

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-08

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-2009-ACT-008>

Gestion du document

Référence	CERTA-2009-ACT-008
Titre	Bulletin d'actualité 2009-08
Date de la première version	20 février 2009
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-2009-ACT-008.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-2009-ACT-008/>

1 Vulnérabilité non corrigée dans Adobe Reader

Une vulnérabilité non corrigée a été découverte dans Adobe Reader. Cette dernière permet à une personne malintentionnée d'exécuter du code arbitraire à distance via un fichier au format *PDF* spécialement construit.

Cette faille a fait l'objet de la publication de l'alerte CERTA-2009-ALE-001 référant le bulletin de sécurité Adobe APSB09-01 du 19 février 2009.

Cette vulnérabilité est exploitée sur l'Internet et des éditeurs antivirus ont déjà intégré des signatures de codes malveillants tentant de compromettre des machines via cette faiblesse. Ces codes malveillants sont reconnus sous différents noms :

- Trojan.Pidief.E ;
- Exploit-PDF.i ;
- Bloodhound.PDF.6.

En attendant qu'un correctif soit publié, le CERTA recommande d'appliquer les mesures suivantes :

- utiliser un lecteur alternatif ;

- désactiver *JavaScript* dans le lecteur afin de limiter les risques d'exécution de la charge utile ;
- n'ouvrir un fichier au format *PDF* que si celui-ci provient d'une source de confiance ;
- se connecter avec un compte d'utilisateur aux droits limités.

Documentation

- Alerte du CERTA CERTA-2009-ALE-001 du 20 février 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-001/>
- Bulletin de sécurité Adobe APSB09-01 du 19 février 2009 :
<http://www.adobe.com/support/security/advisories/apsb09-01.html>

2 Incident de la semaine

A la recherche du contact perdu

Cette semaine le CERTA a eu besoin de contacter à plusieurs reprises un hébergeur dont plusieurs sites internet ont été compromis. Pour rentrer en contact avec un hébergeur, il peut être utile de consulter les renseignements de la base *RIPE*. Cette base (interrogeable par le commande *whois <adresse IP>* ou *whois <nom de domaine>*) indique, habituellement, les coordonnées d'un responsable technique.

Le CERTA constate fréquemment que des adresses électroniques personnelles sont utilisées dans les enregistrements de cette base de données. Or les évolutions de carrière, les modifications d'organisation ou les déménagements ne sont pas toujours répercutés dans la base *RIPE*. Dès lors, il devient difficile de rentrer en contact avec une personne susceptible de traiter un incident. Les temps de traitements peuvent alors s'allonger et des informations concernant l'incident peuvent transiter par des boîtes aux lettres de personnes parties ou n'ayant plus de rapport avec le traitement d'incident.

Le CERTA rappelle que la base *RIPE* doit être tenue à jour. Les responsables des enregistrements sont également invités à suivre les évolutions et les ajouts des différents champs de cette base de données. L'utilisation d'une adresse fonctionnelle peut limiter les modifications de la base.

Documentation

- Site internet du RIPE Network Coordination Centre :
<http://www.ripe.net>

3 Exploitation de la vulnérabilité ms09-002

L'une des deux vulnérabilités corrigées dans le bulletin ms09-002, est actuellement exploitée.

Pour rappel, ce bulletin qui a fait l'objet de l'avis CERTA-2009-AVI-059 concerne des vulnérabilités dans Microsoft Internet Explorer 7. Les cas observés sur l'internet sont intéressants car si la faille concerne une vulnérabilité d'Internet Explorer, le vecteur d'infection est pourtant un document *.doc* (mais au format XML).

L'ouverture du document provoque la consultation d'une page web spécialement conçue pour exploiter la vulnérabilité en question et pour exécuter du code arbitraire.

Dans le cas analysé par le CERTA, le *shellcode* ainsi exécuté provoque le téléchargement et l'exécution d'un code malveillant. Il intercepte également trois fonctions de Windows pour cacher d'éventuels messages d'erreur provoqués par Internet Explorer.

