Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 décembre 2007
N° CERTA-2007-ACT-050

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-50

Gestion du document

Référence	CERTA-2007-ACT-050
Titre	Bulletin d'actualité 2007-50
Date de la première version	14 décembre 2007
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-2007-ACT-050.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-2007-ACT-050/

1 Multiplicité de services et conséquences

Le CERTA a traité cette semaine une compromission de serveur liée à la découverte d'un compte à mot de passe faible utilisé pour plusieurs services (SSH, FTP). Jusqu'ici, rien de bien nouveau : un attaquant balaie des plages d'adresses à la recherche de serveurs SSH en écoute sur le port 22/tcp, et pour chaque serveur trouvé, il essaie de nombreuses combinaisons de noms de compte et de mots de passe. Ces attaques sont très fréquentes, il suffit de lire ses journaux pour s'en convaincre.

La particularité de cet incident réside dans le fait que le compte avec le mot de passe faible utilise l'interpréteur de commandes (*shell*) `/bin/false`. Autrement dit, lorsque l'attaquant a rejoué les identifiants découverts, il a été immédiatement déconnecté, le système n'étant pas capable de fournir un *shell* valide.

Là où d'autres auraient abandonné, notre attaquant a persévéré : il a découvert un service FTP en écoute sur le port 21/tcp pour lequel il n'est pas nécessaire de disposer d'un *shell* valide. L'intrus a donc rejoué les identifiants récupérés sur le serveur lors de l'attaque contre le service SSH pour se connecter en FTP, et a déposé plusieurs fichiers, notamment un *shell* écrit en PHP.

L'attaque ne s'arrête pas là : un serveur HTTP étant également présent sur le système, l'attaquant a ensuite effectué une connexion sur ce serveur et a appelé le *shell* PHP précédemment déposé. Cette méthode lui a finalement permis d'obtenir un accès sur le système avec les droits... de l'utilisateur `www-data` !

Il est important de préciser que les *shell* PHP sont accessibles par tous et que certains attaquants utilisent des moteurs de recherches pour en découvrir. L'incident que nous venons de décrire a ainsi permis à d'autres intrus de se connecter sur le serveur par l'intermédiaire du *shell* PHP installé.

Recommandations :

Les recommandations d'usage sont toujours les mêmes : il est généralement conseillé de ne pas concentrer plusieurs services sur une même machine. Il est fréquent de voir des services FTP et/ou SSH sur des serveurs HTTP, souvent pour mettre à jour le contenu Web. Il est toutefois possible de restreindre les plages d'adresses et les comptes autorisés à se connecter, notamment à l'aide de filtrage. Enfin, il est rappelé que l'attaque n'aurait peut-être pas été possible si des mots de passe plus forts avaient été utilisés.

2 SquirrelMail compromis ?

Le site de *SquirrelMail* annonce que la version 1.4.12 en téléchargement a été compromise et modifiée. En effet, l'empreinte `MD5` des versions 1.4.12 téléchargées ne correspondait pas à l'empreinte indiquée sur le site Web. Les développeurs de *SquirrelMail* ont ainsi découvert que les fichiers en téléchargement avaient été modifiés après avoir été proposés en téléchargement. Selon les développeurs, les modifications des fichiers n'auraient pas de conséquences importantes en termes de sécurité.

Il est toutefois recommandé, pour tous ceux qui auraient téléchargé la version 1.4.12 entre le 08 décembre 2007 et le 13 décembre 2007, de recommencer cette opération et de vérifier que l'empreinte `MD5` est bien valide.

Documentation :

- Annonce du 13 décembre 2007 sur le site de SquirrelMail :
  http://www.squirrelmail.com

3 Mac OS 10.5 est compatible SUSv3

Pour des raisons de compatibilité, `Apple` a mis l'accent sur la normalisation de son système d'exploitation Mac OS 10.5 et des modifications y ont donc été apportées pour qu'il soit compatible `SUSv3` (*Single UNIX Specification*). Le système repose sur de nombreux projets libres qui n'ont pas les moyens de s'engager dans le processus compliqué de la certification. Ces projets pourront bénéficier des efforts d'`Apple`, les modifications apportées pouvant être réintégrées aux sources originelles.

