Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 août 2013
N° CERTA-2013-ACT-031

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-031

1 Clés USB, encore et toujours un risque pour le SI

Comme mentionné par le passé, l'utilisation de clés USB non maitrisées présente un risque important pour la sécurité du SI.

Cette menace est aujourd'hui d'autant plus importante que depuis quelques semaines, certains constructeurs commercialisent des clés piégées prêtes à l'emploi, utilisant un mécanisme d'émulation d'un périphérique clavier plutôt que l'utilisation des fonctionnalités dîtes d'exécution automatique (Autorun).

Cette technique, bien que déjà connue dans le milieu de la recherche en sécurité, n'en reste pas moins efficace et permet d'exécuter une charge malveillante lors de la connexion de la clé à un poste Windows.

De plus, même si les modèles actuels semblent limités au système de Microsoft, des clés utilisant des principes similaires pourraient voir le jour sur d'autres systèmes.

D'un point de vue extérieur, rien ne permet aujourd'hui de différencier ce type de clé piégée d'une clé saine. Il est cependant possible d'observer les activités malveillantes car elle fait apparaitre une invite de commandes lors de son insertion.

Le CERTA recommande, une nouvelle fois, de prendre garde à ce type de périphériques aujourd'hui largement accessibles. Il est notamment nécessaire de sensibiliser les utilisateurs à ce type d'attaque afin qu'ils puissent prévenir rapidement la chaîne SSI en cas de comportements suspects.

Documentation

- Bulletin d'actualité CERTA-2013-ACT-029, périphériques USB promotionnels et cadeaux électroniques : http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-029/index.html

2 Migration des certificats de Google vers des clés de 2048 bits

Google a annoncé récemment qu'une importante migration de ses certificats SSL était en cours de déploiement. La mise à jour repose sur le remplacement des clés RSA 1024 bits vers des clés RSA 2048 bits. Cette évolution concerne également la clé de l'autorité de certification racine utilisée pour signer les certificats SSL.

Ce renforcement de la sécurité est cohérent avec la partie "mécanismes cryptographiques" du référentiel général de sécurité (RGS) qui mentionne que la taille minimale du module RSA doit être de 2048 bits pour une utilisation ne devant pas dépasser 2020 (et 4096 au delà de 2020).

Le CERTA recommande une revue de l'usage des certificats dans votre système d'information, afin de vous assurer qu'aucune application critique ne repose sur des clés faibles et de procéder sans délai au renouvellement des certificats concernés vers de nouveaux certificats conformes aux recommandations du RGS.

Documentation

- Google certificates upgrade in progress :
  http://googledevelopers.blogspot.fr/2013/07/google-certificates-upgrade-in-progress.html
- Mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
  http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

3 Rappel des avis émis

Dans la période du 26 juillet au 01 août 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-439 : Multiples vulnérabilités dans Apache OpenOffice
- CERTA-2013-AVI-440 : Multiples vulnérabilités dans HP Network Node Manager I
- CERTA-2013-AVI-441 : Multiples vulnérabilités dans HP LoadRunner
- CERTA-2013-AVI-442 : Multiples vulnérabilités dans phpMyAdmin
- CERTA-2013-AVI-443 : Vulnérabilité dans ISC BIND
- CERTA-2013-AVI-444 : Multiples vulnérabilités dans Wireshark
- CERTA-2013-AVI-445 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-446 : Vulnérabilité dans HP SiteScope
- CERTA-2013-AVI-447 : Vulnérabilité dans EMC NetWorker
- CERTA-2013-AVI-448 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-449 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-450 : Multiples vulnérabilités dans le système SCADA GE Proficy HMI/SCADA
- CERTA-2013-AVI-451 : Vulnérabilité dans Adobe Digital Editions
- CERTA-2013-AVI-452 : Vulnérabilité dans de multiples produits Cisco
- CERTA-2013-AVI-453 : Vulnérabilité dans Cisco WAAS
- CERTA-2013-AVI-454 : Multiples vulnérabilités dans VMware ESX et ESXi
- CERTA-2013-AVI-455 : Multiples vulnérabilités dans TYPO3
- CERTA-2013-AVI-456 : Multiples vulnérabilités dans le système SCADA Siemens Scalance W-7xx
- CERTA-2013-AVI-457 : Multiples vulnérabilités dans le système SCADA Siemens WinCC

Gestion détaillée du document

02 août 2013 version initiale.