Chamilo LMS: Stored XSS via Malicious File Upload in Social Post Attachments Leads to Arbitrary JavaScript Execution

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-34161
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 21:16:26 UTC
Updated	2026-04-17 15:38:09 UTC
Description	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, a Stored Cross-Site Scriptin

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000520000 probability, percentile 0.164070000 (date 2026-04-21)

Problem Types: CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:N/SC:L/SI
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:N/SC:L/SI

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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	Tag
github.com/chamilo/chamilo-lms/releases/tag/v2.0.0-RC.3	security-advisories@github.com	github.com	
github.com/chamilo/chamilo-lms/security/advisories/GHSA-273p-jw9w-3g22	security-advisories@github.com	github.com	
github.com/chamilo/chamilo-lms/commit/7c4965e48769d1d06413836429e386816a...	security-advisories@github.com	github.com	
github.com/chamilo/chamilo-lms/commit/da671d66a146887be3a16eabc5dcf0a92c...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**