Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 août 2008
N° CERTA-2008-ACT-035

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-35

Gestion du document

Référence	CERTA-2008-ACT-035
Titre	Bulletin d'actualité 2008-35
Date de la première version	29 août 2008
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-2008-ACT-035.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-2008-ACT-035/

1 Des mots de passe trop faibles

Cette semaine le CERTA a traité un incident relatif à la compromission de plus de 300 machines en France. Le CERTA a été informé par le CERT-Renater de la présence sur l'Internet d'un fichier recensant les identifiants de connexion SSH de plus de 5000 machines dans le monde. Le CERTA a rapidement informé les victimes potentielles et les hébergeurs de ces machines. Dans la cadre de la coopération internationale, le CERTA a informé ses homologues de l'existence de cette liste.

Les identifiants de connexion, présents dans cette liste, semblaient être le résultat d'attaque par dictionnaire révélant des mots de passe triviaux comme :

- un mot d'un dictionnaire ;
- un mot de passe inférieur à 8 caractères ;
- un mot de passe identique au compte ;
- des chiffres ajoutés avant ou après un mot du dictionnaire.

Le CERTA rappelle qu'un bon mot de passe (dit *fort*) doit être difficile à deviner, même à l'aide d'outils automatisés, mais facile à retenir pour l'utilisateur. La note d'information du CERTA sur les mots de passe pourra aiguiller le lecteur dans ses choix.

Certains comptes compromis révèlent également un défaut de paramétrage du serveur :

– présence d'un service SSH inutile ;
– autorisation de se connecter avec un utilisateur ayant des droits d'administration ;
– comptes de services autorisés à se connecter par SSH.

Le CERTA rappelle également que les services permettant l'accès distant doivent être arrêtés, quand ils ne sont pas utiles, ou limités aux machines et comptes autorisés.

De plus, dans l'actualité de cette semaine, le CERTA a été informé que des individus malveillants se servaient d'identifiants SSH compromis pour élever leurs privilèges sur les machines et installer des boites à outils malveillantes (*rootkits*). Il est donc important, suite à une compromission, d'analyser et de surveiller le comportement du serveur.

1.1 Documentation

– Note d'information du CERTA sur les mots de passe :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
– Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

2 Des paquets (RPM) de Red Hat SSH compromis

Vendredi 22 août 2008, la société Red Hat a publié un bulletin de sécurité faisant état de deux problèmes :

– la correction d'une vulnérabilité ancienne, CVE-2007-4752 ;
– la falsification de paquets après une intrusion en août 2008, CVE-2008-3844.

La falsification a consisté en l'ajout d'un cheval de Troie dans certains paquets SSH. La société estime que les mesures prises pour le canal officiel de distribution des paquets, Red Hat Network, sont suffisantes pour contrer la distribution des paquets illégalement modifiés. Elle alerte donc les utilisateurs qui se procurent les paquets par des moyens alternatifs. Red Hat fournit un script en langage de commande (*shell*) pour déceler la présence de paquets falsifiés sur un ordinateur.

Sans douter de l'honnêteté de la société Red Hat, il convient de se rappeler de la difficulté de cerner une intrusion, y compris pour une société de cette nature. Par conséquent, il est prudent de surveiller le trafic des ordinateurs utilisant les systèmes d'exploitation Red Hat.

La portée de l'intrusion peut également être difficile à estimer sur un système victime de la fraude. Ainsi, le script de détection de paquets contrefaits ne devrait pas être exécuté sur un ordinateur suspect. Il devrait être exécuté à partir d'un système sain (liveCD ou machine autre ayant le disque de l'ordinateur suspect en périphérique)

Le CERTA recommande de récupérer les logiciels auprès des éditeurs ou des mirroirs et distributeurs officiels. La société Red Hat met en garde contre l'acquisition de RPM SSH par des canaux autres que son réseau.

2.1 Documentation

– Référence CVE CVE-2008-3844 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3844
– Bulletin de sécurité de Red Hat :
http://rhn.redhat.com/errata/RHSA-2008-0855.html
– Script de recherche de paquets compromis :
http://www.redhat.com/security/data/openssh-blacklist.html

3 Mise à jour de MS08-051

Dans son lot de mises à jour du mois d'août 2008, Microsoft a corrigé trois vulnérabilités présentes dans différentes versions de son logiciel PowerPoint et permettant l'exécution de code arbitraire à distance. Comme d'habitude, les mises à jour étaient disponibles automatiquement via Microsoft Update et Office Update, et manuellement via le centre de téléchargement. L'éditeur a cependant indiqué la semaine dernière que les fichiers mis à disposition sur le centre de téléchargement étaient des mauvaises versions. Selon Microsoft, les fichiers proposés corrigeaient tout de même les vulnérabilités décrites dans le bulletin, mais ne contenaient pas d'autres mises à jour de fiabilité et de sécurité importantes.

Ainsi, toutes les personnes ayant effectué la mise à jour via le centre de téléchargement sont invitées à télécharger la nouvelle mise à jour notée « version 2. » Les utilisateurs qui ont installé le correctif pour MS08-051 via Microsoft Update ou Office Update n'ont pas besoin de le réinstaller.

