

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

0



Valid

Reported on Dec 25th 2021

### Title

Stored XSS in `custom_attributes`

### Description

Relying on frontend URI check without verifying it on the backend allows to inject arbitrary JS code.

### Steps to reproduce

1. Create a custom attribute, set its type to `Link`
2. Navigate to any conversation, click on the right sidebar.
3. Add a custom attribute, set its value to any valid URI.
4. While intercepting traffic save a new value, observe an outgoing request to `/api/v1/accounts/2/conversations/1/custom_attributes`
5. In `POST` request's body use something like:

```
{
  "custom_attributes":{
    "{yourAttributeName}":"javascript:alert(document.domain)"
  }
}
```

6. Click on the link, trigger an XSS.

Note: it works in Safari and Firefox, not Chrome

### Proof of Concept

Video PoC

Chat with us

# Impact

This vulnerability is capable of running arbitrary JS code.

CVE

CVE-2022-0526

(Published)

Vulnerability Type

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

Severity

High (7.3)

Visibility

Public

Status

Fixed

Found by

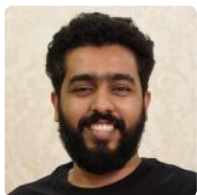


Scaramouche

@scara31

unranked

Fixed by



Muhsin Kelo

@muhsin-k

maintainer

This report was seen 409 times.

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

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

Scaramouche a year ago

Researcher

Sorry, forgot to add my rationale on it: this exploit may be abused by an **Agent** to leverage its privileges to **Admin**

Chat with us

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

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

We have sent a third and final follow up to the **chatwoot** team. This report is now considered stale. 10 months ago

**Muhsin Keloth** validated this vulnerability 10 months ago

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

The fix bounty is now up for grabs

**Muhsin Keloth** marked this as fixed in **2.2.0** with commit **9f37a6** 10 months ago

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

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us

[terms](#)

[privacy policy](#)

[Chat with us](#)