Authenticated SQL Injection in statistics.ajax.php users_active action (2.0 RC2)

Moderate **ywarnier** published **GHSA-w8c4-c7r8-qgw2** 9 hours ago

Package

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

Affected versions	Patched versions
2.0.0 RC2	2.0

Description

Vulnerability Details

This is an **incomplete fix for CVE-2026-30881** (GHSA-5ggx-x2cv-4h44). The fix applied `Security::remove_XSS()` to `date_start` / `date_end` parameters in the `get_user_registration_by_month` action (lines 27-28), but the **same parameters are used without any sanitization** in the `users_active` action (lines 300-301) in the same file.

Vulnerable Code

File: `public/main/inc/ajax/statistics.ajax.php`

Lines 300-305 (VULNERABLE — no sanitization):

```
$startDate = $_REQUEST['date_start'];
$endDate = $_REQUEST['date_end'];
$extraConditions .= " AND created_at BETWEEN '$startDate' AND '$endDate' ";
```

Compare with lines 27-28 (FIXED for CVE-2026-30881):

```
$dateStart = Security::remove_XSS($_POST['date_start']);
```

```
$dateEnd = Security::remove_XSS($_POST['date_end']);
```

Three different sanitization approaches for the same parameters in the same file — lines 300-301 have NO sanitization.

Impact

- Authenticated admin can extract any data from the database via time-based blind SQL injection
- Same impact as CVE-2026-30881 but via a different code path in the same file

Proposed Fix

Apply `Database::escape_string()` to lines 300-301:

```
$startDate = Database::escape_string($_REQUEST['date_start']);
$endDate = Database::escape_string($_REQUEST['date_end']);
```

Note: Static analysis identified 3 different sanitization patterns for the same parameters in the same file. The vulnerability was confirmed through source code comparison with the CVE-2026-30881 fix.

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-33714

Weaknesses

▶ CWE-89

Credits

morimori-dev Reporter