Cross-site Scripting (XSS) - DOM in chatwoot/chatwoot

1

Valid Reported on Dec 26th 2021

Title

XSS in markdown link-maker

Description

While chatting with a client, both sides may use markdown. However, neither client's nor Chatwoot inner user's input is verified.

Steps to reproduce.

Note: this works in Safari and Firefox, not Chrome.
I will use Telegram bot.
1. Start a conversation as an attacker with Chatwoot staff using created Telegram bot.
2. Send payload `[clickMe](javascript:alert(document.cookie))` as a message.
3. As a Chatwoot staff click on the link, trigger an XSS.
Also it is possible to create a malicious link as a staff (e.g. leave it in other's staff conversation in order to trigger an XSS on their side).
1. While intercepting your traffic send a message `[clickMe](https://google.com)` to pass frontend check.
2. In the outcoming `POST` request to `/api/v1/accounts/2/conversations/1/messages` modify the body, so it looked something like this:

```
{
    "content":"[click](javascript:alert(document.cookie))",
    "private":false,
    "echo_id":"{yourId}",
    "cc_emails":"",
    "bcc_emails":""
}
```

3. As some other staff click on the link, trigger an XSS.

I'm leaving a video PoC for both cases:

Video PoC

Possible remediation

Verify message content.

Impact

This vulnerability is capable of running an arbitrary JS code.

CVE
CVE-2022-0542
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - DOM

Severity
High (8.8)

Visibility
Public

Status
Fixed

Found by

Scaramouche
@scara31
unranked

This report was seen 675 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

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

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

Pranav Raj S validated this vulnerability 10 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. 9 months ago

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

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

Sojan Jose marked this as fixed in **2.7.0** with commit **dd1fe4** 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

FAQ

contact us

terms

privacy policy