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

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

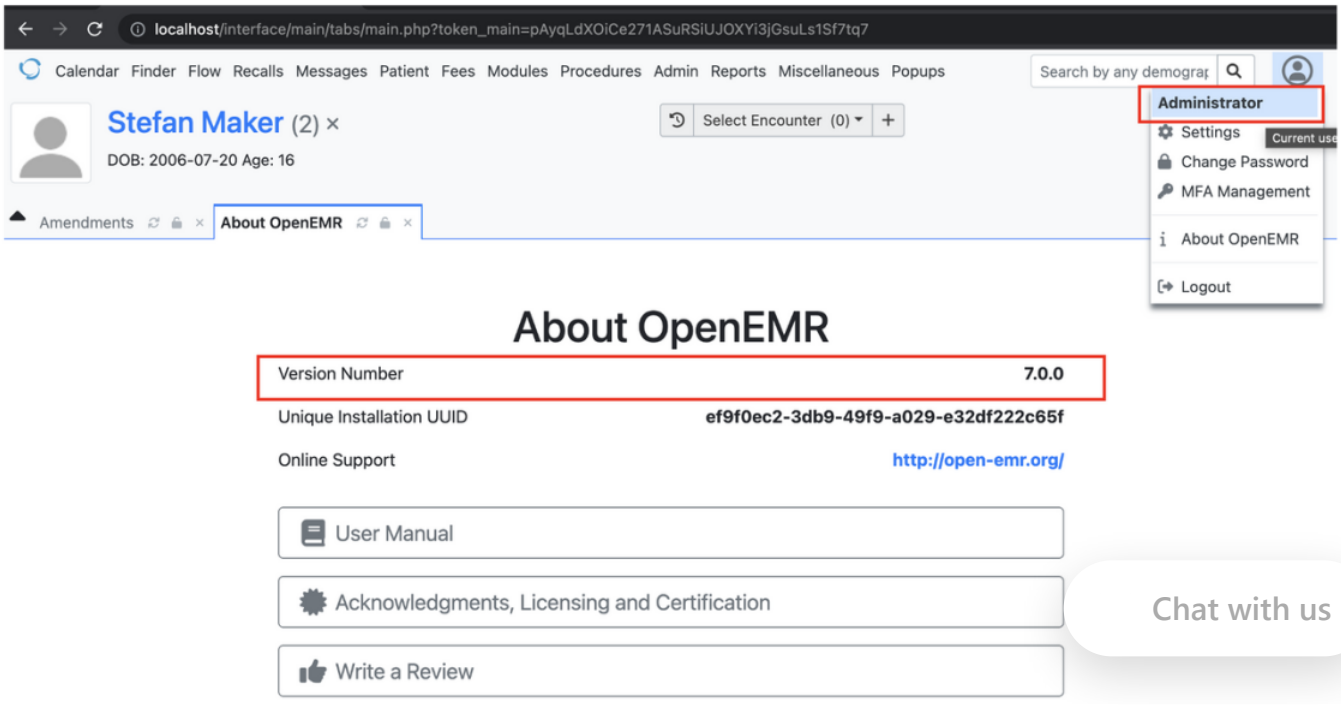
It is recommended to implement access control check to ensure the user is authorized for the requested object on the GET method.

