# Un milliard de terminaux Android touchés par une faille de sécurité sans précédent

Une faille de sécurité de grande ampleur a été découverte dans le système d'exploitation mobile Android par un groupe composé de **chercheurs de l'université de l'Indiana et de Microsoft** (lien vers leur publication).

Cette vulnérabilité concerne **le système de mise à jour de l'OS**, affublé ici d'une faiblesse architecturale qui permet une élévation de privilèges des logiciels lors de la mise à niveau du système.

Les '**Pileup flaws**' fonctionnent de façon simple. Imaginons une application Android qui a besoin de certains droits pour accéder aux nouvelles fonctions de géolocalisation. Ces fonctionnalités ne sont apparues qu'avec Android 4.3

L'application est installée sur un terminal Android 4.2, qui n'a pas à gérer cette permission, car elle n'existe pas sur cette version de l'OS. Aussi, le système ne signale pas ce point à l'utilisateur. Toutefois, lors de la mise à jour du terminal vers Android 4.3, **l'autorisation sera automatiquement accordée à l'application**. C'est ici que réside la faille trouvée par les chercheurs.

## Plus d'un milliard de terminaux concernés

À ce jour, **toutes les versions d'Android sont concernées** par cette vulnérabilité, et plusieurs applications tentent de l'exploiter. L'ensemble des terminaux Android serait donc potentiellement touché. Potentiellement seulement, car de nombreuses permissions existent depuis les versions les plus anciennes d'Android : appels, SMS, accès aux fichiers système, etc.

Il est à noter également que les applications ne font ici qu'obtenir des droits que vous leur auriez probablement accordées. Le problème est que **l'utilisateur n'en est pas averti lors de l'installation**. En aucun cas la barrière qui isole les applications du système n'est compromise.

Malgré tout, le risque reste bien réel. Ainsi, entre Android 4.0 (API Level 14) et Android 4.4 (API Level 19) sont apparus les droits de se lier à un service NFC, d'accéder au dictionnaire utilisateur, de lire et écrire dans un flux social, de géolocaliser le terminal, ou encore de demander à une application de répondre à un appel (source).



---

**Voir aussi**

Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales