Previously created sessions continue being valid after MFA activation [namelessmc.com] in namelessmc/nameless

1

Valid Reported on Aug 6th 2022

Description

Hello Team I found one issue related to your 2FA system on
`https://namelessmc.com/user/settings/?do=enable_tfa&s=2`

Vulnerability Type:

Improper Access Control - Generic

STEP TO REPRODUCE:

1- access the same account on `https://namelessmc.com/` in two devices
2- on device `'A'` go to
`https://namelessmc.com/user/settings/?do=enable_tfa&s=2` > complete all steps to change the 2FA system
-> Now the 2FA is activated from Phone number/Email
3- back to device `'B'` reload the page
-> The session is still active and also I have updated the new email.
4- For More Details To Check the POC

Proof of Concept:

POC VIDEO

Impact

In this scenario when 2FA is changing the other sessions of the account are not invalidated. 2FA is required to login. I believe the expected and recommended behavior here is to terminate the other sessions> request a new login> request the 2FA code> account access again

Occurrences

settings.php L24-L135

References

- https://hackerone.com/reports/667739

CVE
CVE-2022-2820
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (7)

Registry
Other

Affected Version
2.0.1

Visibility
Public

Status
Fixed

Found by

AGNIHACKERS
@agnihackers
amateur

This report was seen 504 times.

We are processing your report and will contact the namelessmc/nameless t[illegible] hours. 4 months ago

Chat with us

Sam validated this vulnerability 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

AGNIHACKERS 4 months ago Researcher

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

AGNIHACKERS 4 months ago Researcher

@admin can you pls assign a CVE for this?

AGNIHACKERS 4 months ago Researcher

@Sam waiting for bounty . This is High vulnerability.

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

Sam 3 months ago Maintainer

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 469bab 3 months ago

Sam marked this as fixed in v2.0.2 with commit 469beb 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

settings.php#L24-L135 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 High 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