Discoverer/Reporters

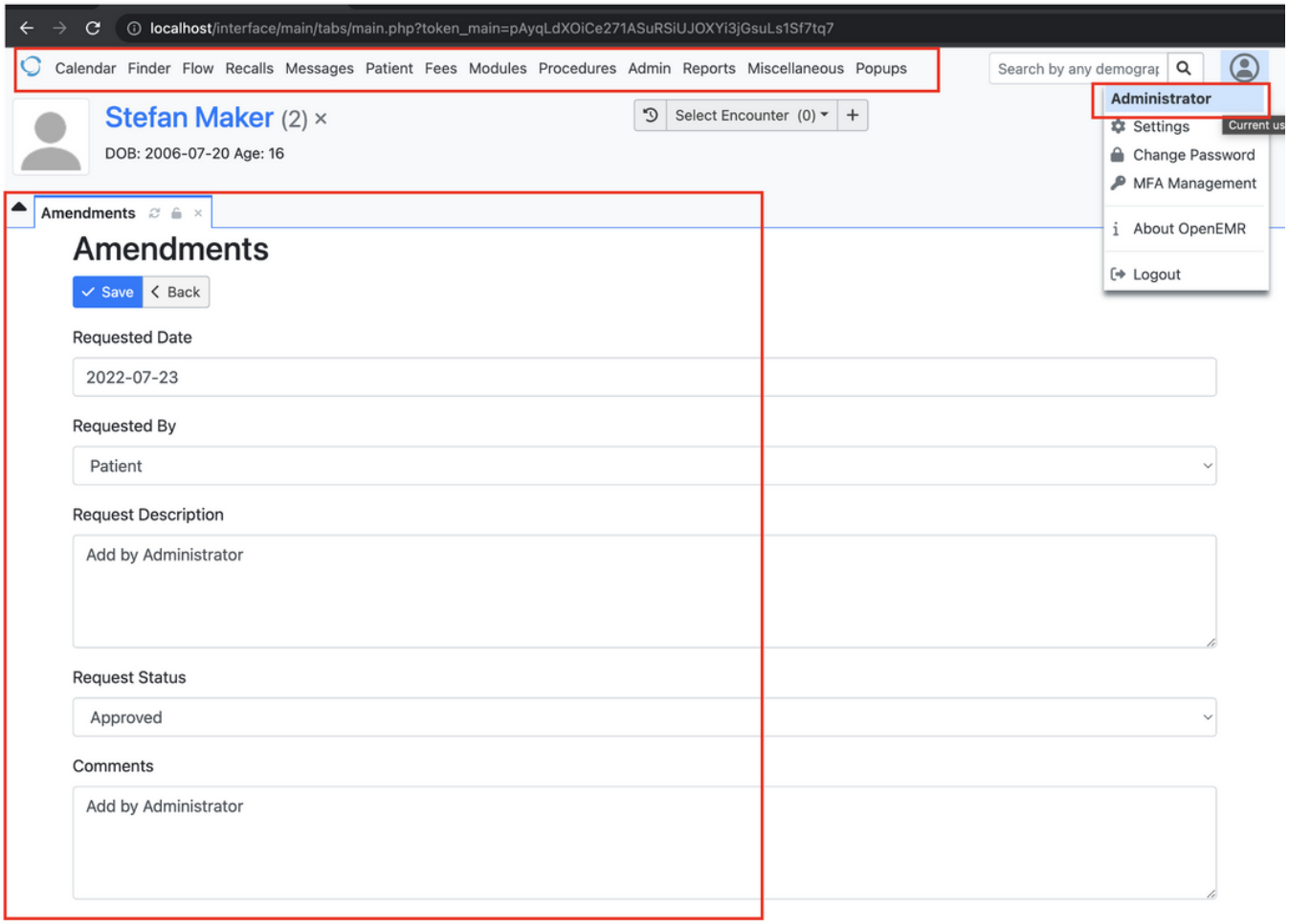
Ammarit Thongthua, Rattapon Jitprajong and Nattakit Intarasorn from Secure D Center Research Team

