Unauthenticated Information Disclosure via Missing Auth on CloneSite client.log.php

Moderate **DanielnetoDotCom** published **GHSA-99j6-hj87-6fcf** 4 days ago

Software

WWBN/AVideo

Affected versions

<= 26.0

Patched versions

None

Description

Summary

The `plugin/CloneSite/client.log.php` endpoint serves the clone operation log file without any authentication. Every other endpoint in the CloneSite plugin directory enforces `User::isAdmin()`. The log contains internal filesystem paths, remote server URLs, and SSH connection metadata.

Details

The entire file at `plugin/CloneSite/client.log.php`:

```
<?php
include '../../videos/cache/clones/client.log';
```

No authentication check. The log file is populated by `cloneClient.json.php` which writes operational details during clone operations:

```
// plugin/CloneSite/cloneClient.json.php:118
$log->add("Clone (2 of {$totalSteps}): Geting MySQL Dump file [$cmd]");
```

The `$cmd` variable contains wget commands with internal filesystem paths, and rsync command templates with SSH connection details (username, IP, port).

Compare with sibling endpoints:

- `plugin/CloneSite/index.php` checks `User::isAdmin()`
- `plugin/CloneSite/changeStatus.json.php` checks `User::isAdmin()`
- `plugin/CloneSite/clones.json.php` checks `User::isAdmin()`
- `plugin/CloneSite/delete.json.php` checks `User::isAdmin()`

Proof of Concept

```
curl "https://your-avideo-instance.com/plugin/CloneSite/client.log.php"
```

If the CloneSite feature has been used, the response contains wget commands, filesystem paths, SSH metadata, and SQL dump file locations.

Impact

Unauthenticated disclosure of internal infrastructure details that could aid targeted attacks against the clone source server.

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

Recommended Fix

Add an admin authentication check at `plugin/CloneSite/client.log.php`, before the include:

```php
require_once '../../videos/configuration.php';
if (!User::isAdmin()) {
    http_response_code(403);
    die('Access denied');
}
```

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-2026-35452

Weaknesses

▶ CWE-200

Credits

 **adrgs** Reporter

 **aisafe-bot** Finder