



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 janvier 2010
N° CERTA-2010-ACT-003

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-03

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-2010-ACT-003>

Gestion du document

Référence	CERTA-2010-ACT-003
Titre	Bulletin d'actualité 2010-03
Date de la première version	22 janvier 2010
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-2010-ACT-003.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-2010-ACT-003/>

1 Vulnérabilités dans Microsoft Windows

Le CERTA a publié deux alertes de sécurité affectant les systèmes d'exploitation Windows.

La première référencée CERTA-2010-ALE-001 porte sur l'existence d'une vulnérabilité dans les versions 6, 7 et 8 d'Internet Explorer et qui permet à un utilisateur malveillant, au moyen d'une page web, d'un courriel ou d'un document bureautique spécialement construit, d'exécuter du code arbitraire à distance.

L'éditeur Microsoft a reconnu que cette vulnérabilité a fait l'objet d'exploitation sur l'Internet. Il a également publié une mise à jour de sécurité hors cycle pour Internet Explorer le 21 janvier 2010. Cette mise à jour permet de corriger la vulnérabilité citée dans l'alerte du CERTA, mais également plusieurs autres vulnérabilités dont l'exploitation peut provoquer l'exécution de code arbitraire.

Une deuxième alerte, CERTA-2010-ALE-002, a été publiée par le CERTA le 21 janvier 2010 sur une vulnérabilité dans le sous-système MS-DOS de Microsoft Windows toutes versions 32-bit. Cette vulnérabilité permet à un utilisateur local d'élever ses privilèges au moyen d'un fichier exécutable spécialement construit. Dans l'attente d'un correctif et afin de limiter l'exploitation de cette vulnérabilité, le CERTA a publié des moyens de contournement provisoire destinés à empêcher l'accès au sous-système MS-DOS.

Documentation

- Avis CERTA-2010-AVI-025 du 22 janvier 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-025/>
- Alerte CERTA-2010-ALE-001 du 15 janvier 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-001/>
- Avis CERTA-2010-ALE-002-001 du 21 janvier 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-002/>

2 L'ANSSI recrute !

Depuis le 7 juillet 2009 et la création de l'Agence Nationale de la Sécurité des Systèmes d'Information, les domaines des compétences et les tâches incombant à l'ANSSI se sont fortement élargis. Afin d'assurer ces nouvelles missions, de nombreuses offres d'emploi ont été publiées sur le site Internet de l'agence.

Une vingtaine de nouveaux postes sont d'ores et déjà ouverts.

Les fiches détaillées des postes sont disponibles à la page suivante :

http://www.ssi.gouv.fr/site_rubrique27.html

Cette croissance des effectifs va continuer pendant les mois et années qui viennent. Nous invitons donc les personnes qui seraient intéressées par un avenir professionnel au sein de l'ANSSI à consulter régulièrement cette page ou à suivre le fil RSS dédié disponible à l'adresse ci-après :

http://www.ssi.gouv.fr/site_page_offredemploi_id_rubrique_27.html

Tous les profils sont recherchés de l'ingénieur junior à l'expert en passant par des chefs de projet, et ce dans tous les domaines de la sécurité (cryptographie, terminaux mobiles, réseaux sécurisés, traitement d'incident, informatique industrielle, ...).

3 Les applications client-serveur

Dans le cadre d'applications client-serveur, le modèle de type client lourd demeure encore très utilisé. Ce modèle fait référence à une architecture dans laquelle l'utilisateur dispose d'une application qui contient l'essentiel du code et des traitements applicatifs. Cette application se connecte à un serveur composé d'un service de gestion de base de données. Ainsi, l'essentiel des traitements est effectué par l'application sur le poste client.

D'importantes erreurs de conception sont généralement constatées. Les plus courantes sont détaillées dans l'exemple ci-dessous.

3.1 Description

L'application du poste client se connecte à la base de données via un protocole propriétaire, qui n'inclut la plupart du temps aucun dispositif de sécurité et n'assure ni l'intégrité ni la confidentialité des échanges réseau. L'application, via un compte générique *SQL* inscrit en dur, se connecte à la base de données et vérifie elle-même les comptes qui sont stockés dans une table des comptes applicatifs. Facteur aggravant, les mots de passe sont stockés en clair dans celle-ci. Si une gestion des droits est mise en place, l'application est en charge de brider les interfaces de l'utilisateur selon ses autorisations récupérées dans la base de données.

3.2 Critiques et risques

Ce type d'application présente un certain nombre de défauts structurels importants qu'il est très difficile de corriger sans refondre complètement l'application :

- le compte générique d'accès de l'application et son mot de passe, sont fixés dans le code de l'application et sont facilement retrouvables, soit en rétro-ingénierie du programme, soit en écoutant le trafic réseau. Ce compte permet alors de se connecter directement à la base de données et de récupérer ou de modifier tout ou partie de son contenu, en outrepassant le contrôle des droits des profils utilisateurs ;
- le stockage en clair des mots de passe doit être proscrit, car une compromission des informations de la base de données permet à un attaquant de les récupérer immédiatement et d'essayer de les utiliser dans d'autres applications ;
- tout flux réseau doit inclure des mécanismes d'intégrité et de confidentialité (notamment pendant la phase d'authentification de l'utilisateur) pour contrer les attaques réseau de type écoute ou homme du milieu (*man*

in the middle), permettant d'effectuer des requêtes en tant qu'un autre utilisateur après l'authentification de celui-ci ;

- les attaques par injections *SQL*, très fréquentes dans un contexte d'application Web, sont également possibles dans les applications avec client lourd, qui in fine se connectent sur des systèmes de gestion de bases de données.

3.3 Corrections

Face à ce constat, il convient, dans la mesure du possible, de respecter les principes suivants lors des phases de conception des applications de type client-serveur :

- les mots de passe ne doivent jamais être stockés en clair dans la base de données, mais être conservés sous forme d'empreinte numérique (*hash*), si possible avec une graine (*salt*) ;
- les communications doivent reposer sur des protocoles ouverts, facilement manipulables par des services classiques (par exemple flux *XML* dans des requêtes *HTTP*, permettant d'utiliser des serveurs mandataires) ;
- les dispositifs de protection doivent reposer eux aussi sur des protocoles standards et largement éprouvés (par exemple *TLS*) ;
- les services côté serveur doivent être configurés de façon sécurisée (gestion des comptes par défaut, bridage des fonctionnalités comme les modules *UTL* dans *Oracle*, configuration des listeners, ...) ;
- dans le cas d'une application deux tiers, l'authentification et la gestion des droits utilisateur doivent être exclusivement gérés par le serveur de base de données. Chaque utilisateur doit disposer d'un compte nominatif associé à un groupe, pour lequel les droits applicatifs seront accordés et déclinés en droits *SQL* ;
- les entrées des utilisateurs doivent être filtrées côté serveur, afin de n'autoriser qu'une liste de caractères ou de valeurs nécessaires au fonctionnement de l'application et en prenant soin d'encoder certains caractères spéciaux pouvant être interprétés par le système de gestion de bases de données.

Cependant, le modèle de type client lourd est en perte de vitesse au profit d'un modèle de type client léger, dans lequel le traitement applicatif est déporté sur un serveur dédié. Ce modèle est généralement appelé modèle trois tiers : client, serveur applicatif et base de données. Dans celui-ci, le client n'a alors plus qu'un rôle d'affichage et de saisie et ne doit plus conserver de traitement applicatif de type script *JavaScript* ou code mobile (*ActiveX* ou applet *Java*). Il convient aussi de préférer des applications clientes et des protocoles standardisés, par exemple un navigateur Web utilisant le protocole *HTTPS*. Toutefois, le principe d'authentification dans le modèle trois tiers est généralement mal conçu. Le serveur applicatif ne doit disposer d'aucun compte générique d'accès à la base de données et utiliser un compte fourni par l'utilisateur, via un principe de délégation d'authentification (comme dans le cas d'une application deux tiers).

4 Fin des mises à jour de sécurité pour Debian 4.0 (etch)

Cette semaine le projet Debian a annoncé la fin du support des mises à jour de sécurité pour la version 4.0 de son système d'exploitation GNU/Linux : Debian. Cette version *etch*, déjà qualifiée d'obsolète par le projet depuis la sortie de la version 5.0 *lenny*, ne doit donc plus être utilisée en production et doit être impérativement remplacée par la version 5.0 dans les plus brefs délais.

