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

2 September 2026

Advisory 220: WPMU DEV Dashboard WordPress Plugin Authentication Bypass Vulnerability (CVE-2026-76581).

Release Date: 28th August 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 System/Network administrators that operate WordPress websites using the WPMU DEV Dashboard plugin with Hub Single Sign-On enabled. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-76581 is a critical authentication bypass vulnerability in the WPMU DEV Dashboard WordPress plugin. The flaw is a canonicalization weakness in the plugin's Hub Single Sign-On (SSO) authentication process: the plugin constructs its HMAC-SHA-256 signature differently at two separate stages, once over a token, hashed state, redirect URL and domain concatenated without delimiters, and once verified using only the token, state and redirect fields, omitting the domain entirely.

This inconsistency lets an unauthenticated attacker forge a valid signature for the second verification stage by rearranging values from the first, without ever needing a valid API key or credentials. If the Hub SSO account the forged session maps to holds administrator privileges, the attacker gains complete control of the WordPress installation.

What are the systems affected?

The following version(s) are affected:

- WPMU DEV Dashboard 5.0.1 and earlier - (Affected)

WPMU DEV Dashboard 5.0.2 and later - (Not affected, patched)

The fix, released 24 August 2026, stores the stage-one HMAC signature server-side and rejects any replayed signature presented at stage two. Site administrators should confirm their installed plugin version from the WordPress admin dashboard.

What does this mean?

Typical attack flow:

1. **Initiate the SSO handshake with an empty redirect**
    - The attacker starts the Hub SSO stage-one process with an empty redirect parameter, obtaining a valid signature that in fact covers the token, state, and domain values.
2. **Replay the signature to forge stage two**
    - The attacker places the domain value into the redirect field when calling stage two, causing the token/state/redirect combination checked there to match the forged signature from stage one, and the request validates as legitimate.

Attack vectors:

- Remote, unauthenticated network requests directly against the site's Hub SSO endpoint - no API key or credentials required.
- Any WordPress site with WPMU DEV Dashboard installed and Hub SSO enabled.

Successful exploitation may allow attackers to:

- Create a valid, authenticated WordPress session mapped to a Hub SSO account without any credentials.
- Gain complete control of the WordPress installation if that account holds administrator privileges — installing plugins, modifying themes, stealing credentials, or achieving remote code execution.

Mitigation process

CERTVU recommends the following:

1. Update WPMU DEV Dashboard immediately

- Upgrade to WPMU DEV Dashboard 5.0.2 or later without delay.

2. Audit Hub SSO account mappings
3. Review WordPress admin accounts
4. Audit the estate for the affected product
5. Monitor WPMU DEV's and Wordfence's security advisories for further updates

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

Reference

1. https://gbhackers.com/critical-wordpress-plugin-flaw-2/
2. https://www.cve.org/CVERecord?id=CVE-2026-76581