Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2012
N° CERTA-2012-ACT-028

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-028

Gestion du document

Référence	CERTA-2012-ACT-028
Titre	Bulletin d'actualité 2012-028
Date de la première version	13 juillet 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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-028.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-028/

1 *Mac OS X Mountain Lion* : renforcement de la sécurité grâce à *Gatekeeper* ?

La prochaine version du système d'exploitation Mac, *OS X Mountain Lion*, inclura une nouvelle fonctionnalité nommée *Gatekeeper*. L'objectif est de se prémunir contre l'installation d'applications téléchargées potentiellement malveillantes.

Concrètement *Gatekeeper* propose trois niveaux de paramétrage définissant les applications autorisées à être installées en fonction de leur provenance. Ainsi, du choix le plus restrictif au moins restrictif, il est possible d'autoriser :

- seulement les applications téléchargées sur le *Mac App Store* ;
- seulement les applications téléchargées sur le *Mac App Store* ou signées par un développeur Apple identifié (choix par défaut) ;
- n'importe quelle application.

Le principe de n'autoriser que les applications venant du *Mac App Store* apporte, en théorie, une sécurité accrue du fait de la vérification automatique effectuée par Apple du comportement des programmes soumis avant de les

rendre disponibles. Quelques exemples montrent toutefois qu'il peut y avoir des exceptions où la version d'une application sur le *Mac App Store* serait moins sûre que son homologue disponible en dehors du magasin d'Apple.

En premier lieu, prenons l'exemple d'un programme recevant une mise à jour de sécurité. Il y a parfois un délai entre la sortie de la nouvelle version de l'application sur le site de l'éditeur et la disponibilité de celle-ci dans le *Mac App Store*. Pendant cette période, la fonctionnalité *Gatekeeper* réglée sur le choix le plus restrictif déconseillera l'installation de la version la plus à jour.

Un deuxième exemple concerne les cas où une application doit être modifiée pour se plier aux conditions du *Mac App Store*, limitant ses fonctionnalités. Ce point peut être gênant pour un logiciel de sécurité, comme cela a été le cas pour *ClamXav* (voir Documentation).

Gatekeeper peut renforcer la sécurité. Toutefois, le CERTA recommande aux utilisateurs de cette fonctionnalité couplée au *Mac App Store* de peser les avantages et inconvénients. Pour certaines applications, il peut être plus pertinent de les télécharger directement sur le site de l'éditeur en question.

1.1 Documentation

- Présentation de *Gatekeeper* :
  http://www.apple.com/osx/what-is/security.html
- Article Sophos du 21 juin 2012 sur *Gatekeeper* :
  http://nakedsecurity.sophos.com/2012/06/21/mac-app-store-gatekeeper-security/

2 Mise à jour mensuelle de Microsoft

Le mois dernier, le CERTA avait publié une alerte concernant *XML Core Services*. La vulnérabilité a été corrigée par *Microsoft* ce mardi, nous fermons donc le document « CERTA-2012-ALE-003 ».

Concernant la mise à jour mensuelle de Microsoft, neuf bulletins ont été publiés. Trois d'entre eux concernant *Internet Explorer*, *Microsoft Data Access Components* et *XML Core Services* sont considérés comme critiques. La vulnérabilité mentionnée dans l'avis sur XML Core Services est actuellement exploitée par des attaquants.

Les différentes vulnérabilités corrigées permettent :

- l'exécution de code arbitraire à distance ;
- l'élévation de privilèges ;
- l'atteinte à la confidentialité des données ;
- l'atteinte à l'intégrité des données ;
- l'injection de code indirecte à distance.

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

Documentation :

- Alerte CERTA-2012-ALE-003 du 14 juin 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-003/
- Synthèse des bulletins de sécurité Microsoft du mois de juillet 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-jul

3 Rappel des avis émis

Dans la période du 6 juillet 2012 au 12 juillet 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-369 : Vulnérabilité dans HP ProtectTools Enterprise
- CERTA-2012-AVI-370 : Vulnérabilité dans Pidgin
- CERTA-2012-AVI-371 : Vulnérabilités dans Asterisk
- CERTA-2012-AVI-372 : Vulnérabilité dans eZ Publish eZOE
- CERTA-2012-AVI-373 : Vulnérabilités dans VLC
- CERTA-2012-AVI-374 : Vulnérabilités dans HP Operations Agent
- CERTA-2012-AVI-375 : Vulnérabilité dans Microsoft XML Core Services
- CERTA-2012-AVI-376 : Vulnérabilité Microsoft Visual Basic pour Applications

– CERTA-2012-AVI-377 : Vulnérabilités dans Microsoft Internet Explorer
– CERTA-2012-AVI-378 : Vulnérabilité dans Microsoft Data Access Components
– CERTA-2012-AVI-379 : Vulnérabilités dans des pilotes du noyau Windows
– CERTA-2012-AVI-380 : Vulnérabilité dans l'interpréteur de commande Windows
– CERTA-2012-AVI-381 : Vulnérabilité dans le protocole de chiffrement TLS
– CERTA-2012-AVI-382 : Vulnérabilité dans Microsoft SharePoint
– CERTA-2012-AVI-383 : Vulnérabilité dans Microsoft Office pour Mac
– CERTA-2012-AVI-384 : Multiples vulnérabilités dans les produits Cisco TelePresence
– CERTA-2012-AVI-385 : Vulnérabilités dans Google Chrome

4 Actions suggérées

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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

13 juillet 2012 version initiale.