IDOR allowing an attacker to view private notes of other users (<=2.0-RC.2)

Moderate **ywarnier** published **GHSA-fm35-2hvw-564q** 9 hours ago

Package

v1.11.36 (PHP)

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

Description

Summary

The Chamilo LMS notebook module allows any authenticated student to read the private course notes of any other user on the platform by manipulating the notebook_id parameter. When a user requests the editnote action, the application fetches the note content from the database using only the supplied integer ID — with no check that the requesting user owns that note. The note's title and full HTML body are then rendered inside the edit form and returned to the attacker's browser.

The ownership check exists in the write path (updateNote(), delete_note()) but is entirely absent from the read path (get_note_information()), creating a read-only IDOR that exposes all private notes across the LMS.

Impact

An attacker can enumerate and access private study notes and exam preparation material from other students - Instructor personal notes entered through the same interface - Notes containing sensitive personal information users believed were private.

Mitigation

Add an ownership check to get_note_information() matching the pattern already used in updateNote() and delete_note():

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-2026-34370

Weaknesses

▶ CWE-285

Credits

 **abhiabhi2306** Reporter