UI REDRESSING in openemr/openemr

0

✓ Valid   Reported on Jun 20th 2022

Description

Clickjacking is a portmanteau of two words ‘click’ and ‘hijacking’. It refers to hijacking user’s click for malicious intent. In it, an attacker embeds the vulnerable site in an transparent iframe in attacker’s own website and overlays it with objects such as button using CSS skills. This tricks users to perform unintended actions on vulnerable website, thinking they are doing those on attacker’s website. Clickjacking, also known as a "UI redress attack".

Proof of Concept

```
1. Go to this URL: http://web.clickjacker.io/test?url=http:%2F%2Fdemo.opene
2. Observe that the website is getting embeded in an Iframe.
3. Observe that the headers x-frame-options and content-security-policy fra
```

Impact

Users are tricked into performing all sorts of unintended actions are such as typing in the password, clicking on ‘Delete my account’ button, liking a post, deleting a post, commenting on a blog. In other words all the actions that a normal user can do on a legitimate website can be done using clickjacking.

References

- https://huntr.dev/bounties/a9ec1eef-98a0-4201-85ea-b111b3e86246/
- https://cwe.mitre.org/data/definitions/1021.html
- https://huntr.dev/bounties/47cc6621-2474-40f9-ab68-3cf62389a124/

CVE

CVE-2022-2734
(Published)

Vulnerability Type

CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Severity

Critical (10)

Registry

Other

Affected Version

<==1.2.15

Visibility

Public

Status

Fixed

Found by

tharunavula

@tharunavula

amateur

This report was seen 526 times.

We are processing your report and will contact the **openemr** team within 24 hours. 5 months ago

We have contacted a member of the **openemr** team and are waiting to hear back 5 months ago

We have sent a follow up to the **openemr** team. We will try again in 7 days. 5 months ago

We have sent a second follow up to the **openemr** team. We will try again in 10 days. 5 months ago

We have sent a third and final follow up to the **openemr** team. This report is now considered stale. 5 months ago

Brady Miller 4 months ago

Chat with us

Thanks for the report and looking into this. Am going to validate this (and working on a fix), however am unclear of the critical severity. What is the thought process on that and did you use however am unclear of the critical severity. What is the thought process on that and did you use a nvd calculator or some other objective measure for that?

tharunavula 4 months ago Researcher

Hi team,

This is the cwe https://cwe.mitre.org/data/definitions/1021.html

Regards,
Tharun

Brady Miller validated this vulnerability 4 months ago

tharunavula has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Brady Miller 4 months ago Maintainer

A preliminary fix has been posted in commit 203243467675e85b8b479c778e44ae1aac8bad55

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!

We have sent a fix follow up to the **openemr** team. We will try again in 7 days. 4 months ago

We have sent a second fix follow up to the **openemr** team. We will try again in 10 days. 4 months ago

Brady Miller marked this as fixed in **7.0.0.1** with commit **203243** 4 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Chat with us

Brady Miller 4 months ago Maintainer

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.

tharunavula 4 months ago Researcher

@admin can you assign CVE and public this.

Jamie Slome 4 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