

Faute de correctif, comment protéger son smartphone de la faille Android du piratage par MMS

ÉCLAIRAGE - Un simple MMS peut potentiellement infecter 950 millions de smartphones Android. Google a déployé un correcteur mais chaque fabricant doit désormais l'adapter à son logiciel.

PAR **BENJAMIN HUE, AVEC AFP** | PUBLIÉ LE 28/07/2015 À 12:14

| MIS À JOUR LE 29/07/2015 À 09:08

Aux dires des chercheurs qui ont révélé son existence, il s'agit du pire logiciel malveillant de l'histoire des systèmes d'exploitation pour mobiles. **Une faille critique a été découverte dans l'OS pour smartphones Android** de Google. Celle-ci peut permettre à des pirates informatiques de prendre le contrôle de ces appareils via un simple SMS, un message contenant un média graphique, sonore ou vidéo. **Près d'un milliard d'appareils sont potentiellement concernés.**

Comment fonctionne la faille ?

"Les attaquants n'ont besoin que de votre numéro de téléphone. En l'utilisant, ils peuvent exécuter des programmes à distance via un fichier spécialement conçu pour cela et délivré par MMS", a précisé lundi 27 juillet **la société de sécurité informatique Zimperium**, à l'origine de la découverte. Zimperium ajoute que le MMS utilisé pour l'attaque peut même être détruit avant que le propriétaire du smartphone ne le lise. L'intrusion peut donc ne jamais être constatée.

La faille repose sur une fonctionnalité native d'Android baptisée **"Stagefright"**, **la bibliothèque multimédia qui pré-télécharge automatiquement les extraits vidéo attachés à des MMS** pour éviter à leur destinataire d'avoir à attendre pour les visionner. Les pirates sont capables de cacher des programmes malveillants dans ces fichiers vidéo, en exécutant du code informatique, et ils seront du coup activés même si le propriétaire du smartphone ne lit pas le message, détaille Zimperium.

Qui est concerné ?

"N'importe qui peut être ciblé par ce type d'attaque, prévient-elle. Ces failles sont extrêmement dangereuses car elles ne nécessitent pas une action de la victime pour être exploitées". D'après la société de sécurité informatique, quelque 95% des smartphones opérant sous Android, soit environ 950 millions d'appareils, sont à risque. Soit **tous les mobiles équipés de la version 2.2 jusqu'à la plus récente, Android 5.1 Lollipop**. Seuls les mobiles équipés des versions antérieures à la 2.2 sont donc épargnés.

Que se passe-t-il si mon smartphone est infecté ?

Une fois installé, le logiciel malveillant peut permettre au pirate d'effectuer toutes sortes d'opérations en arrière plan sur le téléphone sans que son propriétaire ne s'en aperçoive. Il peut **voler des données, espionner son activité, activer la webcam, le micro, consulter les mails** et tous les fichiers qui transitent par le portable et ainsi de suite. Il ne semble pas toutefois que des pirates aient déjà utilisé la faille.

Quelle est la réponse de Google ?

Dans un article du magazine *Forbes*, le chercheur en sécurité Joshua Drake, membre de la société Zimperium, explique que **les vulnérabilités d'Android sont connues depuis le mois d'avril**. La société Zimperium dit avoir informé Google du problème et lui avoir fourni des patches de sécurité pour y remédier, "mais malheureusement ce n'est que le début de ce qui sera une très longue procédure de mise à jour".

La raison ? **Si Google a bien déployé un correctif, ce n'est pas lui qui contrôle les mises à jour d'Android** sur les appareils utilisant le logiciel, mais les fabricants des téléphones et même parfois les opérateurs téléphoniques qui doivent l'appliquer sur leur version du logiciel Android. Certains s'y sont déjà employés, comme Asus ou HTC, indique *Le Figaro*. Pour les autres, il faudra patienter. Et les appareils datant de plus de 18 mois pourraient même ne jamais recevoir de patch.

Ces derniers vont pourtant devoir agir vite. Car davantage de détails sur le fonctionnement de la faille Android devraient être dévoilés lors de deux conférences importantes qui réuniront hackers et experts en sécurité informatique au début du mois d'août.

Comment s'en protéger ?

En attendant d'installer un correctif, les possesseurs de smartphone Android peuvent se prémunir partiellement des attaques en modifiant les réglages de leurs terminaux. Il faut se rendre dans "SMS/MMS", puis sélectionner "menu", "paramètres" pour **désactiver "l'extraction ou la récupération automatique" des MMS**. Il est aussi possible de rendre impossible la réception de MMS dans les "paramètres de stockage".

Il semble également que la faille concerne plus particulièrement les utilisateurs de **Hangout**, l'application de messagerie la plus courante sur Android. Il est donc également possible de **désactiver Hangout** dans les paramètres généraux en allant dans l'onglet "application de messagerie par défaut" et en sélectionnant "messagerie".

MERCREDI 29 JUILLET

01H44

dms79

Vive WindowsPhone...

MARDI 28 JUILLET

17H40

tiensdonc

Ils ont l'air bien ces hommes et femmes dans les transports ou dans la rue les yeux fixés sur leur smartphone quitte à ne pas voir la crotte du chien . Plus se parler, plus se regarder pour échanges de sourires et de dragues et après ça va sur des sites une fois de plus payant chercher l'âme soeur . Pauvre monde de sots.

17H35

tiensdonc

Un portable pour téléphoner ou recevoir un appel pourquoi pas bien que le téléphone fixe à la maison avec une box c'est tellement mieux. A quoi bon dépenser dans le total inutile. Le résultat est qu'en plus les personnes ne se parlent plus, triste monde.

15H11

Dane123

Merci, c'est fait!