IDOR in /api/course_rel_users Allows Unauthorized Enrollment of Arbitrary Users into Courses (<=2.0-RC.2)

High **ywarnier** published **GHSA-x373-8j9j-g5pj** 9 hours ago

Package

Chamilo LMS (PHP)

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

Description

Summary

The /api/course_rel_users endpoint is vulnerable to Insecure Direct Object Reference (IDOR) / Broken Object Level Authorization (BOLA). An authenticated attacker can modify the user parameter in the request body to enroll any arbitrary user into any course without proper authorization checks.

This results in unauthorized manipulation of user-course relationships and may lead to privilege escalation, data exposure, and integrity compromise, making it a high severity issue.

Details

The application exposes an API endpoint: `POST /api/course_rel_users`

This endpoint accepts a JSON payload containing a user field:

```
{
  "user": "/api/users/{user_id}",
  "course": "/api/courses/{course_id}",
  "relationType": 0,
  "status": 5
}
```

Root Cause:

- The backend trusts user-supplied input for the `user` field.
- There is no server-side authorization check to verify that:
  - The requester owns the referenced `user_id`, or
  - The requester has permission to act on behalf of other users.

As a result, attackers can:

- Replace the `user` ID with another user's ID
- Perform actions (course enrollment) on behalf of that user

Evidence:
From the response:

```
"user": {
  "@id": "/api/users/5970",
  "username": "jbaker",
  "fullName": "Natheo Ribatto"
}
```

This confirms that the backend processes and applies the attacker-controlled user reference.

Impact

An attacker can:

- Enroll any user into any course
- Manipulate user-course relationships
- Potentially:
  - Grant unintended access to course materials
  - Bypass enrollment controls
  - Disrupt application integrity

Affected Parties:

- All users of the platform
- Administrators (if privilege boundaries exist via course roles)
- Organization data integrity

Fix

`2a9f060` `bd2ba34` `c9c30cd`
or update to v2.0 stable.

Severity

High 7.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-34602

Weaknesses

No CWEs

Credits

 **Aastha2602** Reporter