3.1 Documentation

– Bulletin de sécurité MS08-051 du 12 août 2008, mis à jour le 20 août 2008 :
http://www.microsoft.com/france/technet/security/Bulletin/MS08-051.mspx

4 Gestion externalisée des marque-pages

À l'instar de certains services qui permettent de partager des fichiers entre une machine professionnelle et une machine « à domicile » (voir *Foldershare* dans le bulletin d'actualité CERTA-2007-ACT-015), il existe des services disponibles sur l'Internet qui facilitent la gestion des marque-pages. Le principe est le même : il s'agit de transmettre à un tiers « de confiance » un ensemble de pointeurs vers vos sites préférés.

La transmission de vos signets à un tiers peut servir à réaliser des statistiques. Néanmoins, il s'agit d'une fuite d'informations qui peut avoir des conséquences, notamment en termes de sécurité :

– des liens internes professionnels peuvent être indexés. Confier à un tiers de tels marque-pages peut donner des renseignements sur l'architecture interne du réseau ;
– certains signets sont suffisamment explicites pour dévoiler des centres d'intérêt de l'utilisateur ou de son entreprise/organisme ;
– les signets d'un utilisateur peuvent être exploités dans le cadre d'une attaque ciblée. En effet, un attaquant peut chercher à insérer un code malveillant (via une injection SQL par exemple) dans une des pages indexées dans votre navigateur.

Avant de faire appel à un tel service, il est important de vérifier que celui-ci est conforme à votre politique de sécurité et d'être sensibilisé aux risques qui en découlent.

4.1 Documentation

– Bulletin d'actualité CERTA-2007-ACT-015 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-015/

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 le 21 et le 28 août 2008.

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 22 au 28 août 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-427 : Vulnérabilité dans divers produits Trend Micro
- CERTA-2008-AVI-428 : Vulnérabilités dans des mises à jour sous Red Hat
- CERTA-2008-AVI-429 : Vulnérabilité de Xen
- CERTA-2008-AVI-430 : Vulnérabilité dans Ruby
- CERTA-2008-AVI-431 : Vulnérabilité de IBM DB2

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.formation.ssi.gouv.fr

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.

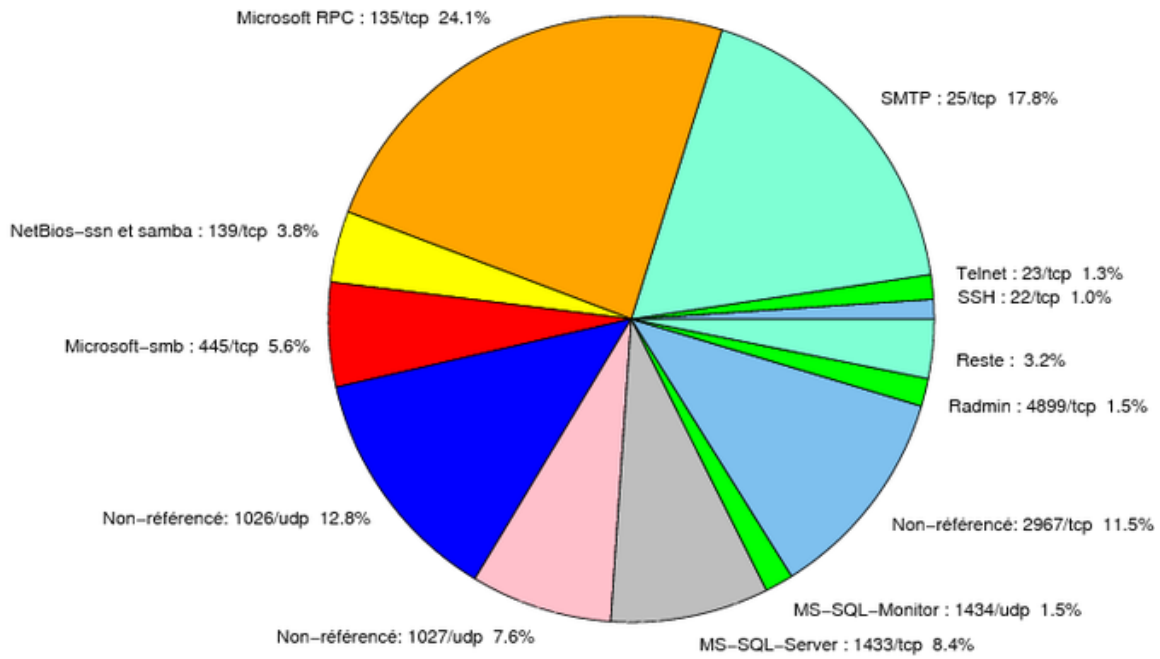

FIG. 1: Répartition relative des ports pour la semaine du 21.08.2008 au 28.08.2008

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/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT

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	24.08
25/tcp	17.81
1026/udp	12.75
2967/tcp	11.47
1433/tcp	8.44
1027/udp	7.55
445/tcp	5.56
139/tcp	3.8
1434/udp	1.51
4899/tcp	1.48
23/tcp	1.3
22/tcp	1.04
1080/tcp	0.89
137/udp	0.8
80/tcp	0.74
3128/tcp	0.41
21/tcp	0.23
3389/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 8
3 Paquets rejetés 9

Gestion détaillée du document

29 août 2008 version initiale.