Google corrige une faille critique OpenSSL vieille de 5 mois dans Android

Le bulletin de sécurité de mars corrige pas moins de 35 vulnérabilités critiques affectant Android, et une quarantaine classées comme «hautes». Un mois chargé, donc, pour la sécurité des smartphones opérés par l'OS de Google. Ce dernier en a profité pour corriger une faille vieille de cinq mois propre aux bibliothèques de chiffrement SSL.

Plus précisément, référencée CVE-2016-2182, la vulnérabilité en question est liée à OpenSSL, la solution de chiffrement Open Source dont la faille Heartbleed qui avait défrayée la chronique il y a bientôt trois ans. Elle touche également la solution maison BoringSSL de Google qui s'appuie sur OpenSSL, et peut être exploitée en forçant la bibliothèque à traiter un certificat trop long ou une liste de révocation de certificats à partir d'une source non approuvée.

Une faille précédemment corrigée par la communauté

Ce qui est étonnant, c'est que la faille OpenSSL avait été corrigée en septembre dernier par la communauté. Il aura donc fallu plus de cinq mois à Google pour implémenter le correctif dans Android. Un délai potentiellement justifié par le fait que les développeurs d'OpenSSL avaient considéré le risque d'exploitation comme bas alors qu'il n'affectait pas les connexions chiffrées TLS car *« les limites d'enregistrement rejettent un certificat surdimensionné avant son analyse »*, expliquent-ils selon ce que rapporte *ComputerWorld*.

Une analyse que ne partageait pas nécessairement Google qui craignait qu'un attaquant utilisant un fichier formaté pour exploiter la brèche de sécurité puisse causer une corruption de mémoire et ouvrir la voie à l'exécution de code malveillant avec les privilèges administrateur. Autrement dit, un risque considéré comme critique alors que l'exécution d'un tel code est en mesure de compromettre complètement l'intégrité du terminal.

Deux bulletins mensuels

Parmi les autres correctifs d'importance, soulignons ceux qui comblent les neuf trous de sécurité de Mediaserveur, le composant Android chargé du traitement des fichiers multimédia et régulièrement affecté de vulnérabilités depuis près de deux ans. Enfin, soulignons la correction du composant vérificateur de récupération système dont l'exploitation locale pouvait mener à obtenir les droits administrateur et l'accès au noyau de l'OS.

Comme c'est la règle depuis juillet 2016, Google sépare son bulletin de sécurité mensuel en deux éditions. Celles de mars sont datées du 1er et du 5. La première concerne les vulnérabilités propres à Android qui, dans ce cadre, affectent tous les smartphones sous l'OS de la firme de Mountain View (y compris les siens). Le second bulletin y ajoute les correctifs propres aux composants des

terminaux (des puces Qualcomm, Nvidia, Broadcom, Mediatek…) et ne seront appliqués qu'aux appareils concernés. Rappelons que les smartphones de Google, Nexus et autres Pixel, reçoivent automatiquement en OTA (par les airs) la mise à jour de sécurité. Pour les autres, la mise à jour est soumise au bon vouloir de leurs constructeurs et des opérateurs revendeurs.

Lire également
Des millions de voitures connectées à la merci d'applications Android
Le schéma de verrouillage des mobiles Android piratable par vidéo
Android en tête des vulnérabilités de sécurité référencées en 2016