

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2008-19

---

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-2008-ACT-019>

---

### Gestion du document

Référence	CERTA-2008-ACT-019
Titre	Bulletin d'actualité 2008-19
Date de la première version	09 mai 2008
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-2008-ACT-019.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-2008-ACT-019/>

## 1 Les incidents traités cette semaine

### 1.1 Sites de filoutage à répétition

Le CERTA a traité cette semaine un cas de filoutage (imitation de site bancaire) sur un serveur mutualisé. En soi, l'incident n'a rien d'exceptionnel, mais ce qui est intéressant ici, c'est le caractère répétitif. En effet, après avoir informé l'hébergeur, le premier site de filoutage a disparu. Mais d'autres sites de *phishing* ont progressivement peuplé le serveur.

Ainsi, le premier jour, un site de filoutage était installé. Le lendemain, deux autres sites faisaient leur apparition, dans deux répertoires différents. Le surlendemain, deux nouveaux sites étaient installés, dans d'autres répertoires encore.

L'hébergeur a sous-estimé la portée de l'incident. La présence d'un site de *phishing* n'est qu'une manifestation visible d'une vulnérabilité exploitable. L'existence d'un faux site bancaire divulgue publiquement la fragilité d'un serveur, ce qui peut susciter l'intérêt de nombreux intrus. Généralement, de nombreuses intrusions font suite à l'installation d'un site de filoutage, soit parce que la vulnérabilité exploitée n'a pas été correctement identifiée, soit parce qu'au moins une porte dérobée a été installée suite à une intrusion.

Il est souvent conseillé, après une intrusion, de déconnecter la machine du réseau et de faire procéder à un examen des journaux (au moins). Les victimes cherchent souvent à maintenir la continuité de service malgré l'incident, en oubliant parfois que les intrus ont souvent suffisamment de privilèges pour arrêter ou entraver le service.

## 1.2 Attaque par Injection SQL

Cette semaine, le CERTA a traité un incident relatif à la compromission d'un site Internet. Les individus à l'origine de cet incident, ont profité de failles de sécurité de plusieurs pages web pour insérer des directives SQL. Le but de cet injection était de polluer la base de données servant à engendrer les pages web. Une seule instruction a permis de modifier tous les champs texte de la base et d'y insérer du code `javascript` malveillant. L'objectif de ce code était de compromettre les navigateurs des clients du site web.

Ces attaques sont de plus en plus automatisées et il est commun de trouver dans les journaux des connexions des directives SQL « chiffrées » passées en argument.

Ainsi l'instruction suivante :

```
CAST(0x4400450043004C004100520045002000400054002000760061007200630068006100720028003200350035002900 AS NVARCHAR(4000))
```

est traduite par le serveur comme :

```
CAST(DECLARE @T varchar(255) AS NVARCHAR(4000))
```

Pour éviter ou limiter l'impact de ces attaques, le CERTA recommande :

- de contrôler le contenu et la validé des variables avant de les utiliser ;
- de prévenir l'utilisation de certaines directives SQL par l'utilisateur Internet ;
- d'utiliser un utilisateur au droits limités pour la création du site web ;
- de surveiller régulièrement les journaux des connexions afin de mettre en évidence certaines compromissions ou tentatives.

### Documentation

- Note d'information du CERTA sur la sécurité des applications Web et les vulnérabilités de type « injection de données » :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001/>

## 2 Attention aux services paradoxaux

Dans son bulletin d'actualité du 26 janvier 2007 le CERTA présentait les risques des sites Internet proposant de vérifier la sécurité des identifiants. Cette semaine, le CERTA tient à mettre en garde ses lecteurs sur les sites proposant de tester la sensibilité des employés à des attaques par filoutage. Par exemple, il existe un site Web qui propose de dupliquer le site d'une société et d'envoyer de faux courriels à certains employés afin de connaître l'impact d'une campagne de filoutage (*phishing*). Sous couvert d'une activité qui semble légitime, ces sites pourraient également servir à alimenter des bases de données d'utilisateurs crédules. Ces utilisateurs deviendraient alors des proies privilégiées pour de réelles campagnes de filoutage.

