huntr

Cross-site Scripting (XSS) - Stored in convos-chat/convos

0



Reported on Dec 27th 2021

Description

The Convos is an open source multi-user chat that runs in a web browser. You can't use SVG extension in Convos' chat window, but you can upload .html extension. This causes Stored XSS. Also, after uploading a file, it does not log in, and XSS occurs even if you connect.

Proof of Concept

Username: whwjddnjs142@gmail.com

Password: qwer12211@

- 1. Open the https://demo.convos.chat/login and Login as to above account
- 2. Go to https://demo.convos.chat/chat/irc-demo-irc-convos/<chat room name>
- 3. File Upload a html file
- 4. When you upload a file, an upload link is created in the comment form.
- 5. Please connect after attaching ".html" after the link

Video : https://www.youtube.com/watch?v=AfrsOY2SONc





Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

CVE

CVE-2022-21650 (Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Chat with us

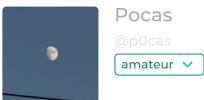
Severity High (7.3

Visibility

Status

Fixed

Found by



This report was seen 303 times.

We are processing your report and will contact the **convos-chat/convos** team within 24 hours. a year ago

Pocas modified the report a year ago

We have contacted a member of the **convos-chat/convos** team and are waiting to hear back a year ago

A convos-chat/convos maintainer validated this vulnerability a year ago

Pocas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A convos-chat/convos maintainer marked this as fixed in 6.48 with commit 5c0ale a year ago

The fix bounty has been dropped 🗶

This vulnerability will not receive a CVE x

A convos-chat/convos maintainer a year ago

Thank you! Appreciate it:)

Maintainer

Chat with us

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team