L'intérêt de passer par Microsoft Word pour exploiter la vulnérabilité est double :

- forcer l'utilisation d'Internet Explorer, même si l'utilisateur consulte d'ordinaire l'Internet à l'aide d'un navigateur alternatif ;
- outrepasser le mode protégé sur Windows Vista.

Dans le cas analysé par le CERTA, l'exploitation de la vulnérabilité est totalement silencieuse (aucun message d'erreur n'est affiché). Il est donc impératif de mettre à jour son système si ce n'est déjà fait. Pour les personnes n'ayant pas cette possibilité, la désactivation du *JavaScript* dans les options d'Internet Explorer (décocher « *scripts ASP* ») rend le code d'exploitation de la vulnérabilité inopérant.

Documentation

- Avis du CERTA CERTA-2009-AVI-059 du 11 février 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-059/>

4 Vulnérabilité de djbdns

Selon un chercheur en informatique, une vulnérabilité serait présente dans le serveur de noms (DNS) : `djbdns`. `Djbdns` est un serveur constitué de plusieurs composants bien distincts, chacun dédié à une fonction bien précise. Ainsi, on trouvera une partie s'occupant de gérer l'ensemble des requêtes pour sa zone (`tinydns`), un autre composant responsable de la mise en cache des requêtes clientes (`dnscache`) ou enfin une partie responsable du support des transferts de zone (`axfr-get`). Ces trois principaux éléments sont mis en œuvre au sein d'un super-service nommé `daemontools` s'occupant du support réseau à la manière de `inetd`.

Or, il semble qu'il existe une vulnérabilité dans la partie gestion de cache : `dnscache`. En effet, ce composant ne met pas en cache les requêtes de type SOA (*Start Of Authority*). L'enregistrement SOA donne les informations nécessaires à l'identification de l'autorité pour une zone donnée. Le fait que ces requêtes ne soient pas mises en cache permettrait à un attaquant de réaliser une attaque de type empoisonnement de cache en envoyant de très nombreuses requêtes au serveur vulnérable.

Il lui est alors possible d'usurper l'identité du serveur autorité pour la zone pointée dans le champ SOA légitime. Le serveur `dnscache` vulnérable donnera alors une réponse erronée à ses clients.

Le chercheur ayant découvert cette vulnérabilité propose un correctif *non officiel* permettant à `dnscache` de prendre en compte correctement les requêtes de type SOA à l'adresse `http://www.your.org/dnscache` en l'attente d'un correctif officiel fourni par le développeur responsable du projet : `http://cr.jp.to`.

Il est à noter enfin que cette vulnérabilité ne touche que la partie « cache » de `djbdns`. Les autres composants comme `tinydns` ou `axfr-get` ne sont pas affectés par la vulnérabilité.

5 Debian 5.0 Lenny

Le 14 février 2009, une nouvelle version stable de la distribution GNU/Linux Debian a été publiée. Celle-ci est estampillée 5.0 et a pour surnom *Lenny*.

Cette nouvelle mouture embarque bien évidemment de nombreuses mises à jour notamment au niveau des interfaces graphiques, du serveur X et sur de nombreux applicatifs. La prise en charge du format Adobe Flash et Java a été simplifiée.

Du point de vue de la sécurité, les correctifs sont installés par le processus d'installation avant le premier redémarrage. Le nombre d'applications utilisant les droits du *superutilisateur* a été réduit, ainsi que le nombre de ports ouverts après une installation standard. La construction de plusieurs paquets a été effectuée avec les options de sécurité de GCC, de même de quelques applications comme PHP qui intègre le correctif de durcissement *Suhosin*.

Enfin une nouvelle image autonome, dite « Live », a fait son apparition et permet de démarrer une machine avec cette distribution sans installation préalable. Cette nouvelle fonctionnalité existe pour les architectures *i386* et *amd64*.

6 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 12 et le 19 février 2009.

