GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

3 September 2026

Advisory 237: LiteLLM MCP Authentication Bypass via OAuth2 Passthrough Fallback (CVE-2026-59822).

Release Date: 2nd September 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and DevOps/AI engineering teams that deploy or operate LiteLLM as a self-hosted AI gateway or Model Context Protocol (MCP) proxy. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-59822 is an authentication-bypass vulnerability in LiteLLM, an open-source AI Gateway/proxy server (developed by BerriAI, 53,800+ GitHub stars, listed adopters include Stripe, Netflix, and Google ADK) that provides unified API access to 100+ LLM providers and supports the Model Context Protocol (MCP), an emerging standard for connecting AI agents to external tools and data sources. The flaw sits in LiteLLM's MCP Streamable HTTP endpoint: an unauthenticated attacker can supply a fabricated, unregistered Bearer token in the Authorization header, and instead of rejecting the failed key validation, an OAuth2 passthrough fallback path substitutes an empty UserAPIKeyAuth() object in place of a real authenticated identity, allowing the forged request through to MCP tooling and any connected services without a valid LiteLLM key.

What are the systems affected?

The following version(s) are affected:

- BerriAI LiteLLM before 1.84.0 – (Affected)

BerriAI LiteLLM 1.84.0 and later – (Not affected, patched)

LiteLLM is typically self-hosted (via pip package, Docker image, or Helm chart) rather than centrally auto-updated by the vendor, so this fix will not reach an existing deployment on its own.

What does this mean?

Typical attack flow:

1. **Send a forged MCP request**
    - An attacker sends a request to a reachable LiteLLM MCP Streamable HTTP endpoint carrying an arbitrary, unregistered Bearer token in the Authorization header - no valid LiteLLM API key is required.
2. **Exploit the broken authentication fallback**
    - LiteLLM's key validation fails as expected, but its OAuth2 passthrough fallback path substitutes an empty UserAPIKeyAuth() object instead of rejecting the request, so the forged request is treated as authenticated and passed through to MCP tooling and any connected services without ever presenting a valid credential.

Attack vectors:

- A network-based, unauthenticated request against any LiteLLM MCP Streamable HTTP endpoint reachable from the attacker's network position - public internet, internal network segment, or a neighbouring trust zone.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N) - a single crafted HTTP request is sufficient to trigger the bypass.

Successful exploitation may allow attackers to:

- Access MCP tools and any external services, APIs, or data sources connected to that LiteLLM instance without ever presenting a valid LiteLLM key.
- Read and, depending on the tools' own permissions, potentially act on the data and systems reachable through the MCP tool-calling surface, using the compromised gateway as a pivot into whatever backend services (databases, internal APIs, file stores, etc.) the organization has connected via MCP.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Upgrade LiteLLM to version 1.84.0 or later, where this authentication-bypass vulnerability is fixed (GitHub Security Advisory GHSA-7488-6r32-c95q, pull request #26463, commit 73869f0faf7d11ee21adcb5f91b8c33a340b6c2c). Because LiteLLM is self-hosted, this requires a deliberate redeploy — confirm the running instance has actually reached the fixed version.

2. Apply the vendor’s interim workaround if immediate upgrade isn’t possible
3. Audit the estate for LiteLLM deployments
4. Restrict network exposure to MCP endpoints
5. Review MCP endpoint access logs and connected tool permissions

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-59822
2. https://github.com/BerriAI/litellm/security/advisories/GHSA-7488-6r32-c95q