

Account Takeover [namelessmc.com] in namelessmc/nameless



Reported on Aug 6th 2022

Description:

Hello team, while i was testing on <https://namelessmc.com/login/> i noticed that there is no ratelimit protection on POST login form, so an attacker can takeover the account by brute forcing the password field

Steps to reproduce:

- 1- go to <https://namelessmc.com/login/>
- 2- Enter username and any password
- 3- Capture the request with burpsuite and start bruteforcing with our wordlist

POC Screenshot:

Attack
Save
Columns
7. Intruder attack of namelessmc.com - Temporary attack - Not saved to project file

Results
Target
Positions
Payloads
Resource Pool
Options

Filter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|------------|--------|-------|---------|--------|---------|
| 190 | 142545 | 302 | | | 818 | |
| 191 | loveme | 302 | | | 818 | |
| 192 | gabriel | 302 | | | 822 | |
| 193 | alexander | 302 | | | 820 | |
| 194 | cheese | 302 | | | 820 | |
| 195 | passw0rd | 302 | | | 814 | |
| 196 | 142536 | 302 | | | 820 | |
| 197 | namelessmc | 302 | | | 828 | |
| 198 | peanut | 302 | | | 826 | |
| 199 | 11223344 | 302 | | | 816 | |
| 200 | thomas | 302 | | | 824 | |
| 201 | angel1 | 302 | | | 820 | |

Request
Response

Pretty
Raw
Hex
Render
\n

```

1 HTTP/2 302 Found
2 Date: Sat, 06 Aug 2022 06:32:02 GMT
3 Content-Type: text/html; charset=UTF-8
4 X-Frame-Options: SAMEORIGIN, SAMEORIGIN
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: /
9 Cf-Cache-Status: DYNAMIC
10 Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
11 Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=a504LoW%2BRfkf53qZpOjFK9dUj45f"}]}
12 Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
13 Server: cloudflare
14 Cf-Ray: 7365bba2c89f8513-BOM
15 Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

```

?
⚙️
←
→
Search...
0 matches

Finished

Patch recommendation:

Add ratelimit protecion on POST login endpoints/parameters

Impact

Account takeover

Occurrences

 login.php L1-L331

Chat with us

CVE

CVE-2022-2821

(Published)

Vulnerability Type

CWE-304: Missing Critical Step in Authentication

Severity

Critical (9.8)

Registry

Other

Affected Version

2.0.0

Visibility

Public

Status

Fixed

Found by



AGNIHACKERS

@agnihackers

amateur ✓



This report was seen 614 times.

We are processing your report and will contact the **namelessmc/nameless** team within 24 hours. 4 months ago

We have contacted a member of the **namelessmc/nameless** team and are waiting to hear back 4 months ago

Sam validated this vulnerability 4 months ago

AGNIHACKERS has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chat with us

AGNIHACKERS 4 months ago

Researcher

@maintainer are you happy to assign a CVE? please confirm, then only admin can move further

AGNIHACKERS 4 months ago

Researcher

@Sam waiting for bounty . This is critical vulnerability.

AGNIHACKERS 4 months ago

Researcher

@admin can you pls assign a CVE for this?

Jamie Slome 4 months ago

Admin

Happy to assign a CVE once we get the go-ahead from the maintainer 👍

AGNIHACKERS 4 months ago

Researcher

@maintainer are you happy to assign a CVE ? Please confirm

We have sent a fix follow up to the **namelessmc/nameless** team. We will try again in 7 days.

4 months ago

AGNIHACKERS 4 months ago

Researcher

@maintainer are you happy to assign a CVE ? Please confirm

Sam 3 months ago

Hi, apologies for the delay.

Yes I am happy to go ahead with assigning a CVE.

Sam marked this as fixed in v2.0.2 with commit **98fe4b** 3 months ago

The fix bountv has been dropped ❌

Chat with us

the fix being has been dropped ❌

This vulnerability will not receive a CVE ❌

login.php#L1-L331 has been validated ✔️

AGNIHACKERS [3 months ago](#)

Researcher

@admin maintainer as given the permission for assigning CVE. So please assign a CVE for this report

Jamie Slome [3 months ago](#)

Admin

Sorted 👍

AGNIHACKERS [3 months ago](#)

Researcher

@admin waiting for bounty . This is critical vulnerability.

Jamie Slome [3 months ago](#)

Admin

There is no bounty for this report. You should see the potential bounty for a report when you submit it.

Sign in to join this conversation

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us

[hacktivity](#)

[about](#)

[leaderboard](#)

[team](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)