REST API Self-Privilege Escalation (Student → Teacher) (<=1.11.36)

High **ywarnier** published **GHSA-3gqc-xr75-pcpw** 5 hours ago

Package

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

Affected versions	Patched versions
<= 1.11.36	1.11.38

Description

Summary

Any authenticated user with a REST API key can modify their own `status` field via the `update_user_from_username` endpoint. A student (`status=5`) can change their status to Teacher/CourseManager (`status=1`), gaining course creation and management privileges.

Details

Affected code: `main/inc/lib/webservices/Rest.php` (Lines 2690-2810)

The `updateUserFromUserName()` method checks authorization at line 2710:

```
if (!api_is_platform_admin() && $userId != $this->user->getId()) {
    self::throwNotAllowedException();
}
```

This allows any user to modify **their own** profile. The method then sets sensitive fields without value validation:

```
case 'status':
    $user->setStatus($value);   // Line 2767 - No restriction on value
    break;
case 'roles':
    $user->setRoles($value);    // Line 2758 - Can assign any role
```

```
    break;
case 'auth_source':
    $user->setAuthSource($value); // Line 2764 - Can change auth method
    break;
```

The developers acknowledged this risk with a TODO at line 2688:

```
@todo make a safe version for use by the final user on its account
```

In Chamilo: `status=1` = Teacher/CourseManager, `status=5` = Student.

Impact

- Student can become Teacher/CourseManager
- Can create courses, manage course content, grade students
- Can modify own `auth_source`, `roles`, `active`, `enabled`, and 25+ other sensitive fields
- Breaks the trust model where only administrators should assign Teacher roles

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-2026-33706

Weaknesses

▶ CWE-269

Credits

8l4nnk Reporter