



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 février 2007
N° CERTA-2007-ACT-005

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-05

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-005>

Gestion du document

Référence	CERTA-2007-ACT-005
Titre	Bulletin d'actualité 2007-05
Date de la première version	02 février 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-005.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-005/>

1 Activités en cours

1.1 Cacti

Réactivité des attaques suite à l'apparition d'une vulnérabilité :

Le 02 janvier 2007 nous avons publié un avis de sécurité (<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-001>) concernant une vulnérabilité du logiciel *Cacti*. *Cacti* est un logiciel de supervision de l'activité de l'architecture informatique. Ce logiciel était vulnérable à des attaques par injection de requêtes SQL.

L'analyse des fichiers journaux d'un serveur, montre, dès le 29 décembre 2006, des tentatives de connexion à un service *Cacti*. A partir du 26 janvier 2007, le serveur recevait directement des tentatives d'injection de requêtes SQL, tentant d'exploiter la vulnérabilité de *Cacti*.

Le CERTA rappelle que la surveillance des fichiers journaux doit faire partie des pratiques naturelles lors de l'exploitation des serveurs. Dès l'apparition d'une vulnérabilité, celle-ci est rapidement exploitée et intégrée dans des outils de balayage, ou *scan*. Les avis de sécurité du CERTA indiquent où trouver les correctifs de sécurité. Les tentatives d'exploitation de la vulnérabilité doivent être attentivement surveillées au niveau des journaux. Ceux-ci doivent alors être appliqués une fois validés.

2 La reconnaissance vocale sous Windows Vista

2.1 Présentation

Cette semaine, une version du système d'exploitation de Microsoft Windows, nommée Vista, est apparue dans le commerce en France.

Elle offre plusieurs fonctionnalités, dont l'une faisait grand bruit médiatique, avant même sa sortie : il s'agit de la reconnaissance vocale, ou *Speech Recognition*.

Ce service permet avec la voix et l'aide d'un microphone, de lancer des commandes, ouvrir des applications, écrire des documents, etc.

Il ne nécessite pas un étalonnage très strict, ce qui présente moins de contraintes liées à l'utilisation.

Le service n'est pas activé par défaut à l'installation de Windows Vista. Il le sera après sa configuration par démarrer => Tous les programmes => Accessoires => Options d'ergonomie => Reconnaissance Vocale de Windows.

Une vulnérabilité a été identifiée cette semaine, associée à ce service. Il prendrait en compte le signal restitué par les haut-parleurs. Des exemples ont montré qu'il était possible, lors de la navigation sur une page Web pointant vers des fichiers contenant du son, d'exécuter des commandes sur la machine, à l'insu de l'utilisateur.

Cette vulnérabilité, déjà rencontrée sous un autre système d'exploitation, permettrait à une personne malveillante d'exécuter des commandes, soit par le biais de fichiers audio diffusés (envoyés par courrier électronique, téléchargés, etc.), soit au cours de la visite de pages Web.

Cette vulnérabilité n'est pas, à la date de la publication de ce bulletin, corrigée par l'éditeur Microsoft.

2.2 Recommandations du CERTA

Le CERTA rappelle à cet égard quelques bonnes pratiques qui restent valables :

- Vérifier que la reconnaissance vocale est désactivée par défaut : elle se manifeste par l'entrée `sapisvr.exe` dans le gestionnaire de tâches.
- Désactiver, ou mieux, débrancher le microphone quand celui-ci n'est pas nécessaire ;
- Naviguer sur des sites de confiance, avec un navigateur correctement configuré (par défaut, l'interprétation des codes ActiveX, Java et Javascript doit être désactivée) ;
- N'ouvrir que des documents de confiance ;
- Avoir un système et un antivirus mis à jour ;
- Ouvrir par défaut une session sans droit d'administration particulier.

De manière générale, il est toujours préférable, en terme de sécurité du moins, de patienter un peu avant de se lancer dans l'installation opérationnelle d'un produit « tout beau tout neuf », qu'il s'agisse d'un système d'exploitation, d'un navigateur, ou d'un autre logiciel.

3 Les systèmes d'exploitation sur appareil mobile

3.1 Le problème

Il existe de nombreux dispositifs nomades (téléphone mobile, assistant personnel numérique, etc.) qui utilisent des systèmes d'exploitation, comme par exemple Microsoft Windows Mobile, Symbian, PalmOS, Linux. Il s'agit de versions adaptées au matériel.

De la même manière que leur *grand frère* sur PC, ces systèmes d'exploitation embarqués peuvent également souffrir de vulnérabilités. Si la procédure de mise à jour est très souvent automatique dans un cas, elle l'est beaucoup moins dans l'autre.

