

Cross-Site Request Forgery (CSRF) in firefly-iii/firefly-iii0

ValidReported on Nov 23rd 2021

Description

CSRF to disable 2FA

Proof of Concept

```
<a href="http://10.0.2.15/profile/delete-code">CLICK ME!</a>
```

Impact

This vulnerability is capable of tricking users to disable 2FA.

CVE

CVE-2021-4005

(Published)

Vulnerability Type

CWE-352: Cross-Site Request Forgery (CSRF)

Severity

Medium (4.3)


Visibility

Public

Status

Fixed

Found by



haxatron

@haxatron

pro

Fixed by



James Cole

@jc5

maintainer

This report was seen 401 times.

We are processing your report and will contact the firefly-iii team within 24 hours. a year ago

haxatron

a year ago

Researcher

My apologies for submitting the reports earlier regarding /debug and /flush. I was under the assumption that the /debug and /flush was available to only admin users, as the /flush UI only appeared in the Administration panel.

haxatron

modified the report

a year ago

haxatron

modified the report

a year ago

haxatron

a year ago

Researcher

With further testing on the application after I made the reports, I discovered another CSRF unprotected endpoint which allows for a state-change, the endpoint is as listed above.

James Cole

a year ago

Maintainer

Nice find, that's an important one to fix. No worries about the other endpoints, keep it up!

James Cole

validated this vulnerability

a year ago

haxatron

has been awarded the disclosure bounty

✓

The fix bounty is now up for grabs

Jamie Slome

a year ago

Admin

Are we able to mark a fix against this report, and we can go ahead and publish the CVE!

James Cole a year ago

Maintainer

Not yet I completely forgot about it.:D

Jamie Slome a year ago

Admin

No worries, take your time! 🍷

James Cole marked this as fixed in 5.6.6 with commit 03a160 a year ago

James Cole has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team