

LiteLLM Security Incident | Official Company Documentation

PRINT-READY SOURCE SUMMARY | October 21-23, 2026 | Primary sources: LiteLLM only

This independent printable reference summarizes two incident reports published by LiteLLM. It is not a reproduction of either report, and it does not claim to be an official LiteLLM PDF. The original company publications are linked below for direct verification.

Source 1 — Completed root-cause investigation

Official title: The attack chain behind the v1.107.0 LiteLLM release

Published: October 23, 2026

Authors: Oliver Jensen, Director of Security, and Mateo Wang, AI Engineer

Original URL: <https://docs.litellm.ai/blog/security-incident-oct-21-2026-attack-chain>

Company-established findings:

- On May 27, 2026, an internal configuration file containing a LiteLLM Agent Platform master key was committed to a public GitHub repository. The publication was removed, but that master key was not revoked.
- On October 10, an attacker used the still-active master key to access the internal Agent Platform and retrieve a GitHub CLI OAuth token associated with a GitHub organization owner.
- The attacker used repository workflows to extract additional secrets, including maintainer GitHub credentials, and obtained broad access to software release infrastructure.
- On October 21, the attacker bypassed repository protections, redirected a release workflow toward an attacker-controlled lookalike repository, and used compromised identities to authorize publication.
- The malicious version 1.107.0 was published to PyPI and container registries. LiteLLM states its October 23 report is the authoritative reconstruction and supersedes preliminary explanations.

Documented release sequence (UTC)

- May 27: configuration file containing master key publicly committed.
- October 10: attacker accessed Agent Platform and obtained owner token.
- October 21, 11:39-11:40: malicious Python package wheels published to PyPI.
- October 21, 11:46: compromised container images published.
- October 21, by 13:23: PyPI package quarantined; by 14:20 Docker Hub tags removed or repointed to clean images.

Source 2 — Initial incident notice and affected artifacts

Official title: Contained: Oct 21, 2026 LiteLLM release v1.107.0 Compromised

Published: October 21, 2026

Authors: Krrish Dholakia, Ishaan Jaffer, Oliver Jensen, and Nate Armstrong

Original URL: <https://docs.litellm.ai/blog/security-incident-oct-21-2026>

- The affected PyPI artifact was `litellm==1.107.0`, all seven wheels, available from approximately 11:39:51 to 13:23 UTC on October 21.
- Affected public container tags included `v1.107.0`, `latest`, `main-latest`, and `main-stable` in the specified exposure windows.
- LiteLLM states earlier package versions were not affected by this malicious release, and customers using its separate private enterprise release were not affected.
- The company described malware capable of stealing credentials and loading remote-code-execution tools.
- For systems that executed affected releases, LiteLLM advises treating accessible secrets as compromised, removing malicious startup files, rebuilding environments where practical, rotating keys, and reviewing cloud audit activity.

What LiteLLM does not establish in these statements

The reported estimate of roughly 49,000 PyPI downloads and observations of subsequent AWS credential testing were reported by independent researchers. These are not presented here as LiteLLM-confirmed incident counts. Download totals also do not equal a confirmed number of compromised organizations.

Suggested TRJ document credit

LiteLLM, *The attack chain behind the v1.107.0 LiteLLM release*, official root-cause analysis, October 23, 2026; and *Contained: Oct 21, 2026 LiteLLM release v1.107.0 Compromised*, official incident notice, October 21, 2026.

Source basis: both official LiteLLM reports accessed October 26, 2026. Follow the source URLs above for the complete current company statements.