Improper Restriction of Excessive Authentication Attempts in firefly-iii/firefly-iii

0

Valid Reported on Jul 21st 2021

Improper Restriction of Excessive Authentication Attempts. The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.
STEPS FOR REPRODUCTION:
1)Go to https://demo.firefly-iii.org/login 2)Enter the username and password 3)Capture the request 4)Set the field for password and start bruteforcing the password
I was able to brute force the password with a list of around 200+ usernames, the no. of attempts must be reduced to less than 10

Impact

This vulnerability is capable of, if the attacker uses the correct password list, it can lead to account takeovers.

Occurrences

login.twig L74

CVE
CVE-2021-3663
(Published)

Vulnerability Type
CWE-307: Improper Restriction of Excessive Authentication Attempts

Severity
Medium (5.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

sudheendra17
@sudheendra17
unranked

Fixed by

James Cole
@jc5
maintainer

This report was seen 565 times.

We have contacted a member of the **firefly-iii** team and are waiting to hear back a year ago

James Cole validated this vulnerability a year ago

sudheendra17 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

James Cole a year ago Maintainer

Nice find, should be fixed now on the demo site. Fix will be part of the next release.

James Cole marked this as fixed with commit afc9f4 a year ago

James Cole has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

Jamie Slome a year ago Admin

@James - the content of the CVE to be published:

https://github.com/418sec/cvelist/blob/CVE-2021-3663/2021/3xxx/CVE-2021-3663.json

James Cole a year ago Maintainer

cool!

sudheendra17 a year ago Researcher

hi, is the disclosure bounty for this program $0 or $80, because I can saw 80$ while searching for this program

sudheendra17 a year ago Researcher

hi @admin is the disclosure bounty for this program $0 or $80, because I saw 80$ while searching for this program

Jamie Slome a year ago Admin

@sudheendra17 - this was given a bounty reward of $0 as the CWE type / vulnerability type is blacklisted. This is because it is non-code vulnerability type. Feel free to read our disclosure policy for more information:

Policy

Jamie Slome a year ago Admin

@James - the CVE is now pending, and should be published shortly by the CVE team.

Ref

Sign in to join this conversation