INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 06:33 UTC

CVE-2026-9757: The GEO my WP plugin for WordPress is vulnerable to SQL Injection via the 'swlatlng' and 'nelatlng' ...

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0253
Type	CVE Vulnerability
CVE ID	CVE-2026-9757
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0009 (25th percentile)
Affected Products	GEO my WP plugin for WordPress, all versions up to and including 4.5.5
Published	2026-05-30T10:16:23.980
Discovery Source	Nvd

Executive Summary

A high-severity SQL injection flaw in the GEO my WP WordPress plugin (versions up to 4.5.5) allows unauthenticated attackers to extract data directly from the site's database without logging in. Any WordPress site running an affected version with the Posts Locator shortcode on a public page is exposed. The business risk is unauthorized access to the full WordPress database, which may include user credentials, personal data, and site configuration.

Technical Analysis

CVE-2026-9757 (CWE-89) is an unauthenticated SQL injection vulnerability in GEO my WP plugin for WordPress, all versions through 4.5.5. The 'swlatlng' and 'nelatlng' parameters are read from $_SERVER['QUERY_STRING'] via parse_str(), bypassing WordPress's wp_magic_quotes sanitization, which does not cover server-variable-sourced input. The plugin's gmw_get_locations_within_boundaries_sql() function splits each parameter on ',' via explode() and interpolates resulting fragments directly into a SQL BETWEEN clause with no is_numeric() validation, (float) casting, esc_sql() sanitization, or $wpdb->prepare() parameterization. Exploitation requires no authentication and succeeds when the [gmw form="results" form_id=N] shortcode is present on a publicly accessible page and at least one post has an associated gmw_location row. CVSS base score: 7.5. EPSS: 0.00087 (0.25th percentile). Not currently listed on CISA KEV. No vendor CVSS vector provided. As of 2026-03-04, vendor patch status is unconfirmed. Monitor the

WordPress plugin repository for updates.

Action Checklist

1. Step 1: Containment, Identify all WordPress instances running GEO my WP version 4.5.5 or earlier (check wp-content/plugins/geo-my-wp/readme.txt for version). If a page publicly exposes the [gmw form="results"] shortcode, either take that page offline or restrict access until patched. Block malformed query string requests containing comma-delimited coordinate parameters at the WAF layer using a rule targeting the 'swlatlng' and 'nelatlng' parameters. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Query web server and application logs for GET requests containing 'swlatlng' or 'nelatlng' parameters with values that include SQL metacharacters (single quotes, UNION, SELECT, OR, AND, double dashes, semicolons, or non-numeric content beyond expected float,float format). In Apache/Nginx access logs, filter on the query string pattern. In WordPress, enable query logging via the built-in WP_DEBUG_LOG feature (wp-config.php) or a third-party logging plugin and review for unexpected SQL errors from gmw_get_locations_within_boundaries_sql(). Reference: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1190 (Exploit Public-Facing Application).
3. Step 3: Eradication, Update GEO my WP to the first version that resolves CVE-2026-9757 once the vendor releases a patched build. Monitor the official WordPress plugin repository at wordpress.org/plugins/geo-my-wp/ for a patched release. If no patch is available, disable the plugin entirely until remediation is confirmed. Do not rely solely on WAF rules as a permanent fix. Reference: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery, After patching, confirm the installed version is the remediated release by re-checking readme.txt. Re-enable any pages or shortcodes that were taken offline during containment. Review the WordPress database for signs of unauthorized data extraction: unexpected user accounts (wp_users table), modified wp_options values, or injected content. Rotate WordPress database credentials and salts (wp-config.php) if log review indicates successful exploitation. Reference: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), D3-CRO (Credential Rotation).
5. Step 5: Post-Incident, Conduct a review of all WordPress plugins for similar patterns: direct use of $_SERVER superglobals without sanitization, string interpolation into SQL without $wpdb->prepare(). Implement a Web Application Firewall rule set covering OWASP CRS SQL injection signatures as a persistent control layer. Establish a plugin inventory and update cadence. Reference: NIST SI-4 (System Monitoring), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), D3-UAP (User Account Permissions).

Detection Guidance

Monitor web server access logs (Apache, Nginx, or CDN/WAF logs) for GET requests to any URL where query string parameters 'swlatlng' or 'nelatlng' contain values that do not match the expected float,float pattern (e.g., '40.7128,-74.0060'). Flag values containing SQL keywords (UNION, SELECT, FROM, WHERE, INSERT, DROP), comment sequences (-- or /*), quote characters (' or "), semicolons, or URL-encoded equivalents (%27, %22, %3B, %2D%2D). In WordPress debug logs, watch for SQL errors originating from

gmw_get_locations_within_boundaries_sql(). A SIEM query targeting these parameter names in HTTP query strings across all ingested web logs is the primary detection path. No public exploitation IOCs (attacker IPs, domains, file hashes) have been reported for this CVE. Monitor for future threat intelligence updates from CISA, MITRE, and VulnCheck. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), MITRE ATT&CK T1190.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-9757	T1
CVE-2026-9757 - Vulnerability Details - OpenCVE	https://app.opencve.io/cve/CVE-2026-9757	T3

Source	URL	Tier
CVE-2026-9757 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-9757	T3
CVE-2026-24157: NVIDIA NeMo Framework RCE Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-24157/	T3
CVE-2026-26157 Common Vulnerabilities and Exposures - SUSE	https://www.suse.com/security/cve/CVE-2026-26157.html	T3

Generated 2026-06-02 06:33 UTC by TJS Security Command Center