huntr

Accounting User Can Download Patient Reports in openemr in openemr/openemr

0

✓ Valid Reported on Mar 11th 2022

Vulnerability Type

Insecure Direct Object Reference

Affected URL

https://localhost/openemr/interface/patient_file/report/custom_report.php

Affected Parameters

“Issue_7”

Authentication Required?

Yes

Issue Summary

Non-privilege users (accounting & front-office) can download patient reports containing medical reports and documents by sending a request to a vulnerable end-point. There is no Access Control enforced, therefore, any authenticated user of OpenEMR can download patient records by just tampering the “Issue_7” parameter to any valid number. By incrementing this value, an unauthorized user can download patient records.

Recommendation

Implement ACL check to ensure that only authorized users of OpenEMR system are able to download patient documents from the vulnerable end-point.

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 OpenEMR as Admin and capture the POST request to the following end-point: `https://localhost/openemr/interface/patient_file/report/custom_report.php`
In Burp, the HTTP POST request, cookie “OpenEMR” & parameter “issue_7” can be tampered.

```
Host: 192.168.0.141
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 155
Origin: http://192.168.0.141
Connection: close
Referer: http://192.168.0.141/openemr/interface/patient_file/report/patient
Cookie: OpenEMR=E6toaL3R-180fA2-MIw80a-G7PJPCapZxrTYIzY%2Cofj5CXEG

Upgrade-Insecure-Requests: 1

include_demographics=demographics&include_billing=billing&pdf=1&issue_8=%2
```

Replace the “OpenEMR” Cookie with Accountant Cookie and increment the “issue_7” parameter to any valid number eg “issue_7=/15/” to access patient documents.

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-2022-1177
(Published)

Vulnerability Type

CWE-1220: Insufficient Granularity of Access Control

Severity

Medium (6.5)

Visibility

Public

Status

Fixed

Found by

r00t.pgp

@r00tpgp

amateur ✓

This report was seen 683 times.

We are processing your report and will contact the **openemr** team within 24 hours. 9 months ago

r00t.pgp modified the report 9 months ago

r00t.pgp modified the report 9 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

A **openemr/openemr** maintainer validated this vulnerability 8 months ago

r00t.pgp has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **openemr/openemr** maintainer 8 months ago Maintainer

This has been fixed in master and rel-610 branches and will be in OpenEMR's next production release (6.1.0).

A **openemr/openemr** maintainer 8 months ago Maintainer

OpenEMR 6.1.0 was released, today which fixes this issue.

A **openemr/openemr** maintainer marked this as fixed in **6.1.0** with commit **a2e918** 8 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

r00t.pgp 8 months ago Researcher

Hi, Kindly issue a CVE for this vulnerability. Tq

r00t.pgp 8 months ago Researcher

Dear @admin i've already ping the maintainer, could you please follow up on the CVE creation? Tq

Dear @maintainer, could you kindly confirm that CVE can be created for this report? Tq

A **openemr/openemr** maintainer 8 months ago Maintainer

Hi, I consent to creation of CVE.

Jamie Slome 8 months ago Admin

Sorted 👍

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us