Cross-site Scripting (XSS) - Stored in openemr/openemr

1

Valid Reported on May 10th 2022

Description

openemr / openemr is vulnerable to Cross-site Scripting (XSS) - Stored

Proof of Concept

```
// Poc
<script>alert(document.cookie)</script>
```

steps to reproduce:

```
1) login open emr patient portal https://demo.openemr.io/openemr/portal/inc

2) goto my profile in https://demo.openemr.io/openemr/portal/home.php

3)click on pending review.

4)add the payload in the first name /middle name  (<script>alert(document.c

5) click  submit changes

6) after that we get an with Error: Patient was successfully updated

7) on clicking  pending review  the xss wil be triggered
```

Impact

This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie

that user's account through the stolen cookie.

CVE

CVE-2022-2494
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.3)

Registry
Packagist

Affected Version
<=6.1.0

Visibility
Public

Status
Fixed

Found by

bugruto
@bugruto
unranked

This report was seen 571 times.

We are processing your report and will contact the **openemr** team within 24 hours. 7 months ago

We have contacted a member of the **openemr** team and are waiting to hear back 7 months ago

We have sent a follow up to the **openemr** team. We will try again in 7 days. 6 months ago

bugruto modified the report 6 months ago

We have sent a second follow up to the **openemr** team. We will try again in 10 days. 6 months ago

A **openemr/openemr** maintainer validated this vulnerability 6 months ago

bugruto has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

A **openemr/openemr** maintainer 6 months ago Maintainer

A preliminary fix for this has been placed in our development codebase at https://github.com/openemr/openemr/commit/152e551208e6de534ab194c87e9ffa4d56d294a8

The fix will officially be released in the next OpenEMR 6.1.0 patch 2 (6.1.0.2). After we release this patch, I will then mark this item as fixed (probably in about a month).

bugruto 6 months ago Researcher

@admin can cve be assigned to this issue?

Jamie Slome 6 months ago Admin

If the maintainer is happy to proceed, we can assign and publish a CVE for this report 👍

We have sent a fix follow up to the **openemr** team. We will try again in 7 days. 6 months ago

A **openemr/openemr** maintainer 6 months ago Maintainer

Hi, Lets not make this public until we release this fix in our next patch (6.1.0.2), which will likely be in several weeks. I will let you know when we release the patch and will then I will mark this item as officially fixed. thanks.

Jamie Slome 6 months ago Admin

Great, thanks for the update 👍

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

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

stale. 6 months ago

A openemr/openemr maintainer marked this as fixed in 7.0.0 with commit 152e55 4 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

A openemr/openemr maintainer 4 months ago Maintainer

This was fixed in OpenEMR 7.0.0, which was just released.

A openemr/openemr maintainer 4 months ago Maintainer

also, ok to assign cve

Jamie Slome 4 months ago Admin

Sorted 👍

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us