iOS et OS X, un piratage par de simples images

iOS et OS X victimes du syndrome « Stagefright ». L'année dernière, des failles dans Android avaient été découvertes et exploitées à partir d'un simple MMS envoyé. Les bugs étaient situés dans la bibliothèque logicielle de l'OS mobile pour lire plusieurs formats de fichiers vidéo.

Des chercheurs de l'équipe de Talos, branche sécurité de Cisco, ont présenté une série de vulnérabilités critiques dans l'OS mobile d'Apple. Trois de ces failles peuvent conduire à l'exécution de code à distance. Parmi elles, une s'appuie sur la façon dont iOS gère les fichiers TIFF dans diverses applications. Un bug doté d'un fort potentiel d'exploitation.

Dans un blog, les membres de Talos expliquent que la vulnérabilité, CVE-2016-4031, « est particulièrement préoccupante, car elle peut être déclenchée dans toutes les applications qui utilisent l'API Image I/O d'Apple pour le rendu des images TIFF ». Et d'ajouter, « *des attaquants peuvent placer un code malveillant dans différents vecteurs comme des iMessages, des pages web malveillantes, des MMS, ou d'autres pièces jointes vérolées* ». Les spécialistes constatent que dans le cas des iMessages, la faille est exploitable sans avoir besoin de l'interaction avec l'utilisateur, car le rendu des images se fait automatiquement par défaut. A noter que ce bug touche iOS en version 9.3.2 et antérieures, ainsi que OS X 10.11.15.

OpenEXR et Bitmap dans le viseur

Les images sont encore au centre des autres failles découvertes par l'équipe de Talos. Deux (CVE-2016-4629, CVE-2016-4630) concernent le format de fichiers OpenEXR, développé par Light and Magic pour créer des effets visuels. Avec ce bug, il est possible de créer des images malveillantes contenant du code capable de s'exécuter à distance et de provoquer des saturations mémoire.

Toujours dans les images, l'API Core Graphics sous iOS et OSX contient aussi sa faille (CVE-2016-4637) par rapport au format de fichier BMP (Bitmap). « L'entête du fichier BMP comprend des informations sur la taille, la disposition et le type d'image. Un bug existe dans le traitement de la hauteur de l'image. Cette dernière peut être manipulée pour exécuter du code à distance dans les applications utilisant l'API Core Graphics d'Apple », précisent les chercheurs de Cisco.

Apple sollicité a livré des correctifs pour l'ensemble des vulnérabilités découvertes par l'équipe de Talos. Les utilisateurs sont donc invités à télécharger la version 9.3.3 d'iOS et les versions Mavericks 10.9.5, Yosemite 10.10.5 ou El Capitan 10.11.6 pour OS X.

A lire aussi :

Windows 7 et iOS 9, les deux OS les plus utilisés du marché
iOS : le bug du 1er janvier 1970 exploitable à distance

Crédit Photo : Denys Prykhodov-Shutterstock