

Cross-Site Request Forgery (CSRF) in kevinpapst/kimai2

Valid Reported on Nov 20th 2021

0

CSRF Set 1 (modify invoice status [Medium severity])

Description

CSRF in saving invoices / modifying status of invoices (pending and cancel only)

Proof of Concept

The following state-changing endpoints are vulnerable to CSRF

```
GET /en/invoice/save-invoice/9/5?searchTerm=&daterange=2021-11-01%20-%202020-11-30
GET /en/invoice/change-status/2/canceled
GET /en/invoice/change-status/2/pending
GET /en/invoice/?createInvoice=true&searchTerm=&daterange=2021-11-01%20-%202020-11-30
```



Impact

Attackers can trick users to modify status of invoices, potentially disrupting invoice tracking.

CSRF Set 2 (modify search favourites [Low severity])

Description

CSRF in adding / deleting search favorites

Proof of Concept

The following state-changing endpoints are vulnerable to CSRF

```
GET /en/invoice/?removeDefaultQuery=InvoiceQuery
GET /en/invoice/?searchTerm=&daterange=2021-11-01++2021-11-30&tags=&export
```



Impact

Although very low severity, these state-changing actions are CSRF unprotected.

Occurrences

- actions.html.twig L1L35

invoice save / pending frontend
- index.html.twig L226L234


save all invoices js
- InvoiceController.php L153L177

save-invoice backend
- AbstractController.php L230L234

removeDefaultQuery backend
- InvoiceController.php L184L205

invoice status change (pending / cancel) backend
- InvoiceController.php L89L96

save all invoice backend

 index.html.twig L215L223

save-invoice.js

CVE  
CVE-2021-4033  
(Published)


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

Severity  
Medium (6.5)

Visibility  
Public

Status  
Fixed

Found by




haxatron

@haxatron

pro

Fixed by



Kevin Papst

@kevinpapst

unranked

This report was seen 377 times.

- We are processing your report and will contact the **kevinpapst/kimai2** team within 24 hours.

a year ago
- We have contacted a member of the **kevinpapst/kimai2** team and are waiting to hear back

a year ago
- We have sent a follow up to the **kevinpapst/kimai2** team. We will try again in 7 days.

a year ago

Kevin Papst a year ago

Maintainer

Sorry for not replying earlier @haxatron. Thanks for your report!

You are right that there is no CSRF protection. am not sure that I agree that this is a problem or even a risk, so I'll leave it open until I find enough time to look into the code. Will keep you updated.

haxatron modified the report a year ago

haxatron a year ago

Researcher

Thank you for the response @maintainer!

I have added 4 more CSRF unprotected state-changing endpoints related to modifying the status of invoices. You may choose to fix whichever endpoints that are detailed in this report.

Kevin Papst validated this vulnerability a year ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Kevin Papst a year ago

Maintainer

Again: awesome work @haxatron - I need a litte more time to fix them, but for now I can say that they are all valid.

Kevin Papst submitted a patch a year ago

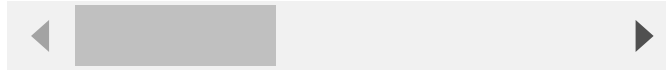
haxatron a year ago

Researcher

Thanks for submitting the fix! can confirm its patched. However there is an error in the save-invoice field.

There is a two token parameters in the save-invoice endpoint (eg.

```
GET /en/invoice/save-invoice/9/5?token=gYcEqImSbT1xMzzTbMf0hYrYzv9PPuZHw2TdbFQ8UbY&se:
....
It will show an error message
....
Changes could not be saved:
[] This form should not contain extra fields.
....
```



**haxatron** a year ago

**Researcher**

create\_invoice seems to be working fine, its just save-invoice

**Kevin Papst** a year ago

**Maintainer**

I fixed the "save-invoice" issue.  
@haxatron if you write me an email I will send you a little "thank you" for all the fantastic feedback!

**haxatron** a year ago

**Researcher**

Thanks for fixing all the issues!

For me, responding and / or fixing these reports are thanks enough! 😊

**Kevin Papst** a year ago

**Maintainer**

:D verify generous! Still, the offer stands, so send me a message whenever you want.

Tell me: do you see the "Confirm fix" button as well? Is the idea that I click it (as I did in the past) or do you actually verify the fix and hit that button?

**haxatron** a year ago

**Researcher**

I think you have to click it 😊

**Kevin Papst** marked this as fixed in 1.16.7 with commit 1da26e a year ago

**Kevin Papst** has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

actions.html.twig#L1L35 has been validated ✓

index.html.twig#L226L234 has been validated ✓

InvoiceController.php#L184L205 has been validated ✓

index.html.twig#L215L223 has been validated ✓

InvoiceController.php#L153L177 has been validated ✓

AbstractController.php#L230L234 has been validated ✓

InvoiceController.php#L89L96 has been validated ✓

Sign in to join this conversation