Le CERTA rappelle l'impérieuse nécessité de n'utiliser en production que des systèmes maintenus par l'éditeur et correctement mis à jour.

5 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>

- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1937>
- Note d'information du CERTA sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

6 Rappel des avis émis

Dans la période du 15 au 21 janvier 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-019 : Vulnérabilité dans TYPO3
- CERTA-2010-AVI-020 : Vulnérabilité dans BIND DNSSEC
- CERTA-2010-AVI-021 : Vulnérabilités dans Adobe Shockwave Player
- CERTA-2010-AVI-022 : Multiples vulnérabilités dans Apple Mac OS X
- CERTA-2010-AVI-023 : Multiples vulnérabilités dans Realplayer et Helix Player

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 oeuvre (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 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique63.html

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.

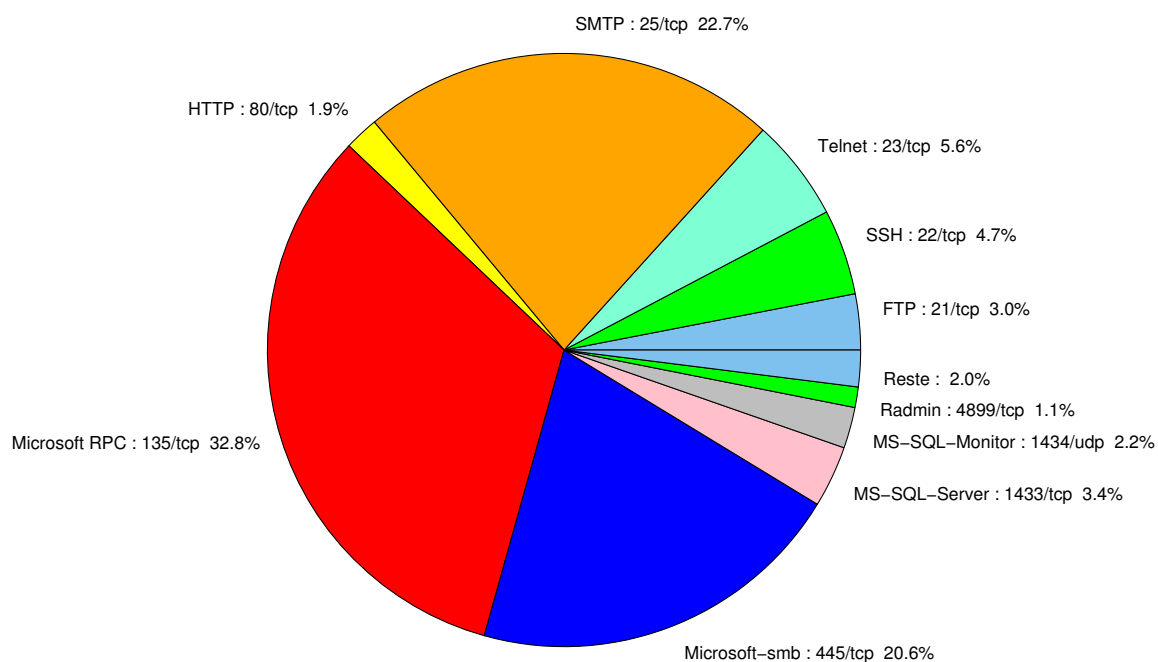


FIG. 1: Répartition relative des ports pour la semaine du 15 au 21 janvier 2010

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 CERTA-2007-ALE-005-001
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	-	CERTA-2007-AVI-320
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	-	- CERTA-2007-AVI-008
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 CERTA-2007-AVI-321
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 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
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 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
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
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183

6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
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	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

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

port	pourcentage
135/tcp	32.75
25/tcp	22.74
445/tcp	20.63
23/tcp	5.65
22/tcp	4.66
1433/tcp	3.35
21/tcp	3.04
1434/udp	2.23
80/tcp	2.11
4899/tcp	1.11
2967/tcp	0.62
3389/tcp	0.43
119/tcp	0.37
3128/tcp	0.18
9898/tcp	0.06

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 janvier 2010 version initiale.