3.1 Les effets

Les modifications touchant aussi bien les interfaces de bibliothèques que les commandes *shell*, cela peut entraîner des dysfonctionnements de certaines applications en fonction de la version du système où elles sont exécutées. Si, dans la majorité des cas, il s'agit d'ajout de fonctionnalités n'affectant pas les anciens programmes, quelques différences, listées et décrites par `Apple`, peuvent tout de même concerner l'exécution de programmes. `Apple` propose des moyens de contourner ces différences, soit en utilisant des directives de compilation, soit en utilisant des variables d'environnement forçant la compatibilité ascendante. Par exemple, l'initialisation de la variable `COMMAND_MOD=legacy` permet de forcer l'ancien comportement des commandes des *shell*.

Dans les différences notables, la commande `ps` n'interprète plus de de la même façon l'option `-u`. Alors que dans la version précédente, elle définissait les informations à afficher (le nom de l'utilisateur et l'heure du lancement du processus), dans la nouvelle version, elle permet de définir l'utilisateur dont on veut voir les processus en cours (`-u[nom]`). Ainsi, la commande `ps -aux` retourne `ps: No user named 'x'`. Cependant, il est possible de l'utiliser de l'ancienne syntaxe, en initialisant la variable `COMMAND_COM`. Ainsi la ligne de commande suivante fonctionne : `COMMAND_COM=legacy ps -aux`

3.2 Remarques

Même si `Apple` fournit un certain nombre de moyens de contournement, un changement de système d'exploitation doit toujours être réfléchi et validé avant d'être déployé. De plus, respecter les normes lors de la réalisation d'un projet est la meilleure façon d'optimiser la compatibilité du développement dans le temps.

4 Vulnérabilités Microsoft

Le CERTA a publié cette semaine 7 avis portant sur des vulnérabilités touchant des produits Microsoft, qui correspondent à des bulletins de sécurité publiés par l'éditeur le mardi 11 décembre. Sur ces 7 bulletins de sécurité, 5 ont un risque d'exécution de code arbitraire à distance. Ces 5 avis concernent les éléments suivants :

- une vulnérabilité dans le service *Message Queuing de Microsoft Windows* (MS07-065, CERTA-2007-AVI-536) ;
- deux vulnérabilités dans *Microsoft DirectX* (MS07-064, CERTA-2007-AVI-535);
- une vulnérabilité dans *SMBv2* (MS07-063, CERTA-2007-AVI-534) ;
- une vulnérabilité dans le traitement de fichiers `ASF` par *Windows Media Player* (MS07-068, CERTA-2007-AVI-539) ;
- plusieurs vulnérabilités dans le navigateur *Internet Explorer* (MS07-069, CERTA-2007-AVI-540).

Enfin, deux avis concernent également des élévations de privilèges, dont la deuxième serait d'ores et déjà exploitée :

- une vulnérabilité dans le noyau de *Windows Vista* (MS07-066, CERTA-2007-AVI-537) ;
- une ancienne vulnérabilité dans le pilote *Macrovision* (MS07-067, CERTA-2007-AVI-538) ;

Tous les systèmes d'exploitation sont touchés par ces vulnérabilités. Le CERTA recommande l'installation sans délai des correctifs de sécurité.

Par ailleurs, Microsoft a également publié le Service Pack 1 d'Office 2007, qui contient notamment de nombreux correctifs de sécurité.

Documentation

- CERTA-2007-AVI-534 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-534/index.html
- CERTA-2007-AVI-535 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-535/index.html
- CERTA-2007-AVI-536 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-536/index.html
- CERTA-2007-AVI-537 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-537/index.html
- CERTA-2007-AVI-538 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-538/index.html
- CERTA-2007-AVI-539 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-539/index.html
- CERTA-2007-AVI-540 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-540/index.html

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 05 et le 13 décembre 2007.

