QuadRooter, 4 vulnérabilités qui menacent des millions de smartphones Android

Dans le cadre de la Def Con 24 de Las Vegas, conférence dédiée à la sécurité, des chercheurs de Check Point ont dévoilé QuadRooter, un ensemble de quatre failles (d'où le nom de la menace) qui affecterait quelque 900 millions de smartphones et tablettes Android. A savoir ceux équipés de chipsets Qualcomm qui alimentent quelques 65% du marché des terminaux LTE (4G). Autant dire que la majorité des modèles 4G sont concernés, y compris les plus récents comme les Google Nexus 5X, 6 et 6P, mais aussi des appareils réputés sécurisés comme le Blackphone ou le Priv de Blackberry sans oublier les incontournables Galaxy S7 et S7 Edge de Samsung.

« Si l'une des quatre vulnérabilités est exploitée, un attaquant peut déclencher des élévations de privilèges dans le but d'obtenir un accès root à l'appareil », énonce Adam Donenfeld, responsable de l'équipe de recherche mobile chez l'éditeur de solutions de sécurité. Un accès privilégié au cœur du système qui donnerait à l'attaquant le contrôle total du terminal et un libre accès aux données qui y sont stockées. Même celles qui sont chiffrées à partir d'une solution de gestion des terminaux mobiles (MDM)? Check Point ne le précise pas. Néanmoins, le chercheur ajoute que *« l'accès pourrait également fournir à un attaquant des fonctionnalités telles que le keylogging (enregistrement de la saisie, NDLR), le suivi GPS, et l'enregistrement vidéo et audio »* aux dépens de l'utilisateur légitime. Il faut néanmoins que ce dernier installe une application corrompue pour que l'attaquant puisse accéder au système. Un vecteur d'attaque classique dans l'univers Android qui oblige l'utilisateur à la plus grande vigilance lorsqu'il s'apprête à télécharger une nouvelle application. Mais, au moins, dans le cas présent, les risques d'exploitation ne passent pas par un e-mail, un SMS et autre page web vérolés.

Vulnérabilités presque toutes corrigées par Google

Si Check Point a profité de la Def Con pour revenir sur QuadRooter, Qualcomm avait déjà révélée les failles critiques issues des pilotes qui accompagnent ses composants électroniques. Elles sont référencées CVE-2016-2059, CVE-2016-2503, CVE-2016-2504 et CVE-2016-5340. Le fabricant a fourni les correctifs au fil des mois, dont le 28 juillet dernier pour CVE-2016-5340. Un correctif arrivé trop tardivement pour que Google puisse l'intégrer à son bulletin de sécurité du 1er août à l'attention des partenaires constructeurs.

Si les utilisateurs d'un smartphone Nexus bénéficient automatiquement des correctifs de sécurité, les autres devront attendre que le constructeur et/ou l'opérateur daignent l'intégrer dans leur processus de mises à jour pour protéger leurs clients (qui eux-mêmes devront appliquer les éventuels patchs). Dans l'attente du correctif manquant dans le cadre du programme Android Open Source Project (AOSP) de Google, les fabricants peuvent appliquer directement les patchs fournis par Qualcomm, via sa plate-forme Aurora Security Advisories.

En attendant qu'opérateurs et distributeurs de terminaux assurent la mise à jour auprès de leurs clients, Check Point a mis en ligne l'application QuadRooter Scanner sur Google Play afin de vérifier

si un smartphone est vulnérable ou non. De son côté, Google déclare n’avoir constaté aucune exploitation massive des failles exposées dans son dernier bulletin de sécurité.

Lire également

Une vulnérabilité vieille de 5 ans menace des millions de terminaux Android
Une faille découverte dans les réseaux mobiles GSM et 4G LTE
Le chiffrement des smartphones Android n’est pas incassable

crédit photo © Kwangmoozaa – shutterstock