



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 novembre 2006
N° CERTA-2006-ACT-046

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-46

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-046>

Gestion du document

Référence	CERTA-2006-ACT-046
Titre	Bulletin d'actualité 2006-46
Date de la première version	17 novembre 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-046.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-046/>

1 Activité en cours

1.1 Défiguration

Un cas de défiguration de site web a été traité par le CERTA cette semaine. Il s'agit de l'exploitation d'une faille de *phpMyAdmin* qui a permis de voler des identifiants de connexion.

Le CERTA constate que de plus en plus d'incidents de sécurité sont liés au vol de mots de passe dans des bases SQL qui sont rejoués ensuite par FTP.

Recommandations :

Le CERTA recommande de ne pas utiliser les mêmes mots de passe pour les différents services d'une même machine afin de limiter les possibilités en cas d'exploitation d'une vulnérabilité. Par ailleurs, la multiplicité des services sur une même machine affaiblit considérablement la sécurité globale de celle-ci. Une séparation des services doit, dans certains cas, être envisagée.

1.2 Les postes en libre service

Le CERTA a traité cette semaine un incident impliquant un poste mis en libre service. Ce dernier a été utilisé par des personnes malintentionnées, afin de participer à une attaque informatique. Ce poste, bien que protégé par un antivirus, contenait pourtant plusieurs programmes malveillants (espionnage, virus, chevaux de troie et publiciels). Cet ordinateur ne semblait pas faire l'objet d'un traitement particulier dans le système d'information malgré son utilisation.

Le CERTA met en garde contre l'utilisation des machines dites à libre service. Celles-ci doivent faire l'objet de la plus grande surveillance, et les accès de ces ordinateurs doivent être restreints et journalisés.

2 Des vulnérabilités critiques pour certains produits Wi-Fi

Cette semaine, plusieurs vulnérabilités ont été publiées, concernant des pilotes de matériels sans-fil Wi-Fi. Les pilotes concernés sont les suivants :

- Broadcom BCMWL5.SYS (version 3.50.21.10) ;
- D-Link A5AGU.SYS pour les adaptateurs USB D-Link DWL-G132 (version 1.0.1.41) ;
- NetGear WG111v2.SYS pour les adaptateurs USB NetGear WG111v2 (version 5.1213.6.316).

Broadcom est pour l'instant le seul constructeur à avoir corrigé les problèmes. Cependant, les vendeurs d'ordinateurs portables adaptent souvent les pilotes pour leurs produits, et les mises à jour de ces derniers ne sont pas encore effectuées (à l'exception de Linksys).

Les vulnérabilités concernent les couches les plus basses des protocoles 802.11 :

- les pilotes Broadcom concernés ne gèrent pas correctement des réponses aux requêtes de sondage (`Probe`) qui incluent un champ d'identifiant SSID trop long ;
- les pilotes D-Link concernés ne gèrent pas correctement les balises (`Beacons`) qui contiennent des informations sur les taux de transfert excédant 36 octets ;
- les pilotes NetGear concernés ne gèrent pas correctement les balises contenant des informations dont la taille totale excède 1100 octets.

Ces vulnérabilités ne sont pas très complexes, et ne sont pas corrigées pour le moment. Elles ciblent directement les pilotes des cartes sans-fil, ce qui signifie aussi que la grande majorité des solutions de sécurité existantes (WPA, VPN, 802.11i, IPsec, etc) ne protègent pas convenablement contre celles-ci.

Intuitivement, il est souvent plus facile d'adresser des paquets malveillants à une machine cible via une connexion sans-fil, à une distance de plusieurs centaines de mètres, que de s'introduire dans le réseau pour accéder directement à la même machine.

Recommandations du CERTA :

Le CERTA recommande donc les actions suivantes :

- surveiller les mises à jour des constructeurs pour appliquer les correctifs. Ceci n'est pas nécessairement automatique ;
- auditer et recenser les appareils sans-fil utilisés et déployés dans le réseau ;
- sensibiliser les personnes utilisant des appareils communicants nomades à désactiver, quand cela n'est pas nécessaire, les interfaces sans-fil ;
- ne pas utiliser de technologies sans-fil qui offriraient une porte d'entrée évidente à des réseaux sécurisés d'autre part (pare-feux, VPN, etc).

3 Vulnérabilités Microsoft

Microsoft a publié ses correctifs mensuels cette semaine : les bulletins MS06-066 à MS06-071 qui ont fait l'objet des avis CERTA-2006-AVI-495 à CERTA-2006-AVI-500. Il existe déjà des codes d'exploitation disponibles sur l'Internet pour les vulnérabilités MS06-067, MS06-070 et MS06-071 (respectivement avis CERTA-2006-AVI-496, CERTA-2006-AVI-499 et CERTA-2006-AVI-500). Il est possible que la vulnérabilité affectant le service *Station de Travail* de Microsoft Windows fasse l'objet d'un ver. Les machines sous Windows 2000 sont plus exposées que celles sous Windows XP (nécessité d'avoir des droits Administrateur pour réaliser l'attaque sous Windows XP).

D'autre part, Microsoft a cessé de publier des correctifs pour Windows XP SP1.

Recommandations :

Il est conseillé d'appliquer les correctifs de sécurité Microsoft (conformément à votre politique de sécurité) et de réfléchir à la migration des machines sous Windows XP SP1 vers un OS maintenu. Par ailleurs, le filtrage des ports 139/tcp et 445/tcp peut être mis en place pour empêcher l'exploitation depuis l'Internet de la vulnérabilité décrite dans l'avis CERTA-2006-AVI-499.

4 Simplification des installations par un tiers

Certains logiciels se proposent d'installer et de configurer un ensemble d'applications tierces, afin de simplifier cette succession d'opérations. A valeur illustrative, Google propose en version beta un outil nommé `Google Pack` (<http://pack.google.com>). Il s'agit d'une suite de logiciels, jugés essentiels par Google. Cela inclut pour le moment : Google Earth, Google Desktop, Google Picasa, et la barre d'outils Google pour Internet Explorer ; mais aussi Mozilla Firefox, Norton Antivirus 2005 (édition spéciale de démonstration), Adobe Reader 7, Real Player, Ad-Aware ou Skype.

Un autre exemple a été présenté dans la note d'information CERTA-2006-INF-06, à propos des applications fournies avec les clés de type U3.

Il est bien sûr possible de personnaliser les applications à installer mais ce procédé peut présenter divers désavantages qu'il est important de considérer :

- les installations sont faites par un tiers ; on est donc obligé de faire confiance à ce dernier quant aux applications à configurer et à exécuter ;
- un procédé de mise à jour est proposé par le tiers ; il n'est pas nécessairement validé par les éditeurs des applications ou par la PSSI.

Le fait de laisser installer par un tiers l'ensemble des applications de sa machine fournit à ce dernier l'occasion de centraliser une quantité d'informations non négligeable (voire presque totale) sur l'état de la machine.

Cette décision doit donc être mûrement réfléchie, et n'est pas recommandée par le CERTA.

5 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 09 et le 16 novembre 2006.

6 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/>

7 Rappel des avis et mises à jour émis

Durant la période du 10 au 16 novembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-489 : Vulnérabilité dans HP OpenView
- CERTA-2006-AVI-490 : Vulnérabilités des pilotes pour les puces Wi-Fi Broadcom
- CERTA-2006-AVI-491 : Plusieurs vulnérabilités de Citrix MetaFrame
- CERTA-2006-AVI-492 : Multiples Vulnérabilités dans AVG-Antivirus
- CERTA-2006-AVI-493 : Vulnérabilité dans les produits 3Com SuperStack 3 Switch 4400
- CERTA-2006-AVI-494 : Vulnérabilité de Novell BorderManager
- CERTA-2006-AVI-495 : Vulnérabilités dans le service Client pour NetWare de Microsoft Windows
- CERTA-2006-AVI-496 : Multiples vulnérabilités de Microsoft Internet Explorer
- CERTA-2006-AVI-497 : Vulnérabilité de Microsoft Agent
- CERTA-2006-AVI-498 : Multiples vulnérabilités dans Adobe Macromedia Flash Player pour Windows
- CERTA-2006-AVI-499 : Vulnérabilité du service Station de Travail de Microsoft Windows
- CERTA-2006-AVI-500 : Vulnérabilité de Microsoft XML Core Services
- CERTA-2006-AVI-501 : Multiples vulnérabilités dans les produits VMware
- CERTA-2006-AVI-502 : Vulnérabilité dans Lotus Domino NRPC
- CERTA-2006-AVI-503 : Vulnérabilités dans Bugzilla

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

- CERTA-2006-AVI-398-002 : Vulnérabilité dans Adobe Flash Player
(ajout de la référence au bulletin Microsoft MS06-069)
- CERTA-2006-AVI-482-001 : Vulnérabilités des produits Mozilla
(ajout des références aux bulletins de sécurité Mandriva et Slackware)

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 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.

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 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.

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.

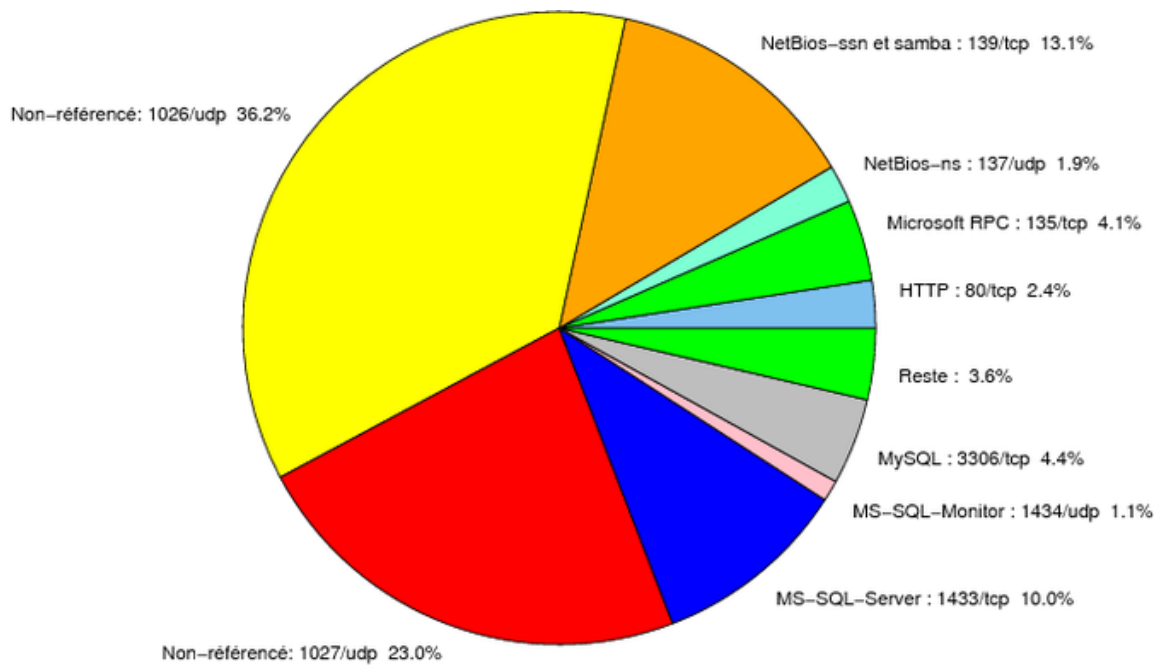


FIG. 1: Répartition relative des ports pour la semaine du 09.11.2006 au 16.11.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
22	TCP	SSH	-	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
23	TCP	Telnet	-	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
25	TCP	SMTP	-	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
42	TCP	WINS	-	http://www.certa.ssi.gouv.fr/site/CEI
80	TCP	HTTP	-	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
106	TCP	MailSite Email Server	-	-
111	TCP	Sunrpc-portmapper	-	http://www.certa.ssi.gouv.fr/site/CEI
119	TCP	NNTP	-	http://www.certa.ssi.gouv.fr/site/CEI
135	TCP	Microsoft RPC	-	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI
137	UDP	NetBios-ns	-	http://www.certa.ssi.gouv.fr/site/CEI
139	TCP	NetBios-ssn et samba	-	http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI http://www.certa.ssi.gouv.fr/site/CEI

				http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE
2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

TAB. 2: Correctifs correspondant aux ports destination des paquets re-jetés

port	pourcentage
1026/udp	36.18
1027/udp	23.02
139/tcp	13.13
1433/tcp	10.02
3306/tcp	4.41
135/tcp	4.13
80/tcp	2.43
137/udp	1.93
1434/udp	1.07
4899/tcp	0.93
1080/tcp	0.89
3128/tcp	0.54
25/tcp	0.26
15118/tcp	0.17
443/tcp	0.09
5554/tcp	0.05
23/tcp	0.04
143/tcp	0.03
119/tcp	0.01

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

17 novembre 2006 version initiale.