Non-Privilege User Can View Patient's Disclosures in openemr/openemr

0

Valid Reported on Mar 28th 2022

Vulnerability Type

Insecure Direct Object Reference

Affected URL

https://localhost/openemr-6.0.0/ /interface/patient_file/summary/record_disclosure.php?editlid=X

Method

GET

Parameter

editlid

Authentication Required?

Yes

Issue Summary

Non-privilege users (accounting, front office) can view patient's disclosures and have the capability to add, edit and delete the patient's disclosures. This function is not visible to non-privilege users upon viewing patient's dashboard but a non-privilege users can directly send a GET request to the vulnerable endpoint and view it.

Recommendation

The OpenEMR cookie must be checked against the document parameters se
request to https://localhost/openemr-

6.0.0/interface/patient_file/summary/record_disclosure.php to ensure that only cookies belonging to Admin or privileged users are allowed to view and use the features in forms administration.

Credits

Aden Yap Chuen Zhen (chuenzhen.yap2@baesystems.com)
Rizan, Sheikh (rizan.sheikhmohdfauzi@baesystems.com)
Ali Radzali (muhammadali.radzali@baesystems.com)

Issue Reproduction

Login to EMR using admin and we can see there is Disclosures in the patient's dashboard. Click on "Edit".

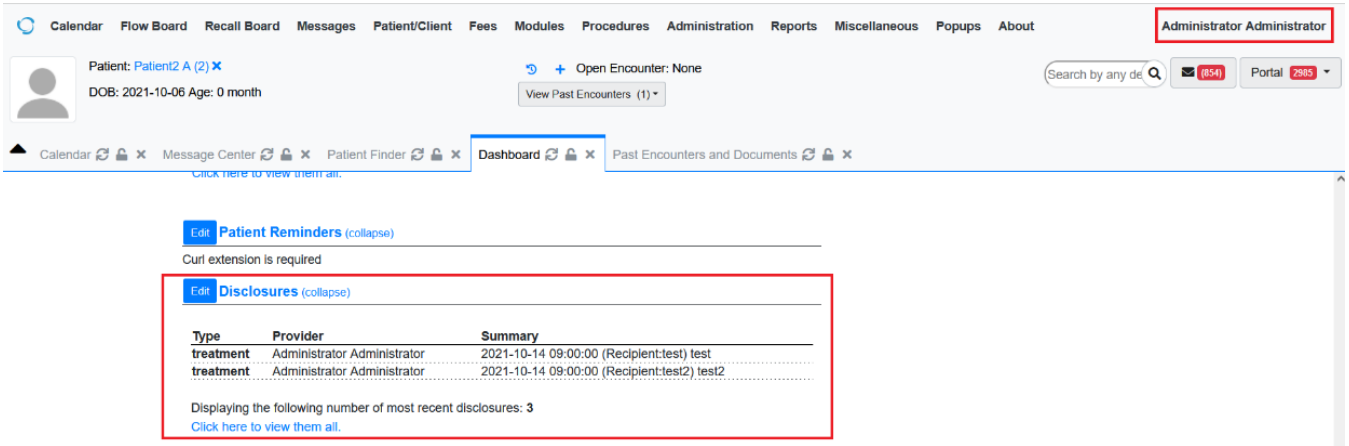


Figure 1: Login as Administrator and View Patient's Disclosures

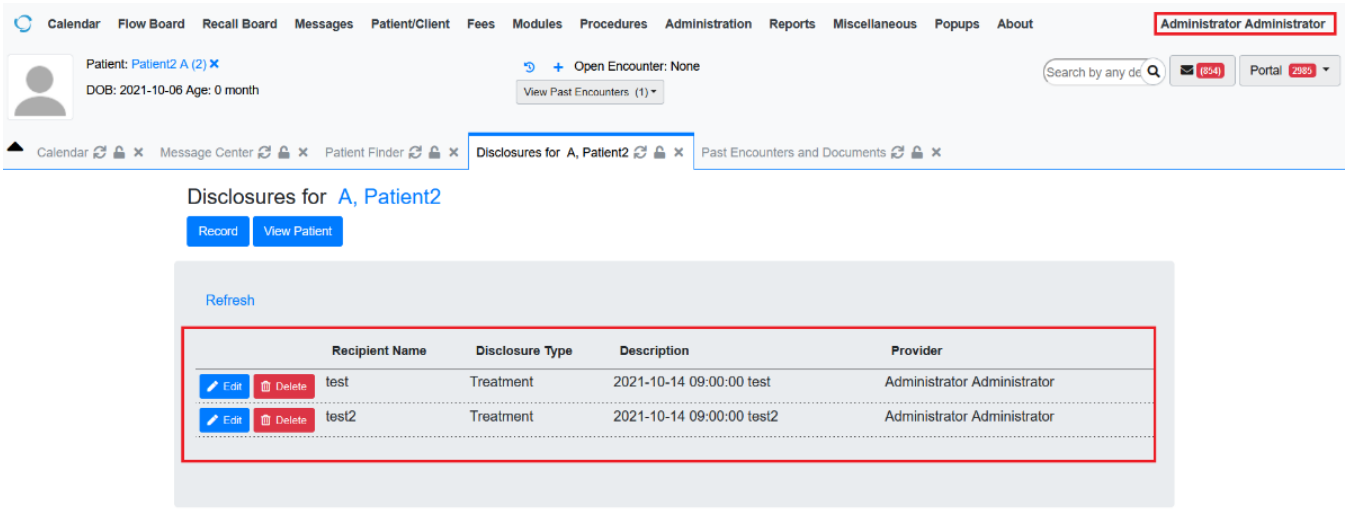


Figure 2: Admin View List of Disclosures

Now, using a non-admin account, Eg Accountant user should not be able to view the patient's disclosures.

