Sécurité : la faille Stagefright revient et s'en prend à Android 5.0

La faille Stagefright fait son retour (si tant est qu'elle ait vraiment disparu des radars). Joshua Drake qui, en juillet dernier, avait dévoilé la vulnérabilité touchant potentiellement 1 milliard de terminaux Android, a découvert de nouvelles brèches dans l'OS mobile, même après que celui-ci ait été patché.

Le chercheur et vice-président de Zimperium Mobile Labs fait remonter deux nouvelles failles à la surface : la première concerne Android depuis sa conception, la seconde repose sur une vulnérabilité introduite dans Android 5.0 « Lollipop », jusqu'à présent relativement épargné. Ce n'est guère surprenant. Lors de la présentation de la vulnérabilité à la Black Hat de Las Vegas en août dernier, Joshua Drake précisait que d'autres problèmes exploitant des mécanismes proches de Stagefright 'épisode 1' avaient été découverts et que *« l'histoire [était] loin d'être terminée »*.

Prise de contrôle distant du terminal

Les risques découlant de ce que l'on appellera désormais Stagefright 2.0 sont quasiment identiques à ceux de la précédente version. A savoir l'accès aux données et fonctions du terminal qui recevrait un SMS ou un message Hangout conçu à des fins malveillantes. Et ce, sans même que l'utilisateur n'ait à l'ouvrir (une simple prévisualisation suffit). Rappelons que la faille touche la bibliothèque éponyme d'Android permettant de lire plusieurs formats de vidéo. Le chercheur de Zimperium avait constaté qu'il était possible de contourner les mécanismes de protection d'Android (la *sandbox*) et d'exécuter du code à distance en faisant lire par le terminal une simple vidéo corrompue au niveau des métadonnées. En cas de succès de l'attaque, les assaillants pouvent alors accéder à la mémoire de stockage de l'appareil, à l'appareil photo, au microphone ou encore installer d'autres applications sans que l'utilisateur ne s'en rende compte… Un vrai cauchemar.

Le correctif de Google avait consisté à interdire le traitement automatique du fichier vidéo corrompu par la librairie laissant à l'utilisateur le risque d'en lancer lui-même la lecture. Mais, pour Zuk Avraham, président et fondateur de Zimperium cité par *Treathpost*, il suffit de pousser l'utilisateur à ouvrir un fichier vidéo corrompu sur une page web (via le navigateur du smartphone) par des méthodes de phishing. On peut aussi imaginer des méthodes d'attaque de type Homme-du-milieu (man-in-the-middle) exploitant la faille ou, plus classiquement, de pousser l'*exploit* depuis une application tierce, indique la société de sécurité.

Car rien n'a été corrigé au niveau de la bibliothèque Stagefright. *« La bibliothèque elle-même est très vulnérable ; elle renferme beaucoup d'erreurs de codage*, déclare Zuk Avraham à nos confrères américains. *Le traitement des média n'est pas aussi sûr qu'il devrait l'être. »* Référencée CVE-2015-6602, la première vulnérabilité touche Android depuis sa version initiale, via le composant libutils. L'autre faille, qui n'a pas encore de CVE assigné, a été introduite dans libstagefright d'Android 5.0, qui fait appel à libutils de manière vulnérable. Selon Zimperium, un fichier MP3 ou MP4 corrompu suffit donc à exploiter la vulnérabilité en question.

Une vulnérabilité appelée à durer

A moins de réécrire Stagefright, les vulnérabilités propres à cette bibliothèque d'Android risquent de perdurer. *« Déterminer toutes les manières possibles dont un composant de bibliothèque de base a été utilisé à travers l'écosystème Android est une tâche insurmontable*, explique Zimperium dans une FAQ. *Chaque morceau de code qui utilise la bibliothèque vulnérable doit être inspecté pour voir si elle appelle une API au sein de libutils de façon non sécurisée. Ensuite, chaque utilisation potentiellement vulnérable devra être inspectée et analysée individuellement. »* La faille Stragefight n'a probablement pas fini de faire parler d'elle.

En raison des risques qu'elles font peser, ces vulnérabilités n'ont pas été rendues publiques. Alerté dès le 15 août, Google a déclaré à *Treathpost* qu'un correctif avait été livré à ses partenaires constructeurs le 10 septembre dernier. A eux de le diffuser auprès de leurs utilisateurs finaux. De son côté, Mountain View corrigera la faille pour ses Nexus à l'occasion de la prochaine mise à jour mensuelle le 5 octobre prochain. Il restera à vérifier l'efficacité de ce nouveau correctif. Le précédent avait facilement été contourné comme l'avait démontré Jordan Gruskovnjak, chercheur en sécurité chez Exodus, en août dernier.

Lire également
Des smartphones Android vendus en ligne avec des malwares préinstallés
Le mediaserver d'Android : un nid de failles de sécurité
Une faille Android permet de remplacer une application légitime par une autre