



Chamilo LMS: IDOR in the Notebook Module allows an attacker to view other users' private notes

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

Summary

CVE	CVE-2026-34370
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 22:16:31 UTC
Updated	2026-04-22 18:46:34 UTC
Description	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, the notebook module contains a vulnerability that allows an attacker to view other users' private notes.

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from security-advisories@github.com

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

EPSS: 0.000320000 probability, percentile 0.091300000 (date 2026-04-22)

Problem Types: CWE-285 | CWE-639 | CWE-285 CWE-285: Improper Authorization | CWE-639 CWE-639: Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chamilo	Chamilo Lms	2.0.0	alpha1	All	All
Application	Chamilo	Chamilo Lms	2.0.0	alpha2	All	All
Application	Chamilo	Chamilo Lms	2.0.0	alpha3	All	All
Application	Chamilo	Chamilo Lms	2.0.0	alpha4	All	All
Application	Chamilo	Chamilo Lms	2.0.0	alpha5	All	All
Application	Chamilo	Chamilo Lms	2.0.0	beta1	All	All
Application	Chamilo	Chamilo Lms	2.0.0	beta2	All	All
Application	Chamilo	Chamilo Lms	2.0.0	beta3	All	All
Application	Chamilo	Chamilo Lms	2.0.0	rc1	All	All
Application	Chamilo	Chamilo Lms	2.0.0	rc2	All	All
Application	Chamilo	Chamilo Lms	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Chamilo	Chamilo-lms	affected < 2.0.0-RC.3	Not specified

References

Reference	Source	Link	Tags
github.com/chamilo/chamilo-lms/releases/tag/v2.0.0-RC.3	security-advisories@github.com	github.com	Product, Release
github.com/chamilo/chamilo-lms/security/advisories/GHSA-fm35-2hvw-564q	security-advisories@github.com	github.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

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](#)