Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mai 2009
N° CERTA-2009-ACT-020

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-20

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-2009-ACT-020`

Gestion du document

Référence	CERTA-2009-ACT-020
Titre	Bulletin d'actualité 2009-20
Date de la première version	15 mai 2009
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-2009-ACT-020.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-2009-ACT-020/

1 Mise à jour Microsoft du mois de mai

Cette semaine, Microsoft a émis le bulletin MS09-017 portant sur 14 vulnérabilités affectant Microsoft PowerPoint. L'une des vulnérabilités (CVE-2009-0556) n'est autre que celle ayant fait l'objet de l'alerte CERTA-2009-ALE-005 du 03 avril 2009 et exploitée depuis maintenant plus d'un mois.

Dans son bulletin, Microsoft annonce également avoir retiré la possibilité d'ouvrir des fichiers de type `PowerPoint 4.0` avec PowerPoint 2000 et PowerPoint 2003. Cela était déjà le cas pour Office 2003 depuis le service pack 2 et pour Office 2007. En effet, 6 des 14 vulnérabilités concernent la conversion de fichiers de type `PowerPoint 4.0`. L'éditeur a émis un bulletin expliquant comment rétablir la possibilité d'ouvrir ce type de document si nécessaire (KB970980).

De plus, le dernier moteur de conversion utilisé par Office 2003 SP3 a été repris pour Office 2000 et Office XP. Trois des autres vulnérabilités affectant des fichiers de type `PowerPoint 95`, le code concernant ces fichiers a été en partie réécrit et renforcé.

Enfin, il est important de souligner que tous les logiciels affectés n'ont pas été corrigées. En effet, Microsoft Works 8.5 et 9.0, Microsoft Office 2004 et 2008 pour Mac et le convertisseur de fichiers Open XML pour Mac n'ont pas encore de correctif disponible. Pour rappel, Office 2004 pour Mac est concerné par la vulnérabilité

exploitée actuellement. Toutefois, aucun code d'exploitation fonctionnant sur MacOS n'a pour le moment été vu par le CERTA. Il convient néanmoins de rester vigilant tant que la mise à jour n'est pas disponible.

Microsoft Works 8.5 et 9.0, ainsi que Microsoft Office 2008 pour Mac et le convertisseur de fichiers Open XML pour Mac ne sont, quant à eux, seulement concernés que par la vulnérabilité CVE-2009-0224 qui n'est pas exploitée à la date de rédaction de ce bulletin.

1.1 Documentation

- Avis CERTA-2009-AVI-185 du 13 mai 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-185/
- Bulletin MS09-017 du 12 mai 2009 :
  http://www.microsoft.com/technet/security/bulletin/ms09-017.mspx
- Bloc-notes « Security Research & Defense » :
  http://blogs.technet.com/srd/
- Rétablir le support des fichiers PowerPoint 4.0 :
  http://support.microsoft.com/kb/970980

2 Procédures de correction complexes

2.1 Présentation

Voici un exemple concret d'application de correctif complexe. Il s'agit d'une vulnérabilité concernant Adobe Flash signalée en 2002 (CVE-2003-0208). Cette vulnérabilité était initialement une fonctionnalité offerte pour pointer depuis des animations multimédia vers des publicités.

Elle consiste à renseigner la variable `clickTAG` qui est ensuite utilisée par `getURL(clickTAG)`. Cette propriété, quand la variable est incorrectement contrôlée, peut être exploitée pour lancer des attaques d'injection de code indirecte (`XSS`).

```
http://nom_du_site.tld/(...)/fichier.swf?clickTag=[URL pour le XSS]
```

Le correctif proposé par l'éditeur consiste à contrôler dans le code source Flash le format de la variable `clickTAG` avec un test de la forme :

```
if (clickTAG.substr(0,5) == "http:") {
        getURL(clickTAG);
}
```

Il ne s'agit donc pas d'un correctif du lecteur Flash à appliquer mais d'une révision complète des éléments développés en Flash et mis en ligne. Cette tâche est fastidieuse. Des récents articles de presse soulèvent à nouveau le problème en indiquant que plusieurs sites n'ont pas, à la date de rédaction de cet article, corrigé le problème. Les moteurs de recherche actuels permettent en revanche de les identifier assez rapidement.

