

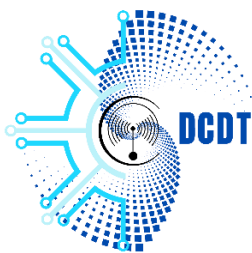
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

10 September 2026

**Advisory 289: cPanel & WHM EmailTrack SQL Injection Leading to Root
Remote Code Execution (CVE-2026-67401).**

Release Date: 9th 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, hosting providers, and System/Network administrators that operate a server running cPanel & WHM. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-67401 is a critical SQL injection vulnerability in the EmailTrack functionality of cPanel & WHM, the world's most widely-used web hosting control panel software, used by hosting providers, Internet Service Providers, and website operators globally to manage shared and dedicated hosting servers. The flaw allows any authenticated hosting account holder with mail-related privileges.

What are the systems affected?

The following version(s) are affected:

- cPanel & WHM release lines 11.110, 11.134, 11.136, and 11.138 (all versions prior to the fixed builds below) - (Affected)
- WP Squared release line prior to 11.138.1.9 - (Affected)

cPanel & WHM 11.110.0.143, 11.134.0.55, 11.136.0.39, or 11.138.0.4 and later; WP Squared 11.138.1.9 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Obtain a routine mail-enabled hosting account**
 - An attacker obtains or already holds any authenticated cPanel hosting account with mail-related privileges. The kind of low-level access included by default with almost any ordinary shared-hosting plan, requiring no special administrative permission.
2. **Exploit the EmailTrack SQL injection to write a file and execute code as root**
 - The attacker sends crafted input to the vulnerable EmailTrack functionality, injecting SQL that lets them create an arbitrary file in a suitable server location. The attacker uses this to deploy a malicious payload or script, which then executes with root privileges, giving the attacker complete control of the server and every hosting account on it, not just their own.

Attack vectors:

- A network-based attack requiring only a routine, mail-enabled cPanel hosting account, it does not a special or elevated privileges, and no user interaction from anyone else, are required.

Successful exploitation may allow attackers to:

- Escalate from a single, low-privileged hosting account to full root-level control of the entire underlying server.
- Access, modify, or destroy the websites, email, and data of every other hosting account on the same server. A single malicious or compromised customer account can compromise an entire multi-tenant hosting environment.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay
 - Update cPanel & WHM to 11.110.0.143, 11.134.0.55, 11.136.0.39, or 11.138.0.4 (matching your current release line), or WP Squared to 11.138.1.9, as applicable. No workaround exists.
2. Confirm the update reached every server, not just one
3. Review recently-created files and cron jobs for signs of compromise
4. Audit hosting account activity where multi-tenant risk is highest

Report any suspected compromise of a cPanel & WHM server to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-67401>
2. <https://support.cpanel.net/hc/en-us/articles/43187903921559>