Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2012
N° CERTA-2012-ACT-006

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-06

Gestion du document

Référence	CERTA-2012-ACT-006
Titre	Bulletin d'actualité 2012-06
Date de la première version	10 février 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 Le cloisonnement de *Flash Player* arrive sur *Firefox*

Cette semaine, Adobe a sorti une nouvelle version bêta de l'extension *Flash Player* pour le navigateur *Firefox*. La particularité de cette nouvelle version, aussi appelée mode protégé de *Flash Player*, est l'apport de mécanismes de cloisonnement (*sandboxing*), augmentant la sécurité grâce à la surveillance ou la limitation des actions effectuées par *Flash Player*.

Cette fonction est comparable au mode protégé d'*Adobe Reader X* ou au mode protégé de *Flash Player* du navigateur *Chrome*. Pour implémenter le cloisonnement, Adobe se base sur les mécanismes de sécurité offerts par le système d'exploitation *Windows*. Le processus *Flash Player* s'exécute ainsi avec des privilèges restreints qui limitent ses possibilités d'action. Lorsque ce processus cloisonné a besoin d'effectuer une action nécessitant de plus hauts privilèges, il doit faire une demande à un processus mandataire (appelé *broker*) qui, après vérification, va effectuer l'action à sa place si la demande est légitime. Le processus mandataire est donc responsable de mettre en œuvre une politique de sécurité et constitue, pour le processus cloisonné, la porte d'entrée sur le reste du système d'exploitation. Pour de plus amples détails, les lecteurs intéressés pourront consulter une série d'articles publiés par Adobe dont les liens se trouvent dans la section *Documentation*.

Le but de cette fonctionnalité est de limiter les dégâts d'une éventuelle exploitation de vulnérabilité dans *Flash Player*. Pour arriver à leurs fins, les attaquants devront désormais franchir, en plus, la barrière du cloisonnement. Selon Adobe, depuis sa sortie en novembre 2010, aucune exploitation réussie n'a encore été observée sur le mode

protégé d'*Adobe Reader X*.

Actuellement, cette version est disponible seulement pour les versions 4.0 ou supérieures de *Firefox*, sur les systèmes *Windows Vista* et *Windows 7*. Rappelons également que cette version est encore en bêta, par conséquent, il est déconseillé de l'installer sur des machines en production avant la sortie de la version finale, prévue cette année.

Documentation

- Annonce de la sortie sur le blog d'Adobe :
  http://blogs.adobe.com/asset/2012/02/flash-player-sandboxing-is-coming-to-firefox.html
- Articles techniques sur la méthode de cloisonnement utilisée dans *Adobe Reader X*, comparable à la méthode utilisée dans *Flash Player* pour Firefox :
  http://blogs.adobe.com/asset/2010/10/inside-adobe-reader-protected-mode-part-1-design.html
  http://blogs.adobe.com/asset/2010/10/inside-adobe-reader-protected-mode-%E2%80%93-part-2-%E2%80%93-the-sandbox-process.html
  http://blogs.adobe.com/asset/2010/11/inside-adobe-reader-protected-mode-part-3-broker-process-policies-and-inter-process-communication.html
  http://blogs.adobe.com/asset/2010/11/inside-adobe-reader-protected-mode-part-4-the-challenge-of-sandboxing.html

2 Contrôle des mécanismes d'accès à distance

Actuellement, le code source d'une version datant de 2006 du logiciel *pcAnywhere*, développé par la société Symantec, a été divulgué sur Internet. Ce logiciel permet la prise de contrôle à distance de postes. Le CERTA recommande à tous les utilisateurs de mettre à jour ce logiciel. Certaines vulnérabilités ont été découvertes dans ce logiciel.

Il semble également important de rappeler la nécessité de restreindre les accès à ce type de services à un ensemble limité de postes. Qu'il s'agisse de serveur FTP permettant de mettre à jour un site Web, d'un service de connexion ou prise de contrôle à distance, ou tout autre point d'entrée sur un système d'information à usage restreint, il convient non seulement de maintenir une politique de mot de passe raisonnée, mais également lorsque cela est possible, de limiter les accès à ces ressources aux seuls postes administrateurs.

En effet, dans un incident récent, il est apparu que des identifiants de connexion FTP ont pu être dérobés par une personne malveillante. Ceux-ci ont ensuite été utilisés pour accéder à un serveur en production, depuis une adresse IP différente du poste où ils ont été dérobés. Une simple liste blanche d'adresses IP autorisées à se connecter au serveur FTP aurait rendu beaucoup plus difficile l'exploitation des identifiants dérobés.

3 Utilisation des noms de domaines accentués

L'AFNIC a annoncé qu'elle va autoriser les noms de domaines accentués pour les différents domaines de premier niveau qu'elle gère. Du 3 mai au 3 juillet 2012, les détenteurs de noms de domaines sans accent auront la possibilité d'obtenir un nom de domaine accentué équivalent. Passé cette date, la règle du « premier arrivé, premier servi » s'appliquera.

Le CERTA met en garde contre les possibilités de « typosquatting » liées à l'apparition de ces nouveaux caractères et recommande la réservation des nouveaux noms de domaines possibles.

Documentation

- Document de l'AFNIC décrivant les nouvelles spécifications :
  http://www.afnic.fr/medias/documents/afnic-idn-specifications-techniques.pdf

4 Rappel des avis émis

Dans la période du 28 janvier 2012 au 09 février 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-052 : Multiples vulnérabilités dans Drupal
- CERTA-2012-AVI-053 : Vulnérabilités dans Bugzilla
- CERTA-2012-AVI-054 : Vulnérabilités dans Mac OS X
- CERTA-2012-AVI-055 : Vulnérabilité dans PHP
- CERTA-2012-AVI-056 : Vulnérabilités dans Blue Coat Reporter
- CERTA-2012-AVI-057 : Vulnérabilité dans EMC Documentum
- CERTA-2012-AVI-058 : Vulnérabilité dans Skype
- CERTA-2012-AVI-059 : Vulnérabilités dans DotNetNuke
- CERTA-2012-AVI-060 : Vulnérabilité dans EMC Documentum xPlore
- CERTA-2012-AVI-061 : Vulnérabilité dans Xen
- CERTA-2012-AVI-062 : Vulnérabilité dans IBM AIX
- CERTA-2012-AVI-063 : Multiples vulnérabilités dans Apache pour HP-UX
- CERTA-2012-AVI-064 : Vulnérabilités dans RealPlayer
- CERTA-2012-AVI-065 : Multiples vulnérabilités dans JBoss Operations Network
- CERTA-2012-AVI-066 : Vulnérabilité dans JBoss Enterprise Platform
- CERTA-2012-AVI-067 : Vulnérabilité dans Red Hat Network Satellite
- CERTA-2012-AVI-068 : Vulnérabilité dans Red Hat Network Proxy
- CERTA-2012-AVI-069 : Vulnérabilités dans Google Chrome
- CERTA-2012-AVI-070 : Vulnérabilité dans Avaya Interaction Center

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

- CERTA-2011-AVI-630-001 : Multiples vulnérabilités dans Adobe Flash Player (ajout du bulletin Oracle)
- CERTA-2012-AVI-032-001 : Vulnérabilités dans pcAnywhere (ajout du CVE CVE-2012-0290)

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

10 février 2012 version initiale.