COMMUNITY CONTENT

Home › Submit › 784459

Submit #784459: MAC-SQL The latest version SQL Injection

Title	MAC-SQL The latest version SQL Injection
Description	MAC-SQL is a multi-agent collaborative Text-to-SQL framework that utilizes large language models (LLMs) to convert natural language queries into SQL statements. The system processes user input through three agents (Selector, Decomposer, and Refiner) and executes the generated SQL against SQLite databases without proper validation or sanitization. The vulnerability exists in the complete trust chain between user input, LLM output, and SQL execution. Malicious users can exploit this through prompt injection attacks, manipulating the LLM to generate arbitrary SQL statements that are then executed directly on the database server. The core issue is located in the Refiner agent's _execute_sql method (core/agents.py:672-698), which executes LLM-generated SQL without any filtering. While a 120-second timeout is implemented, it is totally enough for crashing the server
Source	https://github.com/Ka7arotto/cve/blob/main/MAC-SQL/issue.md
User	Goku (UID 80486)
Submission	03/21/2026 02:38 AM (16 days ago)
Moderation	04/04/2026 11:50 PM (15 days later)
Status	Confirmed
VulDB entry	[wbbeyourself MAC-SQL up to 31a9df5e0d520be4769be57a4b9022e5e34a14f4 Refiner Agent core/agents.py _execute_sql sql injection]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling