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

0

Valid Reported on Jan 27th 2022

Description

Livehelperchat is vulnerable to stored cross site scripting.

Proof of Concept

1 . Login to the demo account
2 . Go to settings --> Live help configuration -->Visual settings for the visitor --> widget theme -->new --> name field
3 . Add payload in name field and click save
4 . Go to setting -->embed code --> questionary embed code --> click page embed code alert will trigger.
payload {{constructor.constructor('alert(1)')()}}

Impact

This vulnerability is capable of stolen the user cookie

CVE
CVE-2022-0394
(Published)

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

Severity
Medium (5.3)

Visibility
Public

Status
Fixed

Found by

Asura-N

@asura-n

noisy

This report was seen 359 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

Asura-N 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 **d7b854** 10 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

hacktivity
about
leaderboard
team
FAQ
contact us
terms
privacy policy