Faille TCP : 80 % des terminaux Android sont touchés

Environ 8 terminaux Android sur 10 sont concernés par la faille TCP dévoilée la semaine dernière, dans le cadre de la conférence Usenix. Soit environ 1,4 milliard de machines dans le monde. Rappelons que, lors de cette conférence spécialisée sur la sécurité, des chercheurs de l'Université de Californie et du laboratoire de recherche de l'armée américaine ont montré comment cette faille, née de l'implémentation d'un nouveau standard (RFC 5961) sous Linux, permet à un assaillant d'identifier des machines communiquant entre elles via TCP et, dans tous les cas, de mettre fin à cette connexion. Si les échanges ne sont pas chiffrés, l'assaillant peut même injecter des contenus frauduleux au sein de la communication.

Présente dans Linux depuis la version 3.6 du noyau, sortie en 2012, cette vulnérabilité accompagne également un grand nombre de moutures d'Android, depuis la version KitKat (4.4), selon les chercheurs de Lookout, une société spécialisée dans la sécurité des terminaux mobiles. Une conséquence assez logique, l'OS mobile exploitant le noyau Linux. Pour le chercheur en sécurité de Lookout, Andrew Blaich, si d'autres failles Android comme Stagefright ou Quadrooter pouvaient être plus critiques, l'attaque décrite par les chercheurs s'avère pratique et à la portée de bon nombre de hackers.

La version Nougat est aux fraises

Présentée dans un article de recherche intitulée « *Off-Path Exploits : Global Rate Limit Considered Dangerous* », la faille ne nécessite pas qu'un assaillant se place sur le chemin de la connexion (contrairement à une attaque dite Man-in-the-Middle). Par ailleurs, il suffit qu'une des deux extrémités de la connexion soit sensible au bug pour rendre l'échange piratable. Le fait qu'une large part des terminaux fonctionnant sur l'OS mobile le plus déployé au monde soit concernée par la faille ne fait donc qu'accroitre un potentiel déjà important, en raison du poids de Linux sur les serveurs Web. D'autant que les processus de mises à jour sur Android sont plus aléatoires que sur Linux, géré très souvent par des administrateurs professionnels.

A ce jour, un patch comblant la vulnérabilité *Off-Path* (CVE-2016-5696) a bien été produit pour Linux, même s'il n'est pas encore intégré aux principales distributions. Côté Android, selon Andrew Blaich, le correctif n'est pas présent dans les dernières versions développeurs de la version Nougat (Android 7). Ni évidemment dans les moutures de l'OS déployées parmi les terminaux actuellement en vente. Rappelons que les mises à jour de sécurité d'Android passent par les opérateurs et fabricants de terminaux, chargés de déployer les patchs. Seules les machines Nexus, fournies par Google, bénéficient du téléchargement automatique mensuel des correctifs.

Déployer des VPN

« *Si vous faites tourner un parc mobile en entreprise, un certain nombre de terminaux Android sont potentiellement vulnérables à cette forme d'espionnage* », écrit Andrew Blaich, dans un billet de blog. Et

ce dernier de recommander aux RSSI de vérifier que l'ensemble des échanges de données confidentielles de leur entreprise (comme ceux véhiculés par mail) sont bien chiffrés. Et de recourir à un VPN en cas de besoin. Lookout suggère également une solution plus technique (changer la valeur limite d'ACK, l'élément qu'ont exploité les chercheurs), permettant de rendre l'attaque plus difficile.

A lire aussi :

Une faille de sécurité dans TCP permet de pirater la plupart des sites Web

Comment le Machine Learning aide à débusquer les failles de sécurité

© Carlos Amarillo-Shutterstock