



# Chamilo LMS: IDOR in /api/course\_rel\_users Allows Unauthorized Enrollment of Arbitrary Users into Courses

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-34602
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 22:16:31 UTC
<b>Updated</b>	2026-04-22 18:46:22 UTC
<b>Description</b>	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, the /api/course_rel_users endpoint allows unauthorized users to enroll into courses.

## Risk And Classification

**Primary CVSS:** v3.1 7.1 HIGH from security-advisories@github.com

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

**EPSS:** 0.000320000 probability, percentile 0.091750000 (date 2026-04-22)

**Problem Types:** CWE-639 | CWE-639 CWE-639: Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N
3.1	CNA	DECLARED	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	alpha1	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	alpha2	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	alpha3	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	alpha4	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	alpha5	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	beta1	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	beta2	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	beta3	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	rc1	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	2.0.0	rc2	All	All
Application	<a href="#">Chamilo</a>	<a href="#">Chamilo Lms</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Chamilo</a>	<a href="#">Chamilo-lms</a>	affected < 2.0.0-RC.3	Not specified

### References

Reference	Source	Link	Tag
<a href="https://github.com/chamilo/chamilo-lms/releases/tag/v2.0.0-RC.3">github.com/chamilo/chamilo-lms/releases/tag/v2.0.0-RC.3</a>	security-advisories@github.com	<a href="#">github.com</a>	Pro
<a href="https://github.com/chamilo/chamilo-lms/security/advisories/GHSA-x373-8j9j-g5pj">github.com/chamilo/chamilo-lms/security/advisories/GHSA-x373-8j9j-g5pj</a>	security-advisories@github.com	<a href="#">github.com</a>	Ven
<a href="https://github.com/chamilo/chamilo-lms/commit/c9c30cdc48afae57cd6ab012ae2eceafd3...">github.com/chamilo/chamilo-lms/commit/c9c30cdc48afae57cd6ab012ae2eceafd3...</a>	security-advisories@github.com	<a href="#">github.com</a>	Pat
<a href="https://github.com/chamilo/chamilo-lms/commit/2a9f060fa9d50fc9a92ed93af774d26196...">github.com/chamilo/chamilo-lms/commit/2a9f060fa9d50fc9a92ed93af774d26196...</a>	security-advisories@github.com	<a href="#">github.com</a>	Pat
<a href="https://github.com/chamilo/chamilo-lms/commit/bd2ba34c2e74475587e38c74c90c2934e6...">github.com/chamilo/chamilo-lms/commit/bd2ba34c2e74475587e38c74c90c2934e6...</a>	security-advisories@github.com	<a href="#">github.com</a>	Pat
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)