Ces annonces doivent être prises avec le même sérieux que toute mise à jour de sécurité. Il convient de vérifier sur son parc informatique que les vulnérabilités ne sont pas présentes et il faut appliquer si nécessaire les contournements. Cela implique également une maintenance et un suivi des codes des serveurs Web, Flash en particulier.

2.2 Documentation associée

- Base de connaissances Adobe, "Privacy and Macromedia Flash Ad Tracking", 22 mai 2008 :
  http://kb2.adobe.com/cps/186/tn_18614.html
- Google Code, "ArticleFlashSecurityGetURL", "ArticleFlashSecurityClickTAG", 15 novembre 2008 :
  http://code.google.com/p/doctype/wiki/ArticleFlashSecurityGetURL
  http://code.google.com/p/doctype/wiki/ArticleFlashSecurityClickTAG

3 Un ver qui gazouille

3.1 L'actualité

Le mois dernier a vu apparaître un ver d'un type encore marginal (cf. en 2005 le ver `Samy`), et ayant pour cible un site de réseau social : `twitter`. Ce ver exploitait en effet une vulnérabilité dans l'interprétation de certains paramètres du site, induisant ainsi une attaque par injection de code indirecte (*Cross Site Scripting*, ou *XSS*).

3.2 Pourquoi ce type de ver ?

Ce ver est intéressant sur plusieurs aspects. Tout d'abord, il se propage sur la couche 7 du modèle OSI, alors que les vers dit « classiques » utilisent principalement les couches 4 ou 3. Par conséquent, un équipement de filtrage agissant aux niveau 3 ou 4 du modèle OSI ne pourra pas détecter ce ver. Pour qu'un équipement de filtrage périmétrique soit efficace vis-à-vis de ce genre d'attaque, il faudrait que celui-ci soit capable d'inspecter chaque paquet, et ceci pour toutes les couches.

D'autre part, ce type de ver cible les réseaux sociaux, dont le principe sous-jacent réside dans l'interconnexion maximum, faisant fi des précautions : sur ces réseaux sociaux, le challenge est bien souvent d'avoir le plus de contacts possibles, quitte à ne pas les connaître du tout, ce qui serait impensable sur un réseau classique. Imaginons que notre voisin vienne nous demander de se raccorder à notre réseau ADSL ou à notre réseau d'entreprise sous prétexte que nous nous sommes rencontrés une fois. Impensable ! C'est la même chose quand une vague connaissance nous demande de l'ajouter en contact : on crée un lien, une interconnexion entre son navigateur et le nôtre, via une couche applicative élevée.

Enfin, cela montre que des attaques par XSS n'ont pas pour seule conséquence l'atteinte à l'image ou l'affichage d'une boite de dialogue. Du fait du langage relativement évolué utilisé (javascript, vbscript, etc.), il est possible de créer de véritables programmes ayant les même fonctions que les programmes malveillants classiques : accès à des ressources, reproduction par le réseau, vol de données, etc.

3.3 Comment s'en protéger ?

Le CERTA ne tient pas à apporter un jugement de valeur à ce type de sites. En revanche, il est inconcevable d'adopter un comportement différent vis-à-vis des réseaux classiques et des réseaux sociaux. Le principe d'un réseau reste l'interconnexion (de machines, d'individus, de sites, etc.). Afin de réduire les risques, il convient donc de maîtriser ces interconnexions.

D'un point de vue plus pragmatique, la seule mesure efficace permettant, en tant qu'utilisateur, de se prémunir de ce genre d'attaque et de désactiver l'interprétation des scripts (javascript, vbscript, etc.) par défaut. Certains sites nécessitent cependant l'activation de ces fonctionnalités. Il convient à ce moment-là de peser le pour et le contre, et de ne les réactiver qu'en cas d'impérieuse nécessité.

Enfin, du point de vue du développeur, il convient de vérifier pour chaque paramètre variable que l'on ne récupère que les types de données que l'on désire réellement. Par exemple, un nom de famille ne comporte jamais les caractères suivants : %, <, #, etc.

