



MasterStudy LMS <= 3.3.1 - Unauthenticated Privilege Escalation via stm_lms_register AJAX Action

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

Summary

CVE	CVE-2024-2409
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-29 09:15:07 UTC
Updated	2026-04-08 18:21:05 UTC
Description	The MasterStudy LMS plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.3.1.

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security@wordfence.com

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

Problem Types: CWE-266 | NVD-CWE-noinfo | CWE-266 CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Stylemixthemes	Masterstudy Lms	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Stylemix	MasterStudy LMS WordPress Plugin For Online Courses And Education	affected 3.3.1 semver	Not specified
ADP	Stylemixthemes	Masterstudy Lms	affected 3.3.2 semver	Not specified

References

Reference	Source
docs.stylemixthemes.com/masterstudy-lms/changelog-free-version	af854a3a-2127-422b-91ae-364da2661108
www.wordfence.com/threat-intel/vulnerabilities/id/94736152-b365-4b3a-a786-ed49f...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/changeset/3059676/masterstudy-lms-learning-management-system	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Hiroho Shimada (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-03-13T00:00:00.000Z	Vendor Notified
CNA	2024-03-28T00:00:00.000Z	Disclosed

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

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