Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 avril 2012
N° CERTA-2012-ACT-014

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-14

Gestion du document

Référence	CERTA-2012-ACT-014
Titre	Bulletin d'actualité 2012-14
Date de la première version	06 avril 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 Compromission via phpMyFaq

Cette semaine, le CERTA a traité un cas de compromission via une faille de *phpMyFaq*. Cette vulnérabilité, dévoilée par l'éditeur le 25 octobre 2011, affecte les versions 2.6.18 (et antérieures) et 2.7.0 du logiciel. Son exploitation permet l'exécution de code arbitraire à distance.

Un outil permettant d'exploiter automatiquement cette faille est disponible sur l'Internet et est utilisé par des attaquants. La réussite d'une attaque se traduit par une écriture dans le fichier :

<chemin d'installation>*/admin/editor/plugins/ajaxfilemanager/inc/data.php*

Le CERTA recommande aux administrateurs de serveurs Web de vérifier dans les journaux les accès au fichier mentionné ci-dessus et de mettre à jour *phpMyFaq*. La dernière version du logiciel est la version 2.7.4.

Documentation :

- Bulletin de sécurité phpMyFaq du 25 octobre 2011 :
  http://www.phpmyfaq.de/advisory_2011-10-25.php
- Message posté sur le forum de phpMyFaq le 24 octobre 2011 évoquant la vulnérabilité :
  http://forum.phpmyfaq.de/viewtopic.php?t=13402

2 Exploitation d'une vulnérabilité de Java sous Mac OS X

De nombreux utilisateurs de Mac OS X ont été récemment victimes de l'exploitation d'une vulnérabilité de Java (CVE-2012-0507). Cette vulnérabilité, rendue publique et corrigée par *Oracle* en février 2012, a été intégrée par *Apple* pour les versions 10.6.8 et 10.7.3 de son système d'exploitation le 3 avril 2012.

Ces infections nous rappellent qu'aucun système, y compris ceux embarqués dans les téléphones mobiles et les tablettes, n'est à l'abri d'un code malveillant.

Le CERTA recommande d'être vigilant à la mise-à-jour des systèmes et environnements d'exploitation.

Documentation :

- Avis CERTA-2012-085 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-085/
- Bulletin de sécurité Apple HT5228 du 3 avril 2012 :
  http://support.apple.com/kb/HT5228

3 Firefox bloque certaines versions de Java

Les dernières vulnérabilités liées à Java ont poussé *Mozilla* à revoir la politique de sécurité de *Firefox*. Les versions vulnérables de Java (version 6 mises à jour 30 et antérieures ainsi que la version 7 mises à jour 2 et antérieures) ont été ajoutées à la liste des applications bloquées par *Firefox*, afin d'améliorer la sécurité de leurs utilisateurs. La position de *Mozilla* est louable mais apporte également son lot de contraintes. En effet, certaines applications métier nécessitent une version vulnérable de Java pour fonctionner et ne sont donc plus accessibles via *Firefox*. Les développeurs de ce navigateur précisent que leur décision a été fortement influencée par le fait que les vulnérabilités affectant Java sont actuellement massivement exploitées.

D'une manière générale, le CERTA recommande de porter les applications métier qui le nécessitent, afin de les rendre compatibles avec les dernières versions de Java.

Documentation :

- Annonce du 2 avril 2012 sur le blog de Mozilla :
  http://blog.mozilla.com/addons/2012/04/02/blocking-java/

4 Rappel des avis émis

Dans la période du 30 mars au 05 avril 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-181 : Multiples vulnérabilités dans TYPO3
- CERTA-2012-AVI-182 : Multiples vulnérabilités dans Chrome
- CERTA-2012-AVI-183 : Vulnérabilité dans libpng
- CERTA-2012-AVI-184 : Multiples vulnérabilités dans VMware
- CERTA-2012-AVI-185 : Vulnérabilité corrigée dans CheckPoint
- CERTA-2012-AVI-186 : Vulnérabilités dans HP Onboard Administrator
- CERTA-2012-AVI-187 : Vulnérabilité dans IBM Cognos
- CERTA-2012-AVI-188 : Vulnérabilité dans Joomla!
- CERTA-2012-AVI-189 : Vulnérabilité dans HP-UX
- CERTA-2012-AVI-190 : Vulnérabilités dans curl
- CERTA-2012-AVI-191 : Vulnérabilité dans FreeRadius
- CERTA-2012-AVI-192 : Vulnérabilité dans libtiff
- CERTA-2012-AVI-193 : Vulnérabilités dans Cisco WebEx Player
- CERTA-2012-AVI-194 : Vulnérabilité dans HP Business Availability Center

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

06 avril 2012 version initiale.