Unauthenticated Information Disclosure via Disabled CLI Guard in install/test.php

Moderate **DanielnetoDotCom** published **GHSA-hg8q-8wqr-35xx** 4 days ago

Software

WWBN/AVideo

Affected versions

<= 26.0

Patched versions

None

Description

Summary

The `install/test.php` diagnostic script has its CLI-only access guard disabled by commenting out the `die()` statement. The script remains accessible via HTTP after installation, exposing video viewer statistics including IP addresses, session IDs, and user agents to unauthenticated visitors.

Details

The disabled guard at `install/test.php:5-7`:

```
if (!isCommandLineInterface()) {
    //return die('Command Line only');
}
```

The script also enables verbose error reporting:

```
error_reporting(E_ALL);
ini_set('display_errors', '1');
```

It then queries `VideoStatistic::getLastStatistics()` and outputs the result via `var_dump()`:

```
$resp = VideoStatistic::getLastStatistics(getVideos_id(), User::getId());
var_dump($resp);
```

The `VideoStatistic` object contains: `ip` (viewer IP address), `session_id`, `user_agent`, `users_id`, and JSON metadata. The `display_errors=1` setting also leaks internal filesystem paths in any PHP warnings.

The `install/` directory is not restricted by `.htaccess` (it only disables directory listing via `Options -Indexes`) and no web server rules block access to individual PHP files in this directory.

Proof of Concept

```
# Request viewer stats for video ID 1
curl "https://your-avideo-instance.com/install/test.php?videos_id=1"
```

Confirmed accessible on live AVideo instances (HTTP 200).

Impact

Unauthenticated disclosure of viewer IP addresses (PII under GDPR), session identifiers, and user agents. The enabled `display_errors` also reveals internal server paths on errors.

- **CWE**: CWE-200 (Exposure of Sensitive Information)
- **Severity**: Low

Recommended Fix

Uncomment the CLI guard at `install/test.php:6` to restore the intended access restriction:

```
if (!isCommandLineInterface()) {
    return die('Command Line 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-2026-35449

Weaknesses

▶ CWE-200

Credits

 **adrgs** Reporter

 **aisafe-bot** Finder