



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 août 2006
N° CERTA-2006-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-32

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-2006-ACT-032>

Gestion du document

Référence	CERTA-2006-ACT-032
Titre	Bulletin d'actualité 2006-32
Date de la première version	11 août 2006
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-2006-ACT-032.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-2006-ACT-032/>

1 Activité en cours

1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 03 et le 10 août 2006.

2 Bulletins de sécurité Microsoft, août 2006

2.1 Rappel

Microsoft a publié, le 08 août 2006, 12 bulletins de sécurité, dont 9 sont qualifiés de *critiques* et trois d'*importants*. En août 2006, Microsoft aura ainsi publié pour l'année 2006 plus de bulletins critiques que l'ensemble de ceux de l'année 2005 ou 2004. Plusieurs vulnérabilités de ce mois-ci ont été présentées lors des récentes conférences en sécurité BlackHat 2006 et Defcon14. Nous revenons dans les paragraphes suivants sur les points majeurs de ces dernières mises à jour.

2.2 Service Serveur et risques

La plus médiatisée actuellement est la MS06-040 (CERTA-2006-AVI-338). Elle concerne le service Serveur du système d'exploitation Microsoft Windows. Ce service est utilisé pour les RPC (Remote Procedure Call), et de manière plus générale, pour le partage de ressources (fichiers, imprimantes, etc) dans un réseau local. Il est accessible à distance par les ports 139/tcp et 445/tcp.

La vulnérabilité est donc exploitable à distance, et peut entraîner l'exécution de commandes arbitraires par le biais de paquets spécialement conçus et envoyés à la machine vulnérable. Les ports impliqués sont déjà utilisés pour la propagation de nombreux vers, comme Sasser ou Blaster. Des codes d'exploitation visant la vulnérabilité MS06-040 sont déjà disponibles sur l'Internet, et il est possible que ceux-ci soient rapidement intégrés dans le corps d'un nouveau ver.

Microsoft avait publié en juillet 2006 le bulletin MS06-035 ciblant le même service. Suite à la mise à jour référencée par ce dernier, plusieurs personnes ont souligné la possibilité de lancer des attaques par déni de service, s'appuyant sur les modifications effectuées par la mise à jour. Le bulletin MS06-040 est indépendant de ce problème, qui reste non corrigé, comme le souligne une note de Microsoft. Le correctif est en cours d'élaboration.

Le CERTA recommande donc d'appliquer les correctifs mis à disposition par Microsoft, et de bien vérifier que les pare-feux filtrent correctement le trafic à destination de ces ports. Ils doivent être bloqués pour toute connexion depuis l'extérieur du réseau (Internet). Attention toutefois aux postes nomades qui peuvent rendre ce filtrage inefficace. Il est aussi possible d'utiliser le pare-feu ICF (*Internet Connection Firewall*) fourni par Microsoft sur les versions XP et 2003 pour effectuer le filtrage au niveau de chaque machine.

2.3 Résolution de noms

Le bulletin MS06-041 (CERTA-2006-AVI-339) corrige une vulnérabilité survenant lors de la résolution de noms (gestion des noms de machines associées aux adresses IP) par le client DNS ou Winsocks Hostname. Winsock Hostname est une interface API procurant la fonction d'accès au protocole réseau DNS. Cette interface est utilisée par la majorité des applications nécessitant un accès réseau. Le client DNS est, quant à lui, nativement installé sur la plupart des machines pour effectuer la résolution de noms. Les deux partagent plusieurs fonctions en commun, comme `gethostbyname()`.

Dans la mesure où plusieurs applications s'appuient sur cette fonction, et que la vulnérabilité est exploitable à distance via ces dernières, il est vivement recommandé d'appliquer le correctif référencé par le bulletin MS06-041. Par ailleurs, il est fréquent que les applications développées pour Windows importent dans leur répertoire des copies de `.dll` nécessaires (`dnsapi.dll`, `rasadhlp.dll`, etc). Celles-ci ne sont pas nécessairement mises à jour...

2.4 Correction de Microsoft Office et Powerpoint

Le CERTA avait émis une alerte (CERTA-2006-ALE-009) le 15 juillet 2006, concernant la librairie de Microsoft Office `mso.dll`, et plus précisément Powerpoint. Une personne malveillante peut exploiter des vulnérabilités pour construire un document Powerpoint particulier. Quand ce dernier est ouvert sur un système vulnérable, cela provoque l'exécution de code arbitraire.

Les vulnérabilités sont corrigées dans le bulletin MS06-046, et l'avis du CERTA CERTA-2006-AVI-346 en fournit les détails.

