Remote Code Execution via eval() in Platform Settings (2.0 RC2)

High **ywarnier** published **GHSA-hp4w-jmwc-pg7w** 6 hours ago

Package

php **chamilo/chamilo-lms** (Composer)

Affected versions	Patched versions
> 1.11.*, <= 2.0-RC.2	2.0-RC.3

Description

Summary

The `PlatformConfigurationController::decodeSettingArray()` method uses PHP's `eval()` to parse platform settings from the database. An attacker with admin access (obtainable via Advisory 1) can inject arbitrary PHP code into the settings, which is then executed when any user (including unauthenticated) requests `/platform-config/list`.

Details

Affected code: `src/CoreBundle/Controller/PlatformConfigurationController.php:272`

```
private function decodeSettingArray(mixed $setting): array
{
    if (is_string($setting)) {
        $json = json_decode($setting, true);
        if (is_array($json)) return $json;

        $trimmed = rtrim($setting, ';');
        try {
            $evaluated = eval("return $trimmed;");  // LINE 272 - RCE
        } catch (Throwable $e) { ... }
    }
    return [];
}
```

The route `/platform-config/list` (line 39) has **no authentication requirement**. The `catalog.course_catalog_settings` value from the `settings` table is passed to `decodeSettingArray()`, reaching `eval()`.

Impact

Full Remote Code Execution as www-data. An attacker can execute arbitrary system commands, read server files (including .env with DB credentials), establish reverse shells, and fully compromise the server. Combined with Advisory 1, any registered student achieves full server compromise.

Severity

High 8.8 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-33618

Weaknesses

▶ CWE-95

Credits

8l4nnk Reporter