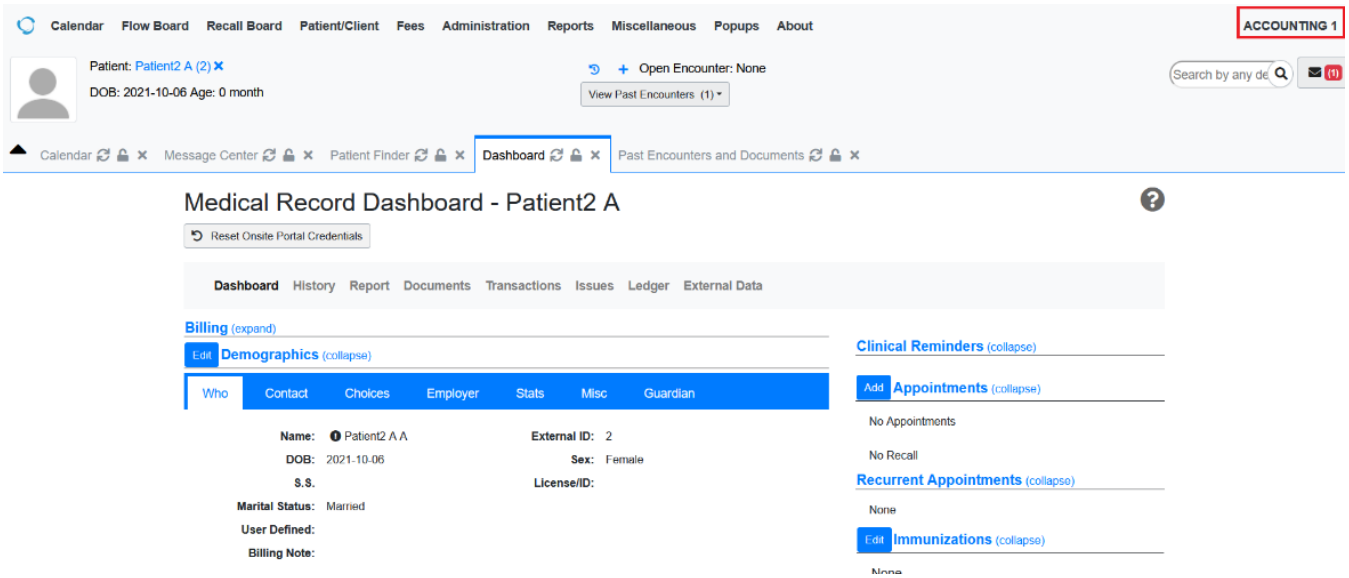


Figure 3: Non-privilege Account Cannot View Patient's Disclosures

Using Burp, we intercept the Admin request to edit the patient's disclosures and swap the "OpenEMR" cookie using an Accountant cookie and we are be able to view the patient's disclosures.

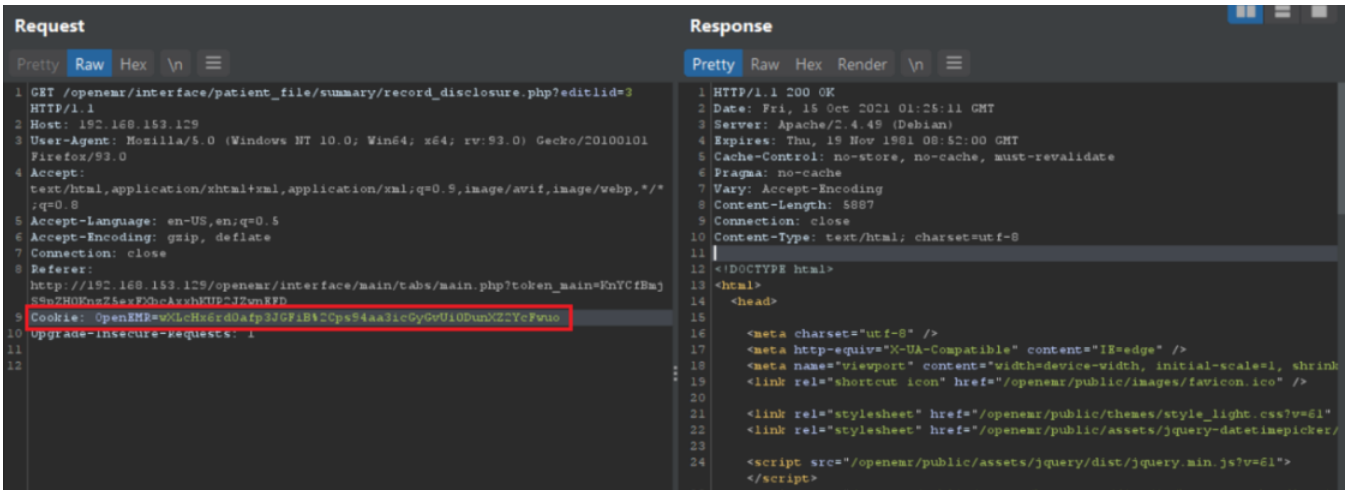


Figure 4: Burp Request Captured Using Accountant Cookie to View Forms Administration

