

8 Reflected XSS on /admin/stats.php

Share:     

TIMELINE

 **solov9ev** submitted a report to [Revive Adserver](#). Feb 6th (2 years ago)
Linked to the report <https://hackerone.com/reports/1083376>
I found a reflected XSS attack on `/admin/stats.php`.

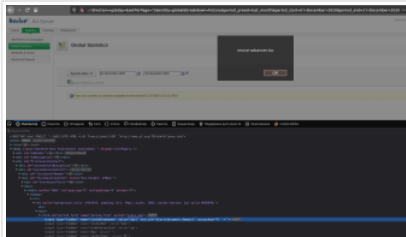
Revive-Adserver version is `revive-adserver-5.1.1`.

This time I found the parameter `statsBreakdown`

- Go to `http://revive-adserver.loc/admin/stats.php?statsBreakdown=day%27%20onClick=alert(document.domain)%20&accesskey=X%20&listorder=key&orderdirection=up&day=&setPerPage=15&entity=global&breakdown=history&period_preset=last_month&period_start=01+December+2020&period_end=31+December+2020`
- 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 F1186275: [2021-02-06_17-59-59.png](#) 171.57 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.


1 attachment:

F1186275: [2021-02-06_17-59-59.png](#)

 **mbeccati** [Revive Adserver staff](#) posted a comment. Feb 6th (2 years ago)
Thanks for your report. We'll verify this one in the next few days. May I ask you to please check other parameters too and eventually add them below?

 **solov9ev** posted a comment. Feb 6th (2 years ago)
Yes, I checked the rest of the parameters, I didn't find any more vulnerabilities. Thanks.

 **mbeccati** [Revive Adserver staff](#) changed the status to **Triaged**. Feb 8th (2 years ago)
Confirmed, thanks again.

 **mbeccati** [Revive Adserver staff](#) closed the report and changed the status to **Resolved**. Feb 9th (2 years ago)
Hi Alexey, you will find the fix for the XSS attached for verification. We are planning to schedule a release on Feb 23rd. As usual, we'll be requesting CVE-IDs, disclosing the report and mention you on the security advisory.

I understand it might be a tricky question, but it'd be great to know if you plan to do some other security research on Revive Adserver anytime soon, just to avoid having a new report open shortly after a release. In case, we might postpone the release to March 2nd.

Thanks again.

1 attachment:

F1189083: [h1-1097217.diff](#)

 **solov9ev** posted a comment. Feb 9th (2 years ago)
Hey!


For several evenings I looked at the system for vulnerabilities and so far I have not found anything else. I think that in a month or two I will do the research again.

 **solov9ev** requested to disclose this report. Feb 9th (2 years ago)
Will we reveal when the time is right?
Best regards, Alexey

 **mbeccati** [Revive Adserver staff](#) posted a comment. Feb 9th (2 years ago)
Yep, we will, thanks again!


 **mbeccati** [Revive Adserver staff](#) cancelled the request to disclose this report. Mar 4th (2 years ago)

we will do the disclosure along with the release as planned, but for now we have to concern to avoid automatic disclosure before the release date.

 solov9ev posted a comment.

All is well, safety is paramount! I will request disclosure on March 16th. Okay?

Mar 4th (2 years ago)

 mbeccati Revive Adserver staff posted a comment.

suppose you can request disclosure again to reset the 30 days timer and we'll accept as soon as we release, or we "force" disclosure on the release day.

Mar 4th (2 years ago)

 mbeccati Revive Adserver staff updated CVE reference to [CVE-2021-22888](#).

Mar 16th (2 years ago)

 mbeccati Revive Adserver staff updated CVE reference to [CVE-2021-22889](#).

Mar 16th (2 years ago)

 mbeccati Revive Adserver staff requested to disclose this report.

Mar 16th (2 years ago)

 erikgeurts Revive Adserver staff disclosed this report.

Mar 16th (2 years ago)