Example PoC Screenshots

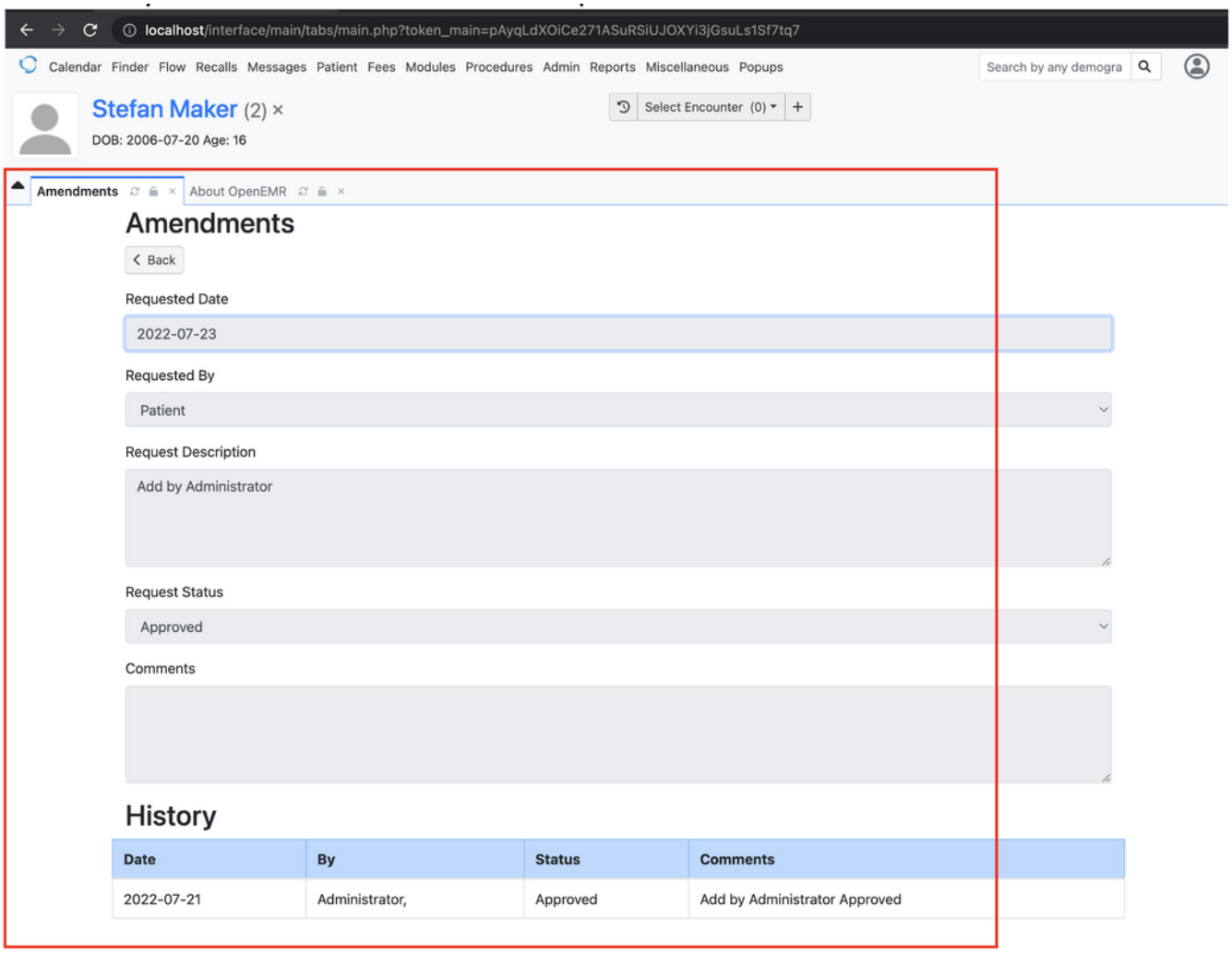
OpenEMR Version 7.0.0



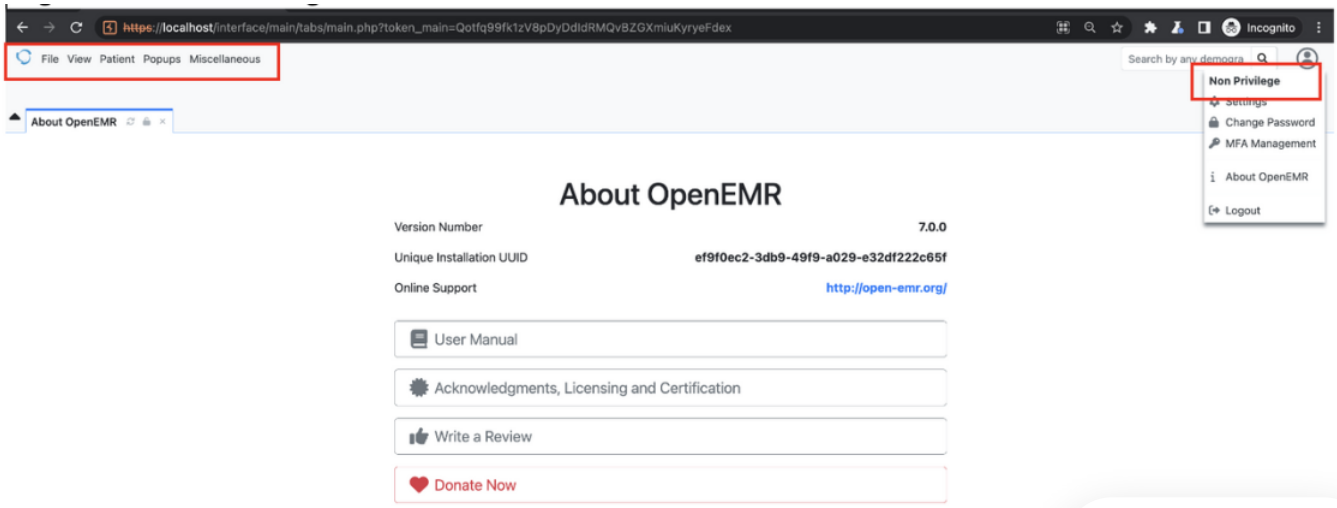
Login with Administrator privilege and add Amendments



