



# MasterStudy LMS <= 3.3.3 - Unauthenticated Local File Inclusion via template

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

## Summary

<b>CVE</b>	CVE-2024-3136
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-04-09 19:15:39 UTC
<b>Updated</b>	2026-04-08 18:21:20 UTC
<b>Description</b>	The MasterStudy LMS plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.3.3 vi

## 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-98 | NVD-CWE-Other | CWE-98 CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

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 3.3.3 semver	Not specified
ADP	Stylemixthemes	Masterstudy Lms	affected 3.3.4 semver	Not specified

### References

Reference	Source
<a href="https://plugins.trac.wordpress.org/changeset/3064337/masterstudy-lms-learning-management-system/">plugins.trac.wordpress.org/changeset/3064337/masterstudy-lms-learning-management-system/...</a>	af854a3a-2127-422b-91ae-364da2661100
<a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/9a573740-cdfe-4b58-b33b-5e50b...">www.wordfence.com/threat-intel/vulnerabilities/id/9a573740-cdfe-4b58-b33b-5e50b...</a>	af854a3a-2127-422b-91ae-364da2661100
<a href="https://plugins.trac.wordpress.org/changeset/3064337/masterstudy-lms-learning-management-system/">plugins.trac.wordpress.org/changeset/3064337/masterstudy-lms-learning-management-system/...</a>	af854a3a-2127-422b-91ae-364da2661100
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	2024-04-01T00:00:00.000Z	Vendor Notified
CNA	2024-04-04T00:00:00.000Z	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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)