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

0

Valid Reported on Nov 1st 2021

Description

Attacker is able to logout a user if a logged in user visits attacker website.

Impact

This vulnerability is capable of forging user to unintentional logout.

Test

Tested on Edge, firefox, chrome and safari.

Fix

You should use POST instead of GET/ANY.

To expand:

One way GET/ANY could be abused here is that a person (competitor perhaps:) placed an image tag with src="<your logout link>" ANYWHERE on the internet, and if a user of your site stumbles upon that page, he will be unknowingly logged out. This is why it should be a POST with a @csrf token.

Note

While this cannot harm a users account it can be a great annoyance and is considered a valid CSRF.

Occurrences

web.php L84

CVE
CVE-2021-3921
(Published)

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

Severity
Medium (5.4)

Visibility
Public

Status
Fixed

Found by

HDVinnie
@hdvinnie
maintainer

Fixed by

James Cole
@jc5
maintainer

This report was seen 384 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

HDVinnie has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

James Cole marked this as fixed with commit 47fa9e a year ago

James Cole has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

web.php#L84 has been validated ✓

Sign in to join this conversation