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

4 September 2026

Advisory 254: GeoDirectory WordPress Plugin Unauthenticated SQL Injection (CVE-2026-84813).

Release Date: 3rd 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 website teams that operate a WordPress site using the GeoDirectory business-directory plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-84813 is a critical, unauthenticated SQL injection vulnerability in GeoDirectory, a WordPress business-directory and classified-listings plugin maintained by AyeCode Ltd with over 10,000 active installations and more than 2.5 million downloads since it was first published in 2014. The vulnerability allows an attacker to inject arbitrary SQL into a database query without needing to authenticate to the WordPress site at all. GeoDirectory has a history of similar SQL injection reports (including issues affecting versions 2.2.24, 2.3.28, and 2.3.61), making this a recurring weakness class in the plugin rather than an isolated one-off.

What are the systems affected?

The following version(s) are affected:

- GeoDirectory through 2.8.174 - (Affected)

GeoDirectory 2.8.175 and later - (Not affected, patched)

GeoDirectory is a self-managed WordPress plugin that does not update itself unless automatic updates are enabled, so this fix will not reach an existing site on its own.

What does this mean?

Typical attack flow:

1. **Send a crafted request to a vulnerable GeoDirectory endpoint**
    - An unauthenticated attacker sends a specially crafted request to a WordPress site running an affected version of GeoDirectory, embedding SQL syntax in a parameter that the plugin fails to properly neutralize before using it in a database query.
2. **Execute arbitrary SQL against the site's database**
    - The injected SQL executes with the privileges of the WordPress database account, allowing the attacker to read data from the database — potentially including user credentials, private listing data, and other sensitive information stored by the site.

Attack vectors:

- A network-based, unauthenticated request against any internet-reachable WordPress site running an affected version of the GeoDirectory plugin.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N). CERTVU is not aware of confirmed active exploitation at the time of writing, but the vulnerability requires no authentication at all, which typically shortens the window before opportunistic scanning begins.

Successful exploitation may allow attackers to:

- Read sensitive data from the site's WordPress database, including user account information, without ever holding a legitimate credential.
- Depending on the specific database permissions and query context, potentially extend the attack to modify data or, in combination with other weaknesses, escalate toward broader site compromise.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update the GeoDirectory plugin to the latest available version through the WordPress admin dashboard (Plugins > Installed Plugins), and confirm via the plugin's own changelog that the update addresses this SQL injection issue. Where automatic updates are not already enabled for plugins, consider enabling them for security-relevant updates going forward.

2. Treat this as urgent given the unauthenticated, no-privilege-required nature of the flaw and GeoDirectory's history of similar SQL injection reports
3. Audit the estate for GeoDirectory installations
4. Consider a Web Application Firewall (WAF) as an interim layer of defence
5. Review database and 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-2026-84813
2. https://wordpress.org/plugins/geodirectory/