Sécurité : les développeurs Rust alertés sur leurs clés API

Développeurs Rust, vous allez devoir créer de nouvelles clés API sur crates.io*.

Le groupe de travail chargé de piloter la sécurité du langage de programmation et de son écosystème a fait cette annonce mardi 14 juillet.

En cause, deux problèmes, aujourd'hui résolus. D'un côté, les clés API étaient stockées en clair. De l'autre, elles dépendaient d'un générateur de nombres aléatoires insuffisamment sécurisé.

Le générateur en question était une fonction PostgreSQL. Un membre de la communauté Rust a constaté qu'en prenant connaissance de suffisamment d'informations, un tiers avait la possibilité de déterminer toutes les clés API générées depuis le dernier redémarrage du serveur de base de données.

> *I found an issue in Rust's package manager. API tokens were generated with a non-secure PRNG and could be predicted, which would allow an attacker to upload malicious packages. Great response from the Rust Security WG!https://t.co/e46S1b9F9M*
>
> *— Jacob H-A (@j4cob) July 14, 2020*

Les modifications nécessaires ont été effectuées pour basculer vers un générateur « sécurisé ». Et pour éviter le stockage en clair (implémentation d'un système de hachage).

Le ton de l'alerte est rassurant. Officiellement, il n'y a pas de traces d'une quelconque attaque et il aurait été « très difficile » d'en lancer une.

** crates.io est le registre officiel des paquets qu'a créées la communauté Rust. Il en regroupe environ 43 000, pour plus de 3,3 milliards de téléchargements.*