

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-02

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-2007-ACT-002>

Gestion du document

Référence	CERTA-2007-ACT-002
Titre	Bulletin d'actualité 2007-02
Date de la première version	12 janvier 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-002.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-002/>

1 Activité en cours

1.1 Webdav

Récemment, des sites publics ont subi l'insertion de pages de revendication par des cyber-délinquants. L'intrusion a été facilitée par l'ouverture sans restriction d'une fonction permettant la modification d'un site web (WebDAV). L'intrusion s'est répétée après la remise en service des sites. Le CERTA rappelle d'une part deux précautions minimales :

- n'ouvrir que les services indispensables ;
- authentifier les utilisateurs selon la politique de sécurité ;

D'autre part, à la suite d'une intrusion, la restauration doit se faire sur une base saine et corriger les erreurs de configuration qui ont permis l'incident. Le CERTA aborde cette bonne pratique dans la documentation suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>

1.2 Modification de site Web et indiscretion

Le CERTA a constaté que des sites web publics sont modifiés ou restaurés tout en restant en ligne. Pendant la phase de modification, des informations sur le site ont été accessibles, tant sur la structure de fichiers que sur les logiciels employés et leur version.

Le CERTA recommande de suspendre la mise en ligne du site lors de telles opérations. L'utilisation d'une mire de type « en maintenance » permet d'informer l'internaute sur le caractère temporaire de l'inaccessibilité du site.

1.3 Cloisonnement des sites Internet

Le CERTA a traité cette semaine un incident lié à la défiguration d'un site. La conception de ce dernier n'est pas en cause, mais il était hébergé avec 90 autres sur une même machine.

L'attaque a eu lieu par une requête de type php-include via l'un des sites. Celle-ci a permis de lancer un outil donnant un accès à l'attaquant avec des droits de lecture et d'écriture. Dans ces conditions, il peut visiter toute l'arborescence de tous sites, et y modifier certaines pages.

Il est important pour l'hébergeur, dans le cas où plusieurs sites co-habitent sur une même machine, d'avoir une politique d'accès et de droits de modifications très stricte. Il faut distinguer :

- les utilisateurs et les groupes qui peuvent lire les fichiers des sites ;
- les utilisateurs et les groupes qui peuvent modifier les fichiers ; il en faut au minimum un différent par site, avec des droits particuliers.

La garantie d'un cloisonnement correct entre les sites co-hébergés doit faire partie des critères pour choisir la solution d'hébergement la plus adaptée.

Le CERTA a publié à ce sujet la note d'information :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>

2 Alerte concernant la gestion WMF de Microsoft

Le CERTA a publié ce vendredi, une alerte concernant la manipulation de WMF (pour *Windows MetaFile*) par Microsoft Windows : CERTA-2007-ALE-002.

<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-002/>

La vulnérabilité peut être exploitée au moyen d'un fichier WMF spécialement construit. Un individu peut, par ce biais, insérer le document dans un courriel, ou une page Web, afin de perturber le système vulnérable. Il pourrait, sous certaines conditions, exécuter du code arbitraire sur un système. Cependant, le CERTA n'a pour le moment pas connaissance de code permettant l'exécution de code arbitraire à distance. Il est à noter que cette vulnérabilité concerne toutes les applications qui utilisent le moteur de rendu graphique de Microsoft.

Les mises à jour Microsoft publiées mardi 09 janvier 2007 ne corrigent pas ce problème, mais le CERTA propose des contournements provisoires dans l'alerte CERTA-2007-ALE-002.

Cette alerte fait suite aux vulnérabilités WMF rendues publiques à la fin de l'année 2005. Les bulletins d'actualité mentionnent des cas d'attaques dans l'avis CERTA-2005-AVI-445 et le bulletin d'actualité CERTA-2006-ACT-002.

3 « Month of Apple Bug » (deuxième semaine)

Comme nous vous l'avons indiqué dans CERTA-2007-ACT-001, le projet continue de publier des vulnérabilités sur les produits Apple. Depuis vendredi dernier, on notera les publications suivantes :

- une vulnérabilité dans l'utilitaire de disque de MacOS X permettant potentiellement une exécution de code arbitraire ou un élévation de privilège ;
- une vulnérabilité concernant la gestion du format PDF par l'application Aperçu dans MacOS X. Il est à noter que cette faille implique le format PDF et serait présente également dans des applications comme Adobe Reader versions 5 à 7 mais également xpdf et d'autres logiciels dérivés. Le CERTA a publié la note de communication CERTA-2007-COM-001 sur le sujet ;
- une faille dans la mise en œuvre de Javascript dans l'application Omniweb sous MacOS X ;
- une vulnérabilité dans une application tierce fournie par Apple nommée Application Enhancer permettant une élévation de privilèges. Application Enhancer permet un contrôle plus fin de certaines applications sous MacOS X ;

- plusieurs vulnérabilités concernant la mise en œuvre des images disques au format DMG. Ces images sont utilisées dans l'installation d'applications sous MacOS X.

