Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 29 mars 2013
N° CERTA-2013-ACT-013

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-013

Conditions d'utilisation de ce document : http://www.certa.ssi.gouv.fr/certa/apropos.html
Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-013

1 Sécurité des appareils photographiques numériques

De plus en plus d'appareils photographiques numériques (ou APN) disposent de fonctionnalités leur permettant de communiquer au travers de réseaux TCP/IP. Cette communication sur TCP/IP permet une multitude de fonctionnalités telles que la publication d'images sur les réseaux sociaux ou l'envoi automatique des images capturées.

Au delà des problèmes de confidentialité que peuvent poser la publication des images sur des réseaux sociaux, une équipe de chercheurs a étudié la sécurité de ces appareils.

Les résultats de cette étude montrent que ces équipements peuvent implémenter des fonctions telles que :

- l'envoi des images sur un serveur FTP ;
- la présence d'un serveur HTTP sur l'appareil permettant de récupérer les images stockées, voire d'en prendre de nouvelles ;
- l'utilisation d'un logiciel propriétaire pour communiquer sans restriction avec l'appareil.

Les résultats de l'étude montrent également que les attaques courantes touchant d'autres équipements réseaux restent applicables à ces appareils :

- attaque de l'homme du milieu ;
- déconnexion forcée (envoi d'un paquet TCP avec le drapeau RST activé).

De plus, les nouvelles fonctionnalités introduites par les constructeurs peuvent être détournées par un attaquant en lui donnant la possibilité de :

- récupérer l'ensemble des photos de l'appareil ;
- envoyer de nouvelles photos sur l'appareil ;
- prendre de nouvelles photos à distance ;
- enregistrer l'environnement à distance.

Le CERTA recommande donc d'éviter l'utilisation de ce type d'appareil au sein du système d'information d'entreprise et de sensibiliser les utilisateurs des risques encourus lors de l'utilisation de ces fonctionnalités sur des réseaux publics non sécurisés.

2 Authentification à deux facteurs proposée par Apple

Une récente attaque a montré qu'il était possible pour une tierce personne de remettre à zéro ou de modifier à sa guise le mot de passe d'un compte Apple ID d'un utilisateur arbitraire. Pour y pallier, Apple a dernièrement introduit un mécanisme d'authentification forte à l'instar de ses concurrents tels que Google ou Yahoo. Après

activation, cette authentification sera réclamée lors d'opérations de modifications des informations de compte ou lors d'opérations d'achat sur les plateformes Apple partir de nouveaux périphériques.

En plus du mot de passe utilisateur, ce dernier devra fournir au service un code temporaire de quatre caractères qu'il aura reçu sur son appareil (par exemple sur son téléphone ou Mac). De cette manière, la connaissance du mot de passe n'est plus une condition suffisante la compromission du compte.

Bien que ce mécanisme d'authentification ne soit pas encore disponible en France, son utilisation est vivement conseillée et rejoint les recommandations de sécurité relatives aux mots de passe publiées par l'ANSSI. De manière générale, il est recommandé d'utiliser les mécanismes similaires proposés par les différents services (banques, messageries...).

Documentation

– Note technique - Recommandations de sécurité relatives aux mots de passe
http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

3 Nouvelle vulnérabilité dans TLS avec RC4

Après une actualité chargée ces dernières années (cf. Documentation), le protocole TLS, notamment utilisé pour protéger les sessions en HTTPS, fait à nouveau l'objet d'une publication de faille.

Une équipe de chercheurs a mis au jour une nouvelle attaque (CVE-2013-2566) contre l'algorithme de chiffrement RC4 utilisé dans le protocole SSL/TLS. Un attaquant capable d'intercepter plusieurs centaines de millions de sessions pourrait récupérer quelques octets d'information en clair.

Dans les contextes d'emploi usuels de TLS, les *cookies* et mots de passe sont potentiellement concernés.

Bien que les conditions de l'attaque n'en font pas immédiatement une menace critique, il convient de s'en prémunir. Pour cela, le CERTA recommande idéalement d'utiliser le mode de chiffrement authentifié AES-GCM disponible dans TLS 1.2. Malheureusement, peu de systèmes sont aujourd'hui compatibles avec cette version. Dans les autres cas, il faut donc utiliser des modes de chiffrement par bloc comme CBC, après s'être assuré que les bibliothèques utilisées ne sont pas vulnérables aux attaques comme BEAST ou *Lucky 13*.

Documentation

– Bulletin d'actualité CERTA-2011-ACT-039 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-039/
– Bulletin d'actualité CERTA-2012-ACT-042 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-042/
– Bulletin d'actualité CERTA-2013-ACT-009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-009/
– Référence CVE-2013-2566 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566

4 Vague d'hammeçonnage sur les réseaux sociaux

Le 25 mars 2013, Avast a présenté une nouvelle vague d'hameçonnage sur le réseau social Facebook. Cette attaque a la particularité d'utiliser des applications malveillantes pour subtiliser les mots de passe des utilisateurs. l'application d'hameçonnage se présente sous la forme d'un formulaire légitime d'authentification. Bien que ce formulaire apparaisse au sein de l'environnement Facebook, il transmettra les identifiants à un serveur tiers contrôlé par les attaquants.

Dans un environnement professionnel, par exemple dans une optique de communication via les réseaux sociaux, le CERTA rappelle la nécessiter de sensibiliser les utilisateurs à ce type de menace, et d'être vigilants à l'application des mesures suivantes :

– ne pas installer de modules non-indispensables à la réalisation des besoins, sans autorisation ;
– ne pas utiliser les mêmes identifiants que des comptes personnels ou professionnels ;
– éviter l'utilisation personnelle des réseaux sociaux sur les réseaux de l'entreprise.

Documentation

- Fake Facebook login pages spreading by Facebook applications :
  http://blog.avast.com/2013/03/25/fake-facebook-login-pages-spreading-by-facebook-applications

5 Rappel des avis émis

Dans la période du 22 au 28 mars 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-197 : Vulnérabilité dans Symantec NetBackup Management Console
- CERTA-2013-AVI-198 : Multiples vulnérabilités dans IBM Notes
- CERTA-2013-AVI-199 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-200 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTA-2013-AVI-201 : Vulnérabilité dans Novell ZENworks
- CERTA-2013-AVI-202 : Vulnérabilité dans Microsoft Windows Modern Mail
- CERTA-2013-AVI-203 : Vulnérabilité dans EMC Smarts Network Configuration Manager
- CERTA-2013-AVI-204 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-205 : Multiples vulnérabilités dans Cisco IOS
- CERTA-2013-AVI-206 : Multiples vulnérabilités dans les produits Asterisk
- CERTA-2013-AVI-207 : Vulnérabilité dans les produits EMC

Gestion détaillée du document

29 mars 2013 version initiale.