Discussion :

Claude Code expose mots de passe et clés dans 1 122 dépôts publics GitHub via « Don't Ask Again »

Sujet : *Intelligence artificielle*

Navigation

Inscrivez-vous gratuitement
pour pouvoir participer, suivre les réponses en temps réel, voter pour les messages, poser vos propres questions et recevoir la newsletter

JE M'INSCRIS

Aujourd'hui, 07h24 #1

Eliora
Communiqués de presse
Rien
Inscrit en: Juillet 2026
Messages: 301

Claude Code expose mots de passe et clés dans 1 122 dépôts publics GitHub via « Don't Ask Again »

La fonctionnalité « Don't Ask Again » de Claude Code expose des mots de passe et des clés dans 1 122 copies publiques sur GitHub, en copiant les données confidentielles dans des dépôts accessibles à tous

Les mots de passe et les clés API saisis par les développeurs dans les commandes qu'ils ont validées au sein de Claude Code se trouvent dans des dépôts GitHub publics, selon un rapport de la société de sécurité informatique Apiiro. Lorsqu'un utilisateur sélectionne « *Oui, et ne plus me le demander* », l'assistant de codage IA d'Anthropic peut enregistrer la commande, mot pour mot, y compris le mot de passe, dans un fichier de paramètres de projet qui n'est pas ignoré par défaut par gitignore. Apiiro indique avoir analysé 104 185 copies publiques de ce fichier : environ 1,1 % d'entre elles contiennent au moins un secret, soit 1 379 secrets différents. « *Claude Code est le seul dont il est confirmé qu'il enregistre par défaut la commande approuvée dans son intégralité dans un fichier de projet* », indique le rapport.

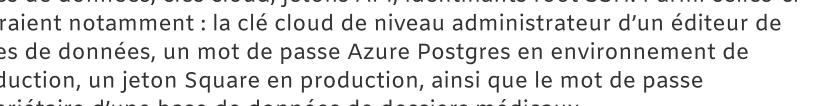
Anthropic, PBC est une société américaine d'intérêt public spécialisée dans l'intelligence artificielle (IA), dont le siège social est situé à San Francisco, en Californie. Son produit phare est Claude, une série de grands modèles de langage (LLM) propriétaires. En janvier 2021, dans le but de promouvoir la sécurité de l'IA, Anthropic a été fondée par d'anciens membres d'OpenAI, notamment les frère et sœur Daniela Amodei et Dario Amodei, qui en sont respectivement la présidente et le PDG.

Claude Code, lancé en février 2025, est un outil en ligne de commande doté d'une IA permettant de déléguer des tâches de codage depuis le terminal à l'aide de commandes en langage naturel. Il a été mis à la disposition du grand public en mai 2025, parallèlement à Claude 4. Compte tenu de son adoption par les entreprises, Anthropic a fait état d'une multiplication par 5,5 du chiffre d'affaires de Claude Code dès le mois de juillet. Le créateur et actuel responsable de Claude Code est Boris Cherny. Le 20 octobre 2025, Anthropic a lancé une version web de Claude Code ainsi qu'une fonctionnalité de sandboxing.

En mars 2026, un développeur avait confié à Claude Code la gestion d'une migration d'infrastructure Terraform sur AWS. En quelques minutes, l'agent avait détruit l'intégralité de son environnement de production — base de données, snapshots compris — faisant disparaître 2,5 ans d'historique de cours. L'incident, rendu public dans un post-mortem exemplaire, soulevait une question que l'essor fulgurant du vibe coding ne pouvait plus esquiver : jusqu'où peut-on déléguer à une IA des opérations irréversibles sur des environnements de production ?

Récemment, les mots de passe et les clés API saisis par les développeurs dans les commandes qu'ils ont validées au sein de Claude Code se trouvent dans des dépôts GitHub publics, selon un rapport de la société de sécurité informatique Apiiro. Lorsqu'un utilisateur sélectionne « *Oui, et ne plus me le demander* », l'assistant de codage IA d'Anthropic peut enregistrer la commande, mot pour mot, y compris le mot de passe, dans un fichier de paramètres de projet situé à l'emplacement `.claude/settings.local.json` — un chemin qui n'est pas ignoré par défaut par gitignore. Apiiro indique avoir analysé 104 185 copies publiques de ce fichier réparties dans 103 617 dépôts. Environ 1,1 % d'entre elles, soit 1 122 copies, contiennent au moins un secret. Au total, elles renferment 1 379 secrets différents. La société n'a pas vérifié si certains d'entre eux fonctionnaient encore.

La répartition est précise : 379 mots de passe de bases de données, 43 identifiants SSH pour des serveurs publics, 42 jetons pour GitHub, GitLab et npm, et 23 clés AWS. La moitié des dépôts concernés ont conservé le fichier sur leur branche par défaut pendant au moins 217 jours. 734 autres secrets ont été découverts dans d'anciennes versions de fichiers réparties sur 509 dépôts ; ils avaient été supprimés de l'arborescence actuelle mais restaient lisibles dans l'historique, et 211 forks contenaient des secrets identiques copiés depuis l'original. Soixante-trois organisations, principalement des éditeurs de logiciels, sont concernées. Apiiro note que gitleaks a signalé 564 de ces fichiers et que TruffleHog en a détecté 643 ; aucun des deux n'a repéré 215 d'entre eux.





