Talos Vulnerability Report

TALOS-2022-1537

WWBN AVideo charts tab selection cross-site scripting (XSS) vulnerability

AUGUST 16, 2022

CVE NUMBER

CVE-2022-26842

SUMMARY

A reflected cross-site scripting (xss) vulnerability exists in the charts tab selection functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

WWBN AVideo 11.6
WWBN AVideo dev master commit 3f7c0364

PRODUCT URLS

AVideo - https://github.com/WWBN/AVideo

CVSSV3 SCORE

9.6 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CWE

CWE-79 - Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)

DETAILS

AVideo is a web application, mostly written in PHP, that can be used to create an audio/video sharing website. It allows users to import videos from various sources, encode and share them in various ways. Users can sign up to the website in order to share videos, while viewers have anonymous access to the publicly-available contents. The platform provides plugins for features like live streaming, skins, YouTube uploads and more.

The PHP file `view/charts.php` is a dashboard that shows several charts about the videos published for the current logged-in user.

```
...
<body class="<?php echo $global['bodyClass']; ?>">
    <?php
    include $global['systemRootPath'] . 'view/include/navbar.php';
    include $global['systemRootPath'] . 'view/charts_body.php';          // [1]
    include_once $global['systemRootPath'] . 'view/include/footer.php';
    ?>
</body>
...
```

`charts.php` includes `view/charts_body.php` [1] which shows the body of the page:

```
...
<ul class="nav nav-tabs">        // [2]
    <li class="active"><a data-toggle="tab" href="#dashboard"><i class="fas fa-
tachometer-alt"></i> <?php echo __("Dashboard"); ?></a></li>
    <li><a data-toggle="tab" id="viewmyVideosReport" href="#myVideosReport"><i
class="fas fa-play-circle"></i> <?php echo __("My Videos"); ?></a></li>
    <li><a data-toggle="tab" id="viewperchannel" href="#menu1"><i class="fas fa-
play-circle"></i> <i class="fa fa-eye"></i> <?php echo __("Video views - per
Channel"); ?></a></li>
    <li><a data-toggle="tab" id="commentthumbs" href="#menu2"><i class="fa fa-
comments"></i> <i class="fa fa-thumbs-up"></i> <?php echo __("Comment thumbs up -
per Person"); ?></a></li>
    <li><a data-toggle="tab" id="videothumbs" href="#menu3"><i class="fas fa-play-
circle"></i> <i class="fa fa-thumbs-up"></i> <?php echo __("Video thumbs up - per
Channel"); ?></a></li>
    <?php echo AVideoPlugin::getChartTabs(); ?>
</ul>
...
<script type="text/javascript">
    $(document).ready(function () {     // [3]
<?php if (!empty($_GET['jump'])) { ?>
            $('#<?php echo $_GET['jump']; ?>').click();
<?php } ?>
    });
</script>
```

The page has a navigation bar shown as tabs [2], and it also has a Javascript function that is used to select a specific tab at page load, depending on the value of the `jump` GET parameter. It’s supposed to be used with a request like `https://192.168.200/view/charts.php?jump=commentthumbs` for selecting the comments tab.

The `jump` parameter is however not sanitized, leading to a straightforward reflected cross-site scripting issue (XSS). This can be used by an attacker, in the worst case, to take over an administrator account, for example by tricking an administrator into clicking on a link that triggers the XSS.

Exploit Proof of Concept

The XSS can be triggered with a request like `https://192.168.200/view/charts.php?jump=x%27);alert(1);//`. It must be performed as a logged-in user.

VENDOR RESPONSE

Vendor confirms issues fixed on July 7th 2022

TIMELINE

2022-07-05 - Vendor Disclosure

2022-07-07 - Vendor Patch Release

2022-08-16 - Public Release

CREDIT

Discovered by Claudio Bozzato of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2022-1536

NEXT REPORT

TALOS-2022-1538