3.4 Documentation associée

- Note d'information CERTA-2002-INF-001, « Vulnérabilité de type *Cross-Site Scripting* », 22 mars 2002 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/
- Note d'information CERTA-2008-INF-003, « Les attaques de type *cross-site request forgery* », 17 décembre 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-003/

4 Trop beau pour être vrai

4.1 Le contexte

Un des correspondants du CERTA a signalé cette semaine une escroquerie par ingénierie sociale avec des méthodes plutôt efficaces et originales. Tout commence par une petite annonce proposant un appartement en location à un prix environ trois fois inférieur à celui du marché. Intéressé, le correspondant prend alors contact par courriel avec le propriétaire. En retour, la personne désirant louer son appartement explique par mél, dans un français plus ou moins correct, qu'elle habite et a été élevée à l'étranger par sa mère et qu'elle a hérité de

l'appartement suite au décès de son père. Elle ne peut procéder à la visite de l'appartement, étant à l'étranger. Elle détaille donc une procédure passant par une agence intermédiaire spécialisée dans la location de biens par des personnes géographiquement éloignées et qui prendra en charge les frais engendrés. La suite à donner était la suivante : envoyer ses coordonnées afin d'établir le contrat et fournir les clés de l'appartement à l'agent. Une confirmation est alors envoyée et un versement du premier loyer exigée afin de déclencher le déplacement de l'agent et la visite de l'appartement.

Lors de la visite soit le contrat était validé soit l'argent était restitué.

4.2 Les vérifications

Le correspondant, méfiant et sensiblisé à différentes escroqueries sur l'Internet, a procédé à quelques vérifications afin de valider ou non la véracité des éléments détaillés :

- la personne se revendiquant propriétaire était connue sur l'Internet et disposait notamment d'un profil sur un réseau social ;
- l'adresse de l'appartement existait et était cohérente avec la description de celui-ci ;
- l'adresse de la propriétaire existait dans la capitale étrangère où elle était censée habiter.

mais:

- l'agence spécialisée, se revendiquant « leader mondial de la location par courriel » était inconnue ;
- le nom de l'agent auquel le versement devait être fait était connu pour d'autres arnaques de même type dans d'autres grandes villes européennes.

4.3 Les recommandations

Le CERTA profite de cette anecdote pour rappeler qu'il est important de toujours vérifier les données fournies avec des sources ouvertes, surtout lorsque la proposition semble trop alléchante. Les informations à disposition sur l'Internet peuvent aussi bien servir l'escroc mais aussi le desservir. Ceci est un exemple de la nécessité de la remontée d'incidents que ces derniers se soient déroulés dans un cadre personnel ou professionnel.

Enfin, les réseaux sociaux permettent de créer des profils qui n'attestent en rien l'existence réelle de la personne.

5 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 07 et le 14 mai 2009.

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=1935
- 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 08 au 15 mai 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-177 : Vulnérabilité dans les produits F-Secure
– CERTA-2009-AVI-178 : Multiples vulnérabilités de Tivoli Storage Manager client
– CERTA-2009-AVI-179 : Vulnérabilité dans FreeType
– CERTA-2009-AVI-180 : Vulnérabilités dans Google Chrome
– CERTA-2009-AVI-181 : Vulnérabilité du noyau Linux
– CERTA-2009-AVI-182 : Vulnérabilité dans Dokeos
– CERTA-2009-AVI-183 : Vulnérabilité dans ClamAV
– CERTA-2009-AVI-184 : Multiples vulnérabilités dans Dokeos
– CERTA-2009-AVI-185 : Multiples vulnérabilités dans Microsoft PowerPoint
– CERTA-2009-AVI-186 : Multiples vulnérabilités dans Apple Mac OS X
– CERTA-2009-AVI-187 : Multiples vulnérabilités dans Apple Safari
– CERTA-2009-AVI-188 : Multiples vulnérabilités dans SquirrelMail
– CERTA-2009-AVI-189 : Vulnérabilités dans Drupal

