Plus de 50% des apps populaires sur Android réutilisent du code faillible

Plus de la moitié des applications Android les plus populaires auraient hérité de failles de sécurité à la suite d'**une réutilisation « inconsidérée » de bibliothèques logicielles**, d'après les ingénieurs de Codenomicon. Ces derniers ont découvert, en avril 2014, la vulnérabilité « Heartbleed » dans la librairie de chiffrement OpenSSL.

Transfert de données personnelles à des tiers

Au moins **50% des applications Android** concernées transmettraient des données personnelles à des réseaux publicitaires tiers sans autorisation de l'utilisateur, et ce en texte clair dans 30% des cas. Par ailleurs, une application sur dix enverrait l'identifiant du terminal mobile (code IMEI) ou des données de géolocalisation à une tierce partie, voire le numéro de téléphone mobile de l'utilisateur. De plus, une application sur dix serait connectée à plus de deux réseaux de publicité.

D'après Codenomicon, entreprise finlandaise spécialisée dans la sécurité informatique, la plupart des développeurs de ces applications n'ont pas connaissance des vulnérabilités qu'ils ont intégré au code. Un développement hasardeux ou des erreurs de logique peuvent être à l'origine d'une vulnérabilité. Malgré tout, des développeurs peuvent aussi agir intentionnellement dans le but de **rendre l'application logicielle vulnérable aux attaques**. Ces bugs sont parfois rapidement identifiés et corrigés, d'autres, comme dans le cas de Heartbleed, ne le sont pas pendant deux ans, observent les analystes.

Enfin, **80% à 90% des applications mobiles**, dans leur ensemble, intègrent des bibliothèques logicielles réutilisées, disponibles pour la plupart en **open source**, a estimé Olli Jarva, Chief Security Specialist chez Codenomicon, dans les colonnes du magazine australien *ITnews*. La pratique devrait théoriquement permettre à la communauté de développeurs de proposer du code de meilleur qualité, du fait du nombre important de contributeurs impliqués. Mais les nombreux bugs identifiés dans OpenSSL ont démontré, selon Codenomicon, que cela n'était pas le cas.

crédit photo © Androgen – Fotolia.com

Lire aussi

Google migre Chrome vers BoringSSL, dérivé d'OpenSSL