LiteLLM version 1.107.0 compromised in supply-chain attack that steals credentials



Attackers compromised LiteLLM's release pipeline on October 21 and published version 1.107.0 with credential-stealing malware to PyPI and Docker registries. Teams should roll back to 1.106.2 and rotate all exposed secrets.

- The LiteLLM release pipeline was compromised on October 21, and version 1.107.0 was pushed to PyPI and the Docker registry.
- All seven PyPI wheels for 1.107.0 were affected, on Windows, Linux and macOS; the maintainer says private enterprise customers were not impacted.
- The malware targets cloud, AI, developer and CI/CD credentials, private keys, browser data and environment variables.
- Three files placed in Python's library directory run every time Python starts, so even running

Python or pip to investigate triggers the malware.

- The recommended clean version is 1.106.2; affected systems should be isolated and rebuilt, and secrets rotated.

The maintainers of LiteLLM, an open-source Python SDK and AI gateway that lets applications reach models from different providers through one API, report that their release pipeline was compromised on October 21. The attacker published version 1.107.0 to PyPI and to the Docker registry. The maintainer describes the release as containing compiled malware that steals credentials and loads remote-code execution tools.

What was affected

All seven PyPI wheels for litellm 1.107.0 were live for roughly two hours on October 21 (UTC). Docker Hub and GHCR tags including v1.107.0 and latest also pointed to compromised images during that day. According to researchers, the application code itself was not altered; the attacker modified only the installation package to add three files (cook.pth, cook.py and sitecustomize.py) to Python's library directory. These run each time Python starts in that environment.

The malware targets cloud and deployment credentials, AI tool credentials and stored provider settings, developer secrets such as Git, npm, PyPI and CI/CD tokens, SSH, GPG and TLS keys, browser data, and environment variables. Stolen data is encrypted before upload to an external address. A detached loader also checks a GitHub-hosted pointer hourly and downloads further Python code to run on the host.

Recovery guidance

The malicious packages have been removed. Anyone who may have installed them should stop affected deployments and inspect environments without launching the Python interpreter, since running Python or pip triggers the payload. Isolate infected systems, rebuild them from clean backups and rotate all exposed secrets immediately. Deleting the LiteLLM directory alone may leave startup files or an active loader behind. The recommended recovery version is 1.106.2, the latest clean release before the attack.

What to do now

1. Identify every system, container image and CI/CD job that installed or pulled LiteLLM 1.107.0, or the latest and main tags, on October 21.
2. Stop affected deployments and inspect them without launching Python or pip; isolate infected hosts and rebuild them from clean backups.
3. Rotate all secrets reachable from affected environments: cloud, Kubernetes, Docker, Git, npm, PyPI, CI/CD, SSH, GPG and TLS keys, and AI provider keys.
4. Pin LiteLLM to 1.106.2 and use version or digest pinning for dependencies and container images instead of floating tags.

5. Review outbound traffic for connections to litellm[.]dev and report confirmed exposure under your internal incident process and applicable NCA or SAMA requirements.