Alerte à partager : Une faille sur Android à corriger d’urgence | Le Net Expert Informatique

	Alerte à partager : Une faille sur Android à corriger d’urgence

Si votre fournisseur de smartphone ou de tablette ne patche pas Stagefright de lui même, ce malware basé sur l'envoi de MMS peut être vraiment effrayant. Mais vous pouvez vous en protéger en respectant quelques étapes.

Franchement, la plupart des gens qui reçoivent les logiciels malveillants recherchent les ennuis. Ils ouvrent un fichier suspect envoyé par une personne qu'ils ne connaissent pas, vont sur un site Internet mal famé, voire téléchargent le dernier film ou jeu à la mode sur BitTorrent. Mais Stagefright, c'est différent. Ce logiciel malveillant basée sur une faille de sécurité se déclenche en recevant un MMS sur un appareil Android non patchées. Et bang, vous êtes piraté.
Stagefright peut attaquer tout smartphone Android, tablette, ou un autre dispositif fonctionnant sous Android 2.2 ou supérieur. Des approximativement quelque 1 milliard de gadgets Android présents sur le marché, Stagefright pourrait, en théorie, toucher 95% d'entre eux. Joshua J. Drake, le vice-président de Zimperium zLabs qui a découvert Stagefright prétend qu'il est parmi les « pires vulnérabilités Android découvertes à ce jour ».
Car la partie vraiment sournoise est qu'il n'est pas nécessaire de consulter le MMS pour être infecté. Si vous utilisez l'application Hangouts de Google , vous êtes infectés sans même consulter cette application de messagerie si l'on vous fait parvenir ce message.

Un malware pas comme les autres
Tout ce que l'attaquant a besoin de faire est d'envoyer ce paquet empoisonné à votre numéro de téléphone. Il allume alors votre appareil, et l'attaque commence. Cela peut arriver si vite que le temps que votre téléphone vous avertisse qu'un message est arrivé, vous avez déjà été piraté. Si par ailleurs vous utilisez l'application native de messagerie proposée avec Android, vous devez ouvrir le MMS, mais pas nécessairement déclencher la vidéo, pour être infecté.
Ce détournement de la sécurité d'Android fonctionne en profitant de la bibliothèque Stagefright incluse dans Android. Ce moteur de lecture multimedia est fourni avec des codecs basés sur des logiciels pour lire plusieurs formats de médias populaires. La faille de sécurité semble provenir du fait que pour réduire la latence de l'affichage vidéo Stagefright traite automatiquement la vidéo avant même que vous ne vouliez la regarder. Joshua J. Drake va révéler les détails de du fonctionnement de Stagefright au Black Hat début Août.

Google a été réactif…
Zimperium à informé Google du problème en Avril. Selon Drake, « Google a agi promptement et appliqué les correctifs à des branches de code interne sous 48 heures ». Une porte-parole de Google mentionne dans une réponse par e-mail : « Nous avons déjà répondu rapidement (…) en envoyant le correctif pour tous les appareils Android à nos partenaires ».

Elle ajoute :
La sécurité est renforcée dans Android : les applications Android sont exécutées dans ce que nous appelons une « sandbox d'application ». De la même manière qu'un bac à sable empêche le sable de sortir, chaque application est installée dans une « sandbox » virtuelle pour l'empêcher d'accéder à autre chose qu'à ses propres composants, ce qui signifie que même si un utilisateur devait installer accidentellement un morceau de malware, il lui est interdit d'accéder à d'autres parties du dispositif.
L'ouverture de l'écosystème améliore la sécurité et rend Android plus puissant. Comme Android est open source, tout le monde peut l'examiner pour comprendre comment il fonctionne et d'identifier les risques potentiels de sécurité. Toute personne peut mener des recherches et faire des contributions pour améliorer la sécurité d'Android.
Google encourage la recherche en matière de sécurité : le programme de récompenses de sécurité Android, lancé en 2015, et le programme Google Patch Rewards, lancé en 2014, récompensent les contributions de chercheurs en sécurité qui investissent leur temps et leurs efforts à aider à rendre les applications plus sûres.
Alors, avec toutes ces précautions, pourquoi une telle agitation? Oui, il s'agit d'une faille de sécurité particulièrement vicieuse, mais le correctif est là… n'est ce pas ?

…mais pas les fabricants
Euh, et bien en fait Android a un autre problème de sécurité bien plus important. À l'exception des appareils Nexus, Google fournit les correctifs de code source, mais ce sont les fabricants de smartphones et les opérateurs qui doivent les faire parvenir aux utilisateurs qui mettent à jour le firmware. Et au 27 Juillet aucun des principaux acteurs de l'écosystème Android n'a annoncé de plan pour fournir le patch. Pour des appareils anciens, les patches pourraient ne jamais être livrés.

Zimperium affirme que le Blackphone de SilentCircle est protégé contre cette attaque depuis la version 1.1.7 de PrivatOS. Firefox de Mozilla a également inclus un correctif pour ce problème depuis la version 38. Et bien sûr Zimperium propose sa propre protection contre les attaques Stagefright avec sa plate-forme de défense de la menace mobile, zIPS.

Voici comment se débrouiller sans patch
Mais ce que Zimperium ne mentionne pas, c'est qu'Android a déjà une excellente façon de bloquer la plupart des attaques de Stagefrights : bloquer tous les messages texte provenant d'expéditeurs inconnus.

Pour paramétrer cela avec Android Kitkat, la version la plus populaire d'Android, ouvrez l'application 'Messenger' et appuyez sur le menu dans le coin supérieur droit de l'écran (les trois points verticaux), puis appuyez sur 'Paramètres'. Une fois là, sélectionnez Bloquer les expéditeurs inconnus, et c'est tout.

Sur Lollipop, où Hangouts est l'application de messagerie par défaut, il n'y a aucun moyen par défaut de bloquer les expéditeurs inconnus. Vous pouvez toutefois sous 'Paramètres' aller aux 'messages multimédia' et désactivez 'Récupérer automatiquement les messages multimédias'.

Avec Lollipop et d'autres versions d'Android, je recommande de vous tourner vers des applications de blocage de SMS tierces. Pour Android 2.3 à 4.3, j'apprécie 'Blocage des Appels et SMS'. Si vous utilisez KitKat ou les versions au dessus, où une seule application de SMS peut être active au même moment, j'apprécie Postman, alias TEXT BLOCKER. Ce programme fonctionne en conjonction avec votre application préférée de textos pour bloquer les expéditeurs inconnus.

Rien de tout cela n'est parfait. Un ami peut toujours être infecté et propager des programmes malveillants. Mais c'est un bon début. La solution de court terme adviendra quand les fabricants et les opérateurs se magneront enfin le train et pousseront le correctif vers leurs clients. Mais compte tenu de leur historique, je ne vais pas attendre et je vais bloquer les MMS. La solution à long terme arrivera quand les entreprises qui utilisent Android commenceront à travailler avec Google pour fournir des correctifs de sécurité le plus rapidement possible, et tout le temps.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/stagefright-a-quel-point-les-utilisateurs-d-android-doivent-ils-etre-inquiets-39823010.htm
Par Steven J. Vaughan-Nichols