Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 septembre 2012
N° CERTA-2012-ACT-037

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-037

Gestion du document

Référence	CERTA-2012-ACT-037
Titre	Bulletin d'actualité CERTA-2012-ACT-037
Date de la première version	14 septembre 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 Windows 8, Internet Explorer 10 et Adobe Flash Player

La prochaine version de *Microsoft Windows (Windows 8)* comprend le navigateur *Internet Explorer 10*, qui intègre nativement le lecteur *Adobe Flash Player*. Cela signifie notamment que ce lecteur ne sera plus mis à jour indépendamment du navigateur. *Microsoft* a annoncé que ces mises à jour commenceront lorsque *Windows 8* sera officiellement mis en vente, le 26 octobre 2012.

Cependant, de nombreux services informatiques ont des contrats privilégiés avec *Microsoft*, qui leur permettent un accès à ses produits avant leur sortie officielle, à des fins de tests. La version finale de *Windows 8* est déjà disponible pour ces contrats, et certains utilisateurs peuvent l'avoir déjà installée sur leur SI d'entreprise. Or, une vulnérabilité majeure de *Flash player* a été publiée après la finalisation de *Windows 8*. En l'absence de mise à jour possible avant le 26 octobre, les utilisateurs sont donc vulnérables.

Le CERTA recommande donc à ceux qui testent actuellement *Windows 8* en environnement opérationnel :

– soit de désactiver *Flash*. Cette opération n'est pas possible via l'interface graphique de *Windows 8* (appelée parfois « Metro »), mais elle peut se réaliser via l'interface classique ;
– soit d'utiliser un navigateur alternatif avec une version à jour de *Flash*.

2 Applications sur ordiphones et données personnelles

La collecte d'informations par les applications sur les périphériques mobiles est aujourd'hui très courante. Celles-ci peuvent être utilisées par des agences publicitaires afin de mieux cibler un profil d'utilisateur.

Récemment, une liste contenant plusieurs millions d'identifiants de terminaux *Apple* appelées *UDID* (*Unique Device ID*) a été publiée sur l'Internet. Seuls, ces identifiants ne permettent pas d'identifier physiquement le propriétaire du périphérique. Dans le cas présent, cette liste contenait également les nom et prénom des personnes "associées" à cet *UDID*, rendant inexistant le principe d'anonymisation des données.

En principe, *Apple* n'autorise pas une application à collecter des données permettant l'identification d'une personne. En pratique, il est très difficile de vérifier une telle règle.

Le CERTA recommande à tout utilisateur de vérifier si l'installation et l'utilisation d'une application est conforme à la PSSI de son entreprise, et aux RSSI de qualifier si celle-ci ne présente pas un risque évident de sécurité pour le SI avant d'en autoriser l'emploi.

3 Mise à jour mensuelle de Microsoft

Ce mois-ci deux avis relatifs aux mises à jour Microsoft ont été publiés. Le premier concerne une vulnérabilité dans *Visual Studio Team Foundation Server 2010 Service Pack 1* « CERTA-2012-AVI-494 » et le deuxième porte sur *System Center Configuration Manager* « CERTA-2012-AVI-495 ».

Les vulnérabilités corrigées permettent :

- de l'injection de code indirecte à distance *(*cross-site-scripting) ;
- une élévation de privilèges.

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

Documentation :

- Synthèse des bulletins de sécurité Microsoft du mois de Septembre 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-sep

4 Rappel des avis émis

Dans la période du 7 au 13 septembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-488 : Multiples vulnérabilités dans HP Business Availability Center
- CERTA-2012-AVI-489 : Multiples vulnérabilités dans IBM Asset and Service Mgmt
- CERTA-2012-AVI-490 : Vulnérabilité dans Xen
- CERTA-2012-AVI-491 : Vulnérabilités dans WordPress
- CERTA-2012-AVI-492 : Vulnérabilité dans le système SCADA Honeywell HMIWeb
- CERTA-2012-AVI-493 : Vulnérabilité dans FreeRADIUS
- CERTA-2012-AVI-494 : Vulnérabilité dans Visual Studio Team Foundation Server
- CERTA-2012-AVI-495 : Vulnérabilité dans System Center Configuration Manager
- CERTA-2012-AVI-496 : Vulnérabilité dans ColdFusion
- CERTA-2012-AVI-497 : Vulnérabilités dans McAfee Firewall Enterprise
- CERTA-2012-AVI-498 : Vulnérabilités dans RSA BSAFE SSL-C
- CERTA-2012-AVI-499 : Vulnérabilité dans RSA BSAFE Micro Edition Suite
- CERTA-2012-AVI-500 : Vulnérabilité dans ISC BIND
- CERTA-2012-AVI-501 : Vulnérabilité dans ISC DHCP

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 CERTA recommande l'application des correctifs de sécurité.

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

14 septembre 2012 version initiale.