Unauthenticated access to Twig template source files exposes application logic (<=1.11.36)

Moderate **ywarnier** published **GHSA-5wjg-8x28-px57** 5 hours ago

Package

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

Affected versions	Patched versions
<=1.11.36	1.11.38

Description

Summary

235 Twig template files (`.tpl`) under `/main/template/default/` are directly accessible without authentication via HTTP GET requests. These templates expose internal application logic, variable names, AJAX endpoint URLs, and admin panel structure.

Details

The Apache configuration does not restrict access to `.tpl` files. These files contain Twig/Smarty template syntax that reveals:

- Admin panel structure and functionality (`admin/settings_index.tpl`)
- AJAX endpoint URLs (`{{ web_admin_ajax_url }}`)
- Conditional logic and permission checks (`{% if _u.is_admin %}`)
- Internal variable names and data flow
- Email templates with notification logic (`mail/new_user_mail_to_admin.tpl`)

This information enables attackers to map the application's internal structure and identify further attack vectors.

Impact

- Application internal logic and structure exposed to unauthenticated attackers
- Admin panel AJAX endpoint URLs revealed (enables targeted attacks)
- Permission check logic visible (helps craft authorization bypass)
- Variable names and data flow exposed (aids in parameter tampering)
- Email template structure revealed (aids in phishing attacks)
- This is an information disclosure that directly supports further exploitation

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-2026-33705

Weaknesses

▶ CWE-538

Credits

 **8l4nnk** Reporter