4

Cross Site Scripting and Open Redirect in affiliate-preview.php file

Share:

TIMELINE

keyurvala submitted a report to Revive Adserver. Mar 14th (3 years ago)

Summary:

Stored XSS can be submitted on the Website using Default Manager, and anyone who will check the report the XSS and Open Redirect will trigger.

Description:

Stored XSS, also known as persistent XSS, is the more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.

Steps To Reproduce:

1. Login with valid credentials of the user.
2. Go to inventory > Website > Website Properties
3. Fill the form and Enter Website URL as "http://Test"><img src=x onclick=window.location="http://google.com">". Click Save Changes.
4. Login with an administrator account.
5. Open http://localhost/hackerone/www/admin/affiliate-preview.php?codetype=invocationTags%3AoxInvocationTags%3Aspc&block=0&blockcampaign=0&target=&source=&withtext=0&charset=&noscript=1&ssl=0&comments=0&affiliateid=1&submitbutton=Generate
6. Click on Header Script Banner there is image click on that it will execute xss or open redirect.

Impact

Impact

Users can redirect the admin user or any normal user to any other website evil.com.

1 attachment:
F748011: XSS_on_Revive.mp4

mbeccati Revive Adserver staff changed the status to ○ **Triaged**. Mar 15th (3 years ago)

Thanks for your report. We will fix the vulnerability in the next release. We have no date planned just yet, we will keep you informed.

About the disclosure, how would you prefer to be mentioned (name, h1 username)?

keyurvala posted a comment. Mar 15th (3 years ago)

Hi Mbeccati,

Thanks for your response. You can mention my name as below detail.
(Name: Keyur Vala, Username: keyurvala).

Regards,
Keyur

erikgeurts Revive Adserver staff updated the severity from Medium to Low. Mar 16th (3 years ago)

mbeccati Revive Adserver staff closed the report and changed the status to ● **Resolved**. May 11th (3 years ago)

Hi Keyur,

we're sorry for the delay. The attached patch will fix the vulnerability.

We still don't have any timeline for a release that will include the low priority fix.

1 attachment:
F823393: h1-819362.diff

keyurvala posted a comment. May 11th (3 years ago)

Hi Mbeccati,

Thanks for your update and feedback.

Regards,
Keyur

mbeccati Revive Adserver staff requested to disclose this report. Jan 19th (2 years ago)

Thanks again for the report. Revive Adserver v5.1.0 has been just released.
The Security Advisory https://www.revive-adserver.com/security/revive-sa-2021-001/ has been published and a CVE-ID will be requested.

keyurvala posted a comment. Jan 19th (2 years ago)

Thanks, @mbeccati for the Update, and Thanks for the CVE-ID.

mbeccati Revive Adserver staff disclosed this report. Jan 20th (2 years ago)