24

Reflected XSS on /admin/stats.php

Share:

TIMELINE

solov9ev submitted a report to Revive Adserver. Jan 21st (2 years ago)

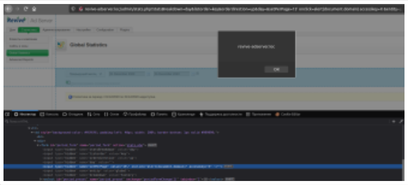
I found a reflected XSS attack on `/admin/stats.php`.

Revive-Adserver version is `revive-adserver-5.1.0`.

- Go to `http://revive-adserver.loc/admin/stats.php?statsBreakdown=day&listorder=key&orderdirection=up&day=&setPerPage=15%27%20onclick=alert(document.domain)%20accesskey=X%20&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 F1166756: ________________2021-01-21_20-31-11.png 130.98 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:
F1166756: ______________2021-01-21_20-31-11.png

mbeccati Revive Adserver staff posted a comment. Jan 21st (2 years ago)

Thanks for your report. We will verify shortly and get back to you.

mbeccati Revive Adserver staff changed the status to ○ **Triaged**. Jan 22nd (2 years ago)

Thanks again. Vulnerability is confirmed, although the suggested exploit payload requires some pretty unlikely key combination to be triggered. Nonetheless worth fixing.

We will soon provide a patch with the fix for you to test. It is likely that we will release 5.1.1 next week, and this fix will be part of it.

solov9ev posted a comment. Jan 22nd (2 years ago)

Thank you!

mbeccati Revive Adserver staff closed the report and changed the status to 0 **Resolved**. Jan 23rd (2 years ago)

I've attached the patch file that should fix this and other potentially dangerous usages of the setPerPage parameter.

Resolving the issue, thanks again.

1 attachment:
F1168843: h1-1083376.diff

mbeccati Revive Adserver staff requested to disclose this report. Jan 23rd (2 years ago)

mbeccati Revive Adserver staff cancelled the request to disclose this report. Jan 23rd (2 years ago)

Sorry, I wrongly requested disclosure now. I'll cancel it, would you mind requesting it so we can accept at release?

solov9ev requested to disclose this report. Jan 23rd (2 years ago)

Okay! Thank you!

mbeccati Revive Adserver staff agreed to disclose this report. Jan 26th (2 years ago)

Revive Adserver v5.1.1 has been released and the SA published: https://www.revive-adserver.com/security/revive-sa-2021-002/

This report has been disclosed. Jan 26th (2 years ago)