4 De l'importance des barres d'état d'un navigateur

4.1 Présentation

Les navigateurs offrent plusieurs options d'affichage. Outre la page de visite, il est souvent possible d'afficher la barre d'état (ou *Status Bar*), qui se trouve généralement en bas de la fenêtre de navigation. Elle se caractérise par différentes zones, comme :

1. la zone de message d'état (*Status Message*) ;
2. la barre de progression (*Progress Bar*) ;
3. les icônes d'état ;
4. la zone de sécurité ;
5. etc.

Cette barre permet de visualiser un certain nombre d'informations dont :

- l'évolution des transactions des pages Web, telle l'adresse du site contacté ou l'état de la connexion (en attente de la réponse du serveur Web, terminée, etc) ;
- l'icône du cadenas associé à une connexion HTTPS ;
- activation de fonctions complémentaires (par exemple les options d'anti-filoutage/phishing sous IE7) ;

Les données présentées dans cette barre d'état sont informelles, et peuvent être modifiées : le CERTA a déjà publié des avis concernant des déficiences de l'affichage de celles-ci, mais elles apportent néanmoins une bonne visibilité sur les activités du navigateur en cours. Il est donc important d'afficher cette barre en permanence.

4.2 Motivations

Une vulnérabilité a été identifiée dans les versions récentes d'Internet Explorer pour les versions 6 et 7. Il s'agit d'un mauvais ordonnancement des tâches, entre les événements asynchrones du navigateur et le rendu synchrone du contenu d'une page.

Une démonstration a été publiée, et consiste à recharger très périodiquement dans la page une section (ou *iframe*) faisant appel à un fichier XML particulier. Elle permettrait à une personne malveillante d'exécuter des commandes par le biais du navigateur vulnérable de l'utilisateur visitant cette page.

Cette vulnérabilité n'est pas encore corrigée. Mais en premier abord, le chargement intempestif du fichier XML est visible dans la barre d'état. Une première façon de détecter que l'on se trouve sur une page suspecte est de voir un état de connexion qui ne se termine jamais, et qui continue à se rafraîchir pendant plusieurs dizaines de secondes. Sans barre d'état, la détection est moins évidente.

4.3 Comment afficher la barre d'état dans les navigateurs ?

Les navigateurs permettent aisément de choisir cette option. Par exemple :

- sous Mozilla Firefox : aller dans l'onglet "Affichage", puis sélectionner "Barre d'état" ;
- sous Microsoft Internet Explorer : aller dans l'onglet "Affichage", puis sélectionner "Barre d'état" ;
- sous Apple Safari : aller dans l'onglet "Présentation", puis sélectionner "Afficher la barre d'état" ;

5 Vulnérabilités sur BrightStor ARCserve

Le CERTA a publié un avis de sécurité concernant plusieurs vulnérabilités dans *Computer Associates BrightStor ARCserve* (avis CERTA-2007-AVI-029). Ces vulnérabilités ne sont pas tout à fait nouvelles, l'une d'entre elles avait été rendue publique en novembre 2006, mais aucun correctif n'existait.

Le 05 janvier 2007, un outil permettant d'exploiter automatiquement cette vulnérabilité a été publié sur l'Internet, et depuis cette date, le SANS constate une augmentation des rejets sur le port 6502/tcp. Le CERTA, pour sa part, n'a pas constaté la moindre activité sur ce port, ni sur les ports 6503/tcp et 6504/tcp (qui sont concernés par d'autres vulnérabilités récentes de *BrightStor ARCserve*), mais recommande toutefois l'application des correctifs de sécurité, et le filtrage de ces ports au niveau des pare-feux.

6 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 04 et le 11 janvier 2007.