Les éditeurs ne corrigent pas systématiquement les vulnérabilités affectant les systèmes d'exploitation pour appareil mobile ; ou sinon, suite à une mise à jour corrigeant une liste cumulée de failles, cela peut impliquer une réinstallation complète du système. Dans cette dernière situation, il se peut aussi que l'appareil perde sa garantie, plaçant l'utilisateur dans un cruel dilemme.

Dans tous les cas, la mise à jour de ces systèmes d'exploitation est un problème complexe pour l'utilisateur.

A valeur d'illustration, deux vulnérabilités, affectant Microsoft Windows Mobile 5.0, Windows 2003 et Windows CE, ont été annoncées cette semaine. Elles permettraient à un utilisateur distant malintentionné de provoquer un déni de service de l'appareil. Par exemple, certaines images au format JPEG construites de manière spéciale

pourraient, par le biais de l'application Images & Vidéos, bloquer l'utilisation normale de l'appareil pendant plusieurs minutes.

Ces éléments réunis font que cette catégorie d'appareil mobile, vulnérables et aux mises à jour hasardeuses ou inexistantes, présentent un risque conséquent pour les systèmes d'informations auxquels ils sont connectés, quelles qu'en soient les motivations :

- pour synchroniser l'agenda ou sa liste de contacts ;
- pour télécharger et mettre à jour un ensemble de documents ;
- pour lire des fichiers multimédias audio ou vidéos ;
- pour installer de nouvelles applications ;
- etc.

Ce problème doit être pris en considération dans la politique de sécurité des systèmes d'information.

3.2 Documentation

- Bulletins de sécurité TrendMicro :
<http://blog.trendmicro.com/trend-micro-finds-more-windows-mobile-flaws/>

4 Problèmes de configuration

Une récente vulnérabilité dans Cisco IOS permet à un utilisateur malintentionné de provoquer un déni de service au moyen d'un paquet SIP (pour Session Initiation Protocol) malformé. Cette vulnérabilité n'affecte que les équipements qui offrent le support du protocole SIP avec une configuration par défaut. Cette vulnérabilité ne toucherait pas les périphériques dont le service a été correctement configuré.

Tout service offert par un système d'information doit avoir été configuré au préalable, ou il n'a pas raison d'être. Les configurations par défaut sont parfois beaucoup trop laxistes en matière de sécurité : on y retrouve des comptes par défaut, des mots de passe par défaut, des interface(s) et/ou port(s) d'écoute(s) par défaut, etc. De tels services ainsi configurés, souvent par facilité ou par négligence, offrent une très bonne opportunité à un utilisateur distant malintentionné de compromettre un système d'information.

5 Month Of Apple Bugs

Voici pour cette semaine les vulnérabilités sur les produits Apple publiées par le projet « Month Of Apple Bugs » :

- Une vulnérabilité le système d'installation de logiciel de Apple MacOS X permettrait de provoquer un déni de service ou l'exécution de code arbitraire ;
- une erreur dans la mise en œuvre de la fonctionnalité Bonjour de iChat permettrait de provoquer un déni de service à distance.

5.1 Réflexions sur la visite de sites

De manière générale, il est à noter que la consultation de sites relevant de la mise à disposition de codes de démonstration comme le projet « MOAB » doit être à éviter. En effet, la vulnérabilité testée par le code mis à disposition peut cacher l'exploitation d'une autre faille non documentée et dont la finalité ne sera pas forcément le simple « test » de vulnérabilité. Il convient donc d'être très prudent vis-à-vis de ce type de sites.

De la même façon, le site hébergeant le code de démonstration ou d'exploitation peut lui-même contenir du code malveillant. Ce cas s'est produit au cours du projet « MOAB », où une image jpeg2000 spécialement construite perturbait le navigateur Safari, à l'ouverture de la page Web. Celle-ci contenait les lignes suivantes :

```
<_img src="bug-files/heat-up.jp2" alt="" height="1" width="1" />
<!-- Never use the macbook at bed again when browsing the MoAB ... -->
```

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 25 janvier et le 01 février 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-2000-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 26 janvier au 01 février 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-056 : Vulnérabilité du serveur DNS BIND
- CERTA-2007-AVI-057 : Vulnérabilités sur Hitachi Web Server
- CERTA-2007-AVI-058 : Vulnérabilités sur CA firewall
- CERTA-2007-AVI-059 : Vulnérabilité dans Trend Micro VirusWall
- CERTA-2007-AVI-060 : Vulnérabilité dans PHP
- CERTA-2007-AVI-061 : Vulnérabilité de Drupal

