GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

14 September 2026

Advisory 308: Masteriyo LMS WordPress Plugin PHP Object Injection Leading to Remote Code Execution (CVE-2026-82845).

Release Date: 12th September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and Website administrators that operate a WordPress site using the Masteriyo LMS plugin to deliver online courses. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-82845 is a critical PHP object injection vulnerability in Masteriyo LMS, a WordPress learning-management-system plugin with over 5,000 active installations, disclosed on 12 September 2026. The plugin improperly processes user-supplied metadata values without adequate validation, allowing an authenticated user with only minimal (low) privileges to inject malicious PHP objects that execute arbitrary code on the server.

What are the systems affected?

The following version(s) are affected:

- Masteriyo LMS (WordPress plugin), all versions before 3.4.1 - (Affected)

Masteriyo LMS, version 3.4.1 and later - (Not affected, patched)

Upgrade the Masteriyo LMS plugin to version 3.4.1 or later without delay. There is no documented workaround, so upgrading is the only complete remediation.

What does this mean?

Typical attack flow:

1. **Obtain or use a low-privileged account, or exploit the unauthenticated file-write variant**
   - An attacker with any low-privileged authenticated account - such as a self-registered student or course enrollee - submits crafted metadata to the plugin; alternatively, an unauthenticated attacker exploits the related file-write variant of the same underlying flaw.
2. **Inject a malicious PHP object and achieve remote code execution**
   - Because the plugin deserializes the supplied metadata without adequate validation, the crafted input is processed as a PHP object, allowing the attacker to execute arbitrary code on the underlying server.

Attack vectors:

- A network-based attack against any WordPress site running an affected version of Masteriyo LMS, requiring only a low-privileged account (such as self-registration for a course) in the authenticated variant, or no account at all in the file-write variant.
- No user interaction is required (CVSS UI:N).

Successful exploitation may allow attackers to:

- Execute arbitrary code on a WordPress server hosting Masteriyo LMS, using only a low-privileged or, in some cases, no account at all.
- Fully compromise the affected WordPress site, including learner and course data and use it as a foothold to pivot into the wider hosting environment.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately

- Upgrade the Masteriyo LMS plugin to version 3.4.1 or later on every WordPress site where it is installed.

2. Restrict or review course self-registration where patching must be delayed
3. Audit for signs of prior compromise before and after patching
4. Confirm the update reached every affected site

Report any suspected compromise of a WordPress site to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-82845
2. https://wordpress.org/plugins/learning-management-system/