IDOR in Gradebook Allows Cross-Course Evaluation Edit Without Ownership Check (2.0.0 RC)

High **ywarnier** published **GHSA-9h22-wrg7-82q6** 6 hours ago

Package

Chamilo LMS (PHP)

Affected versions

<= 2.0-RC.2

Patched versions

1.11.38, 2.0-RC.3

Description

Summary

An Insecure Direct Object Reference (IDOR) vulnerability in the gradebook evaluation edit page allows any authenticated teacher to view and modify the settings (name, max score, weight) of evaluations belonging to any other course by manipulating the `editeval` GET parameter.

Details

The file `public/main/gradebook/gradebook_edit_eval.php` (lines 14-25) loads a `GradebookEvaluation` entity by the ID value in `$_GET['editeval']` without verifying the evaluation belongs to the teacher's current course context:

```
api_block_anonymous_users();
GradebookUtils::block_students();    // Only blocks students — teachers pass

$evaledit = Evaluation::load($_GET['editeval']);   // Loads ANY evaluation by ID
if ($evaledit[0]->is_locked() && !api_is_platform_admin()) {
    api_not_allowed();                             // Only blocks LOCKED evals
}
$form = new EvalForm(
    EvalForm::TYPE_EDIT,
    $evaledit[0],                                  // Form populated with victim eval da
```

```
    ...
);
```

`Evaluation::load($id)` fetches the `gradebook_evaluation` table row by integer ID with no course-scoping filter. The only authorization check is whether the evaluation is "locked" — there is no verification of course ownership.

Impact

- View and modify evaluation names, max scores, and weights in any course
- Academic integrity violation — tamper with grading criteria
- Combined with CVE Candidate #004, an attacker can both edit evaluations and delete results
- Evaluation IDs are sequential integers, easily enumerable

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-2026-32930

Weaknesses

▶ CWE-639

Credits

ik0z Reporter