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

- CERTA-2007-AVI-001-001 : Vulnérabilités dans Cacti
(ajout des références aux bulletins de sécurité de Suse, Mandriva et Debian)
- CERTA-2007-AVI-002-001 : Vulnérabilité dans VLC media player
(ajout des références aux bulletins de sécurité de Gentoo et Debian)
- CERTA-2007-AVI-020-001 : Multiples vulnérabilités dans Fetchmail
(ajout des références aux bulletins de sécurité Gentoo, Mandriva et Ubuntu)
- CERTA-2007-AVI-025-002 : Multiples vulnérabilités de Xorg
(ajout des références aux bulletins de sécurité Gentoo et Debian)
- CERTA-2007-AVI-035-001 : Vulnérabilités de Squid
(ajout des références aux bulletins de sécurité de Suse, Mandriva et Ubuntu)
- CERTA-2007-AVI-055-002 : Vulnérabilité de GTK2
(ajout de la référence au bulletin de sécurité Debian)
- CERTA-2007-AVI-056-004 : Vulnérabilité du serveur DNS BIND
(ajout de la référence au bulletin de sécurité Fedora)

Et l'alerte suivante a été modifiée :

- CERTA-2006-ALE-014 : Vulnérabilités dans Microsoft Word
(annonce d'une nouvelle vulnérabilité par Symantec et ajout des références au bulletin de sécurité Microsoft)

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.

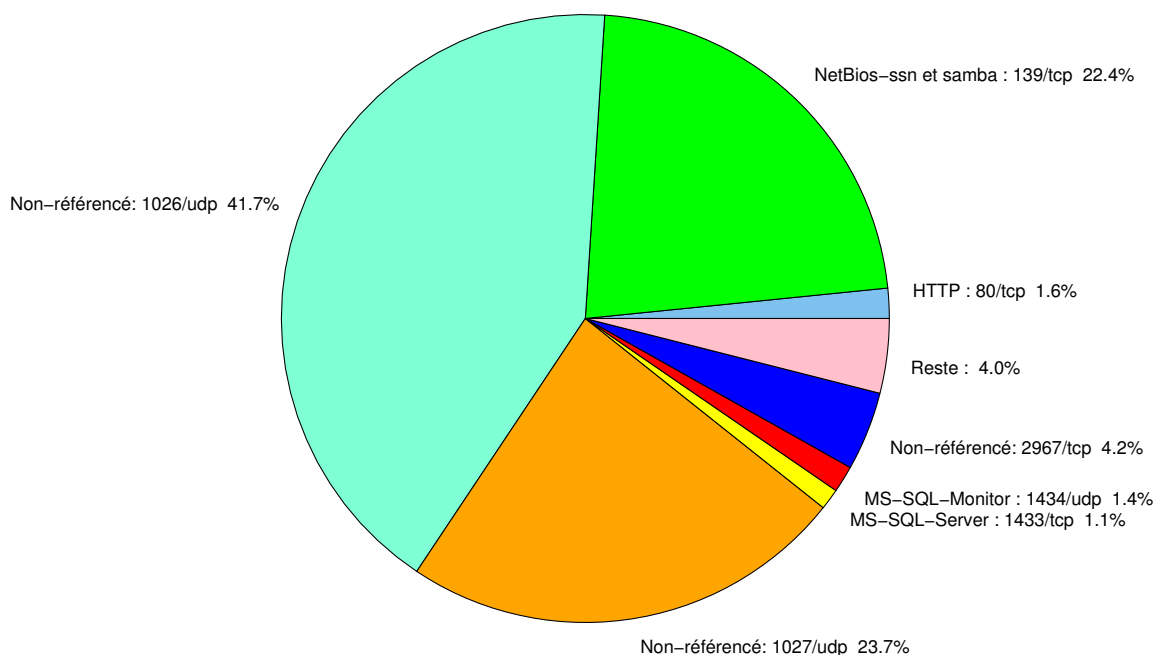


FIG. 1: Répartition relative des ports pour la semaine du 25.01.2007 au 01.02.2007

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	Yellow Worm	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	41.65
1027/udp	23.66
139/tcp	22.38
2967/tcp	4.19
80/tcp	1.59
1434/udp	1.41
1433/tcp	1.11
4899/tcp	0.99
1080/tcp	0.93
137/udp	0.75
3128/tcp	0.39
25/tcp	0.27
443/tcp	0.07
3306/tcp	0.05
143/tcp	0.01

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

02 février 2007 version initiale.