



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2010
N° CERTA-2010-ACT-040

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-40

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-040>

Gestion du document

Référence	CERTA-2010-ACT-040
Titre	Bulletin d'actualité 2010-40
Date de la première version	08 octobre 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-040.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-040/>

1 Mise à jour des produits Adobe Reader et Acrobat

Cette semaine, Adobe a publié une mise à jour pour ses produits Adobe Reader et Adobe Acrobat. Ce correctif comble 23 vulnérabilités dans les branches 8 et 9 pour toutes les plateformes supportées. Cet ensemble de correction a fait l'objet de l'avis CERTA-2010-AVI-470.

L'une de ces 23 vulnérabilités, détaillée dans l'alerte CERTA-2010-ALE-014, avait été activement exploitée sur l'Internet. Le CERTA rappelle donc qu'il est impératif de mettre le plus rapidement possible à jour ces applicatifs afin de limiter les risques de compromission de son SI.

Documentation

- Avis CERTA-2010-AVI-470 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-470/>
- Alerte CERTA-2010-ALE-014 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-014/>
- Bulletin de sécurité Adobe APSB10-21 du 05 octobre 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-21.html>

2 Cybersurveillance de l'activité des salariés par leur employeur

Dernièrement, un site proposant aux employeurs un produit permettant de surveiller l'activité de leurs employés a défrayé la chronique. Cette solution formidable permet d'enregistrer les frappes clavier, de conserver des captures d'écran, d'enregistrer les mots de passe, de faire des captures ICQ, Miranda, Skype, Google Talk, MSN, ...

Cet outil ne peut que faire le bonheur des employeurs, comme en témoigne un directeur sécurité. ... Bien sûr, ce site rappelle qu'il faut faire une déclaration à la CNIL, informer préalablement les employés de la mise en service de cet outil et consulter préalablement le comité d'entreprise.

En effet, le droit du travail considère que l'employeur a le droit de contrôler l'activité professionnelle de ses salariés, mais cela doit s'opérer dans certaines conditions et en respectant certains principes :

- l'informatique doit être au service de chacun ; toutefois, elle ne doit porter atteinte ni à l'identité humaine ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles et privées (article 1er de la loi du 6 janvier 1978) ; la Cour de Cassation reconnaît de son côté que « chacun a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances. . . »
- le recours au contrôle doit être motivé et proportionnel au but poursuivi (art. L 121-8 du Code du Travail).

On peut noter que ce dernier point est totalement « oublié » de la page d'avertissement de ce site commercial, et à ce propos on ne peut considérer comme justifié, pour mener à bien le contrôle de l'activité des salariés, d'utiliser les fonctionnalités d'enregistrement de frappes clavier, enregistrement de mots de passe, captures ICQ, Skype, MSN (dialogue en ligne, ou clavardage comme diraient nos amis québécois)... Au contraire, cela pourrait susciter des poursuites au pénal, notamment en matière d'atteinte au secret des correspondances. Ainsi, il apparaît que l'utilisation de ce type de solution n'est ni conforme au principe de proportionnalité, ni respectueux des principes posés par la loi « informatique et libertés », tant en matière de respect de la vie privée que de finalité.

3 Vulnérabilité dans les libc

Cette semaine, une vulnérabilité touchant la bibliothèque de fonctions *libc* a été rendue publique. Il s'agit d'un problème liée à la fonction *glob()*. Celle-ci permet à son utilisateur de mettre en œuvre le support des caractères génériques (*wildcards*) comme l'astérisque «*», le point d'interrogation «?» ou encore la virgule «,».

Dans la mesure où l'activation de ce support dans certaines applications peut entraîner une importante consommation de mémoire en fonction des *wildcards* utilisés, il existe dans les différentes implémentations de *libc* une variable globale à renseigner dans le code source limitant la consommation de mémoire par la fonction *glob()*. Or dans certains cas, cette variable, bien que correctement renseignée, est inopérante car non-prise en compte par la fonction. Ainsi des attaques visant à saturer les ressources du système vulnérable par le biais de *wildcards* particuliers sont possibles.

Or, la fonction *glob()* est utilisée dans de nombreux cas, en particulier par des serveurs FTP. Ainsi, sont concernés les serveurs standards livrés dans NetBSD, FreeBSD, OpenBSD, Oracle Solaris mais également ceux s'appuyant sur la bibliothèque GNU/libc. De plus, la plupart du temps cette fonctionnalité bien pratique est activée par défaut. Il est donc facile de s'en prendre à un serveur FTP vulnérable en particulier s'il autorise une connexion anonyme (pas d'authentification requise). En fonction de la capacité de la machine et des particularités locales, l'attaque pourra se traduire par de « simples » dysfonctionnements ou par un ralentissement pouvant aller jusqu'à un déni de service complet. Il est à noter que les serveurs SFTP s'appuyant sur les mêmes briques de base (*ftp* et *libc*) peuvent être également vulnérables.

Recommandation :

Pour le moment seul NetBSD a publié un correctif (NetBSD-SA2010-008) corrigeant le problème. Dans tous les autres cas, il conviendra, en attendant une mise à jour, de désactiver la fonctionnalité « *glob* ».

4 Cassage du chiffrement des fichiers de sauvegarde BlackBerry

Un certain nombre d'articles ont annoncé, cette semaine, qu'une société russe commercialisait un produit permettant de casser rapidement la protection des données des BlackBerry.

