

Non-Privilege user can view Patient's Amendments in openemr/openemr

0



Valid

Reported on Jul 21st 2022

Description

We would like to report the vulnerability we found during software testing. The OpenEMR 7.0.0 (latest version) Open-Source electronic health records and medical practice management application has Insecure direct object reference (IDOR) to function "Patient's Amendments", and it never been reported before (We've checked from CVE Official website).

Vulnerability Type

Insecure Direct Object Reference

Affected Page/URL

`https://{URL}/interface/patient_file/summary/add_edit_amendments.php?id=594`



Method

GET

Parameter

id

Authentication Required?

Yes

Chat with us

Vulnerable Source Code

/var/www/localhost/htdocs/interface/patient_file/summary/add_edit_amendments.php (Please see more details in the occurrences section)

Implication

Applications don't always verify the user is authorized for the target object. This results in an insecure direct object reference flaw. A perpetrator, who is an authorized system user (Non-privilege users (accounting, front office)), simply changes a parameter value that directly refers to a system object to another object the user isn't authorized for. As a result, an Insecure Direct Object References (IDOR) vulnerability allowing remote attackers to view the metadata of boards they should not have access.

Recommendation

It is recommended to implement access control check to ensure the user is authorized for the requested object on the GET method.

Discoverer/Reporters

Ammarit Thongthua, Rattapon Jitprajong and Nattakit Intarasorn from Secure D Center Research Team

Example PoC Screenshots

OpenEMR Version 7.0.0

The screenshot shows the OpenEMR interface. At the top, there's a navigation bar with links like Calendar, Finder, Flow, Recalls, Messages, Patient, Fees, Modules, Procedures, Admin, Reports, Miscellaneous, and Popups. A search bar is on the right. Below the navigation bar, a user profile for 'Stefan Maker (2)' is displayed, including a profile picture, name, and DOB: 2006-07-20 Age: 16. A dropdown menu is open, showing options: Administrator (highlighted), Settings, Change Password, MFA Management, About OpenEMR, and Logout. The main content area is titled 'About OpenEMR' and contains the following information:

Version Number	7.0.0
Unique Installation UUID	ef9f0ec2-3db9-49f9-a029-e32df222c65f
Online Support	http://open-emr.org/

Below the table, there are three buttons: 'User Manual', 'Acknowledgments, Licensing and Certification', and 'Write a Review'. A 'Chat with us' button is also visible in the bottom right corner.

♥ Donate Now

Login with Administrator privilege and add Amendments

The screenshot displays the OpenEMR interface. At the top, a navigation bar includes links like Calendar, Finder, Flow, Recalls, Messages, Patient, Fees, Modules, Procedures, Admin, Reports, Miscellaneous, and Popups. A search bar is also present. Below the navigation bar, the patient's name 'Stefan Maker (2)' and their DOB '2006-07-20 Age: 16' are shown. The 'Amendments' form is open, featuring a 'Save' button and a 'Back' button. The form fields are as follows:

- Requested Date:** 2022-07-23
- Requested By:** Patient
- Request Description:** Add by Administrator
- Request Status:** Approved
- Comments:** Add by Administrator

In the top right corner, a user menu is open, showing the role 'Administrator' and options like Settings, Change Password, MFA Management, About OpenEMR, and Logout.

Successfully add Amendments via normal step

Chat with us

localhost/interface/main/tabs/main.php?token_main=pAyqLdXOiCe271ASuRSiUJOXYi3jGsuLs1Sf7tq7

Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups Search by any demogra

Stefan Maker (2) × DOB: 2006-07-20 Age: 16 Select Encounter (0) +

Amendments

< Back

Requested Date
2022-07-23

Requested By
Patient

Request Description
Add by Administrator

Request Status
Approved

Comments

History

Date	By	Status	Comments
2022-07-21	Administrator,	Approved	Add by Administrator Approved

Login with non-Privilege user

https://localhost/interface/main/tabs/main.php?token_main=Qotfq99fk1zV8pDyOdldRMQv8ZGXmliuKyryeFdex

File View Patient Popups Miscellaneous Search by any demogra

About OpenEMR

Non Privilege

- Settings
- Change Password
- MFA Management
- About OpenEMR
- Logout

About OpenEMR

Version Number 7.0.0

Unique Installation UUID ef9f0ec2-3db9-49f9-a029-e32df222c65f

Online Support <http://open-emr.org/>

User Manual

Acknowledgments, Licensing and Certification

Write a Review

Donate Now

Chat with us

Direct access to URL and success to view "Amendments Page"

Sec-Ch-Ua-Platform: "macOS"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4012.91 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: close

Impact

According to openEMR version 7.0.0. It is, therefore, affected by an Insecure Direct Object References (IDOR) vulnerability allowing remote attackers to view the metadata of boards they should not have access on Patient's Medical record Amendments.

