4Jawaly Security Advisory - CVE-2026-4060
==========
Generated: 2026-05-02 20:44 UTC
Advisory URL: https://www.4jawaly.com/geo-mashup-wordpress-sql-injection-vulnerability/

CVE ID: CVE-2026-4060
Severity: HIGH
CVSS Score: 7.5
CWE: CWE-89

EXECUTIVE SUMMARY
The Geo Mashup plugin for WordPress is vulnerable to Time-Based SQL Injection via the 'sort' parameter in all versions up to, and including, 1.13.18. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. The escsql() function is applied but is ineffective in the ORDER BY context because the value is not enclosed in quotes. Additionally, while a sanitizesortarg() allowlist-based sanitizer was added in version 1.13.18, it is only applied in the AJAX code path (sanitizequeryargs()) and not in the render-map.php or template tag code paths. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database via a time-based blind approach.

AFFECTED PRODUCT / COMPONENT
See vendor advisory and affected component details.

RISK FOR HOSTING AND SERVER OPERATORS
This vulnerability may affect websites, hosting panels, plugins, or server-side components. Operators should identify exposed installations, review access controls, inspect logs for suspicious activity, and apply the vendor fix as soon as it becomes available.

RECOMMENDED ACTIONS
1. Update the affected software to the latest patched version. 2. Restrict administrative access and review user privileges. 3. Monitor web server and application logs for exploitation attempts. 4. Apply WAF or virtual patching rules where available. 5. Keep backups and verify recovery procedures.

REFERENCES
- https://plugins.trac.wordpress.org/browser/geo-mashup/trunk/geo-mashup-db.phpL1767
- https://plugins.trac.wordpress.org/browser/geo-mashup/trunk/geo-mashup-db.phpL1785
- https://plugins.trac.wordpress.org/browser/geo-mashup/trunk/render-map.phpL166
- https://plugins.trac.wordpress.org/changeset/3503627/
-
https://www.wordfence.com/threat-intel/vulnerabilities/id/2fa5ae9a-532c-40f9-b70a-217f0f9cd473?source=cve

Prepared by 4Jawaly - Security and Web Hosting Alerts