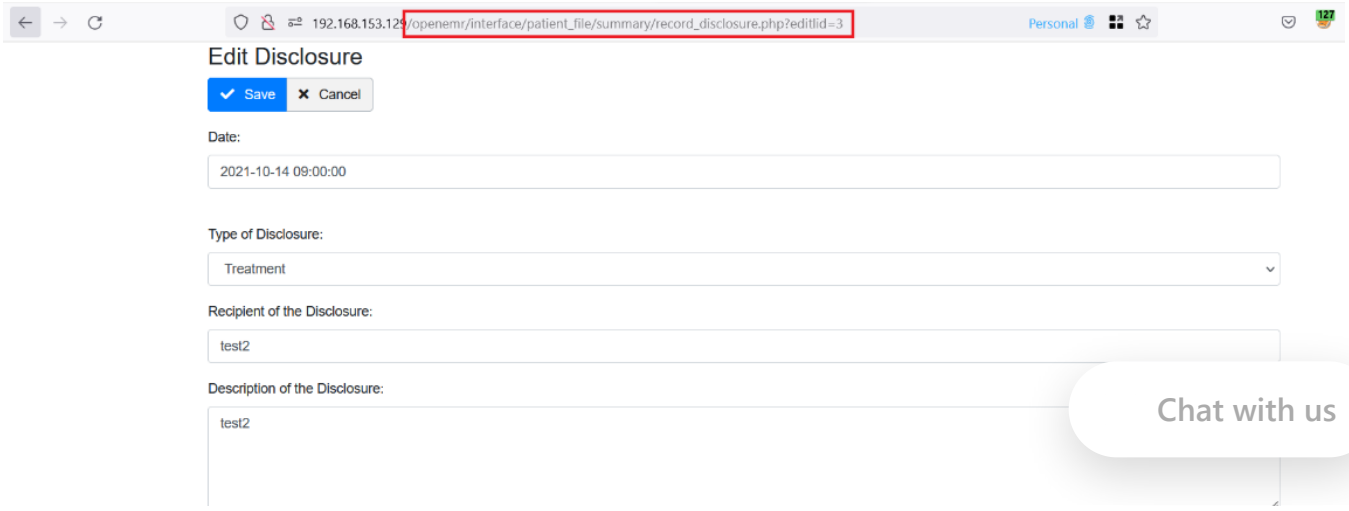


Figure 5: Non-privilege Account Can View Patient 's Disclosures
The Raw Request looks like:

```
GET /openemr/interface/patient_file/summary/record_disclosure.php?editlid=3
Host: 192.168.153.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/201001
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.153.129/openemr/interface/main/tabs/main.php?token_
Cookie: OpenEMR=wXLcHx6rd0afp3JGFiB%2Cps94aa3icGyGvUi0DunXZ2YcFwuo
Upgrade-Insecure-Requests: 1
```

The non-privilege users also have the capabilities to edit, add or delete any patient's disclosures.

References

- This bug was already reported and fix by Openemr project team. Kindly reach out to Brad in case of questions. Details of patch at: https://www.open-emr.org/wiki/index.php/OpenEMR_Patches

CVE
CVE-2022-1459
(Published)

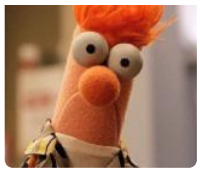
Vulnerability Type
CWE-1118: Insufficient Documentation of Error Handling Techniques

Severity
High (8.3)

Visibility
Public

Status
Fixed

Found by
r00t.pgp



@r00tpgp

amateur

This report was seen 600 times.

We are processing your report and will contact the **openemr** team within 24 hours. 8 months ago

r00t.pgp modified the report 8 months ago

We have contacted a member of the **openemr** team and are waiting to hear back 8 months ago

We have sent a follow up to the **openemr** team. We will try again in 7 days. 8 months ago

We have sent a second follow up to the **openemr** team. We will try again in 10 days. 8 months ago

We have sent a third and final follow up to the **openemr** team. This report is now considered stale. 7 months ago

A **openemr/openemr** maintainer validated this vulnerability 7 months ago

Currently working on a fix for this.

r00t.pgp has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

A **openemr/openemr** maintainer 7 months ago Maintainer

A preliminary fix has been placed in the development codebase: https://github.com/openemr/openemr/commit/fcccf0100ac4ae38342fa682682a5d83b42fcb95

This fix will be included in the next 6.1.0 patch 1 (6.1.0.1) . After we release 6.1.0 patch 1, then we will confirm the fix at that time.

We have sent a fix follow up to the **openemr** team. We will try again in 7 da

Chat with us

A **openemr/openemr** maintainer 7 months ago Maintainer

A openemr/openemr maintainer 7 months ago Maintainer

Patch 1 for 6.1.0 (6.1.0.1) has been released, so this fix is now official.

A openemr/openemr maintainer marked this as fixed in 6.1.0.1 with commit 8f8a97
7 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

r00t.pgp 7 months ago Researcher

Dear @admin kindly issue cve for this fix. Tq

Jamie Slome 7 months ago Admin

Sorted 👍

Sign in to join this conversation