# Stored Cross Site Scripting in openemr/openemr

0

Valid Reported on Mar 11th 2022

## Vulnerability Type

Stored Cross Site-Scripting (XSS)

## Affected URL

https://localhost/openemr-6.0.0/ /controller.php?practice_settings&document_category&action=add_node&parent_id=XX

## Affected Parameter

“name”
Method POST

## Authentication Required?

Yes

## Issue Summary

A stored XSS vulnerability found in ” /controller.php?practice_settings&document_category&action=add_node&parent_id=XX” that allows authenticated user to inject arbitrary web script in one parameter (name). The XSS payload will be fired in the Patient’s documents list of the affected category name if any authenticated user views it.

## Credits

Aden Yap Chuen Zhen (chuenzhen.yap2@baesystems.com) Rizan, Sheikh (rizan.sheikhmohdfauzi@baesystems.com) Ali Radzali (muhammadali.radzali@baesystems.com)



## Recommendation

Ensure to HTML encode before inserting any untrusted data into HTML element content. Ensure all inputs entered by user should be sanitized and validated before processing and

storage. Inputs should be filtered by the application, for example removing special characters such as < and > as well as special words such as script.

### Issue Reproduction

Login as any user that has privileges to add/edit document categories. Accounting should be able to add document categories. (Administration > Practice > Practice Settings)
Click on Add/Edit in any document categories. In this example, we going to add new sub-category in Patient category with our XSS payload. Insert the payload in Category Name and Click on save category once done.

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

The XSS will be fired in the patient's documents on the sub-category that we have created before. For example, an Admin can go to any patient's documents and click on any documents with the same parent category (Patient) of the new sub-category that we created (XSS Payload). The cookies of the admin will be pop out in alert box when click on any document (2021-10-10 payload.txt-21)

## 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-2022-1178
(Published)

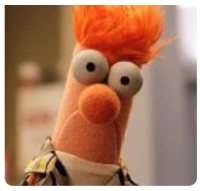
Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by
r00t-pgp



r00t.pgp

@r00tpgp

amateur

This report was seen 743 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

**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 latest patch (patch 4) for 6.0.0, which can be found at https://www.open-emr.org/wiki/index.php/OpenEMR_Patches

A **openemr/openemr** maintainer marked this as fixed in **6.0.0.4** with commit **347ad6** 8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Chat with us

r00t.pgp 8 months ago Researcher

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

Also note that this fix is in the recently released 6.1.0 version.

I consent to creation of CVE.

Jamie Slome 8 months ago Admin

Sorted 👍

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us