Successfully add Amendments via normal step



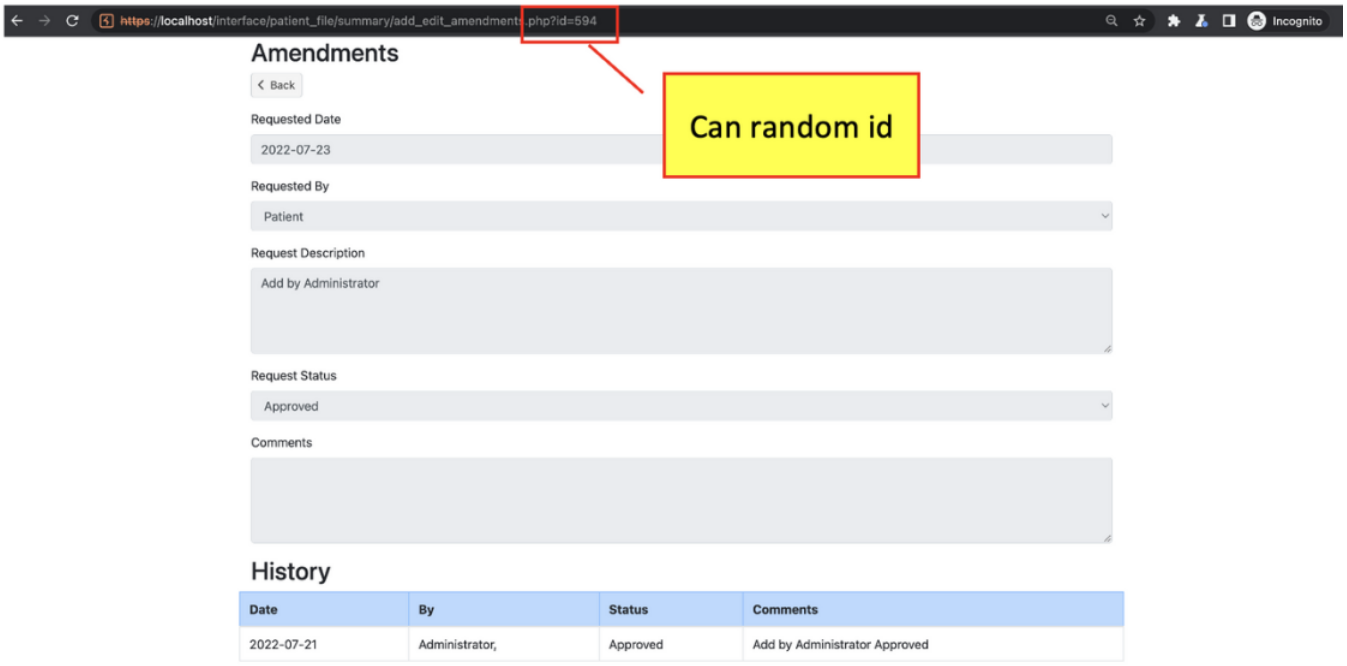
Login with non-Privilege user

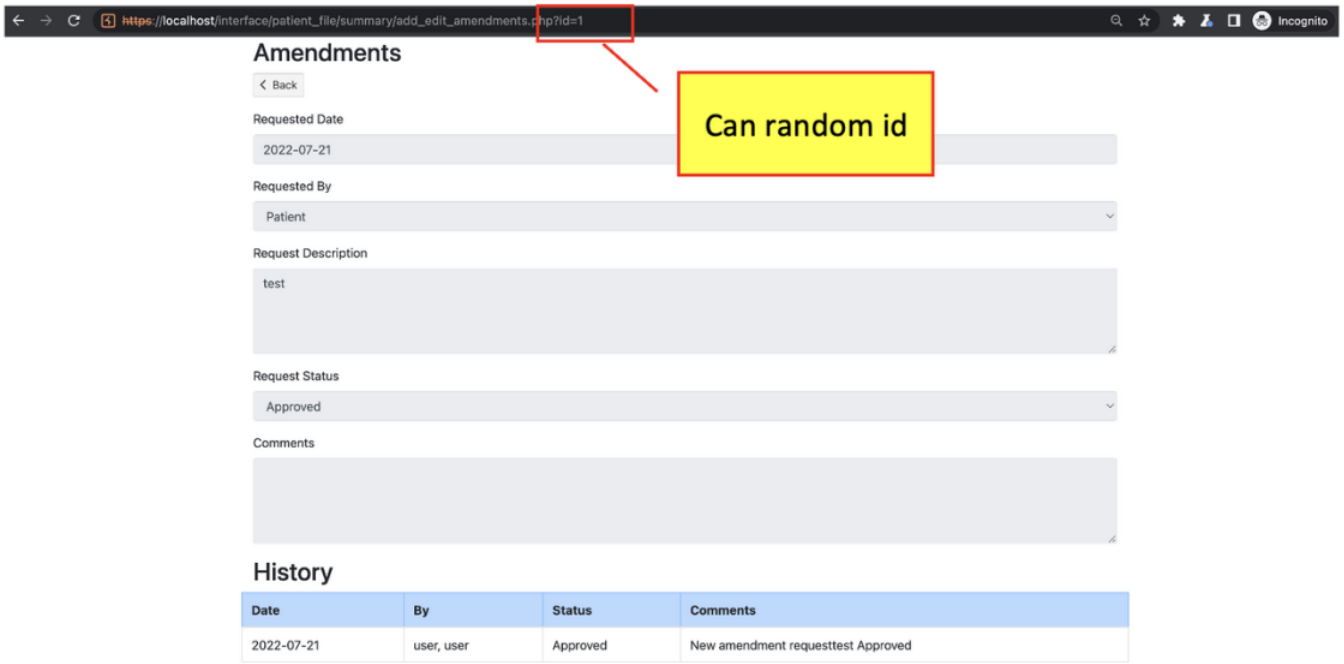


Chat with us

Direct access to URL and success to view “Amendments Page”

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





Insecure direct object reference (IDOR)

```
GET /interface/patient_file/summary/add_edit_amendments.php?id=1 HTTP/1.1
Host: localhost
Cookie: OpenEMR=Xojlqu%2CirL3ibLmkKZOwVyA8rILh1jmpvFR7XDVAPt
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
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: 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

```php
$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');
```

```
$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 hea

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!

