chamilo / **chamilo-lms** Public

Code | Issues 399 | Pull requests 13 | Discussions | Actions | Projects

Stored XSS via Malicious File Upload in Social Post Attachments Leading to Arbitrary JavaScript Execution (<=2.0-RC.2)

Moderate **ywarnier** published **GHSA-273p-jw9w-3g22** 9 hours ago

Package

Chamilo LMS (PHP)

Affected versions	Patched versions
2.0-RC.2	2.0-RC.3

Description

Summary

A Stored Cross-Site Scripting (XSS) vulnerability exists in the social post attachment upload functionality. An authenticated user can upload a malicious HTML file containing JavaScript, which is served back from the application and executed in the browser when accessed via the generated `contentUrl`.

Because the payload executes in the application's origin, this allows attackers to perform actions such as session hijacking, account takeover, and arbitrary actions on behalf of the victim.

Details

The application allows users to upload files via: `POST /api/social_post_attachments`

The server responds with a contentUrl: `"contentUrl": "/r/user/social_post_attachments/<uuid>/view"`

When this URL is accessed, the uploaded file is rendered directly in the browser without proper sanitization or safe content handling.

Key issues:

- Uploaded content is served in an executable HTML context
- No restriction on uploading HTML/JS content
- No `Content-Disposition: attachment` header to force download
- No sanitization or validation of file content

As a result, any JavaScript embedded in the uploaded file executes in the context of the application.

Impact

This is a Stored Cross-Site Scripting (CWE-79) vulnerability.

Affected users:

- Any user who accesses the malicious attachment link

Potential impact:

- Session hijacking (if cookies are accessible)
- Account takeover
- Execution of arbitrary actions on behalf of the victim
- Privilege escalation if an admin user is targeted
- Abuse of LMS functionality (e.g., course manipulation, data access)

Because the payload is stored server-side and executes in the trusted application origin, the vulnerability has a high security impact.

Fix provided

`7c4965e` `da671d6`
or update your development environment to 2.0 stable.

Severity

Moderate 5.1 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	Passive

Vulnerable System Impact Metrics

Confidentiality	Low
Integrity	Low
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

CVE ID

CVE-2026-34161

Weaknesses

No CWEs

Credits

Aastha2602 Reporter