

# Cross-site Scripting (XSS) - Stored in chatwoot/chatwoot

0

✓ Valid

Reported on Feb 9th 2022

## Description

In order to render raw HTML in Vue.js you may use `v-html` attribute, which opens a door for XSS in case of malicious input. Chatwoot actually uses it in several places, such as <https://github.com/chatwoot/chatwoot/blob/develop/app/javascript/dashboard/modules/contact/components/MergeContactSummary.vue>

```
<span
  v-html="
    $t('MERGE_CONTACTS.SUMMARY.DELETE_WARNING', {
      childContactName,
    })
  "
/>
```

Thus, merging a contact where the `childContactName` contains malicious payload (let it be `</>` `<img src=x onerror=alert(1)>`) leads to an XSS.

## Steps to reproduce

1. Either you may set your nickname to a malicious payload as a non-privileged user, or change someone's name as an Agent (to cause XSS on admin's side).
2. As an admin merge a normal user with a one with a payload in nickname.
3. XSS will be triggered.

P.s.: chatwoot uses `v-html` in several other places, I will take a look at them and modify my report in case.

P.s.s.: can't give you a video PoC for this exact XSS because after update my Chatwoot Heroku instance has broken and I can't add a new customers via Telegram, lol

I receive `Wrong response from the webhook: 503 Service Unavailable`

Here is a link just in case:

Chat with us

[https://api.telegram.org/bot5215041570:AAEzj5AkzgttlDgPI1IU\\_7gF58whxoVaTA8/getWebhookInfo](https://api.telegram.org/bot5215041570:AAEzj5AkzgttlDgPI1IU_7gF58whxoVaTA8/getWebhookInfo)

So if you face some problems with reproducibility, then please, let me know, I will install Chatwoot on my local instance.

CVE

CVE-2022-1022

(Published)

Vulnerability Type

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

Severity

High (8.1)

Visibility

Public

Status

Fixed

Found by

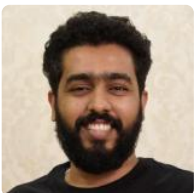


Scaramouche

@scara31

unranked

Fixed by



Muhsin Kelo

@muhsin-k

maintainer

This report was seen 457 times.

We are processing your report and will contact the **chatwoot** team within 24 hours.  
10 months ago

Scaramouche 10 months ago

Just as an addition: I use Telegram to add test customers

Chat with us

We have contacted a member of the **chatwoot** team and are waiting to hear back 10 months ago

We have sent a follow up to the **chatwoot** team. We will try again in 7 days. 9 months ago

We have sent a second follow up to the **chatwoot** team. We will try again in 10 days.  
9 months ago

We have sent a third and final follow up to the **chatwoot** team. This report is now considered stale. 9 months ago

**Sojan Jose** validated this vulnerability 8 months ago

**Scaramouche** has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

We have sent a fix follow up to the **chatwoot** team. We will try again in 7 days. 8 months ago

We have sent a second fix follow up to the **chatwoot** team. We will try again in 10 days.  
8 months ago

We have sent a third and final fix follow up to the **chatwoot** team. This report is now considered stale. 8 months ago

**Muhsin Keloth** marked this as fixed in **2.5.0** with commit **27ddd7** 7 months ago

**Muhsin Keloth** has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us