7 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/>

8 Rappel des avis émis

Durant la période du 05 au 11 janvier 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-005 : Vulnérabilité dans OpenOfficeorg
- CERTA-2007-AVI-006 : Vulnérabilité dans OpenBSD
- CERTA-2007-AVI-007 : Vulnérabilité dans Novell Client
- CERTA-2007-AVI-008 : Vulnérabilité de Eudora Mail Server
- CERTA-2007-AVI-009 : Vulnérabilité de l'antivirus Kaspersky
- CERTA-2007-AVI-010 : Vulnérabilités dans WordPress
- CERTA-2007-AVI-011 : Multiples vulnérabilités dans Drupal
- CERTA-2007-AVI-012 : Multiples vulnérabilités de Cisco secure ACS
- CERTA-2007-AVI-013 : Plusieurs vulnérabilités dans le navigateur Opera
- CERTA-2007-AVI-014 : Vulnérabilités de AIX
- CERTA-2007-AVI-015 : Vulnérabilité de Microsoft Office 2003
- CERTA-2007-AVI-016 : Multiples vulnérabilités de Microsoft Excel
- CERTA-2007-AVI-017 : Vulnérabilités de Microsoft Outlook
- CERTA-2007-AVI-018 : Vulnérabilité VML du système Microsoft Windows
- CERTA-2007-AVI-019 : Vulnérabilités dans Kerberos
- CERTA-2007-AVI-020 : Multiples vulnérabilités dans Fetchmail
- CERTA-2007-AVI-021 : Vulnérabilité de RPC de Solaris
- CERTA-2007-AVI-022 : Vulnérabilité dans ColdFusion
- CERTA-2007-AVI-023 : Vulnérabilité de PacketShaper
- CERTA-2007-AVI-024 : Multiples vulnérabilités dans Adobe Acrobat
- CERTA-2007-AVI-025 : Multiples vulnérabilités de Xorg

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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>

10 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.

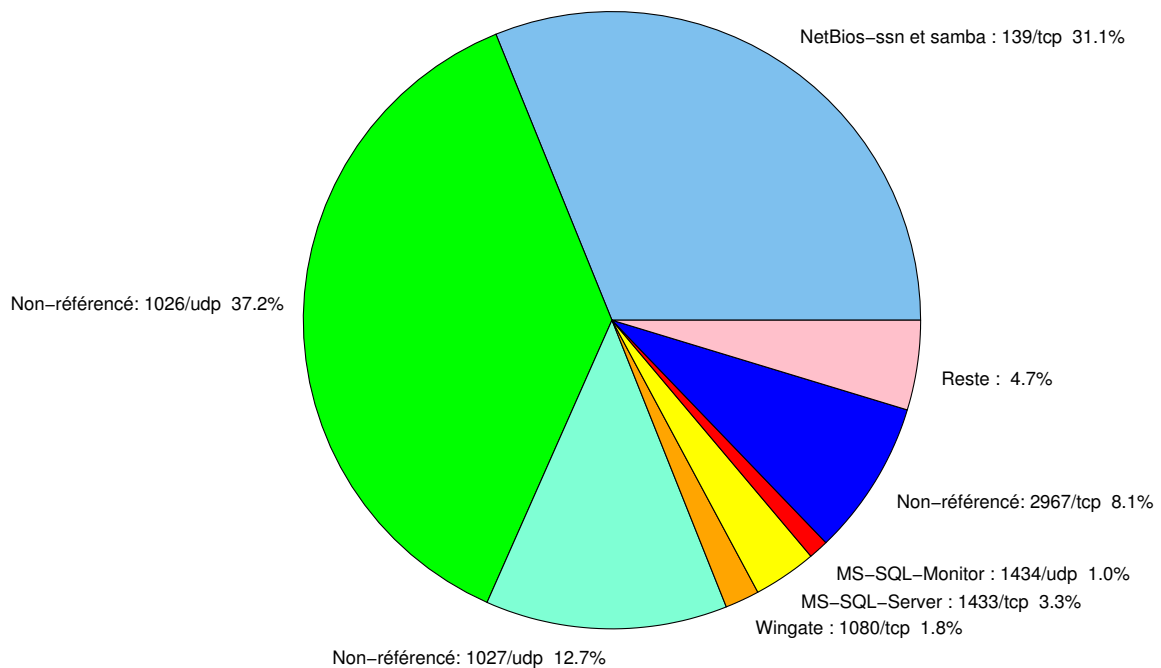


FIG. 1: Répartition relative des ports pour la semaine du 04.01.2007 au 11.01.2007

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	37.23
139/tcp	31.13
1027/udp	12.67
2967/tcp	8.11
1433/tcp	3.31
1080/tcp	1.79
1434/udp	1.04
4899/tcp	0.99
80/tcp	0.92
137/udp	0.7
3306/tcp	0.4
25/tcp	0.38
3128/tcp	0.29
2100/tcp	0.13
15118/tcp	0.11
443/tcp	0.09
3127/tcp	0.06
6129/tcp	0.04
9898/tcp	0.02

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

12 janvier 2007 version initiale.