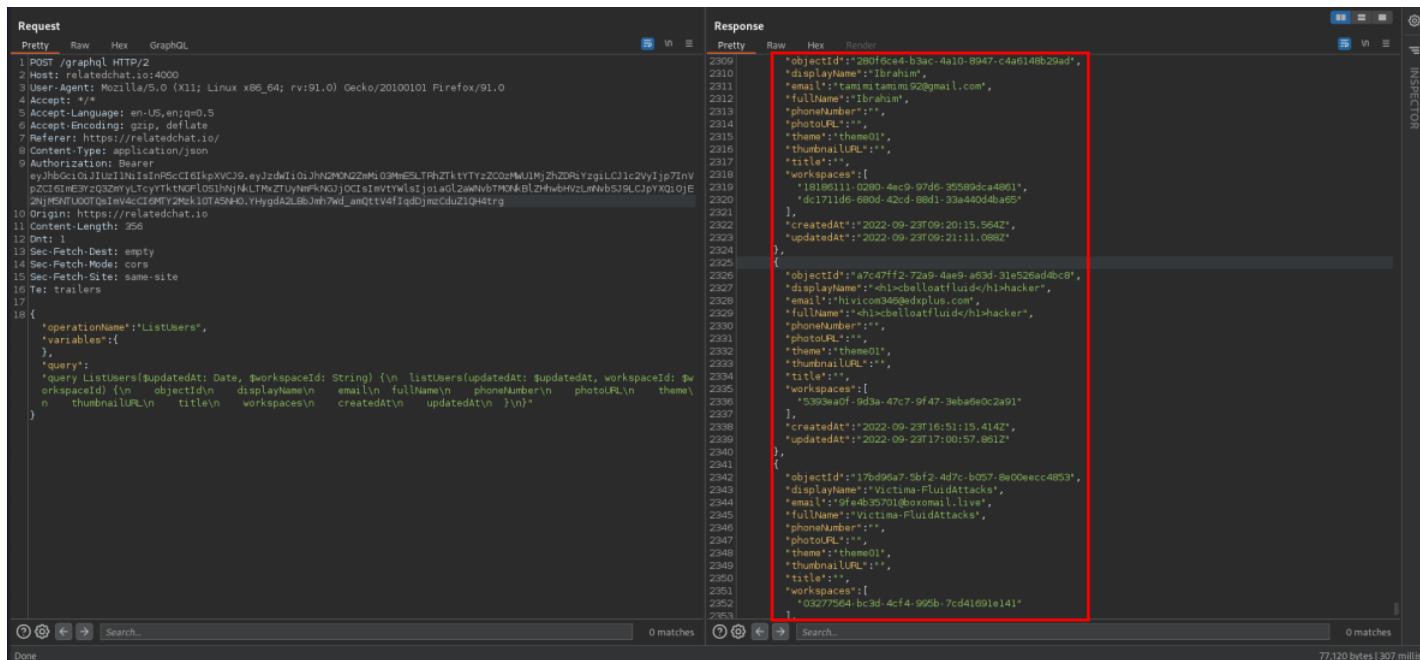
[Allow all cookies](#)

[Show details](#)

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.



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

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](#)

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

[Service Status](#) – [Terms of Use](#) – [Privacy Policy](#) – [Cookie Policy](#)