huntr

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

0

✓ Valid Reported on Oct 23rd 2021

Description

No CSRF in duplicate rule, and modifying the order of the rule group

Proof of Concept

```
<a href="https://demo.firefly-iii.org/rules/duplicate/1">Click Me!</a>
<a href="https://demo.firefly-iii.org/rule-groups/up/1">Click Me!</a>
<a href="https://demo.firefly-iii.org/rule-groups/down/1">Click Me!</a>
```

Impact

This vulnerability is capable of tricking admin users to duplicate rule and modifying order of rule groups
Permalinks selected with reference to this report: https://huntr.dev/bounties/da82f7b6-4ffc-4109-87a4-a2a790bd44e5/

Occurrences

index.twig L105L110

attackers able to duplicate any rule frontend

web.php L925L926

up/down api

EditController.php L117L126

group up backend

RuleRepository.php L76L99

attackers able to duplicate any rule backend

EditController.php L71L81

group down backend

CreateController.php L242L249

attackers able to duplicate any rule backend

RuleRepositoryInterface.php L49L60

attackers able to duplicate any rule

index.twig L48L55

up/down frontend

References

- https://huntr.dev/bounties/da82f7b6-4ffc-4109-87a4-a2a790bd44e5/

CVE
CVE-2021-3900
(Published)

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

Severity
Medium (4.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

James Cole
@jc5
maintainer

This report was seen 408 times.

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

haxatron modified the report a year ago

haxatron modified the report a year ago

James Cole validated this vulnerability a year ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

haxatron a year ago Researcher

Lol I wanted to modify a permalink because I placed the wrong blob but you validated the report right away so nvm

James Cole a year ago Maintainer

Should be fixed, nice find. See the demo site.

James Cole a year ago Maintainer

Yeah I almost knew without looking ^^

James Cole marked this as fixed with commit c2c8c4 a year ago

James Cole has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

index.twig#L105L110 has been validated ✓

EditController.php#L117L126 has been validated ✓

web.php#L925L926 has been validated ✓

RuleRepository.php#L76L99 has been validated ✓

EditController.php#L71L81 has been validated ✓

CreateController.php#L242L249 has been validated ✓

RuleRepositoryInterface.php#L49L60 has been validated ✓

index.twig#L48L55 has been validated ✓

haxatron a year ago Researcher

Am away from computer now, will check later

And yeah, Github is confusing lol

Jamie Slome a year ago Admin

CVE published! 🎊

Sign in to join this conversation