Une faille zero day trouvée et corrigée dans Flash Player

Le centre de recherche de Kaspersky a découvert une faille de type zero day dans le lecteur Flash d'Adobe. Connue sous le nom de code CVE-2014-0515, **la vulnérabilité a été localisée dans le composant Pixel Bender** utilisé pour la lecture des vidéo et des images. Le laboratoire a reçu deux échantillons d'attaques à la mi-avril montrant que la faille avait déjà été exploitée sur un site du gouvernement syrien. **Les chercheurs ont trouvé le conteneur de l'attaque, un fichier vidéo flash (movie.swf)** qui est activable par un utilisateur. En premier lieu, le code malveillant prépare la mémoire dynamique pour l'exploitation de la faille. Il identifie aussi l'OS pour pousser une version modifiée du composant Pixel Bender. Cette adaptation touche donc l'ensemble des OS, Windows, Linux et Mac OS.

Double attaque sur une même faille

Les chercheurs de Kaspersky ont trouvé **des variantes sur l'analyse des deux attaques**. La première comportait un shellcode et deux pour la seconde attaque. « *Le second shellcode est inhabituel* », explique **Vyacheslav Zakorzhevsky**, chercheur en sécurité au Kaspersky Lab. *« Il va chercher sur une adresse DLL pour flash10p.ocx une interaction avec Cisco MeetingPlace Express Add-In version 5×0. »* Ce module est intégré par des participants de webconférence pour voir des documents et des images. Le spécialiste de Kaspersky estime que c**ette seconde attaque était était très ciblée pour visait des personnes qui utilisent les solutions Adobe et Cisco.**

Un correctif à appliquer en urgence

Adobe n'a pas tardé à réagir en mettant en place rapidement un correctif de Flash Player, via une mise à jour de sécurité. Elle concerne les versions 13.0.0.182 et antérieures pour Windows, 13.0.0.201 et antérieures pour Mac OS, ainsi que les versions 11.2.202.350 et antérieures pour Linux. **Ce patch est téléchargeable depuis le site de l'éditeur ou attendre que les navigateurs le télécharge via les mises à jour automatiques**.

crédit photo © Ben Chams – Fotolia

A lire aussi :

Alerte aux failles critiques pour la plate-forme Adobe Flash