



NCSC-2026-0137

Kwetsbaarheden verholpen in LiteLLM door BerriAI

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-05-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

BerriAI heeft kwetsbaarheden verholpen in LiteLLM, specifiek in versies 1.74.2 tot en met 1.83.6.

Duiding

LiteLLM is een veelgebruikte proxy om op gecentraliseerde wijze API's naar een groot aantal LLM systemen te beheren.

De eerste kwetsbaarheid betreft een SQL-injectie in het proxy API key verificatiemechanisme, waardoor niet-geauthenticeerde aanvallers SQL-injectieaanvallen kunnen uitvoeren om proxy databasegegevens te lezen en te wijzigen. Dit kan leiden tot het compromitteren van credentials en verdere ongeautoriseerde toegang tot het systeem. De tweede kwetsbaarheid betreft twee preview endpoints in de MCP server feature die volledige serverconfiguraties accepteren. Elke geauthenticeerde gebruiker met een geldige proxy API key kan hiermee willekeurige commando's uitvoeren op de proxy host, zonder dat hiervoor administratieve rechten vereist zijn. Deze kwetsbaarheid maakt ongeautoriseerde command execution mogelijk.

Oplossingen

BerriAI heeft versie 1.83.7 van LiteLLM uitgebracht waarin beide kwetsbaarheden zijn verholpen. De SQL-injectie is opgelost en de toegang tot de preview endpoints is beperkt tot gebruikers met de PROXY_ADMIN rol. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://github.com/BerriAI/litellm/security/advisories/GHSA-r75f-5x8p-qvmc>
- <https://github.com/BerriAI/litellm/security/advisories/GHSA-v4p8-mg3p-g94g>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-42208	9.3 CRITICAL
➤ CVE-2026-42271	8.7 HIGH

CWE's

CWE	Beschrijving
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

BerriAI
LiteLLM

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.