Des chercheurs exfiltrent une clé privée RSA-1024 d'un logiciel de chiffrement

Une équipe de chercheurs de plusieurs universités a trouvé un bug dans une bibliothèque de chiffrement Open Source donnant les moyens à un attaquant d'extraire la clé privée RSA-1024 utilisée pour chiffrer les données locales.

Les travaux étaient axés sur GnuPG, un logiciel de chiffrement pour Android, Linux, MacOS et Windows. Plus précisément, les chercheurs ont concentré leurs efforts sur Libgcrypt, le module de GnuPG en charge des opérations de chiffrement. Les universitaires se sont appuyés sur la méthode dite de « fenêtre coulissante » permettant d'effectuer des calculs sur des équations mathématiques en arrière-plan du chiffrement des données. Le hic, selon les experts, est que cette méthode de calcul est aussi réputée pour laisser filer des données, dont des bits de la clé privée de chiffrement.

Une attaque par canal auxiliaire non corrigée

Ce bug a été en partie corrigé par l'équipe de Libgcrypt sur 2 des 3 attaques capables de s'emparer d'un bout de la clé privée. La dernière attaque avait été jugée bénigne, car elle ne divulguait qu'une partie de la clé privée. Ainsi, les implémentations de Libgrcrypt qui utilisent des « fenêtres coulissantes de 4 bits à droite et à gauche » émettent 40% de la clé privée, alors que les « fenêtres coulissantes de 5 bits à droite et gauche » ne laissent fuiter que 33% de la clé.

Fort de cette découverte, les chercheurs ont mis au point un algorithme pour récupérer l'ensemble de la clé privée RSA-1024 à partir de ces informations éparses. Une fois ce précieux sésame en main, un attaquant peut aisément lire les fichiers locaux, les courriels, les sauvegardes. Les spécialistes de sécurité ont signalé leurs résultats à l'équipe GnuPG afin qu'elle corrige ce problème. Chose faite avec la publication de Libgcrypt 1.7.8 bloquant cette nouvelle attaque par canal auxiliaire. Le patch a été porté sur différentes distributions Linux comme Debian et Ubuntu. Les responsables de GnuPG ont minimisé l'importance du bug en rappelant que l'attaque exige que le pirate puisse accéder à l'équipement où la clé RSA est utilisée.

A lire aussi :

Communication quantique : plus fort que le chiffrement de bout en bout ?

France et Royaume-Uni s'attaquent au chiffrement… sans livrer la clef

Crédit Photo : Den Rise-Shutterstock