



# 0x00000000 attacks

[Home](#) / [Advisories](#) / [Relatedcode/Messenger 7bcd20b Broken Access Control](#)

## relatedcode/Messenger 7bcd20b - Broken Access Control

### 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](#)

<b>Affected versions</b>	Version 7bcd20b
<b>State</b>	Public
<b>Release date</b>	2022-10-14

### Vulnerability

<b>Kind</b>	Improper authorization control for web services
<b>Rule</b>	<u>039. Improper authorization control for web services</u>
<b>Remote</b>	Yes
<b>CVSSv3 Vector</b>	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
<b>CVSSv3 Base Score</b>	6.5
<b>Exploit available</b>	Yes
<b>CVE ID(s)</b>	<u>CVE-2022-41708</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 does not validate the application permissions correctly. Thanks to this we can access confidential information of any user registered on the server. Here we will see how an attacker manages to access the internal chats of the victim user:



# Impact

An authenticated remote attacker can access internal chat logs of arbitrary users of the application.

## Our security policy

We have reserved the CVE-2022-41708 to refer to this issue from now on.

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

## System Information

- Version: relatedcode/Messenger 7bcd20b
- Operating System: GNU/Linux



### 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](#)

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](#)

[FAQ](#)

[Documentation](#)



### **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](#)