Il est nécessaire de préciser que ce n'est pas la protection des données sur les ordiphones (*smartphones*) qui est concernée mais la protection des fichiers de sauvegarde, stockés hors du *smartphone*. Ces fichiers de sauvegarde sont chiffrés à l'aide de l'algorithme AES avec une clé 256 bits. Ce n'est bien évidemment pas cet algorithme qui est attaqué, mais la fonction de dérivation de clé (PBKDF2), utilisée pour créer une clé AES à partir du mot de

pas de l'utilisateur. Cette fonction n'étant pas correctement utilisée, il est possible de retrouver la clé calculée à l'aide d'une attaque par force brute.

La portée de cette attaque reste limitée par le fait qu'il est nécessaire d'avoir accès au poste où est stocké le fichier de sauvegarde.

5 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/>

6 Rappel des avis émis

Dans la période du 01 au 07 octobre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-461 : Multiples vulnérabilités dans VMware ESX Server
- CERTA-2010-AVI-462 : Vulnérabilité dans HP-UX Directory Server
- CERTA-2010-AVI-463 : Vulnérabilité dans IBM WebSphere Application Server Community Edition
- CERTA-2010-AVI-464 : Vulnérabilité dans les commutateurs 3Com H3C 3100 et 3600
- CERTA-2010-AVI-465 : Vulnérabilité dans IBM DB2 Administration Server
- CERTA-2010-AVI-466 : Vulnérabilités dans les produits Horde
- CERTA-2010-AVI-467 : Vulnérabilité dans Blue Coat ProxySG
- CERTA-2010-AVI-468 : Vulnérabilité dans Novell iManager
- CERTA-2010-AVI-469 : Vulnérabilités dans MySQL
- CERTA-2010-AVI-470 : Vulnérabilité dans Adobe Reader et Adobe Acrobat
- CERTA-2010-AVI-471 : Vulnérabilité dans PostgreSQL
- CERTA-2010-AVI-472 : Vulnérabilité dans Dovecot
- CERTA-2010-AVI-473 : Vulnérabilités dans MantisBT
- CERTA-2010-AVI-474 : Multiples vulnérabilités dans TYPO3
- CERTA-2010-AVI-475 : Vulnérabilité dans Foxit Reader et Foxit Phantom
- CERTA-2010-AVI-476 : Vulnérabilité dans MIT Kerberos

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

- CERTA-2010-AVI-418-001 : Vulnérabilités dans MantisBT (ajout des références CVE)

7 Actions suggérées

7.1 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 réglementaire, 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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 inexplicables 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.

7.7 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

8 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.

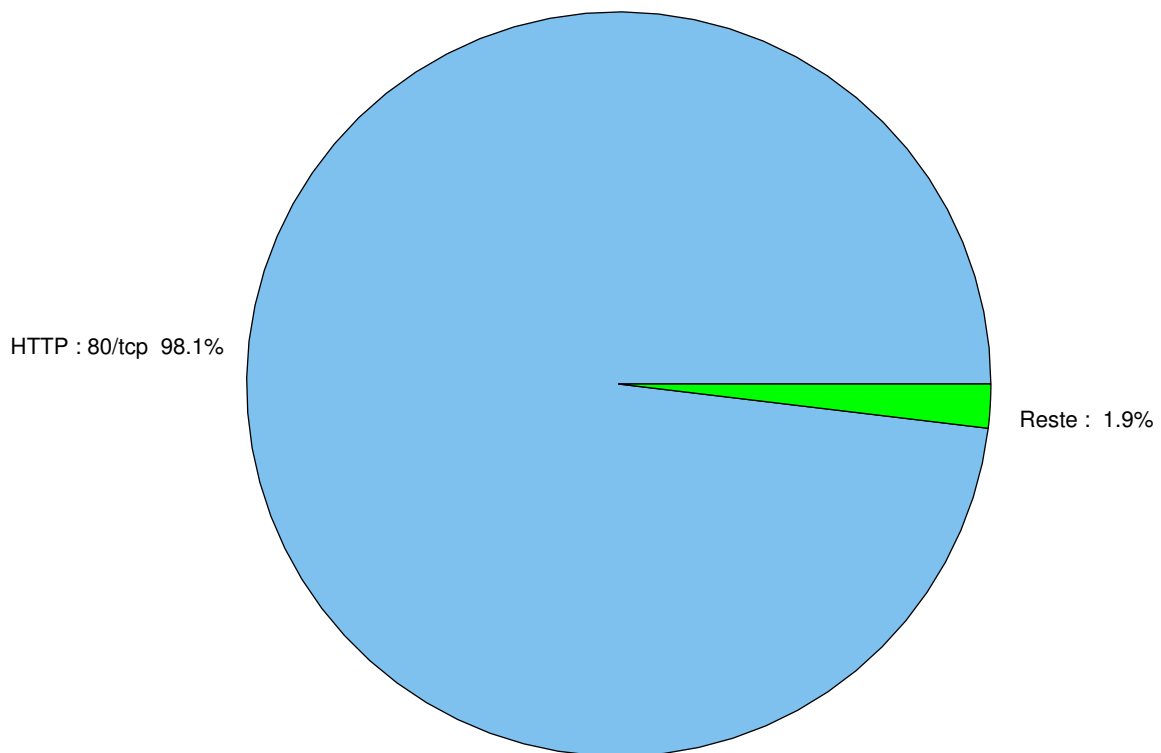


FIG. 1: Répartition relative des ports pour la semaine du 01 au 07 octobre 2010

port	pourcentage
80/tcp	98.17
25/tcp	0.79
445/tcp	0.3
2967/tcp	0.13
1080/tcp	0.11
22/tcp	0.09
23/tcp	0.07
3128/tcp	0.06
3306/tcp	0.04
3389/tcp	0.03
4899/tcp	0.02
1434/udp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

08 octobre 2010 version initiale.