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

31 August 2026

Advisory 208: 101gen Automation Web Platform – Notifications and OTP for WooCommerce Unauthenticated Authentication Bypass Vulnerability (CVE-2026-77264).

Release Date: 21st 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 website administrators, WordPress/WooCommerce developers, and hosting providers that operate the affected plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-77264 is a critical unauthenticated authentication bypass vulnerability in "Automation Web Platform – Notifications and OTP for WooCommerce, Advanced Country Code", a WordPress plugin developed by 101gen. The flaw lies in the plugin's handle_email_otp_return() function, which returns the one-time-password "magic login" token in the HTTP response to a publicly accessible request, instead of delivering it only to the user's registered email address.

An unauthenticated attacker who knows or guesses a target user's email address — including an administrator's — can retrieve this token directly and use it to log in as that user, gaining full account takeover without needing a password. The vulnerability carries a CVSS 3.1 score of 9.8 (Critical) and is classified as CWE-640 (Weak Password Recovery Mechanism for Forgotten Password).

What are the systems affected?

The following plugin and version(s) are affected:

- Automation Web Platform - Notifications and OTP for WooCommerce, Advanced Country Code (WordPress plugin by 101gen), versions up to and including 4.8.6 – (Affected)

No patched version is currently available. The plugin was removed from the WordPress.org Plugin Directory on 20 August 2026, pending a full security review by the WordPress Plugin Team, and is not available for download from that repository.

There is no evidence of active exploitation at the time of this advisory. Given the low complexity of exploitation, the absence of an authentication requirement, and the lack of a published patch, CERTVU treats this as an urgent risk for any site running the plugin.

What does this mean?

Typical attack flow:

1. **Attacker identifies a target email address**
    - The attacker obtains or guesses the email address of a target user, such as a site administrator - often published on the site itself or easily inferred.
2. **Attacker requests the OTP and receives the login token directly**
    - The attacker sends a request to the plugin's public OTP endpoint for that email address. Instead of emailing the one-time token to the user, the plugin includes it directly in the HTTP response, which the attacker then uses to log in as that user with full account privileges.

Attack vectors:

- Direct HTTP requests to the plugin's OTP endpoint targeting known or guessed user/administrator email addresses
- Automated scanning of WordPress/WooCommerce sites to identify installations still running the vulnerable plugin

Successful exploitation allows attackers to:

- Fully take over any user account, including site administrators, without needing a password
- Gain complete control of the WordPress/WooCommerce site — content, orders and customer data — and use it as a foothold for further attacks

Mitigation process

CERTVU recommends the following:

1. Deactivate and Remove the Plugin Immediately
No patched version is currently available. The plugin was pulled from the WordPress.org Plugin Directory on 20 August 2026, pending review.
Do not reinstall the plugin until 101gen publishes a fixed release through an official channel.

2. Restrict access to the OTP endpoint at the web server or WAF level if immediate removal is not possible - as an interim measure only, not a substitute for removing the plugin.

3. Audit for Signs of Compromise
Review administrator accounts, recent logins and site changes for signs of unauthorized access, since exploitation requires no authentication and can leave minimal trace.
4. Rotate Credentials
Reset passwords and invalidate active sessions for all administrator and other privileged accounts as a precaution.
5. Monitor 101gen's official channels and the WordPress.org plugin page for a security release before reinstalling the plugin.

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-77264
2. https://wordpress.org/plugins/automation-web-platform/