huntr

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

0

✓ Valid Reported on Jan 26th 2022

Description

Stored XSS is found in Settings>Live help configuration>Departments->Departments groups->edit When a user creates a new webhook under the NAME field and puts a payload {{constructor.constructor('alert(1)')()}}, the input gets stored, at user edit groupname , the payload gets executed.

Proof of Concept

https://drive.google.com/file/d/1V2dbaOS_h5HCab-C0KUaXOmaurZABVeE/view?usp=sharing

Impact

Through this vulnerability, an attacker is capable to execute malicious scripts.

References

- lovecppp

CVE
CVE-2022-0387
(Published)

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

Severity
Medium (6.3)

Visibility
Public

Status

Status

Fixed

Found by

LoveCpp

@lovecppp

unranked

This report was seen 327 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

LoveCpp 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 **ff70c7** 10 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

about

team

Chat with us