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

0

Valid Reported on Dec 27th 2021

Steps To Reproduce:

1. Navigate to the campaigns section
2. Click on "Create a ongoing campaign"
3. Fill title, message, inbox and URL
4. Then click on "Create" and intercept it
5. Change your url's value to javascript:alert(1) (for example "url" : "https://google.com" to "url" : "javascript:alert(1)"
6. Sent the request
7. We can see in column "URL" , link javascript:alert(1)
8. If user clicks on it, an XSS will be triggered
9. It works only in FireFox and Safari

Impact

Attacker can convinces a victim to visit a URL then he can:

1. Steal users cookies
2. Redirect the user to malicious website

CVE
CVE-2022-0527
(Published)

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

Severity
Medium (6.1)

Visibility
Public

Status
Fixed

Found by

n1k1x86

@n1k1x86

unranked

Fixed by

Muhsin Keloth

@muhsin-k

maintainer

This report was seen 369 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. 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

n1k1x86 modified the report 10 months ago

Muhsin Keloth validated this vulnerability 10 months ago

n1k1x86 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 **a737f8** 10 months ago

Muhsin Keloth has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation