



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 décembre 2006
N° CERTA-2006-ACT-051

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-51

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-051>

Gestion du document

Référence	CERTA-2006-ACT-051
Titre	Bulletin d'actualité 2006-51
Date de la première version	22 décembre 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-051.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-051/>

1 Activité en cours

1.1 Captures de frappes au clavier

Cette semaine, le CERTA a été informé d'un incident de sécurité informatique dû au déploiement d'un outil de capture de données au clavier (*keylogger*) sur les postes des utilisateurs.

Les données sont recueillies par cet outil malveillant lorsque l'internaute remplit des formulaires sur un site Web. À titre d'illustration, voici un aperçu de la nature des captures de consultation de sites Web portées à notre connaissance :

- des données concernant la consultation de plus de 200 sites Web (dans le domaine .fr) ;
- depuis plus de 2500 adresses IP différentes.

Parmi les informations collectées, on trouve :

- des informations de connexion sur des *webmails* ;
- des numéros de sécurité sociale utilisés comme identifiants ;

- des identifiants de connexion pour des sites publics ou commerciaux ;
- des demandes d’acte d’état civil ;
- des informations bancaires (RIB, numéros de cartes).

On notera que le fait que les sites soient sécurisés (https) n’a pas empêché la capture dans la mesure où celle-ci s’effectue sur le poste de l’internaute.

Le CERTA dans le cadre de sa démarche de traitement d’incidents informe les responsables sécurité des serveurs.

Recommandations

Le CERTA attire l’attention des internautes sur l’importance de choisir un poste de travail sain pour procéder à la saisie de données sensibles. Si le poste n’est pas sain, alors la transaction ne peut pas être sûre quelle que soit la solidité des mesures de sécurité mises en place sur le serveur ou entre celui-ci et le poste utilisateur.

Seule l’application rigoureuse des consignes habituelles permet de maintenir un poste sain :

- applications systématiques des mises à jour de sécurité ;
- mise en œuvre d’un pare-feu ;
- suppression des services inutiles ;
- utilisation d’un antivirus à jour ;
- vigilance de l’utilisateur sur les anomalies de fonctionnement ;
- etc.

1.2 Filtrage des flux sortants

Le CERTA a traité un incident suite au signalement d’une machine compromise. Cette dernière envoyait des requêtes à destination d’une machine distante, via le port TCP 6667, associé au service IRC. Ce protocole de messagerie sert également de canal de contrôle dans le cadre de réseaux de machines zombi (*botnet*).

Outre la compromission de la machine, certaines mesures préventives auraient dû être prises, afin d’éviter qu’une machine interne puisse établir des connexions vers n’importe quel port. De manière générale, le CERTA rappelle qu’il est capital de filtrer les tentatives de connexion depuis le réseau interne. Avoir une politique sortante du type

`N_importe_quelle_adresse -> N_importe_quelle_adresse`
peut être dangereuse. Il faut, notamment, considérer les points suivants :

- la politique de filtrage par défaut peut être de tout interdire, puis d’ajouter des règles (ports, adresses) en fonction des besoins ; en l’occurrence, le port destination TCP 6667 n’a pas forcément de raison d’être autorisé, sauf dans un contexte bien particulier.
- les règles utilisées doivent vérifier que les adresses source sortant du domaine interne sont cohérentes avec le plan d’adressage ;
- la journalisation (*log*) doit permettre de récupérer le trafic bloqué. L’administrateur peut ainsi voir plus facilement, à partir de cette source d’informations, quelles machines commencent à s’adresser à des ports non légitimes de machines extérieures.

Ces démarches ne protègent pas des codes ouvrant des connexions sur des ports supposés légitimes (cas des tunnels), mais limitent les risques de rebond d’une machine compromise, et offrent une source intéressante de surveillance du réseau pour l’administrateur.

Il est possible d’utiliser les différents types de proxys pour affiner le filtrage sortant et limiter les effets des tunnels.

Le CERTA recommande la lecture de la note d’information CERTA-2006-INF-001 relative au filtrage et aux pare-feux :

<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001/>

2 Avis Microsoft du mois de décembre 2006

2.1 Les faits

Plusieurs vulnérabilités présentes au moins dans les applications Microsoft Word, Microsoft Works, Microsoft Visionneuse et OpenOffice.org permettent d'exécuter du code arbitraire à distance au moyen d'un fichier au format Word (.doc) spécialement conçu.

Le savoir-faire permettant d'exploiter cette vulnérabilité est largement publié sur l'Internet ainsi que des codes d'exploitation qui sont d'ores et déjà diffusés.

Le CERTA a été informé par l'un de ses correspondants de l'apparition sur ses passerelles de messagerie de documents exploitant cette vulnérabilité. Ces documents ont été détectés et identifiés par les passerelles anti-virales déployées sur ce même réseau. Selon les premières analyses des éditeurs anti-virus ce code d'exploitation tenterait de télécharger et/ou d'exécuter du code malveillant depuis l'Internet.

Le CERTA recommande de porter une attention toute particulière aux journaux d'événements des équipements réseaux (passerelles, parefeux, serveurs mandataires) qui permettraient de déceler toutes anomalies liées à cette vulnérabilité.

Informez le CERTA de tout incident relatif à l'exploitation de cette vulnérabilité.

2.2 Contournement provisoire

- Utiliser un format de document alternatif tel que le format `rtf` (Rich Text File).
- Utiliser un outil alternatif de visualisation et/ou d'édition des documents au format Word (Wordpad sous Microsoft Windows et Abiword sous GNU/Linux).
- Mettre les bases de signatures d'anti-virus à jour.
- Filtrer les documents au format `Word` au niveau des passerelles de périphériques (messagerie, HTTP).
- Ouvrir uniquement les documents au format `Word` provenant de sources de confiance.
- Utiliser un compte n'ayant pas de droit d'administration permet de limiter l'infection au contexte de l'utilisateur.
- Sensibiliser les utilisateurs à informer leur RSSI (Responsable en Sécurité des Systèmes d'Informations) lorsque une erreur survient à l'ouverture d'un document au format `Word`.

3 Concernant le filtrage associé au trafic UDP

Il existe plusieurs procédés pour effectuer des traductions d'adresses (ou NAT pour *Network Address Translation*) permettant à des machines à l'intérieur d'un réseau d'accéder à l'Internet par le biais d'un ensemble d'adresses IP publiques. Les plus courantes font également une traduction au niveau des ports.

Il existe un protocole, décrit dans le RFC 3489, détaillant une méthode pour que deux machines, chacune dans un réseau différent, puissent communiquer entre elles en UDP malgré le NAT. Il s'appelle STUN (*Simple Traversal of UDP through NAT*), et s'utilise avec des applications comme Google Talk ou Skype.

Cette méthode peut permettre, sous certaines conditions, de contacter directement une machine se trouvant derrière un NAT, et peut donc être une violation à la politique de sécurité. Il est important de vérifier que les règles de filtrage, notamment celles liées à UDP, empêchent ce scénario si celui-ci n'est pas autorisé.

En relation avec l'article précédent sur le filtrage, une solution pour contourner ce problème serait, indépendamment du NAT, de filtrer de manière restrictive et rigoureuse les connexions sortantes en UDP.

4 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 14 et le 21 décembre 2006.

5 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>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/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>
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-008/>

6 Rappel des avis émis

Durant la période du 15 au 21 décembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-551 : Vulnérabilité dans HP ILO
- CERTA-2006-AVI-552 : Vulnérabilité dans le client Novell
- CERTA-2006-AVI-554 : Vulnérabilité de l'antivirus Sophos
- CERTA-2006-AVI-555 : Vulnérabilités de Symantec Veritas NetBackup
- CERTA-2006-AVI-556 : Vulnérabilité de GNOME Display Manager (GDM)
- CERTA-2006-AVI-557 : Vulnérabilités de Websphere
- CERTA-2006-AVI-558 : Vulnérabilité dans BitDefender
- CERTA-2006-AVI-559 : Vulnérabilité dans Kerio MailServer
- CERTA-2006-AVI-560 : Vulnérabilité d'IBM DB2
- CERTA-2006-AVI-562 : Vulnérabilités dans Ruby
- CERTA-2006-AVI-563 : Multiples vulnérabilités dans Avaya Predictive Dialing System
- CERTA-2006-AVI-564 : Vulnérabilité de McAfee
- CERTA-2006-AVI-565 : Vulnérabilité dans Typo3
- CERTA-2006-AVI-566 : Vulnérabilités dans MailEnable
- CERTA-2006-AVI-567 : Vulnérabilité dans Computer Associates CleverPath
- CERTA-2006-AVI-568 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2006-AVI-569 : Vulnérabilité MacOS X Quicktime et Quartz

