

Panoptinet

Gardez un oeil sur votre réseau

Une faille de sécurité sur 99% des Android

admin · Thursday, May 19th, 2011



Une étude universitaire allemande (Ulm) dévoilait la semaine dernière une faille de sécurité qui pourrait concerner 99% des smartphones Android. Cette faille peut permettre à des hackers de se connecter à certaines applications sur votre mobile et de manipuler vos données personnelles. Voici comment éviter une telle intrusion.

C'est une faille dans le **processus d'authentification** qui a été percée à jour : lorsque l'on se connecte à certaines applications comme Agenda, Contacts ou Picasa, **Android conserve l'identifiant et le mot de passe pendant 14 jours**. Si l'accès à ces services est réalisé à partir d'une connexion non sécurisée (non HTTPS) comme par exemple un hotspot Wi-Fi, les données d'identification peuvent être **récupérées par un hacker**, qui peut alors les utiliser comme il l'entend : lecture, modification, copie, effacement.

Les utilisateurs Android se connectant avec une **version 2.3.3 ou antérieure** du système mobile Google (Cupcake, Donut, Eclair, FroYo ou une des premières versions de Gingerbread) sont concernés. **Soit près de 99% mobinautes Android !** A la suite de cette annonce, Google a déjà déployé des **correctifs de sécurité** concernant Contacts et Agenda. Un patch pour Picasa devrait être disponible lors des prochains jours.

Comment les utilisateurs Android peuvent éviter la fuite de données

Bien que Google devrait prochainement n'autoriser que les connexions HTTPS pour ces applications, et réserver la connexion Wi-Fi automatique pour les réseaux protégés seulement, les utilisateurs peuvent également agir de leur propre chef :

- **Mettre à jour son Android** en version 2.3.4 dès que possible. Malheureusement, les opérateurs mobiles (Orange, SFR, Bouygues Telecom, etc.) proposent des versions "repackagées" d'Android. Les mises à jour sont par conséquent très tardives : il faut souvent attendre plusieurs semaines ou mois après la mise à jour officielle du système.
- **Désactiver la connexion Wi-Fi automatique** aux réseaux ouverts (hotspots) dans le

menu Paramètres.

- **Laisser le smartphone "oublier" les réseaux Wi-Fi non-protégés** auxquels il s'est connecté par le passé (Paramètres < Sans fil et réseaux < Appui long sur un nom de réseau < "Oublier").
- **Eviter les connexions Wi-Fi** lors de l'utilisation des applications incriminées.

Comment connaître ma version d'Android ?

Si vous souhaitez savoir votre version d'Android pour éventuellement prendre les mesures qui s'imposent, il suffit de consulter votre smartphone :

- Paramètres
- A propos du téléphone
- Version d'Android : la faille décrite dans cet article concerne les versions antérieures à 2.3.4

Dans tous les cas, smartphone, ordinateur ou tablette, rappelez-vous que **se connecter en Wi-Fi sur un hotspot compromet sérieusement toutes les informations** que vous échangez dans les airs : connexions, identifiants, envois de mails, etc. Si vous avez le choix, préférez toujours une connexion sécurisée ! Ou alors, prenez le temps de lire notre fiche [En toute sécurité sur un hotspot](#).

Sources :

[uni-ulm.de](#)

[menly](#)

[clubic](#)

This entry was posted on Thursday, May 19th, 2011 at 10:55 am and is filed under [Autres actualités](#)

You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can leave a response, or [trackback](#) from your own site.