مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited SQL Injection Vulnerability in BerriAI LiteLLM

Tracking #:432318930

Date:11-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical SQL Injection vulnerability, tracked as CVE-2026-42208, has been identified in LiteLLM Proxy API key verification functionality and is currently being actively exploited in the wild.

TECHNICAL DETAILS:

A critical SQL Injection vulnerability, tracked as CVE-2026-42208, has been identified in LiteLLM Proxy API key verification functionality. The vulnerability has been actively exploited in the wild and has been added to Known Exploited Vulnerabilities (KEV) Catalog.
The flaw allows unauthenticated remote attackers to inject malicious SQL queries through crafted Authorization headers sent to exposed LiteLLM API endpoints. Successful exploitation may allow attackers to read or potentially modify database contents, leading to unauthorized access to stored credentials, API keys, and managed proxy resources.

Vulnerability Details:

- CVE ID: CVE-2026-42208
- Severity: Critical
- CVSS v4 Score: 9.3
- CWE: CWE-89 – Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- Affected Product: LiteLLM
- Vendor: BerriAI
- Affected Versions: >= 1.81.16 and < 1.83.7
- Patched Version: 1.83.7

RECOMMENDATIONS:

Immediate Actions

- Upgrade LiteLLM immediately to fixed version or later
- Restrict public access to LiteLLM proxy instances
- Rotate all stored API credentials and tokens
- Review logs for suspicious Authorization header activity
- Audit database contents for unauthorized modifications

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/BerriAI/litellm/releases/tag/v1.83.7-stable