Talos Vulnerability Report

TALOS-2022-1535

WWBN AVideo session id privilege escalation vulnerability

AUGUST 16, 2022

CVE NUMBER

CVE-2022-30605

SUMMARY

A privilege escalation vulnerability exists in the session id functionality of 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-384 - Session Fixation

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 has a feature that allows users to arbitrarily choose the session id to use for a session:

```
function _session_start(array $options = []) {
    try {
        if (!empty($_GET['PHPSESSID'])) {
            if ($_GET['PHPSESSID'] !== session_id()) {
                if (session_status() !== PHP_SESSION_NONE) { // [1]
                    @session_write_close();
                }
                session_id($_GET['PHPSESSID']); // [2]
                //_error_log("captcha: session_id changed to " .
$_GET['PHPSESSID']);
            }
            unset($_GET['PHPSESSID']);
            return @session_start($options);
        } elseif (session_status() == PHP_SESSION_NONE) {
            return @session_start($options);
        }
    } catch (Exception $exc) {
        _error_log("_session_start: " . $exc->getTraceAsString());
        return false;
    }
}
```

The `_session_start()` function above is a wrapper around the builtin `session_start()`, which is called every time a session is started. The code simply allows for setting an arbitrary session id value, based on the `PHPSESSID` get parameter.

This behavior is by definition a “Session Fixation,” whereby an attacker able to trick a user into clicking a link to the AVideo website will automatically achieve the same permissions as said user, because the session id is known as it has been chosen by the attacker.

For example, an attacker may trick the AVideo administrator to click the following link: `https://192.168.1.200/user?PHPSESSID=123456`. We can simulate this with curl:

```
$ curl -k -v 'https://192.168.1.200/user?PHPSESSID=123456' 2>&1 | grep 'Set-
Cookie.*123456'
< Set-Cookie: 84b11d010cced71edffee7aa62c4eda0=123456; expires=Fri, 03-Jun-2022
23:03:04 GMT; Max-Age=3600; pa
```

The function `_session_start()` has been called, which invalidates any currently active session [1], and starts a new one with the session id `123456` [2]. At this point, if the administrator logs into the website within 1 hour (default session cookie expiration time), the `123456` value will be used as session id, and an attacker can simply set this same session id in its session to become administrator.

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-2022-1534

NEXT REPORT

TALOS-2022-1536