Journal : Supply chain attack : La faille chez Trivy entraîne des fuites massives par LiteLLM

24 mar. 2026

10

Posté par **Faya** le 24 mars 2026 à 22:30. **Licence CC By-SA.**
Étiquettes : **intelligence_artificielle**, **fuite_de_données**

Épisode précédent : Trivy compromis une seconde fois : la release v0.69.4 était empoisonnée

Et aujourd'hui on apprend que l'outil open-source LiteLLM (une interface pour gérer plusieurs LLM) utilisait le scanner de vulnérabilité Trivy, entraînant la fuite de nombreux identifiants : *"Anyone who has installed and run the project should assume any credentials available to [the] LiteLLM environment may have been exposed, and revoke/rotate them accordingly."* Un compte se disant "expert en cybersécurité" sur Twitter affirme que le groupe à l'origine de la fuite extorque déjà *"several multi-billion-dollar companies"*. (Aucune idée de la fiabilité de ce compte, juste qu'il a souvent posté très tôt des infos avérées par la suite.)

Bon et puis ça va sans dire mais ça va mieux en le disant : on ne donne pas de clés ni de mots de passe à un LLM. Même si le LLM tourne sur votre infra, si vous y accédez par un quelconque outil, vous ne savez pas ce qui est fait de votre prompt avant ou après transmission au modèle. Après la mode des framework JS et des modules NodeJS, on voit fleurir des dizaines d'outils super-top pour gérer vos agents "10x engineer" mais personne n'a fait de relecture sur ces trucs.

It's jungle out there

(3 commentaires). Markdown EPUB

Inutilisable ?

Posté par **devnewton** (**site web personnel**) le 25 mars 2026 à 08:36. Évalué à 4 (+1/-0).

> on ne donne pas de clés ni de mots de passe à un LLM
>
> 
>
> Donc les 99% de devs qui utilisent un LLM qui a accès à leurs fichiers locaux sont mal faisant ?
>
> --
>
> Ce post est offensant ? Prévenez moi sur https://linuxfr.org/board

Répondre

[^] # Re: Inutilisable ?

Posté par **steph1978** le 25 mars 2026 à 09:36. Évalué à 2 (+0/-0).

> > malfaisant \mal.fə.zɑ̃\
> >
> > Qui se plaît à nuire, à faire du mal à autrui.
>
>
>
> Malfaisant, probablement pas. Imprudents, oui.

Répondre

Relecture

Posté par **Misc** (**site web personnel**) le 25 mars 2026 à 08:52. Évalué à 6 (+3/-0).

> Alors, la, c'est pas exactement la faute de litellm, ça aurait pu arriver quand même n'importe ou vu que le souci était (sauf erreur de ma part) via une action github. Si un soft que tu utilises est backdooré, ç'est un peu mort.
>
>
>
> Mais sinon, j'ai commencé à regarder le code de litellm, parce que j'étais curieux de voir comment il y a pu y avoir autant de code par une équipe si petite en si peu de temps. 382 PR en 1 semaine, 58 auteurs, 19 releases par semaine, il y a clairement de l'automatisation à un moment.
>
> Sans surprise, j'imagine qu'il y a beaucoup de LLM, et c'était l'occasion de voir ce que le code donne (j'avais regardé le depot d'openclaw et j'avais été choqué de voir le bordel à la racine). Et j'ai pas été déçu.
>
> En ouvrant au pif des fichiers, je tombe sur ce code ou j'ai le sentiment que les variables correspondent pas exactement à leur nom. Il y a un deepcopy sans bonne raison, l'organisation des structures semble pifométrique, etc. De même, la fonction get_llm_provider semble faire plus que juste donner le provider, vu que

ça donne aussi une clé d'api et une base (et pas un objet provider propre).

les structures de données semblent assez visiblement inefficaces vu que je vois 3 fois le concept de région (une fois pour aws, une fois pour waston x et une fois pour le reste). Peut être qu'il y a des subtilités qui m'échappe, mais je doute.

Et à la racine, il y a un fichier uv.lock, mais aussi un poetry.lock, et un requirements.txt, en même temps. 3 fichiers pour agents (CLAUDE.md, GEMINI.md, AGENTS.md). Le nettoyage existe pas.

Donc bon, on peut pas blâmer litellm pour la compromission résultant d'un vendeur tierce et sans doute de limitation de Github, mais ça reste en effet du code un peu moche et trop complexe.

Répondre

Envoyer un commentaire

Suivre le flux des commentaires

Note : les commentaires appartiennent à celles et ceux qui les ont postés. Nous n'en sommes pas responsables.

Revenir en haut de page

Derniers commentaires

- Re: Inutilisable ?
- Re: Quid du code?
- Re: Et dans quelque…
- Relecture
- Re: vu de loin
- Inutilisable ?
- azerty
- Re: Je me suis hypé …
- Re: et GrapheneOS
- Re: Quid du code?
- Re: depistado
- Re: et GrapheneOS

Étiquettes (tags) populaires

- intelligence_artificielle
- lionel_jospin
- merdification
- grands_modèles_de…
- états-unis
- sortie_version
- linux
- administration_fran…
- souveraineté_numer…
- bigtech
- google
- bronsonisation

Sites amis

- April
- Agenda du Libre
- Framasoft
- Éditions D-BookeR
- Éditions Eyrolles
- Éditions Diamond
- Éditions ENI
- La Quadrature du Net
- Lea-Linux
- En Vente Libre
- Grafik Plus
- Open Source Initiative

À propos de LinuxFr.org

- Mentions légales
- Faire un don
- L'équipe de LinuxFr.…
- Informations sur le s…
- Aide / Foire aux que…
- Suivi des suggestion…
- Wiki du site
- Règles de modération
- Statistiques
- API pour le dévelop…
- Code source du site
- Plan du site