2.5 Multiples corrections dans Internet Explorer

Le CERTA a mentionné dans les précédents bulletins d'actualité les nombreuses vulnérabilités qui ont été publiées au cours du mois de juillet 2006 sur un site Web. Celles-ci apparaissaient quotidiennement dans un bloc-notes, suite à l'application de nouveaux outils de test sur différents types de navigateurs. Plusieurs d'entre elles visaient Microsoft Internet Explorer.

Microsoft les corrige dans le bulletin MS06-042 (CERTA-2006-AVI-340).

3 Sécurisation des machines Apple MAC

Au cours d'une conférence en sécurité nommée Defcon14, il a été souligné certaines faiblesses du pare-feu de MacOS. Par défaut, ce dernier n'est pas activé. Il est accessible par les Préférences Système, section Partage. Les versions MacOS Panther ne filtrent pas les protocoles UDP et ICMP (ping). Pour la version

MacOS Tiger, il faut indiquer explicitement que ces derniers doivent être bloqués en se rendant dans la sous-section Coupe-Feu -> Avancé. . . . En regardant plus en détail les règles de filtrage, il est possible de voir que certaines exceptions apparaissent, notamment sur le filtrage des ports source UDP, dont certains resteraient autorisés malgré le blocage UDP. Plusieurs services sont accessibles par défaut sur une machine utilisant Mac OS via le protocole UDP : ntpd (pour synchroniser l'heure avec un serveur distant), CUPS (pour gérer les requêtes vers les imprimantes), Bonjour (pour donner des informations au voisinage réseau)...

Recommandations :

Le CERTA recommande donc de :

- modifier directement les règles de filtrage dans les fichiers de configuration du pare-feu de MacOS, qui s'appuie sur le logiciel libre ipfw de FreeBSD. Les règles actuellement en place sont visibles en tapant dans une console la commande suivante : `sudo ipfw list`.
- filtrer en amont par le biais d'un autre pare-feu, de manière redondante, pour garantir que la politique d'accès est bien respectée.

Liens :

- Site d'Apple concernant la sécurité de MacOS :
<http://www.apple.com/fr/macosx/features/security/>
- Documentation de ipfw sous FreeBSD :
<http://www.bsdbooks.net/shells/x21.html>

4 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html>
- Note d'information sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html>
- Note d'information sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1935>

5 Rappel des avis et mises à jour émis

Durant la période du 04 au 10 août 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-327 : Vulnérabilité dans MyBB
- CERTA-2006-AVI-328 : Vulnérabilité dans GnuPG
- CERTA-2006-AVI-329 : Multiples vulnérabilités dans la bibliothèque libTIFF
- CERTA-2006-AVI-330 : Multiples vulnérabilités dans Phorum
- CERTA-2006-AVI-331 : Vulnérabilité dans ATutor
- CERTA-2006-AVI-332 : Multiples vulnérabilités dans PHP
- CERTA-2006-AVI-333 : Vulnérabilité sur Novell GroupWise et WebAccess
- CERTA-2006-AVI-334 : Multiples vulnérabilités dans IBM Informix Dynamic Server (IDS)
- CERTA-2006-AVI-335 : Vulnérabilité dans Drupal
- CERTA-2006-AVI-336 : Vulnérabilité dans ClamAV
- CERTA-2006-AVI-337 : Vulnérabilité dans Webmin & Usermin
- CERTA-2006-AVI-338 : Vulnérabilité dans le Service Serveur de Microsoft Windows

- CERTA-2006-AVI-339 : Vulnérabilités dans Winsock Hostname et le Client DNS de Microsoft Windows
- CERTA-2006-AVI-340 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2006-AVI-341 : Vulnérabilité dans Microsoft Windows
- CERTA-2006-AVI-342 : Vulnérabilité dans Microsoft Management Console
- CERTA-2006-AVI-343 : Vulnérabilité dans Windows Explorer
- CERTA-2006-AVI-344 : Vulnérabilité dans le contrôle ActiveX HTML Help
- CERTA-2006-AVI-345 : Vulnérabilité dans Microsoft Visual Basic for Applications (VBA)
- CERTA-2006-AVI-346 : Multiples vulnérabilités dans Microsoft Office, dont Powerpoint
- CERTA-2006-AVI-347 : Vulnérabilité du noyau de Windows 2000
- CERTA-2006-AVI-348 : Multiples vulnérabilités dans la bibliothèque hlink.dll de Microsoft Windows
- CERTA-2006-AVI-349 : Multiples vulnérabilités du noyau de Microsoft Windows
- CERTA-2006-AVI-350 : Vulnérabilités dans Mysql