Le CERTA recommande d'éviter d'utiliser ce genre de service dont le but pourrait être détourné si des individus malveillants avaient accès aux bases de données des utilisateurs testés. Le CERTA tient également à rappeler que les adresses de courrier électronique nominatives sont des informations personnelles qu'il convient de manier avec précaution.

### Documentation

- Bulletin d'actualité du 26 janvier 2007 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-004/>

## 3 Effets de bord du service pack 3 de Windows XP

Cette semaine, Microsoft a expliqué les effets de bord de l'installation du service pack 3 de Windows XP sur les différentes versions des navigateurs Internet Explorer. Ce service pack n'est toujours pas disponible pour le grand public.

### 3.1 Utilisateurs de Internet Explorer 6

Les utilisateurs de Internet Explorer 6 recevront des mises à jour pour ce navigateur, et aucun effet de bord n'est à prévoir.

### 3.2 Utilisateurs de Internet Explorer 7

Les utilisateurs actuels de Internet Explorer 7 sous Windows XP SP2 recevront également les mises à jour de ce navigateur. Toutefois, après installation du service pack 3i, il sera difficile de désinstaller Internet Explorer 7 pour revenir à la version 6. Pour ce faire, il faudra désinstaller le service pack 3, puis désinstaller Internet Explorer 7. La raison donnée par Microsoft est que le service pack 3 de Windows XP contient de nouveaux fichiers pour Internet Explorer 6, et que la désinstallation de Internet Explorer 7 provoquerait le remplacement de certains de ces nouveaux fichiers par ceux sauvegardés par le système d'installation pendant la première installation de Internet Explorer 7. Ainsi, l'on se retrouverait dans un état dans lequel il y aurait un mélange de nouveaux et d'anciens fichiers pour Internet Explorer 6. L'installation de Internet Explorer 7 après l'installation du service pack 3 de Windows XP ne provoque pas cet effet de bord, car le système d'exploitation sauvegarderait alors les nouvelles versions des fichiers de Internet Explorer 6.

### 3.3 Utilisateurs de Internet Explorer 8 Bêta 1

Les utilisateurs actuels de Internet Explorer 8 Bêta 1 ne se verront pas proposer automatiquement les mises à jour de Windows XP Service Pack 3. Comme pour Internet Explorer 7, il serait alors impossible de désinstaller le nouveau navigateur. Celui-ci étant en version beta, Microsoft estime qu'il est préférable de pouvoir le supprimer.

### 3.4 Recommandations

Toutes les personnes susceptibles de revenir à une version antérieure du navigateur utilisé actuellement doivent impérativement le faire avant l'installation du service pack 3 de Windows XP. Le navigateur peut ensuite être réinstallé après mise à jour du système d'exploitation.

### 3.5 Documentation

- Entrée du 05 mai 2008 sur le bloc-notes de MSDN :  
<http://blogs.msdn.com/ie/archive/2008/05/05/ie-and-xpsp3.aspx>

## 4 Filtrage des adresses MAC

### 4.1 Adresses MAC ?

L'adresse MAC (*Medium Access Control*) est de taille 6 octets (48 bits). Elle identifie normalement de manière unique les interfaces réseau utilisées. Certaines conventions précisent que cette adresse peut être écrite en 6 groupes d'hexadécimaux séparés par le caractère "-" ou ":" afin de rendre sa lecture plus aisée.

Plusieurs protocoles ayant un fonctionnement au niveau 2 des couches protocolaires OSI l'utilisent. On peut citer par exemple :

- Ethernet 802.3 ;
- Wi-Fi 802.11 ;
- Token Ring 802.5 ;
- Bluetooth 802.15.1 ;
- etc.

