# Google corrige les failles logées dans les composants électroniques pour Android

Le bulletin de sécurité d'Android pour ce mois de juin est plutôt chargé. Sur les 21 failles de sécurité corrigées, 6 sont considérées comme critiques et 11 jugées sérieuses. Dans la plupart des cas, les vulnérabilités critiques permettent l'exécution de code à distance sur le terminal affecté par le biais de multiples vecteurs comme l'e-mail, la navigation web et les MMS, quand ils exécutent des fichiers média.

Google met notamment l'accent sur des failles constatées dans les composants électroniques de plusieurs fournisseurs. Qualcomm est particulièrement concerné à travers les pilotes de ses composants vidéo, son et graphiques (GPU). Son concurrent Broadcom est affecté à travers le driver Wifi de son modem sans fil. Les composants de Nvidia et Mediatek ne sont guère mieux lotis. Bref, les principaux fournisseurs de puces pour smartphones sont touchés. Autant dire que les smartphones non concernés par cette nouvelle vague de failles de sécurité doivent se faire rares.

## Mediaserveur affecté de toutes parts

Par ricochet, les vulnérabilités qui touchent le Mediaserveur sont également légion. Elles permettent à un attaquant exploitant un fichier infectieux de provoquer une corruption de la mémoire au cours de la lecture d'une vidéo ou d'un fichier son. Ce qui est d'autant plus problématique que le Mediaserveur dispose de privilèges sur le système que n'ont généralement pas les applications tierces.

Tous les smartphones Nexus de la firme de Mountain View sous Android (versions 4.4.4, 5.0.2, 5.1.1, 6.0 et 6.0.1) sont sensibles à l'ensemble des brèches de sécurité de juin. Mais ses heureux utilisateurs auront la chance de bénéficier d'une mise à jour par les airs (OTA), ce qui devrait leur permettre de ne pas rester longtemps à découvert.

## Mise à jour recommandée pour Android

Ce n'est pas forcément le cas des autres utilisateurs pour qui les mises à jour d'Android dépendent des constructeurs de smartphones (qui doivent générer la nouvelle image corrigée d'Android) et des opérateurs (qui la distribuent). Google a livré cette mise à jour le 2 mai dernier à ses partenaires tels Samsung, LG ou HTC. Dans les 48 heures suivant la diffusion du bulletin de sécurité, l'éditeur verse ensuite le nouveau code à l'Android Open Source Project (AOSP), en direction des constructeurs non directement partenaires.

Google déclare ne pas avoir eu de retour sur d'utilisateurs piratés via l'exploitation de vulnérabilités ou avoir eu connaissance d'attaques massives. Mais, dans tous les cas, la firme recommande de mettre à jour les smartphones potentiellement friables dans les meilleurs délais.

**Lire également**

Une vulnérabilité vieille de 5 ans menace des millions de terminaux Android
Le mediaserver d'Android : un nid de failles de sécurité
WiFi et Mediaserver : Google colmate les trous de sécurité d'Android

**crédit photo © Asif Islam / Shutterstock.com**