Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 mai 2012
N° CERTA-2012-ACT-019

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-19

Gestion du document

Référence	CERTA-2012-ACT-019
Titre	Bulletin d'actualité 2012-19
Date de la première version	11 mai 2012
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques liés aux mises à jour dans des réseaux non maitrisés

Les équipements informatiques de mobilité (ordinateurs portables, ordiphones), de par leur fonction, sont susceptibles d'être utilisés dans des réseaux locaux tiers non contrôlés (aéroports, hôtels, services de Wi-Fi gratuits ou payants à la durée). Les connexions dans ces réseaux induisent des risques particuliers. D'une part, l'utilisateur a rarement des garanties sur les responsables du service. D'autre part, ces réseaux publics sont accessibles à n'importe qui, y compris à des utilisateurs malveillants.

Ces spécificités mettent en danger la confidentialité des échanges et leur intégrité. Des attaques variées peuvent être réalisées dans ces environnements. Il est par exemple possible d'intercepter les pages Web recues par la victime avec des attaques par interposition (*man in the middle*), et d'insérer dans ces pages légitimes du contenu malveillant (par exemple un javascript). Le FBI a d'ailleurs publié cette semaine un bulletin signalant une recrudescence de ce type d'attaque. Dans cet article, nous nous intéresserons au problème des mises à jour logicielles.

La plupart des logiciels commerciaux ou libres modernes installent une fonction de mise à jour automatique. Le logiciel tente régulièrement de se connecter à un serveur Internet pour vérifier l'existence d'une nouvelle version. Lorsqu'une mise à jour est disponible, selon la configuration le logiciel la télécharge et l'installe automatiquement, ou bien demande l'accord de l'utilisateur pour le faire. Ce procédé est parfois vulnérable. Un attaquant qui est capable d'intercepter les requêtes d'interrogation et de fabriquer les réponses peut se faire passer pour le serveur de mise à jour, répondre au logiciel qui l'interroge qu'une mise à jour est disponible et lui envoyer à la place un logiciel malveillant qu'il installera sur la machine. Certains éditeurs se protègent en sécurisant le procédé par des

moyens cryptographiques (chiffrement des échanges, authentification du serveur et signature des mises à jour). Cependant, ils sont encore une minorité.

Des développeurs de logiciels malveillants ont conçu des outils qui rendent très simples ce type d'attaque. L'attaquant va se placer avec un portable dans un réseau local public. Une fois lancé, le logiciel malveillant va utiliser des techniques classiques (par exemple l'empoisonnement ARP) pour identifier et intercepter les requêtes vers des serveurs de mise à jour connus, et répondre à leur place. Ils envoient alors à la victime la fausse mise à jour qui est le programme choisi par l'attaquant (logiciel espion, cheval de Troie, rançongiciel) La fenêtre de mise à jour est dans ce cas la fenêtre légitime du logiciel, l'utilisateur est donc très facilement trompé.

Pour se protéger contre ce type d'attaque, le CERTA recommande :

- de désactiver l'installation automatique des mises à jour sur les portables (configurer pour laisser le choix à l'utilisateur) ;
- de n'accepter les mises à jour qu'à l'intérieur de réseaux de confiance ;
- de désactiver les technologies de type *roaming* (connexion automatique aux réseaux gratuits) et plus généralement, de laisser le Wi-Fi désactivé hors utilisation volontaire.

Les technologies de type VPN permettent de sécuriser plus généralement le trafic des utilisateurs nomades. Encore faut-il s'assurer que tout le trafic de mise à jour de tous les logiciels installés est bien redirigé dans le VPN, ce qui n'est pas le cas quand seul le navigateur utilise le VPN.

Documentation

- Sécurité des solutions de mobilité :
  http://www.securite-informatique.gouv.fr/gp_article712.html
- Acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
- Article du FBI :
  http://www.ic3.gov/media/2012/120508.aspx

2 Stockage en clair du mot de passe FileVault dans Mac OS X Lion

Description

Une vulnérabilité a été corrigée cette semaine dans *Mac OS X Lion*. Cette vulnérabilité affecte les utilisateurs ayant activé FileVault sous *Mac OS X Snow Leopard* et ayant mis a jour leur système en Lion sans passer à FileVault2 (qui chiffre l'ensemble du disque contrairement à la version précédente qui chiffre seulement le répertoire personnel de l'utilisateur). Elle a pour conséquence de stocker en clair le mot de passe de l'utilisateur dans un fichier de journalisation. Ce fichier de journalisation n'est cependant accessible qu'à un utilisateur ayant les droits administrateur.

En supplément de la mise à jour de sécurité corrigeant cette vulnérabilité, Apple a mis à disposition une fiche technique expliquant comment supprimer les traces des mots de passe ayant pu être enregistrés dans le fichier de journalisation. L'éditeur attire également l'attention sur le fait que les copies de sauvegarde et les serveurs syslog peuvent également contenir les mots de passe des utilisateurs en clair.

