Stagefright sème la terreur sur les terminaux Android

Stagefright n'est plus seulement une bibliothèque logicielle utilisée sur **Android** pour lire plusieurs formats de fichiers vidéo. C'est désormais aussi le nom d'une attaque informatique exploitant plusieurs **failles de sécurité** présentes dans cette même bibliothèque.

Les révélations de Joshua J. Drake à ce sujet ont eu l'effet d'une bombe. Ce chercheur chez Zimperium Mobile Labs reviendra plus en détail sur ses travaux début août dans le cadre de la conférence Black Hat USA. Mais il a d'ores et déjà donné le ton : jusqu'à 95 % des smartphones Android pourraient être affectés.

Stagefright abriterait pas moins de sept vulnérabilités répertoriées CVE-2015-1538 à CVE-2015-3829 et non encore décrites, le temps que des correctifs soient diffusés à grande échelle.
L'une des méthodes d'exploitation de ces brèches ne requiert ni un accès physique à l'appareil ciblé, ni même de tromper la vigilance de l'utilisateur en lui faisant ouvrir un quelconque fichier ou installer une application.

Un MMS diabolique

Il suffit en l'occurrence de connaître son numéro et de lui envoyer, par MMS, un message vidéo spécialement conçu pour contourner les mécanismes de protection d'Android (*sandbox*) et permettre l'exécution de code à distance.

À ce moment-là, les pirates ont accès à presque tout sur le téléphone, de l'appareil photo au microphone en passant par la mémoire de stockage. Pire : le contenu du MMS est souvent traité sans même que l'utilisateur l'ouvre. Et les traces peuvent généralement être effacées dès l'attaque exécutée. Seule reste la notification, que l'utilisateur supprimer généralement sans y porter d'attention particulière.

Les versions d'Android les plus vulnérables sont tout simplement les plus anciennes (2.2 « Froyo », 2.3 « Gingerbread », 4.0 « Ice Cream Sandwich »), car elles ne bénéficient pas des couches de protection adéquates. Zimperium a toutefois constaté que les systèmes plus récents – dont Android 5.1.1 « Lollipop » n'étaient pas épargnés.

Ayant communiqué la vulnérabilité à Google en l'accompagnant d'un patch, Joshua J. Drake a été récompensé à hauteur de 1 337 dollars. Le correctif a été appliqué et peut dorénavant être déployée par une mise à jour OTA, précise ITespresso.

Problème : c'est aux constructeurs d'assurer la diffusion. Ce qui n'est pas gagné, a fortiori pour les plus vieux téléphones (11 % des terminaux Android tournent encore sous une version antérieure à la 4.1).

A lire aussi :

Hacking Team : la résurgence de RCS Android inquiète les experts

Gunpoder : encore une nouvelle famille de malwares pour Android

crédit photo © Creativa Images – shutterstock