Sous Bluetooth par exemple, cette adresse porte le nom de `BD_ADDRESS` : elle caractérise l'interface réseau et a aussi une taille de 6 octets.

## 4.2 Le filtrage

Dans des environnements réseau, qu'ils soient filaires ou sans fil (WiFi, Bluetooth, etc.), il peut être intéressant de s'assurer que d'autres équipements physiques ne sont pas « branchés » illégalement. Dans le cas du Wi-Fi par exemple, cela peut aussi éviter que des postes s'associent de façon spontanée ou accidentelle à un point d'accès qui ne leur est pas dédié.

Le filtrage se fait en général sous forme de liste blanche ou noire.

## 4.3 Fausses bonnes idées et recommandations

### 4.3.1 Modifier ses adresses MAC

Modifier une adresse MAC a été proposé par certains constructeurs d'équipements réseau, car il s'agit d'une fonctionnalité intéressante pour les administrateurs souhaitant faire des tests ou ayant des configurations particulières.

La plupart des systèmes d'exploitation permettent ainsi de modifier les adresses MAC des interfaces réseau. On peut citer à valeur d'exemple :

- sous Linux :

```
ifconfig <interface> hw eth XX:XX:XX:XX:XX:XX
```

- sous \*BSD :

```
ifconfig <interface> link XX:XX:XX:XX:XX:XX
```

- sous MacOS (Leopard) :

```
ifconfig <interface> lladdr XX:XX:XX:XX:XX:XX
```

- sous Windows XP : modifier les clés de registre comme :

```
HKLM\SYSTEM\CurrentControlSet\Control\Class\
{4D36E972-E325-11CE-BFC1-08002BE10318}\...
```

et ajouter la variable « NetworkAddress » avec l'adresse XXXXXXXXXXXX (REG\_SZ) à l'interface voulue. Elle se trouve en cherchant la chaîne « DriverDesc » sous regedit.

- sous Cisco IOS : dans le mode de configuration d'interface :

```
mac-address XXXX.XXXX.XXXX
```

Les commandes ne sont pas toujours fonctionnelles directement, car cela peut également dépendre des logiciels matériels des cartes et des possibilités d'interaction qu'ils offrent. De petits utilitaires plus complets permettent ainsi de fonctionner avec un ensemble plus large d'équipements.

L'administrateur peut chercher à vérifier si de telles manipulations ont lieu. Plusieurs techniques s'appuient en particulier sur d'autres champs des en-têtes. Sous 802.11 (Wi-Fi), la valeur *Sequence Control* intègre un numéro de séquence incrémental et peut aider à identifier différentes interfaces utilisant une adresse MAC commune.

### 4.3.2 Les recommandations du CERTA

L'objectif de cet article n'est pas de lister toutes les méthodes pour modifier son adresse MAC ni de détecter de telles manipulations dans un réseau.

Il faut cependant bien comprendre que le filtrage d'adresses MAC n'est pas une méthode d'authentification. Ce n'est également pas une mesure de sécurité suffisante pour contrôler l'usurpation ou l'insertion de nouveaux éléments dans le réseau. Cela fait partie des bonnes mesures à mettre en place pour améliorer la maîtrise du réseau, mais comme toute mesure de sécurité, il est également important d'en connaître les limitations.

## 5 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 01 et le 08 mai 2008.

## 6 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/>

## 7 Rappel des avis émis

Dans la période du 02 au 08 mai 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-223 : Vulnérabilité dans WordPress
- CERTA-2008-AVI-224 : Vulnérabilité dans SNMPc
- CERTA-2008-AVI-225 : Multiples vulnérabilités dans PHP
- CERTA-2008-AVI-226 : Vulnérabilité dans IBM WebSphere Application Server
- CERTA-2008-AVI-227 : Vulnérabilité dans IBM Lotus Expeditor
- CERTA-2008-AVI-228 : Vulnérabilité dans Sun Java System Directory Server
- CERTA-2008-AVI-229 : Vulnérabilité dans Nortel Multimedia Communication Server
- CERTA-2008-AVI-230 : Vulnérabilité dans Akamai Download Manager
- CERTA-2008-AVI-231 : Vulnérabilités dans KDE
- CERTA-2008-AVI-232 : Vulnérabilité dans Sun Solaris

## 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 oeuvre (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 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.

