Unauthenticated FFmpeg Remote Server Status Disclosure via check.ffmpeg.json.php

Moderate **DanielnetoDotCom** published **GHSA-2vg4-rrx4-qcpq** 4 days ago

Software

WWBN/AVideo

Affected versions

<= 26.0

Patched versions

None

Description

Summary

The `plugin/API/check.ffmpeg.json.php` endpoint probes the FFmpeg remote server configuration and returns connectivity status without any authentication. All sibling FFmpeg management endpoints (`kill.ffmpeg.json.php`, `list.ffmpeg.json.php`, `ffmpeg.php`) require `User::isAdmin()`.

Details

The entire file at `plugin/API/check.ffmpeg.json.php`:

```php
<?php
$configFile = __DIR__.'/../../videos/configuration.php';
require_once $configFile;
header('Content-Type: application/json');

$obj = testFFMPEGRemote();

die(json_encode($obj));
```

No `User::isAdmin()`, `User::isLogged()`, or any access control check exists.

Compare with sibling endpoints in the same directory:

- `kill.ffmpeg.json.php` checks `User::isAdmin()`
- `list.ffmpeg.json.php` checks `User::isAdmin()`

Proof of Concept

```
curl "https://your-avideo-instance.com/plugin/API/check.ffmpeg.json.php"
```

Returns information about whether the platform uses a standalone FFmpeg server and its current reachability.

Impact

Infrastructure reconnaissance revealing the encoding architecture. Limited direct impact but aids targeted attack planning.

- **CWE**: CWE-306 (Missing Authentication for Critical Function)
- **Severity**: Low

Recommended Fix

Add an admin authentication check at `plugin/API/check.ffmpeg.json.php:3`, after `require_once $configFile;`:

```
if (!User::isAdmin()) {
    forbiddenPage('Admin only');
}
```

Found by aisafe.io

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None

User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE ID

CVE-2026-35450

Weaknesses

▶ CWE-306

Credits

 **adrgs** Reporter

 **aisafe-bot** Finder