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 07 au 13 décembre 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-524 : Multiples Vulnérabilités dans Sun Solaris
– CERTA-2007-AVI-525 : Vulnérabilité dans FreeBSD
– CERTA-2007-AVI-526 : Vulnérabilités dans Novell BorderManager
– CERTA-2007-AVI-527 : Vulnérabilité dans plusieurs produits Avaya
– CERTA-2007-AVI-528 : Vulnérabilité dans Citrix EdgeSight
– CERTA-2007-AVI-529 : Vulnérabilité dans Cisco Security Agent
– CERTA-2007-AVI-530 : Vulnérabilité dans CiscoWorks
– CERTA-2007-AVI-531 : Vulnérabilité dans Novell NetMail
– CERTA-2007-AVI-532 : Vulnérabilité dans XEN
– CERTA-2007-AVI-533 : Vulnérabilité dans Drupal
– CERTA-2007-AVI-534 : Vulnérabilité dans SMBv2 de Microsoft Windows
– CERTA-2007-AVI-535 : Vulnérabilités dans Microsoft DirectX
– CERTA-2007-AVI-536 : Vulnérabilité dans le service Message Queuing de Microsoft Windows
– CERTA-2007-AVI-537 : Vulnérabilité du noyau Windows
– CERTA-2007-AVI-538 : Vulnérabilité dans le pilote Macrovision
– CERTA-2007-AVI-539 : Vulnérabilité dans le format de fichier Windows Media
– CERTA-2007-AVI-540 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTA-2007-AVI-541 : Vulnérabilité dans MySQL
– CERTA-2007-AVI-542 : Vulnérabilité d'Emacs

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

– CERTA-2007-AVI-516-002 : Vulnérabilité dans avast!
(Ajout de la référence 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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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 œuvre (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 COSSI/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.

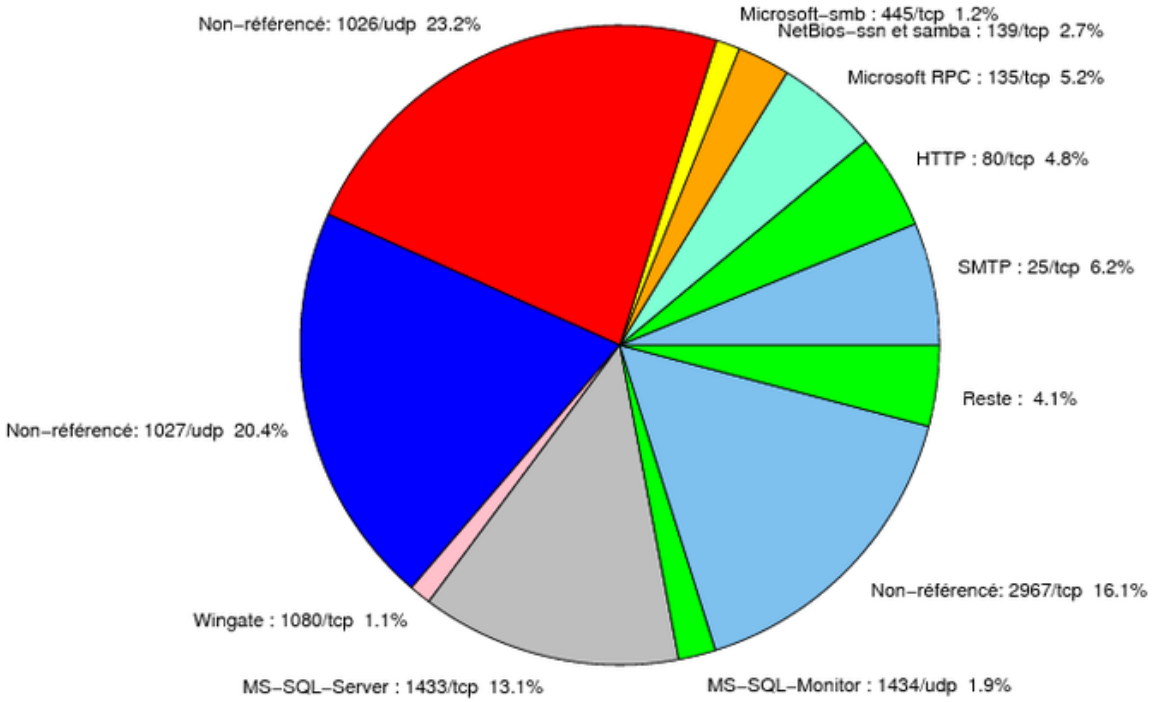

FIG. 1: Répartition relative des ports pour la semaine du 05.12.2007 au 13.12.2007

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
1026/udp	23.19
1027/udp	20.4
2967/tcp	16.06
1433/tcp	13.14
25/tcp	6.19
135/tcp	5.21
80/tcp	4.82
139/tcp	2.65
1434/udp	1.89
445/tcp	1.2
1080/tcp	1.1
4899/tcp	0.98
3306/tcp	0.66
3128/tcp	0.54
137/udp	0.32
21/tcp	0.2
11768/tcp	0.13
3127/tcp	0.06
3389/tcp	0.05
143/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

14 décembre 2007 version initiale.