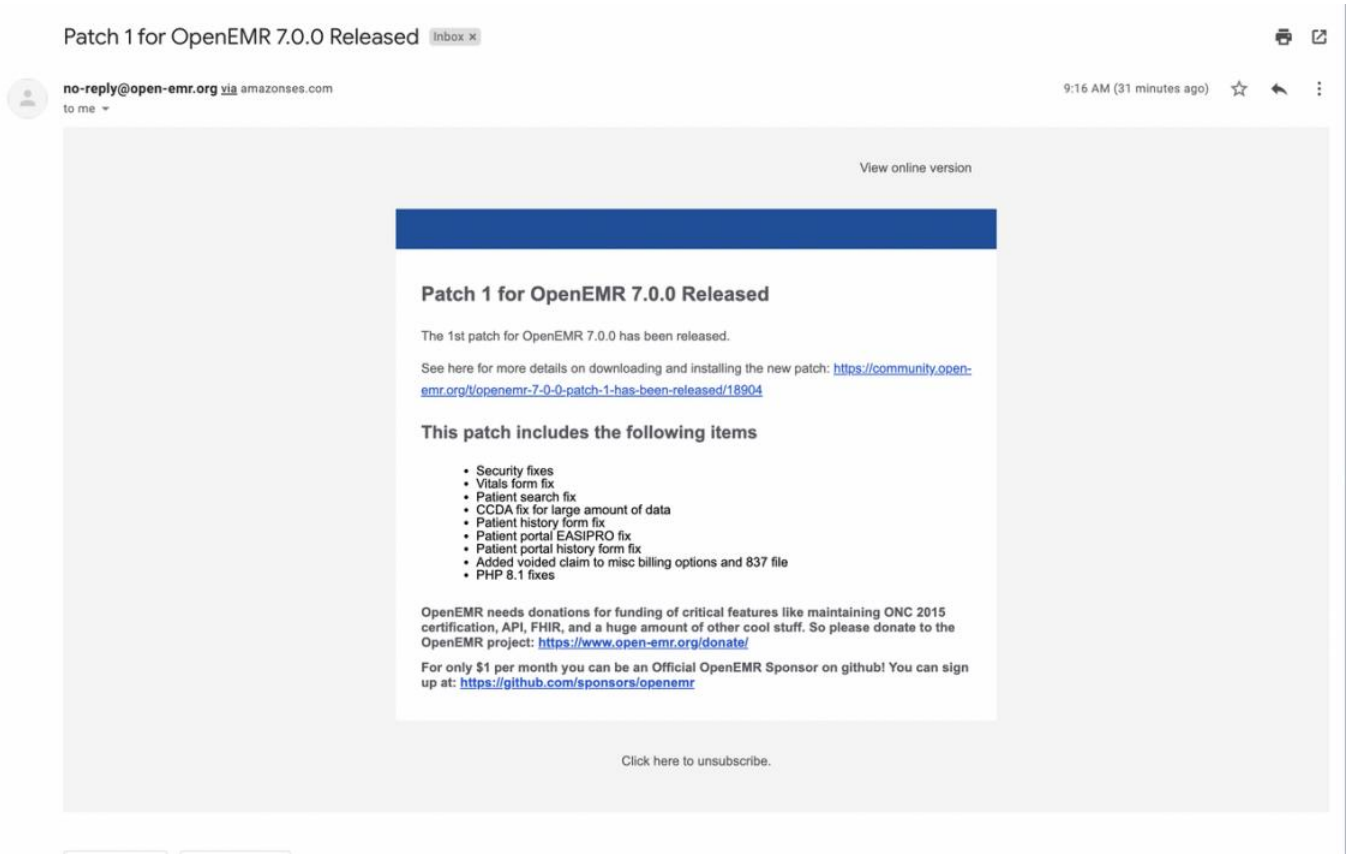
rata99 4 months ago Researcher

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?



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.

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