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

0

Valid Reported on Jan 27th 2022

Description

LiveHelperChat is vulnerable to Stored XSS at the **Name** and **Surname** fields in the **User account** page.

Payload

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

Steps to reproduce

1.Login then go to User account page
(`https://demo.livehelperchat.com/site_admin/user/account`)
2.In the **Name** and **Surname** fields, 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.

Occurrences

edit.tpl.php L91-L99

CVE

CVE-2022-0395
(Published)

Vulnerability Type

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

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

KhanhCM
@khanhchauminh
pro

This report was seen 330 times.

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

Remigijus Kiminas validated this vulnerability 10 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 **8fdb4f** 10 months ago

The fix bounty has been dropped ✘

This vulnerability will not receive a CVE ✘

edit.tpl.php#L91-L99 has been validated ✔

Sign in to join this conversation