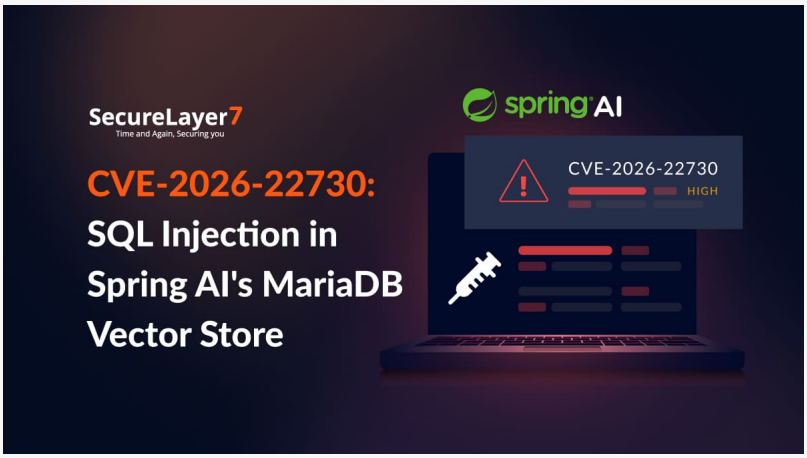
SecureLayer7 Discloses Two High Injection Vulnerabilities in Spring AI

Two injection vulnerabilities in Spring AI's vector store filter layer one SQL, one JSONPath both bypassing metadata-based access controls in RAG applications



Spring AI vulnerability

AUSTIN, TX, UNITED STATES, March 19, 2026 /EINPresswire.com/ -- SecureLayer7 today disclosed two high-severity injection vulnerabilities in Spring AI affecting the vector store metadata filtering layer. Both were found by the Blackf0g team using Bugdazz, SecureLayer7's autonomous penetration testing platform, and reported to the Spring Security team on December 31, 2025. Patches shipped in Spring AI 1.0.4 and 1.1.3 on March 17, 2026.

First one:

> “The injection happens inside the framework's own serialization layer, which is exactly where developers stop looking into the issues.”
>
> *Sandeep Kamble*

CVE-2026-22730 SQL Injection in Spring AI MariaDBFilterExpressionConverter

CVSS 3.1: 8.8 (High) | AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

MariaDBFilterExpressionConverter inserted user-supplied string values into SQL queries without escaping single quotes. An authenticated attacker passing a filter value like ' OR '1'='1 bypasses all metadata-based access controls on the search path and wipes the entire vector store on the delete path.

Affected: Spring AI 1.0.x, 1.1.x
Fix: Spring AI 1.0.4, 1.1.3

https://spring.io/security/cve-2026-22730

Second one:
CVE-2026-22729 JSONPath Injection in Spring AI Vector Stores FilterExpressionConverter

CVSS 3.1: 8.6 (High) | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

AbstractFilterExpressionConverter, the base class shared by the PostgreSQL and Oracle vector store adapters, embedded user-supplied values into PostgreSQL JSONPath predicates without escaping double quotes. A payload of " || $.accessLevel == "admin produces a JSONPath expression that evaluates true for all admin-level documents, bypassing the intended filter. No authentication required.

Affected: Spring AI 1.0.x, 1.1.x
Fix: Spring AI 1.0.4, 1.1.3

https://spring.io/security/cve-2026-22729

Who Is Affected
Applications using spring-ai-mariadb-store, spring-ai-pgvector-store, or spring-ai-oracle-store where user-controlled input reaches FilterExpressionBuilder — for department, role, tenant, or access-level filtering — are affected. The FilterExpressionBuilder API gives no indication that values need external sanitization; applications following the Spring AI documentation patterns were vulnerable.

Remediation
Upgrade to Spring AI 1.0.4 or 1.1.3. Until then, validate filter values against an allowlist before passing them to FilterExpressionBuilder.

About SecureLayer7
SecureLayer7 is an offensive security company based in Austin, TX. The company builds Bugdazz, an autonomous AI penetration testing platform, and conducts security research across application and AI infrastructure.

Website: https://securelayer7.net
Research: https://blog.securelayer7.net
Contact: info@securelayer7.net

Sandeep Kamble
SecureLayer7 cybersecurity INC.
email us here
Visit us on social media:
LinkedIn
X