7 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=1935>
- 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/>

8 Rappel des avis émis

Dans la période du 13 au 20 février 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-066 : Vulnérabilité dans Sun Java System Directory Server
- CERTA-2009-AVI-067 : Vulnérabilités de Safari
- CERTA-2009-AVI-068 : Multiples vulnérabilités dans Apple Mac OS X
- CERTA-2009-AVI-069 : Vulnérabilités dans Java pour Mac OS X
- CERTA-2009-AVI-070 : Multiples vulnérabilités dans Moodle
- CERTA-2009-AVI-071 : Vulnérabilité dans FreeBSD
- CERTA-2009-AVI-072 : Vulnérabilité de Symantec Veritas NetBackup

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 oeuvre (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 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.ssi.gouv.fr/fr/formation/>

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.

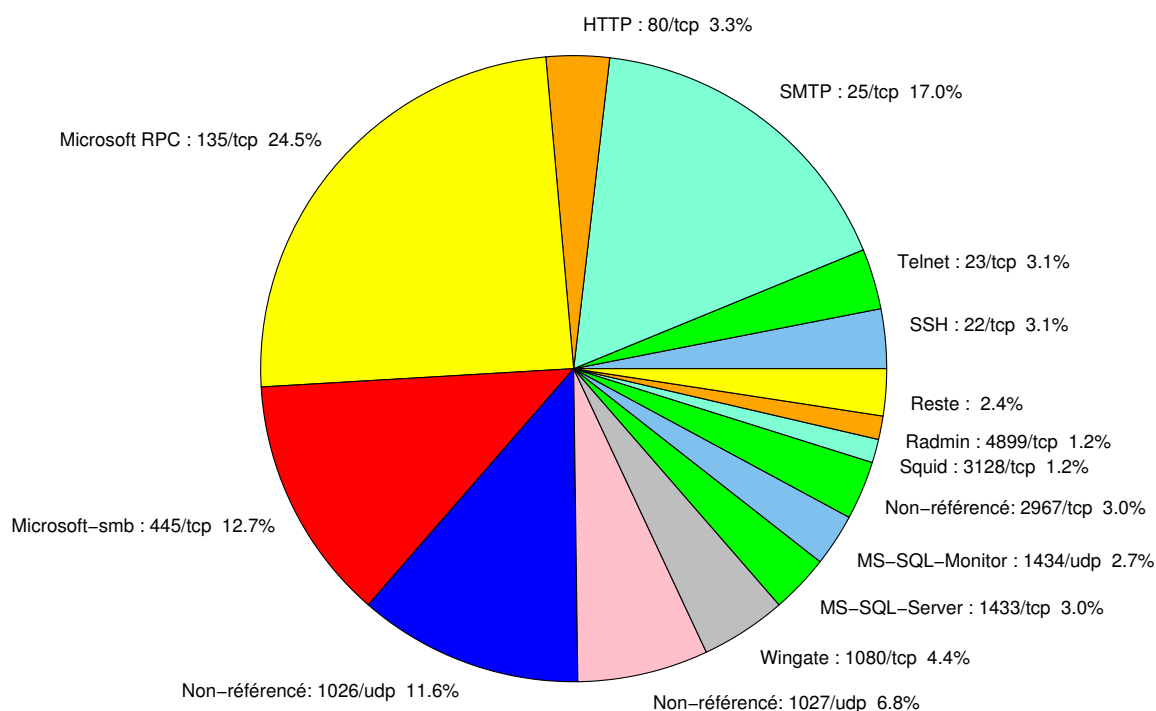


FIG. 1: Répartition relative des ports pour la semaine du 12.02.2009 au 19.02.2009

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	24.55
25/tcp	16.96
445/tcp	12.72
1026/udp	11.6
1027/udp	6.75
1080/tcp	4.42
80/tcp	3.26
23/tcp	3.16
22/tcp	3.07
2967/tcp	3.02
1434/udp	2.7
4899/tcp	1.25
3128/tcp	1.21
21/tcp	0.93
137/udp	0.55
139/tcp	0.46
3389/tcp	0.32
1023/tcp	0.09
42/tcp	0.04

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

20 février 2009 version initiale.