Talos Vulnerability Report

TALOS-2022-1534

WWBN AVideo all cross-site request forgery (csrf) vulnerability

AUGUST 16, 2022

CVE NUMBER

CVE-2022-29468

SUMMARY

A cross-site request forgery (CSRF) vulnerability exists in WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to increased privileges. 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

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

CWE

CWE-352 - Cross-Site Request Forgery (CSRF)

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.

AVideo lacks any Cross-Site Request Forgery protection across the whole application. This means that AVideo has no ability to make sure that a request is intentionally made by the user that performed it.

The simplest way to show how this can be exploited is via the password change feature. To change their own password, a logged-in user can make a request like the following:

```
curl -k 'https://192.168.1.200/objects/userUpdate.json.php' \
  -H 'Cookie: 84b11d010cced71edffee7aa62c4eda0=123456;' \
  --data-raw 'user=admin&pass=newpass'
```

An attacker can trick an administrator into visiting a website that does that same request in the background, leading to a password change where the password is controlled by the attacker. A simple example of such a malicious page is the following:

```
<form id='csrf' method='POST'
action='https://192.168.1.200/objects/userUpdate.json.php'>
  <input type='hidden' name='user' value='admin'>
  <input type='hidden' name='pass' value='newpass'>
</form>
<script>document.getElementById("csrf").submit()</script>
```

Where `192.168.1.200` is more likely the hostname where the AVideo website is hosted. Such a page could be hosted on any attacker-controlled host. Once loaded it will just show a blank page; however, the POST request will automatically happen in the background. If the victim is logged into the AVideo website as administrator, their password will change into “newpass”.

VENDOR RESPONSE

Vendor confirms issues fixed on July 7th 2022

TIMELINE

2022-06-29 - Initial Vendor Contact

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 NEXT REPORT

TALOS-2022-1542 TALOS-2022-1535