Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 novembre 2010
N° CERTA-2010-ACT-047

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-47

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-047`

Gestion du document

Référence	CERTA-2010-ACT-047
Titre	Bulletin d'actualité 2010-47
Date de la première version	26 novembre 2010
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-2010-ACT-047.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-2010-ACT-047/

1 Incident de la semaine

Cette semaine le CERTA a traité un cas de compromission de site web. Le site en question, basé sur un gestionnaire de contenu non mis à jour, présentait tous les symptômes d'une attaque réussie de type injection de code. De prime-abord, une seule page semblait touchée mais, en réalité, plusieurs centaines de pages avaient été modifiées.

Le CERTA a été sollicité pour faire l'analyse des journaux de la machine et diagnostiquer l'ampleur des dégâts commis. Cependant, l'hébergeur n'a pu fournir à la date de ce bulletin qu'un seul mois de journaux à analyser. Or, après une rapide lecture, il est apparu que la compromission initiale datait sans doute de beaucoup plus longtemps. En l'état, l'analyse n'a pas permis de mettre en évidence le point d'entrée utilisé par le ou les attaquants pour compromettre le site.

1.1 Recommandations

En l'espèce, un délai d'un mois était clairement insuffisant pour la conservation des journaux. L'expérience montre qu'il faut parfois remonter plusieurs mois en arrière pour retrouver l'origine d'une compromission. Il convient donc de conserver les journaux sur une période d'au moins un an. En matière de conservation et plus

généralement sur la gestion des journaux, vous pouvez également vous référer à la note d'information CERTA-2008-INF-005.

1.2 Documentation

– Note d'information CERTA-2008-INF-005 :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-005/

2 Sortie d'Adobe Reader X

Le 18 novembre dernier, la version 10 du lecteur de PDF `Adobe Reader` est sortie. La principale nouveauté de cette version est l'ajout d'un mode protégé, basé sur l'utilisation d'un mécanisme de « *bac à sable* », pour les versions `Windows` de cet outil.

2.1 Fonctionnement du mécanisme de bac à sable

Le mécanisme de *bac à sable* mis en place dans cette nouvelle version s'appuie à la fois sur les mécanismes de sécurité de `Windows` (plus particulièrement `Windows Vista/7`) et sur les implémentations existantes telles que le *bac à sable* de `Google Chrome`, ou certains mécanismes mis en place dans `MS Office`.

Le code responsable du rendu du PDF est exécuté à l'intérieur du processus *bac à sable*, les opérations effectuées sur le système par ce code sont limitées au minimum nécessaire.

Afin de limiter ces actions, `Adobe Reader` va appliquer les restrictions suivantes au processus *bac à sable* :
– limitation du jeton d'accès de sécurité du processus ;
– assignation de ce processus à un *job object* avec des restrictions ;
– exécution du processus à un niveau d'intégrité bas (uniquement sur `Windows Vista`, `7` et `Server2008`).

Les actions sur le système, interdites à l'intérieur du *bac à sable* (écriture dans un fichier, d'une clé de registre…) sont relayées à un processus appelé *broker process* qui va autoriser ou non ces actions. Ce processus a le rôle d'un « proxy de confiance ». Il maintient à jour une liste de règles, décrivant les interactions autorisées sur le système, sous forme de liste blanche. Ce processus relaie donc seulement les requêtes faisant partie de cette liste. Un administrateur peut, par l'intermédiaire d'un fichier de configuration, ajouter des règles à cette liste blanche. D'autres règles sont ajoutées dynamiquement à l'exécution (par exemple lors de la sauvegarde d'un fichier, une règle est ajoutée pour pouvoir écrire dans ce fichier).

2.2 Limitations

Pour l'instant seules les opérations d'écritures sont restreintes. Le mécanisme de *bac à sable* ne protège pas des lectures non autorisées du système de fichiers, des accès au réseau ou encore des lectures du presse-papier. Il est cependant prévu d'étendre le contrôle des actions effectuées sur le système aux opérations de lecture.

2.3 Conclusion

En mettant à disposition un mécanisme de bac à sable, cette nouvelle version du lecteur de PDF d'`Adobe` présente une évolution intéressante en matière de sécurité, tout particulièrement dans `Windows Vista/7`.

La présence de ce mécanisme ne dispense cependant pas de maintenir à jour son lecteur PDF. Elle ne représente en effet pas une protection ultime mais simplement un élément de sécurité supplémentaire à combiner avec d'autres éléments tels que la prévention de l'exécution des données (DEP) ou l'allocation non-linéaire de mémoire (ASLR) dans une optique de défense en profondeur.

Enfin, on notera que si par défaut le mode protégé est activé, l'interprétation du *JavaScript* et du *Flash* l'est également. Le CERTA rappelle donc qu'il est fortement recommandé de désactiver par défaut l'interprétation de ces deux langages afin de limiter la surface d'attaque de l'application.

2.4 Documentation

– Blog de l'équipe de développement sécurisé d'Adobe :
http://blogs.adobe.com/asset/

3 Contournement de l'UAC

Cette semaine, le CERTA a été informé d'une vulnérabilité concernant Microsoft Windows permettant à un utilisateur malintentionné une élévation de privilèges en contournant l'UAC (*User Account Control*). Les systèmes vulnérables seraient :

– Microsoft Windows 7 ;
– Microsoft Windows Server 2008 SP2 ;
– Microsoft Windows Vista SP2.

