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

0

Valid Reported on Nov 15th 2021

Description

CSRF in deleting invoice templates

Proof of Concept

```
<a href="https://[KIMAi_URL]/en/invoice/template/7/delete">CLICK ME!</a>
```

Impact

This vulnerability is capable of tricking admin user to delete invoice templates.

Occurrences

InvoiceController.php L457L467 InvoiceTemplateSubscriber.php L37L39

CVE
CVE-2021-3963
(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 379 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 submitted a **patch** 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 **95796a** a year ago

Kevin Papst has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

InvoiceController.php#L457L467 has been validated ✓

InvoiceTemplateSubscriber.php#L37L39 has been validated ✓

Jamie Slome a year ago Admin

Chat with us

CVE published! 🎉

Sign in to join this conversation

2022 © 418sec