Reflected Cross Site Scripting in openemr/openemr

0

Valid Reported on Mar 21st 2022

Vulnerability Type

Reflected Cross Site-Scripting (XSS)

Affected URL

https://localhost/openemr-6.0.0/interface/main/calendar/index.php

Affected Parameters

“newname”

Authentication Required?

Yes

Issue Summary

A reflected XSS vulnerability found in “/interface/main/calendar/index.php” that allows Admin user to inject arbitrary web script in one parameter (newname). The XSS payload will be reflected in the Confirmation page after the user click on Save for the new categories in Calendar.

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.

Credits

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

(muhammadali.radzali@baesystems.com)

Issue Reproduction

Login as an Admin. Click on Administration > Clinic > Calendar and click on Categories after that.

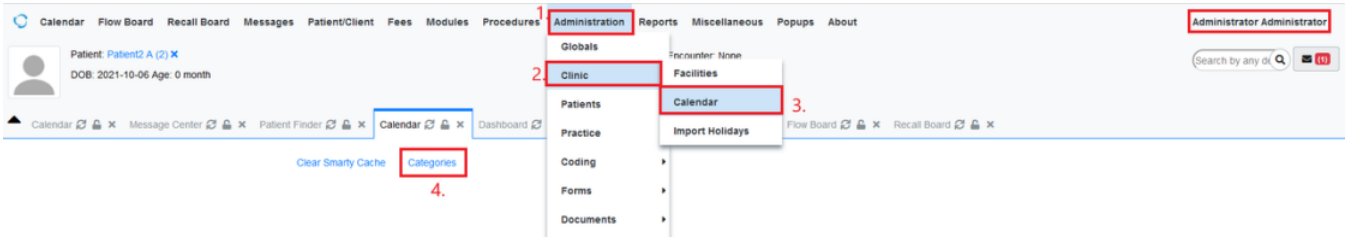

Figure 1: Login as Admin and Go to Calendar (Under Administration)

In New Category, insert this payload in the Name input box. Once done, click on Save.

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

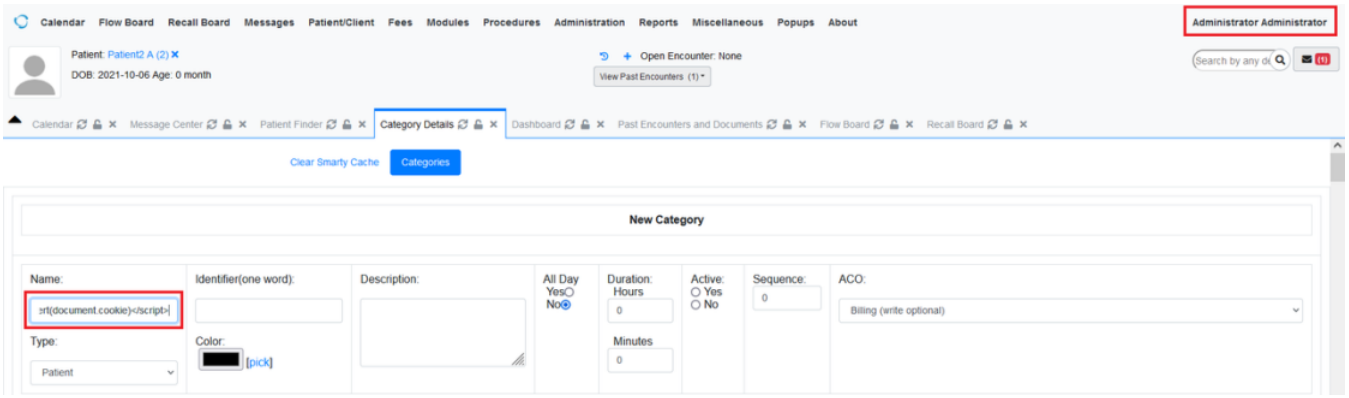

Figure 2: Insert Payload in Name

The XSS will be reflected on the confirmation page with the user cookies.

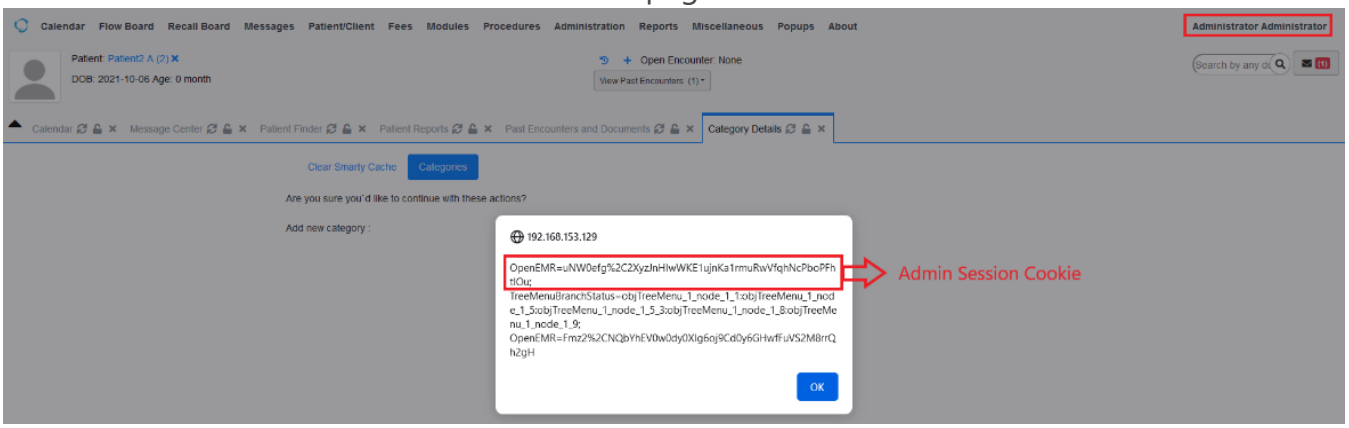

Figure 3: Reflected XSS in Confirmation Page

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-2022-1180
(Published)

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

Severity
Medium (4.6)

Visibility
Public

Status
Fixed

Found by

r00t.pgp
@r00tpgp
amateur

This report was seen 657 times.

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

r00t.pgp modified the report 8 months ago

r00t.pgp modified the report 8 months ago

We have contacted a member of the **openemr** team and are waiting to hear back 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 OpenEMR 6.0.0.4

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 ✖

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 also 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