

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



Valid

Reported on Jan 26th 2022

Description

LiveHelperChat is vulnerable to Stored XSS at the **Name** field in the **Admin themes** of **System configuration**.

Payload

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

Steps to reproduce

- 1.Login then go to **Setting** -> **Live help configuration** tab
- 2.Click on **Admin themes** in **Visual settings for the admin** section
- 3.Click **New** button and input payload `{{constructor.constructor('alert(1)')()}}` in the **Name** field
- 4.Click **Save** button then go to that theme by clicking on that theme name in the list

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



adminthemeedit.php L1-L55



adminnewtheme.php L1-L44



admintheme.form.angular.js L1-L107



adminthemes.php L1-L32

Chat with us

CVE

CVE-2022-0375

(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 350 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 **bbfaa2** 10 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

admintheme.form.angular.js#L1-L107 has been validated ✓

adminnewtheme.php#L1-L44 has been validated ✓

adminthemeedit.php#L1-L55 has been validated ✓

Chat with us

adminthemeedit.php#L1-L55 has been validated ✓

adminthemes.php#L1-L32 has been validated ✓

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us