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

0

Valid Reported on Sep 19th 2021

Description

Hello dear firefly-iii team
I found some CSRFs with low priority in firefly-iii

Occurrences

CurrencyController.php L1-L441

disable/enable any currency

TransactionGroupRepositoryInterface.php L1-L173

clone any transaction

JS index.js L1-L43

disable/enable any currency

TransactionTypeRepositoryInterface.php L1-L56

clone any transaction

web.php L341-L342

disable/enable any currency

JS index.js L1-L29

clone any transaction

TransactionGroupRepository.php L1-L485

clone any transaction

web.php L1015

Attackers able to clone any transaction

CurrencyController.php L314-L332

disable/enable any currency

TransactionTypeRepository.php L1-L86

clone any transaction

show.twig L1-L432

clone any transaction

CreateController.php L1-L134

clone any transaction

CurrencyController.php L216-L273

disable/enable any currency

CVE
CVE-2021-3819
(Published)

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

Severity
Medium (4.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

Fixed by

James Cole
@jc5
maintainer

This report was seen 385 times.

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

James Cole a year ago — Maintainer

That's three, right? disable, enable, clone. I'll check it out :+1:

amammad a year ago — Researcher

Yah clone transactions and enable/disable currencies

James Cole validated this vulnerability a year ago

amammad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

James Cole marked this as fixed with commit 578f35 a year ago

James Cole has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

TransactionTypeRepositoryInterface.php#L1-L56 has been validated ✓

index.js#L1-L43 has been validated ✓

web.php#L341-L342 has been validated ✓

index.js#L1-L29 has been validated ✓

CurrencyController.php#L314-L332 has been validated ✓

TransactionGroupRepository.php#L1-L485 has been validated ✓

web.php#L1015 has been validated ✓

TransactionTypeRepository.php#L1-L86 has been validated ✓

show.twig#L1-L432 has been validated ✓

CurrencyController.php#L1-L441 has been validated ✓

TransactionGroupRepositoryInterface.php#L1-L173 has been validated ✓

CreateController.php#L1-L134 has been validated ✓

CurrencyController.php#L216-L273 has been validated

Jamie Slome a year ago Admin

CVE published!

Sign in to join this conversation