

CVE-2026-59822

BerriAI LiteLLM Improper Authentication Vulnerability

CISA KEV since Sep 2, 2026

Actively exploited

LiteLLM is a proxy server (AI Gateway) to call LLM APIs in OpenAI (or native) format. Prior to 1.84.0, LiteLLM's MCP Streamable HTTP endpoint allowed an unauthenticated attacker to use a fabricated Authorization header to trigger an OAuth2 passthrough fallback path that replaced failed LiteLLM key validation with an empty UserAPIKeyAuth() object, allowing requests to reach MCP tooling without a valid LiteLLM key. This issue is fixed in version 1.84.0.

EVRS 75/100 Urgent priority	CVSS V4.0 8.8 High · NVD	EPSS 0.008 57.2nd percentile · FIRST	CISA DEADLINE Sep 16, 2026 CISA federal deadline · Overdue by 36 days
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.008 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
litellm	< 1.84.0	1.84.0	GitHub

Sources

Vendor guidance	github.com/BerriAI/litellm/commit/73869f0faf7d11ee21adcb5f91b8c33a340b6c2c	Additional guidance	github.com/BerriAI/litellm/security/advisories/GHSA-7488-6r32-c95q
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-59822	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
GitHub advisory	github.com/advisories/GHSA-7488-6r32-c95q	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-42359
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-59822		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.