huntr

Reflected XSS in collectiveaccess/providence

0

✓ Valid Reported on Apr 29th 2022

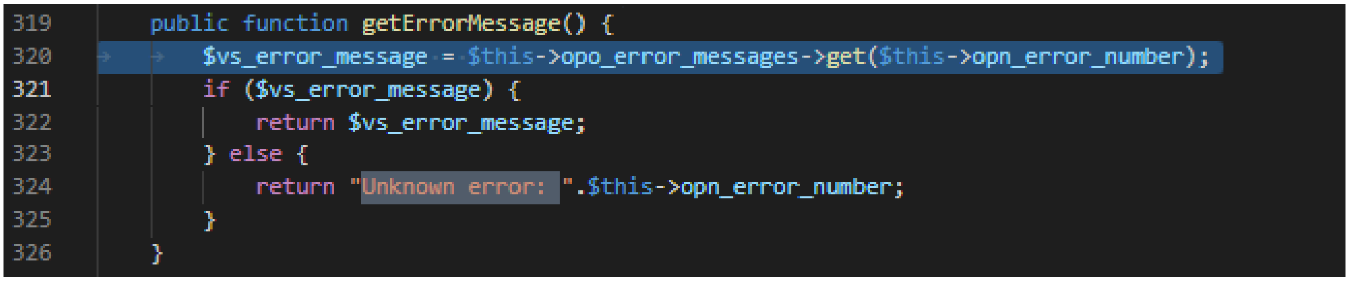
Description

Hello , i found an authenticated reflected xss via path fragment this was exploitable through trusting user input in url path fragement , please note : if you wrote a different payload you need to URL Encode the payload twice

Proof of Concept

```
Enter this url : https://demo.collectiveaccess.org/index.php/system/Error/S
```

Picture:



```
    public function getErrorMessage() {
        $vs_error_message = $this->opo_error_messages->get($this->opn_error_number);
        if ($vs_error_message) {
            return $vs_error_message;
        } else {
            return "Unknown error: ".$this->opn_error_number;
        }
    }
```

Kind Regards,
Rawi (@0xRaw)

Impact

Steal User Cookies or redirect user to malicious sites

References

- XSS In Path

CVE
CVE-2022-1825
(Published)

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

Severity
Medium (5.5)

Registry
Other

Affected Version
1.8

Visibility
Public

Status
Fixed

Found by

0xRaw
@0xraw
legend

This report was seen 511 times.

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

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

CollectiveAccess 7 months ago Maintainer

Not sure how we missing this one :-/ Thank you.

CollectiveAccess validated this vulnerability 7 months ago

0xRaw has been awarded the disclosure bounty ✓

Chat with us

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

CollectiveAccess marked this as fixed in 1.8 with commit 49de45 7 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

0xRaw 7 months ago Researcher

Hello thanks for the quick fix,
Can i have a CVE for this finding ?

Kind Regrads,
Rawi.

Jamie Slome 7 months ago Admin

Sure, we can arrange a CVE - @maintainer, are you happy to proceed with a CVE for this finding?

0xRaw 6 months ago Researcher

hey , @maintainer just dropping by to make sure that if you are ok with arranging a CVE for this finding.

Kind Regards,
Rawi.

Jamie Slome 6 months ago Admin

Sorted 👍

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us