Cross-site Scripting - Reflected in openemr/openemr

0

Valid Reported on Aug 2nd 2022

Description

The `pricelevel` parameter in openemr is vulnerable to reflected XSS

Proof of Concept

Open the web browser to access the website
Access the url:
`http://openemr.vn/interface/forms/fee_sheet/review/fee_sheet_options_ajax.php?pricelevel=%3Cimg%20src%3da%20onerror%3dalert(document.cookie)%3E` --> Alert box will pop up

Image

https://drive.google.com/file/d/1zLXx2NGmUXZEvgk-dlUeJ-3Sq4cLPIMX/view

Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user.

References

- owasp-xss

CVE
CVE-2022-2733
(Published)

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

Severity

Critical (9.6)

Registry
Other

Affected Version
7.0.0

Visibility
Public

Status
Fixed

Found by

Phạm Đăng Chính
@ch1nhpd
amateur

This report was seen 677 times.

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

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

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

Brady Miller validated this vulnerability 4 months ago

Thanks for the report. A preliminary fix has been posted in commit 59458bc15ab0cb556c521de9d5187167d6f88945

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 1-3 weeks. After I do that, then will be ok to make CVE # and make it public.

Thanks!

Phạm Đăng Chính has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Phạm Đăng Chính 4 months ago Researcher

Thank Brady, please let me know once the patch is released.

Brady Miller marked this as fixed in 7.0.0.1 with commit 59458b 4 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

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.

Phạm Đăng Chính 4 months ago Researcher

@admin can we assign a CVE to this vulnerability?

Jamie Slome 4 months ago Admin

Sorted 👍

Sign in to join this conversation