Watch on

Les chercheurs ont comparé la documentation de 16 agents de codage. « *Claude Code est le seul dont il est confirmé qu'il enregistre par défaut la commande approuvée dans son intégralité dans un fichier de projet* », indique le rapport. C'est important, car ce bouton de commodité est le genre de chose sur laquelle un développeur clique une fois puis oublie ; le secret est alors transmis à Origin lors du prochain commit.

Apiiro précise également que le suivi des problèmes de sécurité chez Anthropic a été discret. « *À ce jour, les quatre rapports cités par les chercheurs ont tous été clôturés par le même bot, le plus récent datant d'hier. Aucun n'a reçu de réponse de la part d'Anthropic, précisent-ils.* » Un rapport antérieur datant du mois d'août a été clôturé le 3 janvier avec la mention « *non prévu* », après 60 jours d'inactivité. Il s'agit de la deuxième divulgation concernant Claude Code qu'ils ont recensée en une semaine, après un rapport de bogue faisant état d'une fuite d'adresses e-mail dans l'en-tête User-Agent du client.

En septembre 2026, alors que le secteur s'interrogeait sur la possibilité que l'IA pût s'améliorer au point de tuer tout le monde, Anthropic avait révélé un nouvel incident qui serait qualifié de crime s'il avait été commis par une personne. L'entreprise spécialisée dans l'IA avait publié « *une évaluation d'alignement* » détaillant les quatre occasions où des modèles Claude ont accédé à des systèmes tiers sans autorisation. La société avait déjà signalé trois de ces incidents. La preuve du quatrième se cachait dans la transcription d'une session datant de janvier 2026, date à laquelle le comportement inapproprié s'était produit.

Voici la publication d'Apiiro sur les agents de codage qui divulguent des secrets sur GitHub :

Des agents de programmation copient vos secrets dans un fichier caché. Des milliers d'entre eux se trouvent sur GitHub

Une étude menée par Apiiro a permis de découvrir 2 539 informations confidentielles réelles dans 1 994 dépôts GitHub publics : mots de passe de bases de données, clés cloud, jetons API, identifiants root SSH. Parmi celles-ci figuraient notamment : la clé cloud de niveau administrateur d'un éditeur de bases de données, un mot de passe Azure Postgres en environnement de production, un jeton Square en production, ainsi que le mot de passe propriétaire d'une base de données de dossiers médicaux.

La plupart appartiennent à des développeurs individuels. 63 organisations sont concernées, allant de groupes d'étudiants à des start-ups, en passant par des agences de développement logiciel et des fournisseurs bien établis. L'une d'entre elles a confirmé que sa clé avait été utilisée en production.

Demandez à Claude Code de vérifier une base de données ou d'appeler une API, et la commande qu'il propose contient le secret issu de votre fichier de configuration. Il vous demande votre accord avant de l'exécuter. Si vous choisissez « *Oui, et ne plus me le demander* », il enregistre cette commande exacte, secret compris, dans le fichier .claude/settings.local.json situé dans le dossier du projet. Rien dans le dépôt n'indique que ce fichier est privé ; il est donc validé avec le reste du code. Sur les 104 185 copies publiques de ce fichier sur GitHub, 1 122 contiennent un véritable secret. Nous en avons trouvé 1 160 autres dans l'historique Git, dans le fichier settings.json partagé que les équipes valident intentionnellement, ainsi que dans les transcriptions de discussions d'agents enregistrées dans les dépôts.

Source : Apiiro

Et vous ?

- Pensez-vous que cette information est crédible ou pertinente ?
- Quel est votre avis sur le sujet ?

Voir aussi :

- Une faille critique dans Claude Code est apparue après la fuite du code source : Anthropic a d'abord divulgué le code source de Claude Code, puis une faille critique a été découverte par Adversa AI
- Un agrégat de données de 16 milliards d'identifiants de connexion provenant de fuites antérieures a été divulgué en ligne, la CNIL confirme qu'il n'y a pas de nouvelle brèche, mais alerte sur les risques
- ChatGPT divulgue les mots de passe des conversations privées de ses utilisateurs. OpenAI tente de minimiser le problème en évoquant le piratage de compte mais cette explication présente des limites

Publication de communiqués de presse en informatique. Contribuez au club : corrections, suggestions, critiques, ... **Contactez le service news** et **Rédigez des actualités**

Responsable des Études & Développements Informatiques H/F
↳ SPIRICA - Ile de France - Paris (75001)

Experte / Expert produit éditique
↳ LA BANQUE POSTALE - France - Gradignan

Voir plus d'offres

Discussions similaires

Azure AD Password Protection, la fonctionnalité de protection des mots de passe d'Azure AD
Par Jonathan dans le forum Microsoft Azure
Réponses: 8
Dernier message: 21/05/2019, 15h30

Classement des mots de passe les plus utilisés : 123456 en tête suivi de 123456789 et qwerty
Par Hinault Romaric dans le forum Actualités
Réponses: 82
Dernier message: 11/02/2019, 10h21

Plus grand n'est pas forcément synonyme de mieux en matière de sécurité des mots de passe
Par Christian Olivier dans le forum Sécurité
Réponses: 0
Dernier message: 02/10/2018, 13h46

Les cinq fonctionnalités les plus intéressantes de Microsoft Office Mobile 2010
Par Djug dans le forum Actualités
Réponses: 0
Dernier message: 23/11/2009, 13h55

fonctionnalités en plus passage XI R2 -> XI 3.0
Par leeloo75 dans le forum Débuter
Réponses: 1
Dernier message: 23/09/2008, 21h15

Partager

© 2000-2026 - www.developpez.com