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

- CERTA-2006-AVI-397-002 : Plusieurs vulnérabilités dans Xorg X11 et XFree86 (ajout des références aux bulletins de sécurité Avaya, Red Hat et Gentoo o.)
- CERTA-2006-AVI-439-001 : Multiples vulnérabilités dans Microsoft Excel (ajout de la référence de la mise à jour du bulletin de sécurité Microsoft MS06-059)
- CERTA-2006-AVI-488-001 : Vulnérabilités dans la bibliothèque imlib2 (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2006-AVI-516-001 : Vulnérabilité de GNU tar (ajout des références aux bulletins de sécurité Red Hat, Gentoo, Debian, FreeBSD)
- CERTA-2006-AVI-553-001 : Vulnérabilité de ClamAV (ajout des références aux bulletins de sécurité Gentoo, SuSE, Debian et Mandriva)
- CERTA-2006-AVI-561-001 : Vulnérabilité de ProFTPD (ajout de la référence au bulletin de sécurité Mandriva)

7 Actions suggérées

7.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

7.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

7.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

7.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

7.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

7.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

7.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

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

8 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

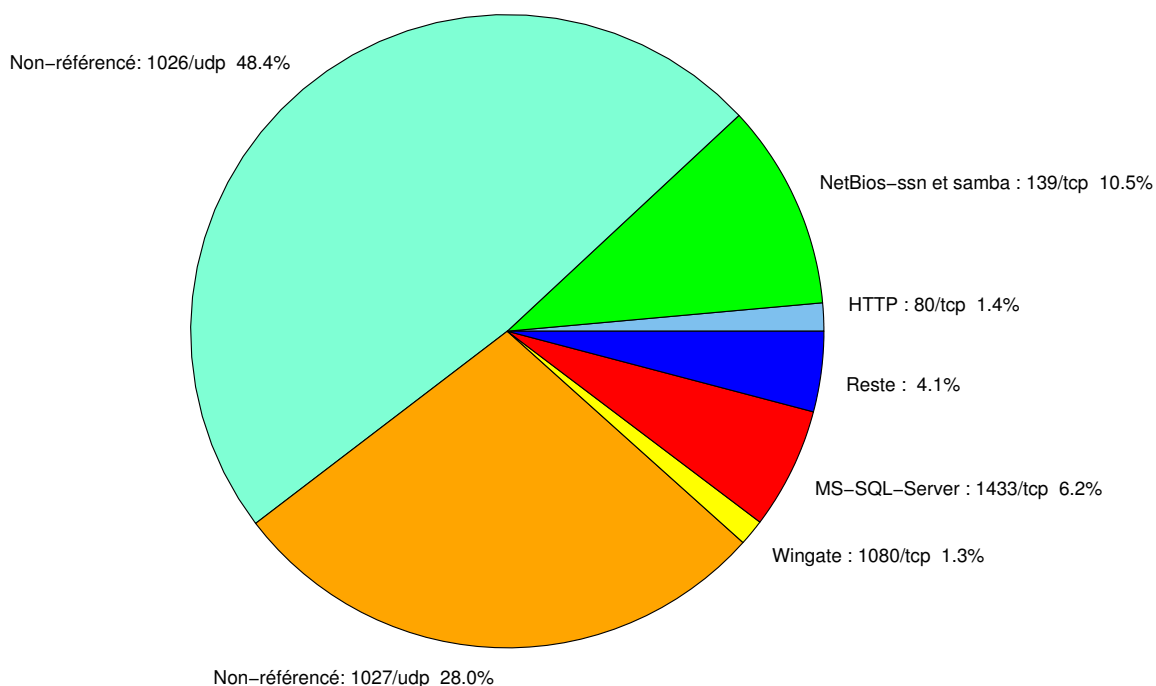


FIG. 1: Répartition relative des ports pour la semaine du 14.12.2006 au 21.12.2006

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	48.44
1027/udp	27.98
139/tcp	10.5
1433/tcp	6.19
80/tcp	1.43
1080/tcp	1.33
137/udp	0.98
4899/tcp	0.77
1434/udp	0.71
22/tcp	0.35
3306/tcp	0.27
25/tcp	0.22
3128/tcp	0.17
143/tcp	0.12
443/tcp	0.11
15118/tcp	0.08
2100/tcp	0.06
5554/tcp	0.03

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

22 décembre 2006 version initiale.