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

– CERTA-2009-AVI-010-001 : Vulnérabilité dans Asterisk
(ajout de la référence au bulletin de sécurité Gentoo)
– CERTA-2009-AVI-120-001 : Multiples vulnérabilités dans OpenSSL
(ajout des références aux bulletins de sécurité Gentoo, Debian, Ubuntu, Sun, FreeBSD et OpenBSD)
– CERTA-2009-AVI-139-001 : Vulnérabilités dans Wireshark
(ajout de la référence au bulletin de sécurité Debian)
– CERTA-2009-AVI-156-001 : Multiples vulnérabilités dans cups
(ajout des références aux bulletins de sécurité Gentoo, Debian, RedHat et SuSE)
– CERTA-2009-AVI-176-001 : Multiples vulnérabilités dans Adobe Reader et Adobe Acrobat
(mise à disposition du correctif par l'éditeur et ajout des références CVE)

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, la DCSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/fr/formation/

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.

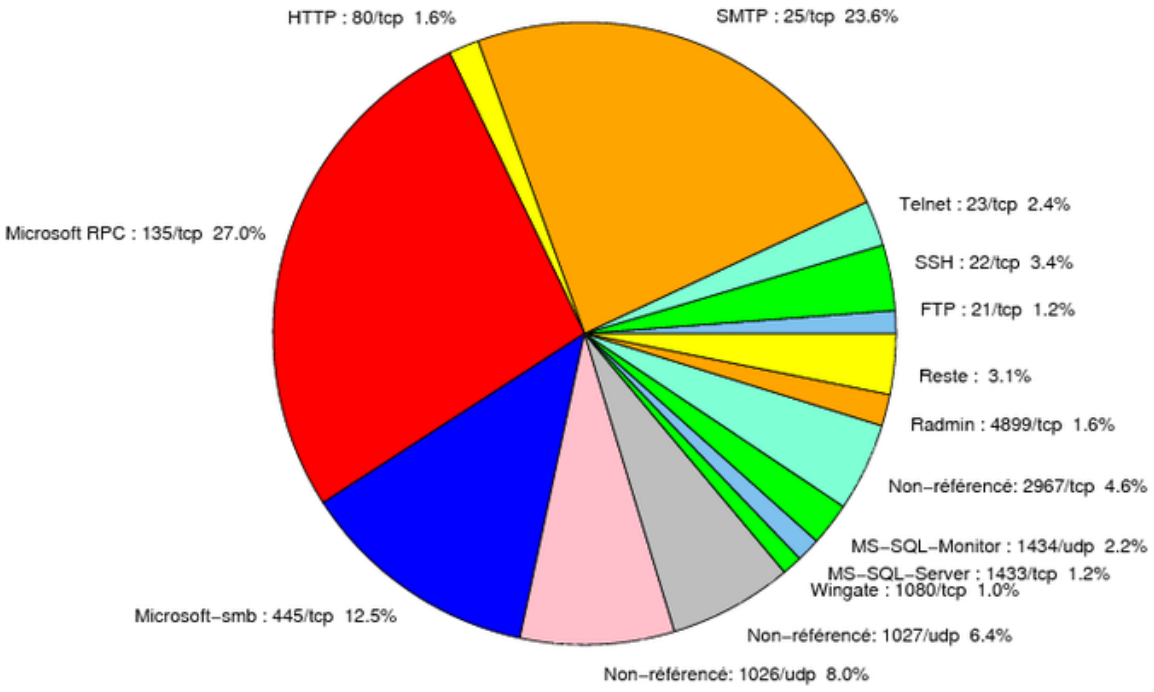

FIG. 1: Répartition relative des ports pour la semaine du 07 au 14 mai 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	27.01
25/tcp	23.6
445/tcp	12.52
1026/udp	8
1027/udp	6.42
2967/tcp	4.59
22/tcp	3.4
80/tcp	2.42
23/tcp	2.36
1434/udp	2.22
4899/tcp	1.63
1433/tcp	1.24
1080/tcp	1.04
3128/tcp	0.85
139/tcp	0.59
3389/tcp	0.45
3127/tcp	0.32
3306/tcp	0.26
111/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 9
3 Paquets rejetés 10

Gestion détaillée du document

15 mai 2009 version initiale.