

WiFi et Mediaserver : Google colmate les trous de sécurité d'Android

Depuis août 2015, **Google** diffuse, sur le modèle de Microsoft avec le Patch Tuesday, un ensemble de correctifs à destination des terminaux Android : le **Nexus Security Bulletin**. Avec 13 failles colmatées, dont 7 critiques, la [fournée de février 2016](#) est dans la moyenne (le record du mois d'octobre tient toujours, avec 21 vulnérabilités critiques sur 30 résorbées).

Les informations avaient été communiquées en amont aux partenaires constructeurs ; en l'occurrence, le 4 janvier. La mise à jour est distribuée aux utilisateurs finaux depuis ce mercredi.

WiFi et Mediaserver sur la sellette

Deux failles de la plus haute importance (CVE-2016-0801 et CVE-2016-0802) se trouvent dans le pilote associé aux puces WiFi de Broadcom. Elles peuvent permettre à un tiers connecté sur le même réseau d'envoyer des données pour corrompre la mémoire et exécuter du code avec le niveau de privilèges maximal.

La composante Mediaserver, qui analyse les fichiers audio et vidéo, est également touchée. Elle abrite deux failles critiques (CVE-2016-0803 et CVE-2016-0804) qui peuvent entraîner une corruption de mémoire via un fichier spécialement conçu (notamment un MMS)... puis la prise de contrôle, à distance, de nombreuses fonctionnalités du terminal.

Le module de mesure de performances pour les puces ARM de Qualcomm est également exposé, à travers la vulnérabilité

CVE-2016-805, qui peut permettre l'exécution de code via une application malveillante. Un appareil pourrait être mis hors service par ce biais. Le même danger existe avec les failles CVE-2016-0806 (dans le pilote WiFi Qualcomm) et CVE-2016-0807 (dans le débogueur).

Des failles mineures classées importantes

Quatre failles sont classées comme « importantes », à défaut d'être référencées comme « critiques » : CVE-2016-0808 (dans Minikin, pour la gestion des polices de caractères), qui peut bloquer temporairement l'accès à un appareil ; CVE-2016-0809 (dans la gestion du WiFi), CVE-2016-0810 (dans Mediaserver) et CVE-2016-0811 (dans la bibliothèque *libmediaplayerservice*), qui permettent de contourner certaines défenses d'Android.

Les failles CVE-2016-0812 et CVE-2016-0813 sont d'une importance « modérée ». Elles se trouvent dans l'assistant d'installation et permettent de réinitialiser un appareil, conclut nos confrères d'[ITespresso](#).

A lire aussi :

[Faible zero day : des millions de serveurs Linux et 66 % du parc Android exposés](#)

[Près de 6 400 nouveaux malwares Android par jour](#)

Crédit Photo : Twin Design-Shutterstock