

# Le mediaserver d'Android : un nid de failles de sécurité

Une autre faille de sécurité affectant la façon dont Android gère les fichiers multimédia vient d'être [mise en évidence par Trend Micro](#). Logée **dans une fonction du mediaserver appelée AudioEffect**, elle permet à une application malicieuse d'effectuer des actions non autorisées. L'exploit détaillé par l'éditeur de solutions de sécurité repose sur une erreur de programmation dans ce composant qui, faute de vérifier la taille des mémoires tampon des logiciels clients (comme les players multimédia), permet à une application conçue à cet effet d'accéder aux fonctions normalement réservées au mediaserver : prise de photos, enregistrement de vidéos, lecture de fichiers MP4, notamment. L'utilisateur devrait toutefois installer cette app pernicieuse pour que l'attaque puisse avoir lieu.

Selon les chercheurs de Trend Micro, la faille (étiquetée [CVE-2015-3842](#)), qui affecte toutes les versions d'Android depuis la 2.3 jusqu'à la 5.1.1, a été signalée à Google en juin. Un correctif, produit par Mountain View et [publié par l'Android Open Source Project](#) le 1<sup>er</sup> août, est disponible et doit désormais être intégré par les constructeurs de smartphones, afin de mettre à jour le gigantesque parc de terminaux Android.

## Un premier correctif... inutile

Les mécanismes de mises à jour d'Android restent perfectibles, même si [la mise au jour d'une autre faille - Stagefright](#) -, affectant elle-aussi les processus de gestion des média, a forcé les constructeurs à réagir. Stagefright, qui permet l'exécution de code à distance après envoi d'un MMS piégé, a été dévoilé fin juillet et détaillé lors de la conférence Blackhat le 5 août dernier. Depuis, plusieurs constructeurs de smartphones ont poussé le correctif vers leur base installée. Et ce, même si ce dernier [s'est avéré finalement inefficace](#), obligeant Google à produire un second patch. Celui-ci serait aujourd'hui entre les mains des partenaires du géant de Mountain View.

L'écosystème Android devra de toute façon s'y habituer. Tant Joshua Drake, le chercheur à l'origine de la découverte de Stagefright, que Trend Micro ont averti que les processus de gestion des fichiers multimédia de l'OS mobile sont susceptibles de renfermer de nombreuses vulnérabilités. La dernière faille découverte par Trend Micro est la quatrième faille touchant le composant mediaserver d'Android dévoilée en quelques semaines.

### A lire aussi :

[Une faille Android permet de remplacer une application légitime par une autre](#)  
[Certifi-gate, la faille qui ouvre les portes d'Android](#)  
[Android, un OS mobile sacrément fragmenté](#)

**Crédit Photo : Zeynep Demir-Shutterstock**