Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 décembre 2010
N° CERTA-2010-ACT-048

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-48

Gestion du document

Référence	CERTA-2010-ACT-048
Titre	Bulletin d'actualité 2010-48
Date de la première version	03 décembre 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-048.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-048/

1 Compromission du serveur de distribution de ProFTPD

Les développeurs de *ProFTPD* ont annoncé sur leur site Web (www.proftpd.org) que le serveur `ftp.proftpd.org` avait été compromis. Cet incident a eu pour conséquence l'ajout d'une porte dérobée dans les sources proposées au téléchargement. Les sources contenues dans le `CVS` n'ont pas été modifiées par les attaquants. Le service de distribution des sources vers les sites miroir (`rsync.proftpd.org`) est hébergé sur le même serveur, ce qui implique que tous les sites officiels proposant le logiciel *ProFTPD* ont été affectés.

Les sources contenant la porte dérobée ont été proposées en téléchargement du 28 novembre 2010 au 02 décembre 2010. Toute personne ayant téléchargé ces fichiers dans cet intervalle de temps est invitée à contacter le CERTA.

Le CERTA recommande, par précaution, à tous les administrateurs de serveur *ProFTPD* de vérifier les signatures des sources.

Documentation :

– Annonce du 1 décembre 2010 de la compromission des sources de ProFTPD sur le site officiel des développeurs :

http://www.proftpd.org/
– Page des signatures MD5 et PGP des sources de ProFTPD :
http://www.proftpd.org/md5_pgp.html

2 Incompatibilité passagère entre Windows 7 64 bits et l'antivirus AVG 2011

2.1 Les faits

Une mise à jour de l'antivirus AVG 2011 perturbait le redémarrage des ordinateurs fonctionnant sous Windows 7 en 64 bits. Le fichier incriminé a été identifié, il s'agit de la mise à jour 3292. Les utilisateurs touchés sont ceux qui ont téléchargé cette mise à jour et tenté de redémarrer leur ordinateur.

L'éditeur donne des indications selon que l'utilisateur :

– n'a pas téléchargé la mise à jour : elle a été ôtée du serveur de mise à jour, le risque est supprimé ;
– a téléchargé, mais n'a pas encore redémarré : un correctif est disponible ;
– a téléchargé et a tenté de redémarré : l'utilisation du disque (cédérom) de secours est détaillée, sous réserve qu'il ait été créé en temps utile.

De son côté, le SANS propose une méthode assez radicale pour les utilisateurs en panne après cette mise à jour et n'ayant pas de disque de secours.

Comme tout logiciel, un antivirus peut contenir une erreur conduisant à des dysfonctionnements majeurs. L'incident permet de tirer deux recommandations :

– d'une part, il est utile de procéder à une vérification de compatibilité de toute mise à jour avec l'existant avant un déploiement général ;
– d'autre part, les systèmes de secours ou de retour à une situation antérieure fonctionnelle doivent être préparés. Il est souhaitable de s'être entraîné à les utiliser afin d'aborder plus sereinement un tel incident.

2.2 Documentation

– Communiqué de l'éditeur AVG :
http://www.avg.com/fr-fr/actualites-articles-de-presse.ndi-394
– Billet du journal du SANS du 03 décembre 2010 :
http://isc.sans.org/diary.html?stotyid=10030

3 Mise à jour non officielle

Le CERTA rappelle, à l'occasion d'une vulnérabilité potentielle dans le noyau Windows publiée sur un site spécialisé, l'importance de n'appliquer que des mises à jour officielles.

Sur ce site spécialisé, il est fait mention d'une vulnérabilité dans le noyau `Windows` qui pourrait permettre à une personne malveillante ayant un accès local au système d'élever ses privilèges ou de provoquer un déni de service.

`Microsoft` n'a cependant pas réagi à cette publication, tandis que des sociétés spécialisées en sécurité informatique ont publié un correctif *non officiel* pour cette vulnérabilité.

L'application de correctifs de sécurité non officiels peut être un risque majeur pour la sécurité du système d'information ou sa productivité.

En effet, au delà des effets de bords induits par l'application de ces correctifs non officiels, par exemple des tests non exhaustifs sur les différentes plateformes, il ne peut être exclu que le correctif ne corrige que partiellement la vulnérabilité ou encore qu'il apporte une nouvelle vulnérabilité.

De plus, le thème des mises à jour de sécurité pour `Windows` est un sujet souvent utilisé lors de l'envoi massif de courriers électroniques non sollicités pour inciter l'utilisateur à exécuter un code malveillant en pièce jointe.

Documentation

– note d'information CERTA-2001-INF-004 sur l'acquisition des correctifs :
http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/

4 Vunérabilités dans HP WebOs

Deux chercheurs ont découvert plusieurs vulnérabilités dans *Palm Pre WebOs 1.4.x*.

L'une d'entre elles permet, à distance et par l'intermédiaire d'une *injection de code indirecte* (XSS) dans l'application des contacts, de récupérer des informations sensibles ou d'exécuter du code arbitraire à distance.

HP aurait corrigé ce problème dans la version 2.0 beta. Cependant, d'autres vulnérabilités similaires ont été reportées par les deux chercheurs.

Le CERTA rappelle qu'il est important de bien considérer les informations pouvant être contenues sur de tels appareils et de réévaluer les menaces contre le SI.

5 Sandbox du lecteur Flash dans Chrome

Le bulletin d'actualité de la semaine dernière présentait la nouvelle version d'*Adobe Reader* qui utilise un mécanisme de *bac à sable* (*sandbox*) dans les versions `Windows`. Cette semaine, c'est l'équipe de développement de `Chromium` qui annonce l'intégration de ce mécanisme pour le lecteur de documents *Flash* utilisé par *Google Chrome* (pour les versions `Windows XP/Vista/7`).