Documentation

- Bulletin de sécurité CERTA CERTA-2012-AVI-272 du 10 mai 2012
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-272/index.html
- Note technique Apple TS4272 du 10 mai 2012 :
  https://support.apple.com/kb/TS4272

3 Informations sur les correctifs de la vulnérabilité CGI de PHP

Le 03 mai 2012 l'organisation PHP a corrigé une vulnérabilité liée à l'utilisation de PHP au moyen de CGI. Cette vulnérabilité permettait de lire le code source des fichiers PHP et d'exécuter du code arbitraire à distance

(voir CVE-2012-1823). Le 08 mai 2012 un deuxième correctif a été diffusé, cette fois avec l'identifiant CVE-2012-2311. Le premier correctif ne prenait pas en compte tous les moyens d'appels de la vulnérabilité, celle-ci était donc toujours présente sur de nombreux systèmes. Des outils permettant l'exploitation automatique de cette vulnérabilité ont été publiés.

Le CERTA recommande l'application de ces deux mises à jours

Documentation

- Bulletin de sécurité CERTA CERTA-2012-AVI-267 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-267/index.html
- Bulletin de sécurité CERTA CERTA-2012-AVI-246 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-246/index.html

4 Mise à jour mensuelle Microsoft

L'éditeur Microsoft a émis le 08 mai 2012 sept bulletins de sécurité pour des correctifs couvrant 23 vulnérabilités. Parmi ces sept bulletins, deux sont considérés comme critiques et les cinq autres sont considérés comme importants.

Les vulnérabilités corrigées permettent d'exécuter du code arbitraire à distance et d'élever ses privilèges.

Les produits corrigés sont :
- Microsoft Office ;
- Microsoft Visio Viewer ;
- la pile TCP/IP de Windows ;
- le gestionnaire de partition de Windows ;
- Silverlight ;
- le *framework* .NET.

Le CERTA recommande l'application de ces mises à jour dès que possible.

5 Rappel des avis émis

Dans la période du 04 au 10 mai 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-246 : Vulnérabilité dans PHP
- CERTA-2012-AVI-247 : Vulnérabilités dans HP Insight Management Agents
- CERTA-2012-AVI-248 : Vulnérabilités dans HP System Health Application and Command Line Utilities
- CERTA-2012-AVI-249 : Multiples vulnérabilités dans VMware
- CERTA-2012-AVI-250 : Multiples vulnérabilités dans Drupal
- CERTA-2012-AVI-251 : Vulnérabilité dans IBM AIX
- CERTA-2012-AVI-252 : Vulnérabilité dans Adobe Flash Player
- CERTA-2012-AVI-253 : Vulnérabilités dans FFmpeg
- CERTA-2012-AVI-254 : Vulnérabilité dans Microsoft Office
- CERTA-2012-AVI-255 : Vulnérabilités dans Microsoft Office
- CERTA-2012-AVI-256 : Vulnérabilité dans Microsoft Visio Viewer
- CERTA-2012-AVI-257 : Vulnérabilités dans la pile TCP/IP de Windows
- CERTA-2012-AVI-258 : Vulnérabilité dans le gestionnaire de partitions de Windows
- CERTA-2012-AVI-259 : Multiples vulnérabilités dans Office, Windows, NET et Silverlight
- CERTA-2012-AVI-260 : Vulnérabilités dans NET Framework
- CERTA-2012-AVI-261 : Vulnérabilités dans Pidgin
- CERTA-2012-AVI-262 : Multiples vulnérabilités dans les produits Apple
- CERTA-2012-AVI-263 : Multiples vulnérabilités dans Adobe Illustrator
- CERTA-2012-AVI-264 : Vulnérabilités dans Adobe Photoshop

– CERTA-2012-AVI-265 : Vulnérabilité dans Adobe Flash Professionnel
– CERTA-2012-AVI-266 : Multiples vulnérabilités dans Adobe Shockwave Player
– CERTA-2012-AVI-267 : Vulnérabilités dans PHP
– CERTA-2012-AVI-268 : Vulnérabilités dans HP Performance Insight
– CERTA-2012-AVI-269 : Vulnérabilité dans CiscoWorks Prime LAN Management
– CERTA-2012-AVI-270 : Vulnérabilités dans Horde IMP
– CERTA-2012-AVI-271 : Multiples vulnérabilités dans Safari
– CERTA-2012-AVI-272 : Multiples vulnérabilités dans OS X Lion
– CERTA-2012-AVI-273 : Vulnérabilité dans IBM AIX

Durant la même période, les publications suivantes ont été mises à jour :

– CERTA-2012-AVI-224-001 : Vulnérabilité dans OpenSSL (ajout du bulletin IBM OS/400)

6 Actions suggérées

6.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

6.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

6.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

6.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

6.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

6.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

6.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

Gestion détaillée du document

11 mai 2012 version initiale.