

1

Open redirect in switch account functionality

Share:

State Resolved (Closed)Disclosed **April 23, 2019 3:05pm +0200**Reported To [Revive Adserver](#)Asset <https://github.com/revive-adserver/revive...>
(Source code)CVE ID [CVE-2019-5433](#)

Weakness Open Redirect

Severity Low (3.1)

Participants

Visibility Disclosed (Full)[Collapse](#)

SUMMARY BY REVIVE ADSEVER



A user having access to the UI of a Revive Adserver instance could be tricked into clicking on a specifically crafted admin `account-switch.php` URL that would eventually lead them to another (unsafe) domain, potentially used for stealing credentials or other phishing attacks.

TIMELINE · EXPORT



[sumni](#) submitted a report to [Revive Adserver](#).

Aug 5th (12 months ago)

To reproduce this vulnerability:

1. You have to be logged in user
2. Enter address: `http://<your_local_installation>/www/admin/account-switch.php?return_url=http://127.0.0.1:12345/test`

This is due to unrestricted redirection url passed in in the `return_url` parameter. I would recommend to use some kind of whitelisting or a check if you are redirecting to the same domain you were before.

Impact

This kind of open redirect vulnerabilities are used in fishing campaigns. I assume that in this case a support request containing a crafted url would have a higher chances of success. For additional malicious url obfuscation you can:

- add some unused parameters that would suggest identifiers of campaigns, other accounts and other revive specific information
- register a domain name similar to the attacked one



[mbeccati](#) posted a comment.

Aug 6th (12 months ago)

Thanks for your report. We will look into it shortly.



[mbeccati](#) changed the status to Triaged.

Aug 7th (12 months ago)

The issue has been confirmed. We will provide a patch so that you can verify if the issue has been fixed. Since this is a very low risk issue, it will be included in the next release, currently planned for Sept-Oct.



[mbeccati](#) posted a comment.

Mar 11th (5 months ago)

We're sorry for the delay: our plans have changed and we're starting to prepare for a new release now. You will find a patch attached, that should fix the issue.

The `return_url` parameter is not accepted anymore and the Referer header is now sanitised before being used.

1 attachment:






F439475: [h1-390663.diff](#)



[mbeccati](#) closed the report and changed the status to Resolved.

Mar 19th (4 months ago)

The fix will be included in the forthcoming 4.2.0 release.

	mbeccati requested to disclose this report.	Mar 19th (4 months ago)
	mbeccati cancelled the request to disclose this report. Will disclose later.	Apr 11th (4 months ago)
	mbeccati requested to disclose this report. Releasing 4.2.0 now.	Apr 23rd (3 months ago)
	erikgeurts disclosed this report. See https://www.revive-adserver.com/security/revive-sa-2019-001/ 	Apr 23rd (3 months ago)