huntr

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

0

✓ Valid Reported on Feb 14th 2022

Description

LiveHelperChat is vulnerable to Stored XSS at the **Company name** field (`customer_company_nameValueParam` parameter) in the **Copyright settings** tab of the **Chat configuration** page.

Payload

```
{{constructor.constructor('alert(1)')()}}
```

Steps to reproduce

1.Login then go to **Chat configuration** page (`https://demo.livehelperchat.com/site_admin/chat/listchatconfig`)
2.Go to **Copyright settings** tab -> **Site settings** tab
2.In the **Your company name - visible in bottom left corner** field, input payload `{{constructor.constructor('alert(1)')()}}`
3.Click **Update** button then you will see the XSS popup will display. Moreover, when you go to the dashboard, the XSS popup will also display here.

Impact

This vulnerability has the potential to deface websites, result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the user's device.

CVE
CVE-2022-0612
(Published)

Chat with us

Vulnerability Type

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

Severity
Medium (6.7)

Visibility
Public

Status
Fixed

Found by

KhanhCM
@khanhchauminh
pro

This report was seen 427 times.

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

Remigijus Kiminas validated this vulnerability 9 months ago

KhanhCM has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in **3.93v** with commit **4d4f1d** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us