Faille Apple Mail : faut-il changer de messagerie ?

Entre ZecOps et Apple, qui a raison ?

Le premier est une start-up américaine spécialisée dans la sécurité des appareils mobiles.
La semaine passée, il a révélé plusieurs failles dans l'application Mail pour iOS. Et affirmé qu'elles avaient permis de prendre pour cible plusieurs personnes d'intérêt, dont des employés d'une entreprise du Fortune 500 et un cadre dirigeant chez un telco japonais.

Apple n'en dément pas l'existence, mais assure ne pas avoir de preuve de leur exploitation.
La firme de Cupertino ajoute ne pas percevoir de risque immédiat : seules, ces vulnérabilités ne suffisent pas à passer outre les défenses d'iOS.

ZecOps lui-même a reconnu qu'il en faut davantage pour espérer prendre le contrôle d'un iPhone ou d'un iPad. Notamment contourner l'ASLR (distribution aléatoire de l'espace d'adressage).

Reste que les failles en question peuvent permettent, selon la start-up, d'exécuter du code à distance dans le contexte de l'application Mail. Avec, pour conséquence éventuelle, la lecture, la modification et la suppression de messages à l'insu de l'utilisateur.

Il est fort probable que ce dernier ne détecte pas l'attaque. En tout cas sur iOS 13 : il suffit que l'application Mail soit ouverte en arrière-plan pour que la faille s'enclenche.
Sur iOS 12, une action est requise de sa part, sauf si l'attaquant a le contrôle du serveur d'envoi.

D'envoi de quoi, au juste ? D'un e-mail qui consomme suffisamment de mémoire pour que soit fait appel à la fonction ftruncate().

Hors limites

Ledit appel se fait dans le contexte d'une autre fonction : MFMutableData, qui s'active lors du téléchargement d'un e-mail au format MIME.

Si les données dépassent une certaine taille, elles sont stockées dans un fichier qui peut ensuite, si nécessaire, être agrandi par itérations à l'aide de ftruncate().

Problème : il n'y a pas de vérifications des erreurs qui pourraient survenir à ce stade. Ou plutôt, un mauvais traitement de la variable que retourne l'appel système (0 en cas de réussite, -1 en cas d'échec). Ainsi l'exécution se poursuit-elle jusqu'à dépasser la capacité du fichier… et entraîner une écriture hors limites.

Avec quelques ajustements, on peut même s'arranger pour exposer la vulnérabilité sans exécuter ftruncate().

Les premières tentatives d'exploitation que ZecOps dit avoir constatées remontent à janvier 2018, sur iOS 11.2.2. Le problème existe toutefois au moins depuis iOS 6, lancé en septembre 2012

parallèlement à l'iPhone 5.

Une deuxième vulnérabilité existe… et a peut-être mené à la découverte de la première. Elle se trouve dans la fonction mmap, destinée à établir une projection des fichiers en mémoire virtuelle… et qui plante lorsqu'elle ne peut y trouver une zone d'adressage suffisamment grande.

Occasionnant un dépassement de tas, elle est plus simple à déclencher sur iOS 12. Le traitement des données se fait en l'occurrence dans le même processus que l'application Mail. Les processus sont séparés sur iOS 13.

Apple a intégré un correctif à iOS 13.4.5, actuellement en bêta. ZecOps entend fournir davantage de détails quand cette version sera ouverte à tous les utilisateurs.

Photo d'illustration © Apple