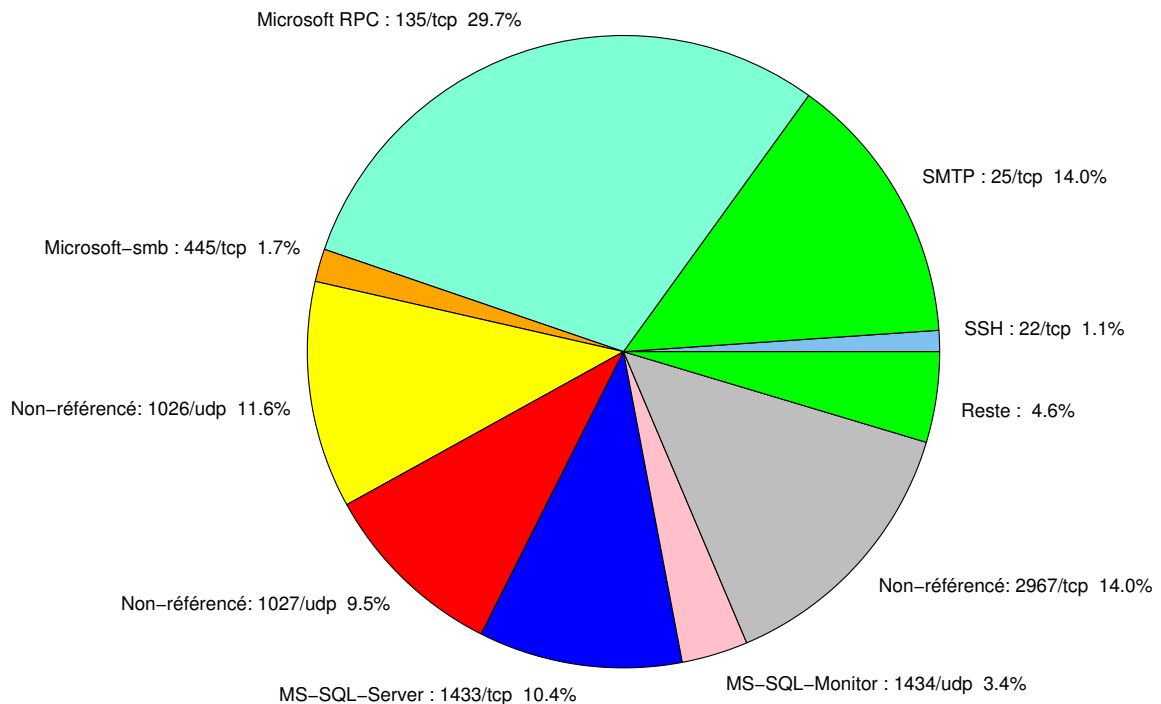


FIG. 1: Répartition relative des ports pour la semaine du 01.05.2008 au 08.05.2008

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

<b>port</b>	<b>pourcentage</b>
135/tcp	29.71
2967/tcp	14
25/tcp	13.96
1026/udp	11.6
1433/tcp	10.41
1027/udp	9.53
1434/udp	3.39
445/tcp	1.67
22/tcp	1.07
4899/tcp	0.87
3306/tcp	0.79
143/tcp	0.63
139/tcp	0.59
80/tcp	0.55
21/tcp	0.23
23/tcp	0.19
3128/tcp	0.03

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	9
3	Paquets rejetés . . . . .	10

## Gestion détaillée du document

09 mai 2008 version initiale.