Insecure Storage of Sensitive Information in chatwoot/chatwoot

0

✓ Valid Reported on Feb 12th 2022

BUG

Stored xss via referer url allow to hijack victim access-token

STEP TO REPRODUCE

From admin account goto https://app.chatwoot.com/app/accounts/42689/settings/inboxes/list and create a inbox of type `website` .
Now get you configuration script from this inbox and save in html file .\

2. Now as a exeternal user view the above file and send a support chat messega while capturing it in burpsuite. Here bellow request is sent to server

```
POST /api/v1/widget/messages?website_token=6vsdbdaUQu21bnz3oFwhqQhW&locale=
Host: app.chatwoot.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://app.chatwoot.com/widget?website_token=6vsdbdaUQu21bnz3oFwh
X-Auth-Token: eyJhbGciOiJIUzI1NiJ9.eyJzb3VyY2VfaWQiOiJlNDFhMWZiOC02MDk5LTQz
Content-Type: application/json
Content-Length: 161
Origin: https://app.chatwoot.com
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
```

```
{"message":{"content":"xss via referer","timestamp":"Sat Feb 12 2022 21:56:
```

Here in this request i changed `referer_url` parameter value to `javascript:alert(document.cookie)` and forward the request .
Now a support message will be created .
3. Now from admin view the above chat message and CONTROL+CLick the referer link and see xss is executed

Video Poc

https://drive.google.com/file/d/1eQmGL0pvcaEcmRG_Tv0sA6-uznId7WYC/view?usp=sharing

IMPACT

I see chatwoot authenticate user using this header `Access-Token,Token-Type,Client,Expiry,Uid` .
And those value present in cookie `auth_data` .
So,using this xss cookie can be steal and also access token can be steal and using those token attacker can control victim acccount

Occurrences

base_controller.rb L1-L110

endPoints.js L7-L97

conversations_controller.rb L1-L56

messages_controller.rb L1-L66

CVE
CVE-2022-1021
(Published)

Vulnerability Type
CWE-922: Insecure Storage of Sensitive Information

Severity
High (7.6)

Visibility
Public

Status
Fixed

Chat with us

Found by

ranjit-git

@ranjit-git

amateur ✓

This report was seen 526 times.

We are processing your report and will contact the **chatwoot** team within 24 hours. 9 months ago

We have contacted a member of the **chatwoot** team and are waiting to hear back 9 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

ranjit-git 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

Sojan Jose marked this as fixed in **2.6.0** with commit **24b20c** 3 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Chat with us

conversations_controller.rb#L1-L56 has been validated ✓

endPoints.js#L7-L97 has been validated ✓

base_controller.rb#L1-L110 has been validated ✓

messages_controller.rb#L1-L66 has been validated ✓

Sign in to join this conversation

Chat with us