Occurrences

 add_edit_amendments.php L92-L109

```
$amendment_id = $amendment_id ?? ($_REQUEST['id'] ?? '');  
if (!empty($amendment_id)) {  
    $query = "SELECT * FROM amendments WHERE amendment_id = ? ";  
    $resultSet = sqlQuery($query, array($amendment_id));  
    $amendment_date = $resultSet['amendment_date'];  
    $amendment_status = $resultSet['amendment_status'];  
    $amendment_by = $resultSet['amendment_by'];  
    $amendment_desc = $resultSet['amendment_desc'];  
  
    $query = "SELECT * FROM amendments_history ah INNER JOIN users u ON  
    $resultSet = sqlStatement($query, array($amendment_id));  
}  
  
// Check the ACL  
$haveAccess = AclMain::aclCheckCore('patients', 'trans');
```

Chat with us

```
$onlyRead = ( $haveAccess ) ? 0 : 1;  
$onlyRead = ( $onlyRead || (!empty($amendment_status)) ) ? 1 : 0;  
$customAttributes = ( $onlyRead ) ? array("disabled" => "true") : null;
```



CVE

CVE-2022-2730

(Published)

Vulnerability Type

CWE-639: Authorization Bypass Through User-Controlled Key

Severity

Medium (6.5)

Registry

Other

Affected Version

7.0.0

Visibility

Public

Status

Fixed

Found by



rata99

@rata99

unranked ▼

This report was seen 453 times.

We are processing your report and will contact the **openemr** team within 24 hours.

4 months ago

We have contacted a member of the **openemr** team and are waiting to hear back.

Chat with us

Brady Miller validated this vulnerability 4 months ago

Thanks for the report. We are working on a fix.

rata99 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **openemr** team. We will try again in 7 days. 4 months ago

Brady Miller 4 months ago

Maintainer

A preliminary fix has been posted in commit 2973592bc7b1f4996738a6fd27d1e277e33676b6

Please do not create a CVE # or make this vulnerability public at this time. I will make this fix official about 1 week after we release 7.0.0 patch 1 (7.0.0.1), which will likely be in about 3-7 weeks. After I do that, then will be ok to make CVE # and make it public.

Thanks!

rata99 4 months ago

Researcher

Hi Brady, Thank you so much.

We have sent a second fix follow up to the **openemr** team. We will try again in 10 days.
4 months ago

rata99 4 months ago

Researcher

Dear @Brady Miller, @admin

Hope you are doing well. We have got the notification email that the 1st patch for OpenEMR 7.0.0 has been released.

Can the CVE be assigned to this issue?

Chat with us

Patch 1 for OpenEMR 7.0.0 Released Inbox X



no-reply@open-emr.org via amazonses.com
to me ▾

9:16 AM (31 minutes ago)



[View online version](#)

Patch 1 for OpenEMR 7.0.0 Released

The 1st patch for OpenEMR 7.0.0 has been released.

See here for more details on downloading and installing the new patch: <https://community.open-emr.org/t/openemr-7-0-0-patch-1-has-been-released/18904>

This patch includes the following items

- Security fixes
- Vitals form fix
- Patient search fix
- CCDA fix for large amount of data
- Patient history form fix
- Patient portal EASIPRO fix
- Patient portal history form fix
- Added voided claim to misc billing options and 837 file
- PHP 8.1 fixes

OpenEMR needs donations for funding of critical features like maintaining ONC 2015 certification, API, FHIR, and a huge amount of other cool stuff. So please donate to the OpenEMR project: <https://www.open-emr.org/donate/>

For only \$1 per month you can be an Official OpenEMR Sponsor on github! You can sign up at: <https://github.com/sponsors/openemr>

[Click here to unsubscribe.](#)

Jamie Slome [4 months ago](#)

[Admin](#)

Just waiting for the go-ahead from the maintainer and then we can assign and publish a CVE for this report 🙌

Brady Miller marked this as fixed in 7.0.0.1 with commit 297359 [4 months ago](#)

The fix bounty has been dropped ❌

This vulnerability will not receive a CVE ❌

add_edit_amendments.php#L92-L109 has been validated ✅

Brady Miller [4 months ago](#)

[Maintainer](#)

OpenEMR patch 1 (7.0.0.1) has been released, so this has been fixed. You have make CVE # and make this public.

[Chat with us](#)

rata99 4 months ago

Researcher

Hi @Jamie Slome @Admin could you please help to assign CVE to this issue? Thank you :)

Jamie Slome 4 months ago

Admin

CVE assigned and will be automatically published in the next couple of hours ♥

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us