Une preuve de concept a déjà été publiée sur l'internet. Elle exploite une vulnérabilité de type dépassement de mémoire tampon dans la fonction *RtlQueryRegistryValues* du driver *win32k.sys* lors de l'accès à des valeurs de registre dont le type a été modifié.

En attendant un correctif de la part de Microsoft, le CERTA rappelle qu'il est nécessaire de ne pas exécuter de programme dont l'origine est inconnue ou suspecte.

Documentation

– Bulletin d'actualité du CERTA CERTA-2009-ACT-049 concernant l'UAC :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-049/

4 Liens utiles

– Mémento sur les virus :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
– Note d'information du CERTA sur l'acquisition de correctifs :
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
– Note d'information du CERTA sur les systèmes obsolètes :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
– Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
– Note d'information du CERTA sur les mots de passe :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
– Note d'information sur la terminologie d'usage au CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
– Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
– Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
http://www.auscert.org.au/render.html?it=1937
– Note d'information du CERTA sur les risques associés aux clés USB :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
– Note d'information du CERTA sur les outils d'indexation et de recherche :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
– Note d'information du CERTA sur la gestion des noms de domaine :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
– Note d'information du CERTA sur le bon usage de PHP :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

5 Rappel des avis émis

Dans la période du 19 au 25 novembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-556 : Vulnérabilité dans VLC
- CERTA-2010-AVI-557 : Vulnérabilité dans Apple MacOS X Server
- CERTA-2010-AVI-558 : Multiples vulnérabilités dans Apple Safari
- CERTA-2010-AVI-559 : Vulnérabilité dans phpBB
- CERTA-2010-AVI-560 : Vulnérabilités dans Wireshark
- CERTA-2010-AVI-561 : Multiples vulnérabilités dans Cisco Videoconferencing
- CERTA-2010-AVI-562 : Vulnérabilité dans DotNetNuke
- CERTA-2010-AVI-563 : Vulnérabilité dans Trend Micro OfficeScan
- CERTA-2010-AVI-564 : Vulnérabilité dans les produits Horde
- CERTA-2010-AVI-565 : Multiples vulnérabilités dans Apple iOS
- CERTA-2010-AVI-566 : Vulnérabilité dans PGP Desktop

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_rubrique67.html

7 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

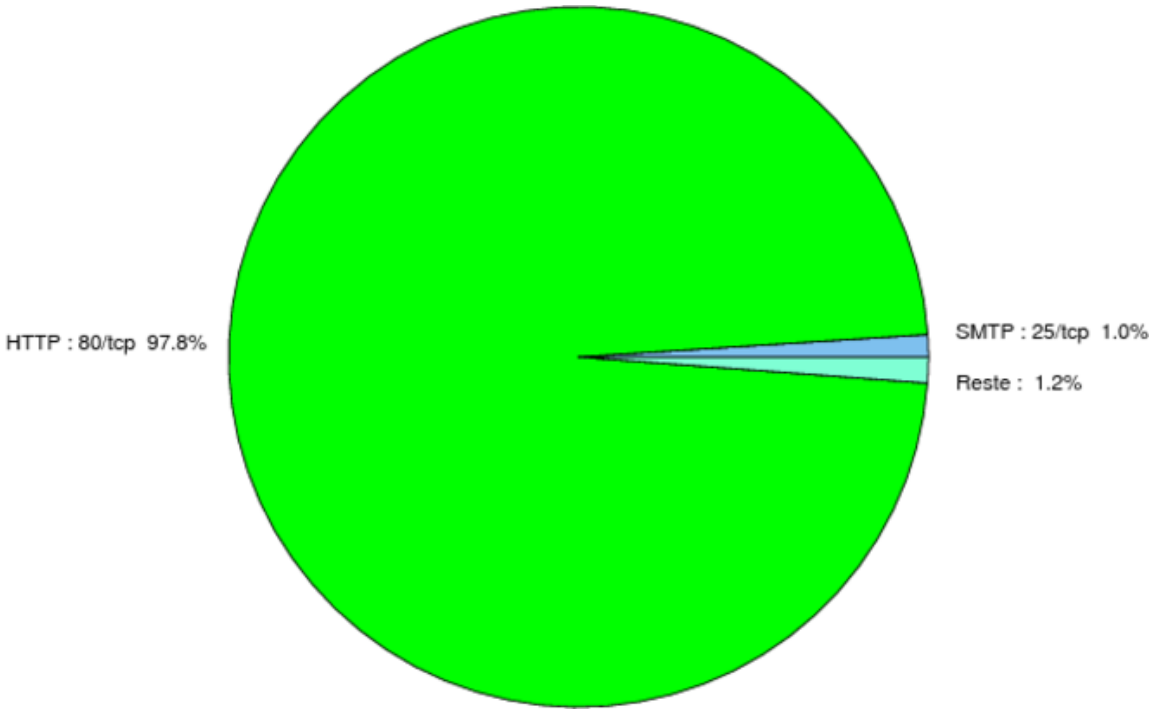

FIG. 1: Répartition relative des ports pour la semaine du 19 au 25 novembre 2010

port	pourcentage
80/tcp	97.88
25/tcp	1.02
1433/tcp	0.28
23/tcp	0.24
445/tcp	0.18
1080/tcp	0.13
22/tcp	0.11
135/tcp	0.06
3389/tcp	0.05
21/tcp	0.04
3306/tcp	0.02

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

26 novembre 2010 version initiale.