Stagefright, de retour, menace des millions de terminaux Android

Google n'en a visiblement pas fini avec Stagefright. Des chercheurs de la société israélienne NorthBit affirment avoir réussi à exploiter pleinement la vulnérabilité dévoilée en juillet 2015 par Zimperium et qui touche la majorité des terminaux sous Android. Elle est considérée comme le pire des bugs de l'OS mobile. Exploitée, la faille donne notamment accès à certaines données du smartphone affecté et permet l'exécution de code à distance. Stagefright (ou plus exactement Libstagefright) est une bibliothèque Android écrite en C++ dont les bugs permettent de corrompre la mémoire à partir de la lecture d'un fichier multimédia (MP3, MP4) compromis.

Une vidéo postée par NorthBit présente l'attaque en question baptisée Metaphor. On y voit comment un pirate récupère des données du terminal mobile après que son utilisateur ait activé un lien vers une vidéo. Son exécution a été réalisée sur un modèle Nexus 5 sous Android 5.0.1. Mais, selon nos confrères de *Wired*, les chercheurs sont parvenus au même exploit sur un LG G3, un HTC One et un Samsung Galaxy S5. La société de sécurité a présenté l'ensemble de ses travaux dans un document PDF posté du GitHub. Ils ont notamment travaillé sur les versions 2.2 à 4.0 et 5.0 et 5.1 d'Android à partir des travaux directement menés par Google, notamment ceux du Project Zero : Stagefrightened.

Une attaque rapide, efficace et discrète

« Bien que le bug existe dans de multiples versions ([implémentées] dans près d'1 milliard de terminaux), il était réputé quasiment inexploitable dans les faits, écrivent les auteurs du document, *essentiellement à cause des corrections apportées aux nouvelles versions d'Android, particulièrement ASLR. »* L'Address Space Layout Randomisation (ASLR), un processus de protection de la mémoire, a été délivré par Google pour les versions 5.0 et 5.1 d'Android. Ce qui laisse supposer que les utilisateurs sous ces environnements sont relativement protégés (contrairement à ceux des versions antérieures). *« Nous avons réalisé une attaque plus générique et pratique que les travaux précédemment publiés*, revendique les chercheurs, *et ce que nous entendons par « pratique » signifie rapide, efficace et discret. »* Comment ? En contournant tout simplement ASLR. Ce qu'ils s'empresse de décrire dans leur document.

En rendant public le pas à pas de cette nouvelle méthode d'exploitation de la librairie Stragefright, NorthBit prend le risque de permettre à des attaquants, cybercriminels ou gouvernements, de faciliter la prise de contrôle à distance de centaines de millions de terminaux Android. A ce jour, aucune attaque Stagefright n'est publiquement connue. Pour combien de temps encore ?

Lire également
Sécurité : la faille Stagefright revient et s'en prend à Android 5.0
Faille Stagefright d'Android : le patch de Google est troué
Stagefright sème la terreur sur les terminaux Android