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2006-AVI-270-001 : Vulnérabilité dans courrier
(ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2006-AVI-267-003 : Vulnérabilité dans GnuPG
(ajout des références aux bulletins de sécurité RedHat, SGI, Suse et Ubuntu)
- CERTA-2006-AVI-271-002 : Multiples vulnérabilités sur OpenOffice
(ajout des références aux bulletins de sécurité Gentoo, Mandriva et Ubuntu)
- CERTA-2006-AVI-299-001 : Vulnérabilité dans libVNCSERVER
(ajout des références aux bulletins de sécurité Gentoo et Suse)
- CERTA-2006-AVI-312-002 : Multiples vulnérabilités dans les produits Mozilla
(ajout des références aux bulletins de sécurité Redhat et Gento)
- CERTA-2006-AVI-315-001 : Vulnérabilité dans Apache httpd
(ajout des références aux bulletins de sécurité Gentoo, SuSE, Mandriva et Ubuntu)
- CERTA-2006-AVI-322-001 : Multiples vulnérabilités dans Ruby
(ajout de la référence au bulletin de sécurité Debian)
- CERTA-2006-AVI-299-002 : Vulnérabilité dans libVNCSERVER
(ajout de la référence au bulletin de sécurité Gentoo concernant x11vnc)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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>

7 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.

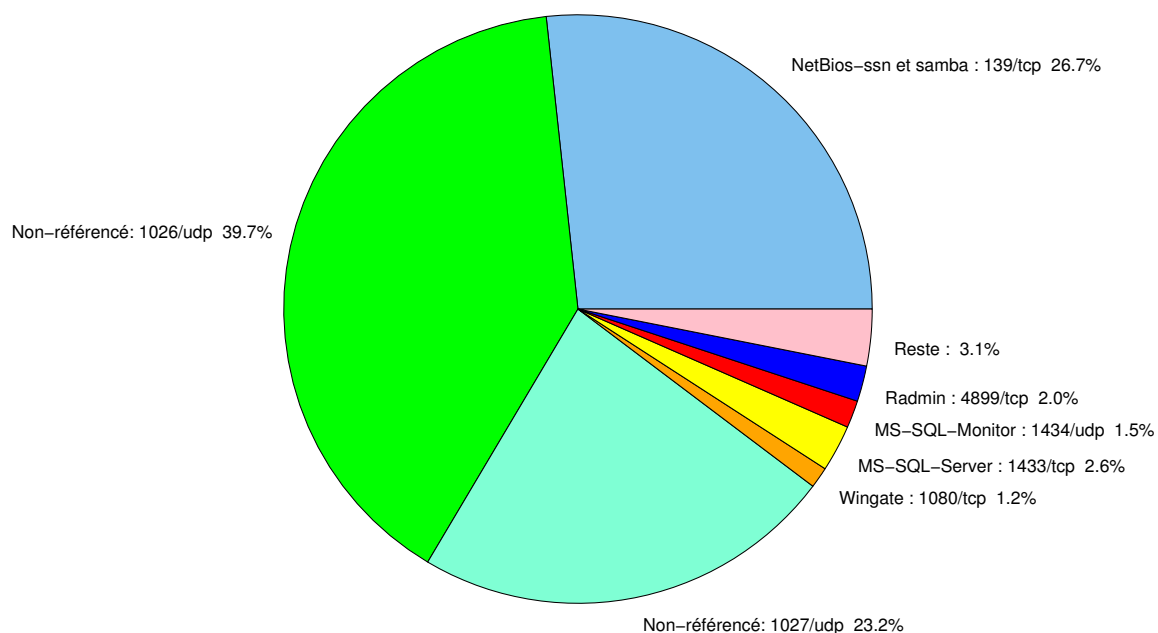


FIG. 1: Répartition relative des ports pour la semaine du 03.08.2006 au 10.08.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	-	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	-	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
80	TCP	HTTP	-	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	-	-
111	TCP	Sunrpc-portmapper	-	CERTA-2003-AVI-052
119	TCP	NNTP	-	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	-	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	-	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	-	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283

				CERTA-2006-AVI-338
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	–	HP System Management	CERTA-2006-AVI-248
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
1026/udp	39.74
139/tcp	26.72
1027/udp	23.24
1433/tcp	2.56
4899/tcp	1.95
1434/udp	1.5
1080/tcp	1.15
137/udp	0.91
80/tcp	0.78
25/tcp	0.41
3128/tcp	0.3
3306/tcp	0.06
143/tcp	0.04
1023/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	7
3	Paquets rejetés	8

Gestion détaillée du document

11 août 2006 version initiale.