huntr

# Improper Access Control in kevinpapst/kimai2

0

✓ Valid Reported on Nov 20th 2021

## Description

Authenticated users can preview invoices which they do not have read access to

## Proof of Concept

To demonstrate this vulnerability, we will use tony_teamlead on the demo site.
1: Login as tony_teamlead.
2: Go to Invoices page, see that there is no Haley-Jaskolski invoice document present on the UI.
3: But if tony_teamlead visits https://demo.kimai.org/en/invoice/preview/4/4, they will be able to see Haley-Jaskolski's invoice document. On the demo-stable website if tony_teamlead visits https://demo-stable.kimai.org/en/invoice/preview/1/4, they will see Crooks Group's document even though they do not have access to it.
4: Attackers can increment the invoice_id up and down - https://demo.kimai.org/en/invoice/preview/{invoice_id}/{file_export_format}, to retrieve invoice documents they do not have access to.

## Impact

Authenticated users can access potentially sensitive financial information they do not have access to

## Occurrences

InvoiceController.php L136L160

CVE
CVE-2021-3992
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (6.5)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

Fixed by

Kevin Papst
@kevinpapst
unranked

This report was seen 362 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

haxatron modified the report a year ago

haxatron modified the report a year ago

Kevin Papst a year ago Maintainer

I don't yet understand that report.
The route you are talking about creates a preview invoice, it's definition is called: /preview/{customer}/{template}
Every user who owns the view_invoice permission is allowed to do that and Teamleads have that permission.

haxatron a year ago Researcher

If you look at the invoice previews as susan_super, the super admin, you actually see all the invoices stored on the server, including Haley_Jakolski's

Thus, I presumed that tony_teamlead does not have access to the Haley_Jakolski's invoice documents because it does not show up in the U UI in the demo development server.

But yet if you go to https://demo.kimai.org/en/invoice/preview/4/4, youll be able to view the documents.

haxatron a year ago Researcher

Hold on, let me add images for more clarity

haxatron a year ago Researcher

1: As susan_super, I can see all invoice documents - Link 1

2: As tony_teamlead, I can only see some of the documents, presumably because I do not have read access to documents I cannot see - Link 2

3: As tony_teamlead, I can still access the documents which I do not have read access to, via previews, for instance Gorzanic Brandike: Link 3

Kevin Papst a year ago Maintainer

Understand, thanks! I need some time to investigate.

haxatron a year ago Researcher

Thus the issue above is that users without access to reading someone's invoice documents, can still access them by previews.

Kevin Papst a year ago Maintainer

Just to clarify: the preview route does not download existing invoice documents, but creates a preview for time-records not yet billed to customers. So for "possible future invoices".
But give me some time to investigate now, I'll let you know :)

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** submitted a **patch** a year ago

**Kevin Papst** marked this as fixed in **1.16.2** with commit **ff9aca** a year ago

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

This vulnerability will not receive a CVE ✗

**InvoiceController.php#L136L160** has been validated ✓

Sign in to join this conversation