Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 27 octobre 2014
N° CERTFR-2014-ACT-043

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-043

1 - Vulnérabilité BadUSB

Au mois d'août, lors de la conférence BlackHat à Las Vegas, les deux chercheurs en sécurité Jakob Lell et Karsten Nohl ont dévoilé une faille touchant potentiellement un grand nombre de périphériques USB. Début octobre, deux autres chercheurs ont publié des codes permettant d'exploiter cette vulnérabilité pour un certain type de contrôleur USB, embarqué dans de nombreuses clés USB.

Détails de la vulnérabilité

La vulnérabilité réside dans le fait qu'il est possible de changer le microcode (firmware) de certains périphériques USB. Après remplacement de ce code par un firmware malveillant, le périphérique USB pourra se présenter au système d'exploitation comme étant d'un autre type, par exemple un clavier, une souris ou une carte réseau.

Il bénéficiera alors des mêmes privilèges que ces périphériques, c'est-à-dire qu'il pourra simuler des frappes sur le clavier ou envoyer des paquets réseau au PC. Il pourra également tenter d'exploiter des vulnérabilités dans le pilote chargé par le système.

Risques

Les risques sont multiples et dépendent du périphérique qui sera chargé. Par exemple, un attaquant sera en mesure d'écrire des commandes à la place de l'utilisateur, de changer des options de configuration du système, de télécharger et d'exécuter des charges malveillantes ou d'enregistrer le trafic réseau.

Recommandations

Ces périphériques malveillants agissent comme de vrais périphériques, en conséquence ils ne peuvent pas être détectés par les antivirus. Néanmoins, il existe plusieurs moyens permettant de réduire la surface d'exposition par rapport à cette attaque.

Sous Windows, il est possible de restreindre les classes de périphériques qui seront reconnues et installées automatiquement grâce à des mécanismes de liste blanche ou de liste noire.

Pour activer la liste noire, il faut se rendre dans "l'éditeur de stratégie de groupe" (gpedit.msc), puis naviguer dans les onglets "Configuration ordinateur" ->"Modèles d'administration" ->"Système" ->"Installation de périphériques" ->"Restrictions d'installation de périphériques". Il faut ensuite activer "Empêcher l'installation de périphériques à l'aide de pilotes correspondant à ces classes d'installation de périphériques" et choisir les classes de périphériques à interdire via leur GUID.
Par exemple, le GUID `{4d36e96b-e325-11ce-bfc1-08002be10318}` contrôle l'installation automatique des claviers USB ; le GUID `{4d36e972-e325-11ce-bfc1-08002be10318}` est l'équivalent pour

les cartes réseau. Pour que cette règle ne s'applique pas aux périphériques déjà installés, la case "Appliquer également aux périphériques correspondants déjà installés" doit être décochée.

Il est possible d'utiliser une liste blanche en activant "Permettre l'installation de périphériques à l'aide de pilotes correspondant à ces classes d'installation de périphériques". Il est nécessaire d'activer la stratégie "Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie" pour que cette règle soit effective.

Une autre possibilité est de désactiver complètement l'installation automatique des nouveaux périphériques USB (un administrateur sera en mesure de les installer manuellement via le gestionnaire de périphériques). Il faut se rendre dans "l'éditeur de stratégie de groupe" (gpedit.msc), puis naviguer dans les onglets "Configuration ordinateur" ->"Modèles d'administration" ->"Système" ->"Installation de périphériques" ->"Restrictions d'installation de périphériques".

Il faut ensuite activer les stratégies "Empêcher l'installation des périphériques amovibles" et "Autoriser les administrateurs à passer outre les stratégies de restriction d'installation de périphériques".

Afin d'informer les utilisateurs et leur indiquer la marche à suivre dans le cas où ils souhaiteraient activer un nouveau périphérique, il est nécessaire d'activer "Afficher un message personnalisé lorsque l'installation d'un périphérique est empêchée par un paramètre".

Il est rappelé aux utilisateurs qu'il convient de :

- ne pas brancher des périphériques USB provenant d'une source non sûre ;
- ne pas brancher ses propres périphériques USB sur des machines inconnues ;
- segmenter l'utilisation des clés USB à des usages précis ;
- considérer qu'un périphérique perdu puis retrouvé ne peut plus être utilisé comme étant de confiance.

Il est également souhaitable de désactiver physiquement ou électriquement les ports USB qui ne sont pas utilisés (par exemple ceux situés derrière les machines) et de vérifier régulièrement les ports fonctionnels afin de détecter des périphériques USB intrus.

Conclusion

Le CERT-FR rappelle que les périphériques USB peuvent être utilisés afin de propager des codes malveillants et conseille de sensibiliser les utilisateurs à ces pratiques.

2 - Malvertising

Le CERT-FR constate que le « Malvertising » reste un vecteur d'attaque important. Ce type d'attaque consiste à utiliser des régies publicitaires compromises afin de rediriger les internautes naviguant sur un site internet légitime vers des pages distributrices de charges malveillantes.

Encore récemment, des sites à forte audience comme `java.com` ou `yahoo.com` ont été exposés à ce type de campagne. La surface d'attaque est importante car les attaquants peuvent exécuter silencieusement des exploits, par exemple en ciblant des vulnérabilités contenues dans des versions obsolètes d'extensions de navigateurs.

Il faut rester vigilant face à cette menace et appliquer les mesures détaillées dans le guide d'hygiène. Les cybercriminels peuvent, grâce à la flexibilité de leurs outils, cibler certaines institutions ou entreprises, en choisissant de ne distribuer leurs charges qu'à une liste d'adresses IP par exemple.

Documentation

- Guide d'hygiène informatique de l'ANSSI :
  http://www.ssi.gouv.fr/hygiene-informatique

3 - Rappel des avis émis

Dans la période du 17 au 26 octobre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-009 : Vulnérabilité dans Microsoft OLE
- CERTFR-2014-AVI-436 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2014-AVI-437 : Vulnérabilité dans Huawei Mobile Partner

- CERTFR-2014-AVI-438 : Multiples vulnérabilités dans Pidgin
- CERTFR-2014-AVI-439 : Multiples vulnérabilités dans Apple iOS
- CERTFR-2014-AVI-440 : Vulnérabilité dans VMWare VSphere Data Protection
- CERTFR-2014-AVI-441 : Multiples vulnérabilités dans Apple QuickTime

Gestion détaillée du document

27 octobre 2014 version initiale.