20 Reflected XSS on /admin/userlog-index.php

Share:

TIMELINE

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

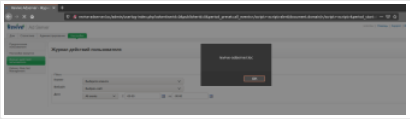
I found a reflected XSS attack on `/admin/userlog-index.php`.

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

- Go to `http://revive-adserver.loc/admin/userlog-index.php?advertiserId=0&publisherId=0&period_preset=all_events%3C/script%3E%3Cscript%3Ealert(document.domain)%3C/script%3E%3Cscript%3E&period_start=&period_end=&setPerPage=10`
- Malicious code executed

Image F1166698: _____2021-01-21_19-31-55.png 63.07 KiB

Zoom in Zoom out Copy Download



Rendered response from server:

Image F1166701: _____2021-01-21_19-32-40.png 98.73 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:
F1166698: _____2021-01-21_19-31-55.png
F1166701: _____2021-01-21_19-32-40.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. 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.

How would you like to be referred to (username, real name) when publishing the security advisory?

mbeccati Revive Adserver staff closed the report and changed the status to **Resolved**. Jan 22nd (2 years ago)

I'm attaching a patch file that should fix the vulnerability and thus resolve the issue. CVE Request and public disclosure is planned for next week.

1 attachment:
F1168119: h1-1083231.diff

solov9ev requested to disclose this report. Jan 22nd (2 years ago)

Refer to me as Alexey Solovyev (solov9ev). Thank you!

Shall we disclose it in a week?

mbeccati Revive Adserver staff posted a comment. Jan 22nd (2 years ago)

A release is tentatively scheduled some time next week in order to fix critical bugs in 5.1.0. As of now, we don't have a date set yet.

As part of the release process we will publish our security advisory, request a CVE-ID and accept the disclosure here on h1.

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)