

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

Valid

Reported on Nov 16th 2021

0

Description

CSRF related to duplicate action. (the duplication occurs first before redirecting to edit form)

Proof of Concept

```
GET /en/admin/teams/{id}/duplicate
GET /en/admin/project/{id}/duplicate
```

Impact

This vulnerability is capable of tricking admin users to duplicate teams

Note

This is probably all the unprotected endpoints for duplicate action vulnerable to CSRF, there may be more, but this is what I have found while looking through the files.

Occurrences

ProjectController.php L427L432	duplicate project backend
TeamController.php L87L102	duplicate team backend
actions.html.twig L1L15	duplicate team frontend
TeamSubscriber.php L36L39	duplicate team subscriber
actions.html.twig L1L15	duplicate project frontend

CVE

CVE-2021-3976

(Published)

Vulnerability Type

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

Severity

Medium (4.3)


Visibility

Public

Status

Fixed

Found by



haxatron

@haxatron

pro

Fixed by



Kevin Papst

@kevinpapst

unranked

This report was seen 317 times.

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

haxatron modified the report a year ago

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

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 marked this as fixed with commit **b28e9c** a year ago

Kevin Papst has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

actions.html.twig#L1L15 has been validated ✓

ProjectController.php#L427L432 has been validated ✓

actions.html.twig#L1L15 has been validated ✓

TeamSubscriber.php#L36L39 has been validated ✓

TeamController.php#L87L102 has been validated ✓

Kevin Papst a year ago

Maintainer

Thanks @haxatron, I found and fix two more duplicate actions with the same problem :-)

Kevin Papst a year ago

Maintainer

Credits, see new release <https://github.com/kevinpapst/kimai2/releases/tag/1.16.2>

haxatron a year ago

Researcher

Thanks, but I think the two other duplicate actions did not duplicate the object before redirecting to the form unlike duplicate project and team I have reported here, so there was no need for the CSRF protection on the two other duplicate actions. :-)

Kevin Papst a year ago

Maintainer

Yeah, that was a late night mistake and is already reverted ... having two CSRF protections on one form is probably too much :D

Jamie Slome a year ago

Admin

CVE published! 🎉

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

part of 418sec

company

about

