# Une faille du WiFi d'Android dévoile les données personnelles

Le Wifi de Google Android refait parler de lui pour ses indiscrétions. Après le scandale de 2012 où les Google Car chargées de prendre des photos pour Street View sniffaient des données privées des réseaux Wifi environnants (lire Street View : Google se défausse sur « l'ingénieur Doe »), la problématique porte cette fois sur la fonctionnalité '**Preferred Network Offload**'. Celle-ci permet aux terminaux Android de maintenir en permanence une liaison Wi-Fi active en se connectant aux réseaux «cachés» (ne diffusant pas leur SSID). Cette fonctionnalité sert notamment à améliorer le service de géolocalisation du terminal. Bien pratique, elle est néanmoins dans le collimateur de l'Electronic Frontier Foundation (EFF), rapporte *ITespresso.fr*.

## Fuite de données de localisation

L'association américaine de défense des libertés civiles vise plus particulièrement la composante Open Source '**wpa_supplicant**', que de nombreuses distributions Linux – dont l'OS mobile de Google – exploitent pour gérer et sécuriser les échanges de données avec des points d'accès sans fil. Celle-ci serait, sur la plupart des appareils équipés d'Android 3.1 «Honeycomb» ou des versions supérieures, à l'origine d'une faille entraînant la fuite de données de localisation quand le terminal est en mode économie d'énergie (écran éteint) et qu'il n'est n'est pas connecté à un réseau WiFi.

C'est la recherche automatique de points d'accès effectuée en arrière-plan qui pose problème. Afin d'accélérer la connexion, l'appareil analyse les réseaux sans fil situés à sa portée et cherche à reconnaître ceux auxquels il a déjà été associé par le passé – et dont il peut éventuellement connaître la clé de chiffrement si l'utilisateur a choisi de la mémoriser. Pour ce faire, il diffuse tous les SSID qu'il a enregistrés… mais sans chiffrer les données. Une absence de sécurisation des données qui les mettent **à portée des premiers curieux connectés à un réseau Wi-Fi** suffisamment proche pour les capter.

## iOS 8 également concerné

Jusqu'à 15 SSID peuvent ainsi être transmis. Ces données sont d'autant plus critiques qu'elles sont directement intelligibles par l'humain et qu'il existe de nombreux services Web permettant de localiser les points d'accès Wi-Fi dans le monde. Elles fournissent également des **indications assez précises sur les lieux fréquentés par l'utilisateur**. Ce qui peut poser problème en matière de confidentialité sur ses déplacements, son emploi du temps, etc. Un problème qui se pose également avec iOS 8 et son système d'adresse MAC («Media Access Control») dynamique.

Conscient du problème, **Google réfléchit à la meilleure façon de le corriger**. «*Une modification [de Preferred Network Offload] perturberait la connexion aux points d'accès masquant leur SSID*», confie un porte-parole de Google interrogé par l'EFF. Et d'ajouter: «*Nous prenons très au sérieux la sécurité des données de géolocalisation de nos utilisateurs.*»

# Désactiver le WiFi en veille

Jeudi dernier, un employé de la firme de Mountain View a publié **un correctif** pour wpa_supplicant. Mais il faudra du temps pour l'intégrer dans le code d'Android tout en composant avec la fragmentation de l'écosystème (de multiples versions de l'OS se partagent le marché). Pour les utilisateurs, il existe une solution temporaire : désactiver le maintien de la connexion Wi-Fi en veille. Mais la consommation de données cellulaires augmentera et l'autonomie de la batterie diminuera. Et ne pas oublier de purger manuellement l'historique des connexions dans les paramètres sur les appareils qui le permettent.

crédit photo © Brian A Jackson – shutterstock

---

**Lire également**

Cupidon injecte la faille Heartbleed dans les routeurs WiFi et Android

Sécurité : neuf applications mobiles sur dix sont vulnérables