

ElcomSoft a découvert la vulnérabilité dans le Système de sécurisation des données de Canon

Moscou, Russie – le 30 novembre 2010 - Le fabricant de logiciels ElcomSoft a recherché le Système Authentique de sécurisation des données de Canon (Canon Original Data Security System), un système de validation pour garantir l'authenticité des images numériques prises avec des appareils photo Canon, et découvert la vulnérabilité. La vulnérabilité offre la possibilité de fabriquer des images qui seront validées comme authentique par le kit de sécurisation des données pour boîtiers EOS de Canon (OSK-E3), sans tenir compte de leur authenticité ou non-authenticité.

Après avoir analysé le matériel de Canon, les chercheurs d'ElcomSoft ont prouvé que des clés secrètes utilisées pour calculer des données d'authentification peuvent être extraites des appareils photo Canon EOS. Les chercheurs ont extrait des clés et les ont utilisées pour ajouter des signatures d'authenticité aux images numériques falsifiées. Les images signées avec une clé extraite étaient validées comme authentiques par le kit de sécurisation des données pour boîtiers EOS de Canon (OSK-E3).

La vulnérabilité existe dans tous les appareils photo Canon fabriqués à ce jour, qui ont la fonction de sécurité. Tous les appareils photo actuels sont sensibles à la vulnérabilité, y compris une gamme complète d'appareils pour usage personnel (par exemple, Digital Rebel XS, aussi connus comme EOS 1000D en Europe et Kiss F au Japon), et professionnel, y compris le plus récent EOS-1D Mark IV.

ElcomSoft ne communique pas des détails techniques. Toutefois, la société a rendu Canon conscient de la vulnérabilité en informant le vendeur comme la tierce partie de confiance, le CERT Coordination Center.

ElcomSoft a mis des images falsifiées validées comme authentiques par OSK-E3, le kit de sécurisation des données pour boîtiers EOS de Canon, à la disposition du public (<http://www.canon.co.jp/imaging/osk/osk-e3/index.html>). Les images sont disponibles sur <http://canon.elcomsoft.com>

À propos du Système de sécurisation des données de Canon

Le système de sécurisation des données a été présenté par Canon Inc. pour sécuriser la validation des images numériques et prouver l'authenticité des images. Des images numériques sont signées par des appareils photo Reflex numériques de Canon avec une fonction de hachage. Des signatures numériques sont incorporées dans toutes les photos prises avec un appareil photo (*). Ensuite l'authenticité d'une image et ses métadonnées qui comprennent le temps et l'endroit (**) de la photo, peuvent être vérifiées en utilisant le kit de sécurisation des données pour boîtiers EOS de Canon (OSK-E3). Le système de sécurisation des données est conçu pour s'assurer que les images et leurs métadonnées ne sont pas modifiées en aucune façon. Les agences de presse les plus importantes au monde, notamment Associated Press, utilisent le système de sécurisation des données de Canon pour garantir que des images numériques sont authentiques et originelles.

(*) On doit activer une fonction incorporée.

(**) Les coordonnées géographiques sont incorporées par certains appareils photo Canon grâce à un récepteur GPS intégré ou externe.

À propos d'ElcomSoft

La société [ElcomSoft Co. Ltd.](http://www.elcomsoft.com) a été fondée en 1990. C'est une compagnie des produits logiciels le siège duquel est situé à Moscou, Russie. ElcomSoft est spécialisée sur les applications de Windows pour les entreprises et utilisateurs finals. Nos logiciels sont utilisés par les fonctionnaires et les enquêteurs, la plupart des sociétés Fortune 500, plusieurs branches de l'armée. ElcomSoft est le Partenaire "Gold" Certifié du Microsoft® et le membre du Programme Intel® Software Partner, membre de l'Association Russe de Cryptologie (RCA), l'Institut de la Sécurité des Ordinateurs. Visitez notre site <http://www.elcomsoft.fr>

Les images falsifiées validées comme authentiques par OSK-E3, le kit de sécurisation des données pour boîtiers EOS de Canon, sont disponibles sur <http://canon.elcomsoft.com>