Insecure Direct Object Reference (IDOR) - User Data Exposure (<=2.0 RC2)

Moderate **ywarnier** published **GHSA-fp2p-fj6c-x3x9** 3 days ago

Package

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

Affected versions

<= 2.0-RC.2

Patched versions

2.0-RC.3

Description

Summary

Any authenticated user (including ROLE_STUDENT) can enumerate all platform users and access personal information (email, phone, roles) via `GET /api/users`, including administrator accounts.

Details

The User API GetCollection operation security is `is_granted('ROLE_USER')`. Since all registered users have ROLE_USER, students can list all users. GET `/api/users/{id}` also allows viewing any user's details.

Impact

All user emails, phone numbers, and roles exposed to any authenticated user. Admin accounts identifiable for targeted phishing. Prerequisite for Advisory 1 (attacker needs own user ID).

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-33736

Weaknesses

▶ CWE-639

Credits

8l4nnk Reporter