La technologie de *sandbox* utilisée se base sur une version modifiée de celle implémentée dans `Chrome`. Cette fonctionnalité sera disponible, dans un premier temps, uniquement dans les versions « développeur » de `Chrome`. Il est bien évidemment déconseillé d'installer ces versions sur un système en production. `Internet Explorer` propose un mécanisme de bac à sable similaire pour le lecteur *Flash*, mais uniquement avec `Windows Vista/7`. Cette nouvelle version de `Chrome` sera donc la seule à proposer le *sandbox* du lecteur *Flash* sous `Windows XP`.

Enfin, on notera qu'il est prévu d'étendre cette protection aux autres systèmes d'exploitation.

6 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/

7 Rappel des avis émis

Dans la période du 26 novembre au 02 décembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-549-001 : Vulnérabilité dans libxml2
- CERTA-2010-AVI-567 : Vulnérabilités dans Apache Tomcat
- CERTA-2010-AVI-568 : Vulnérabilités dans WordPress
- CERTA-2010-AVI-569 : Vulnérabilité dans Kerio Control Web Filter
- CERTA-2010-AVI-570 : Vulnérabilité dans VMware ESX
- CERTA-2010-AVI-571-001 : Vulnérabilités dans Kerberos
- CERTA-2010-AVI-572 : Vulnérabilité dans phpMyAdmin
- CERTA-2010-AVI-573 : Multiples vulnérabilités dans les produits Hitachi Cosminexus

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2009-AVI-482-011 : Vulnérabilité du protocole SSL/TLS (ajout du bulletin IBM WebSphere MQ)
- CERTA-2010-AVI-266-001 : Vulnérabilité dans Samba (ajout des références aux bulletins des distributions)
- CERTA-2010-AVI-449-001 : Vulnérabilité dans bzip2 (ajout des bulletins des distibutions Debian, RedHat, Sun, Suse et Ubuntu)
- CERTA-2010-AVI-510-001 : Vulnérabilités dans Apache (ajout des bulletins de sécurité Fedora, Mandriva et Sun)
- CERTA-2010-AVI-555-001 : Vulnérabilité dans OpenSSL (ajout des références aux bulletins de sécurité FreeBSD et Debian)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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

9 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.

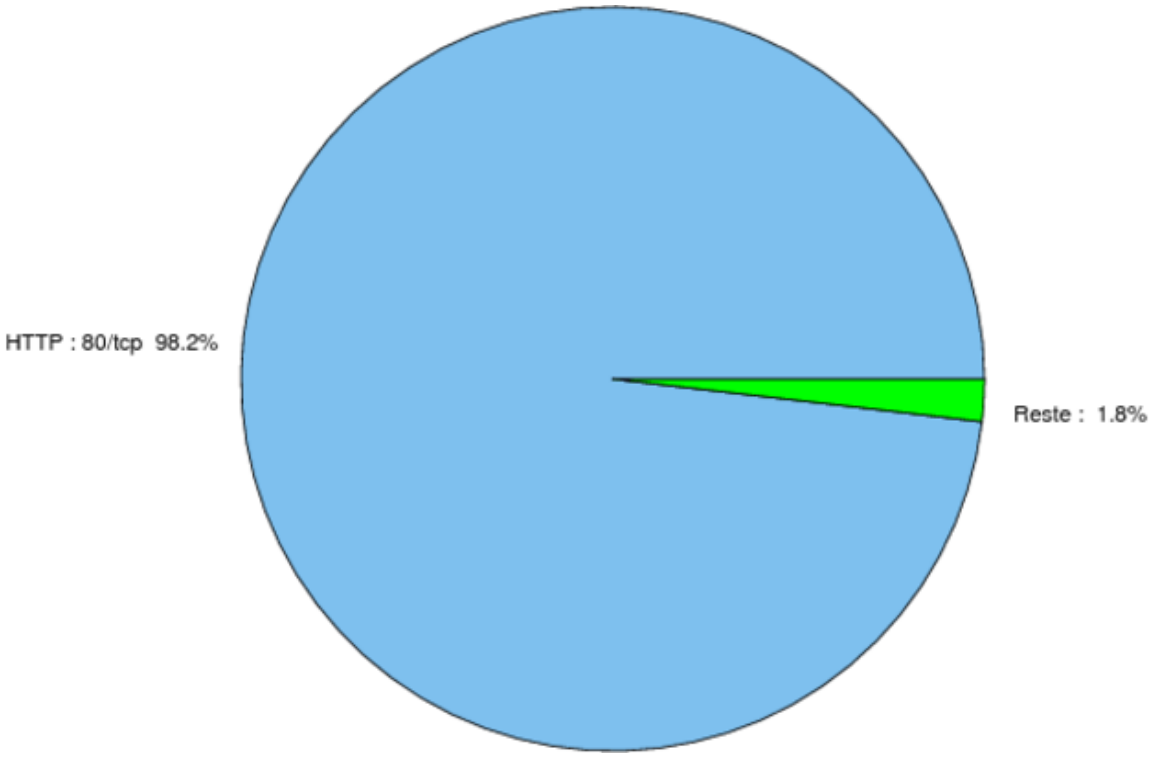

FIG. 1: Répartition relative des ports pour la semaine du 26 novembre au 02 décembre 2010

port	pourcentage
80/tcp	98.29
25/tcp	0.79
1433/tcp	0.22
1080/tcp	0.15
445/tcp	0.13
2967/tcp	0.07
135/tcp	0.06
3389/tcp	0.03
21/tcp	0.02
3306/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

03 décembre 2010 version initiale.