12 Reflected XSS on /admin/stats.php

Share:

TIMELINE

solov9ev submitted a report to Revive Adserver. May 7th (2 years ago)

Hi, Security Team!

Linked to the reports:

- https://hackerone.com/reports/1083376
- https://hackerone.com/reports/1097217

In the past reports, we have corrected Reflected XSS. But recently it turned out that with the parameter `breakdown = affiliates`, this vulnerability still works. (Fixed when parameter `breakdown = history`).

- Go to `http://revive-adserver.loc/admin/stats.php?entity=global&breakdown=affiliates&statsBreakdown=day%27%20onclick=alert(document.domain)%20accesskey=X%20`
- For the payload to be executed, the user needs to press the access key combination for the hidden input field (for Firefox, Alt+Shift+X, see this for other browsers).

Image F1292520: 1.png 57.70 KiB

Zoom in Zoom out Copy Download

Image F1292519: 2.png 38.14 KiB

Zoom in Zoom out Copy Download

Impact

With this vulnerability, an attacker can for example steal users cookies or redirect users on malicious website.

2 attachments:
F1292519: 2.png
F1292520: 1.png

mbeccati Revive Adserver staff posted a comment. May 7th (2 years ago)

Hi Alexey,

thanks for your report.

I wish this had been caught when reviewing previous fixes. We will soon investigate and probably mark this as duplicate of the existing report(s).

mbeccati Revive Adserver staff changed the status to o **Triaged**. May 13th (2 years ago)

The issue is confirmed. We're evaluating the impact and discussing how to approach it. Thanks again.

mbeccati Revive Adserver staff posted a comment. May 28th (2 years ago)

The attached diff should fix the issue and make sure all the stats use the common methods for escaping the input. A release is tentatively scheduled for thursday June 3rd.

1 attachment:
F1318900: h1-1187820.diff

solov9ev posted a comment. Jun 2nd (2 years ago)

It looks good!

mbeccati Revive Adserver staff closed the report and changed the status to • **Resolved**. Jun 3rd (2 years ago)

mbeccati Revive Adserver staff requested to disclose this report. Jun 3rd (2 years ago)

erikgeurts Revive Adserver staff disclosed this report. Jun 3rd (2 years ago)