

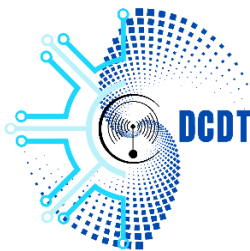
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

8 September 2026

**Advisory 264: MemberDash by LearnDash Unauthenticated Account Takeover
(CVE-2026-16310).**

Release Date: 5th 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, System/Network administrators, and training/membership website teams that operate a WordPress site using the MemberDash plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-16310 is a critical, unauthenticated account-takeover vulnerability in MemberDash, a standalone WordPress membership plugin published by LearnDash - the market-leading WordPress learning management system, with roughly a third of the entire WordPress LMS market and 80,000+ course websites built on its core LearnDash product, used by organisations including Yoast and DigitalMarketer

What are the systems affected?

The following version(s) are affected:

- MemberDash through 1.8.5 - (Affected)

MemberDash 1.8.6 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Submit a registration request with an arbitrary target user ID**
 - An unauthenticated attacker initiates MemberDash's registration process, but supplies the "id" parameter of an existing WordPress user of their choosing, including an administrator - instead of allowing the plugin to assign a new one, exploiting the plugin's failure to validate that the key belongs to the party making the request.
2. **Change the target account's password without alerting the victim**
 - Because MemberDash does not verify the supplied ID against the requester's own session, the attacker's registration request is processed as if it were a legitimate password change for the targeted account, and the victim receives no notification that their credentials have been altered, leaving the account takeover undetected until the legitimate user next attempts to log in.

Attack vectors:

- A network-based, unauthenticated request against any internet-reachable WordPress site running an affected version of the MemberDash plugin.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Change the password of any WordPress user on the affected site, including an administrator, without ever holding a legitimate credential and without alerting the account owner.
- Log in as the compromised user immediately afterward, and where the target is an administrator, gain complete control of the WordPress site, its membership/subscriber data, and any connected payment processing (Stripe/PayPal) configuration.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay
 - Update MemberDash to version 1.8.6 or later (1.8.7 is current) through the WordPress admin dashboard (Plugins > Installed Plugins), and confirm via the plugin's own changelog that the update addresses this account-takeover issue.
2. Treat this as urgent given the unauthenticated, no-privilege-required nature of the flaw and the direct, silent path to administrator account takeover
3. Audit the estate for MemberDash installations
4. Review administrator and other privileged accounts for unauthorized password changes
5. Review web-server access logs for suspicious activity

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-16310>
2. <https://memberdashwp.com/>