

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2010-30

---

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-030>

---

### Gestion du document

Référence	CERTA-2010-ACT-030
Titre	Bulletin d'actualité 2010-30
Date de la première version	30 juillet 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-030.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-030/>

## 1 Incident de la semaine

### Du JavaScript malveillant pour courriel

Dernièrement, le COSSI a constaté une augmentation du nombre de courriels incluant une *iFrame* pour télécharger du code *JavaScript* malveillant. On peut identifier au moins deux cibles pour ce type d'attaque :

- les clients de messagerie intégrant un moteur *JavaScript* avec un modèle *DOM* associé, le modèle *DOM* est alors spécifique et le *JavaScript* malveillant cible ce modèle en particulier ;
- les *Webmails*, qui eux utilisent un navigateur Web qui possède de facto un moteur *JavaScript* et un *DOM* relativement standard. La surface d'attaque est donc bien plus importante que dans le premier cas.

Le CERTA recommande la plus grande précaution lors de l'ouverture d'un message électronique. En particulier, il est conseillé de configurer son client de messagerie pour ouvrir les messages en mode texte uniquement. Dans le cas des *Webmails*, qui sont rarement configurables en lecture texte uniquement, une alternative est d'utiliser une extension au navigateur bloquant l'exécution de code actif.

Les bonnes pratiques liées à l'utilisation de la messagerie sont résumées dans la note d'information du CERTA suivante : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/>.

## 2 La sécurité de WPA/WPA2 mise en péril?

Cette semaine, un chercheur en sécurité présentait, lors d'une conférence, une vulnérabilité de WPA/WPA2. Cette vulnérabilité a été annoncée comme sérieuse dans la presse. Mais, maintenant qu'elle a été dévoilée, qu'en est-il réellement?

Tout d'abord, précisons que cette vulnérabilité n'est pas basée sur une faiblesse de pilote, ou d'implémentation, mais bien sur la dernière spécification 802.11i (<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>). Elle concerne uniquement WPA/WPA2 *Entreprise*, puisqu'elle n'a pas d'incidence sur WPA PSK. Elle ne peut être utilisée qu'à travers une station authentifiée et associée à un point d'accès Wifi, ce qui réduit donc grandement la surface d'attaque.

Pour mémoire, dans le cadre de WPA/WPA2 *Entreprise*, deux types de clés sont utilisées :

- La PTK (*Pairwise Transient Key*), propre à chaque station, utilisée pour protéger le trafic entre la station et le point d'accès.
- La GTK (*Group Temporal Key*), partagée entre toutes les stations, qui est utilisée pour chiffrer ce qui est envoyé sur l'adresse de *broadcast*, depuis le point d'accès, vers les clients.

Une station malveillante peut utiliser la connaissance de la GTK pour forger son propre paquet et l'envoyer sur l'adresse de *broadcast*, en se faisant passer pour le point d'accès. Ce paquet peut ainsi être utilisé, pour faire de l'empoisonnement de cache ARP, et rediriger le trafic des autres stations vers la station malveillante. Les paquets redirigés seront chiffrés, à l'aide de la PTK de la station victime, entre cette dernière et le point d'accès, puis ils seront transmis à la station malveillante, en étant, cette fois, chiffrés par sa propre PTK. Il est important de souligner que, contrairement à ce qui a pu être annoncé, les PTK des autres stations ne sont à aucun moment accessibles à l'attaquant.

La redirection de paquet par une station authentifiée n'a rien de nouveau, cette technique va simplement apporter plus de discrétion puisque la station malveillante usurpe l'identité du point d'accès lors de l'envoi des messages à l'adresse de *broadcast*.

Face à cette vulnérabilité, plusieurs contre mesures sont proposées, comme surveiller les stations émettant des paquets sur l'adresse de *broadcast*, ou même mettre en place des mécanismes d'isolation entre les stations. Il est également important de bien isoler les différents réseaux Wifi selon la nature des données circulant et des personnes se connectant à ces réseaux.

Enfin, le CERTA tient à rappeler qu'il est impératif de rester prudent lors de connexion à des réseaux Wifi publiquement accessibles (lieu de restauration, aéroport, hôtels ...), et des informations qu'on laissera transiter sur ces réseaux.

## 3 Actualité autour de DNSSEC

Cette semaine, lors d'une célèbre conférence sur la sécurité, l'ICANN (Internet Corporation for Assigned Names and Numbers) et la société Verisign ont fait l'annonce que, désormais, l'ensemble des serveurs DNS racines (*root servers*) pouvaient fournir des enregistrements de type DNSSEC valides. Ainsi, les informations fournies par ces serveurs racines peuvent donc maintenant être signées numériquement.

Certains, à tort, anticipent déjà sur le fait que cela permette de réduire un certain nombre d'actions malveillantes sur l'Internet comme le filoutage (*phishing*) ou les pourriels (*spam*) car il sera possible d'identifier le domaine de provenance d'un message de façon « sûre ». Il est clair que le fait de donner la possibilité de vérifier le contenu des zones fournies par les serveurs racines est une avancée notable méritant une communication officielle. Mais il reste tout de même du chemin avant que les différents points suivants soient réglés :

- que chaque TLD (Top Level Domain eg. *.fr*, *.org*, *.com*, etc) signe ses enregistrements ;
- que chaque domaine et sous domaine en fasse de même ;
- que chaque logiciel faisant de la mise en cache DNS soit capable d'exploiter ses informations pour filtrer le bon grain de l'ivraie provenant de serveurs autorité ou d'autres serveurs cache ;
- que les clients DNS ou *resolver* mettent en œuvre cette technologie de signature.
- que l'ensemble des logiciels ou composants sus cités soient dans leur dernière version afin d'utiliser pleinement ces nouvelles fonctionnalités ;
- que l'ensemble des équipements (pare-feu, routeur, mandataires, ...) soit compatible avec les subtilités liées à DNSSEC (cf. CERTA-2010-ACT-005) ;
- et enfin, que chaque utilisateur soit à même d'appréhender la différence de comportement à adopter vis-à-vis d'un domaine signer d'un autre qui ne le serait pas ;

– etc.

Tout ceci constitue des obstacles techniques, organisationnels et humains qu’il faudra surmonter pour atteindre l’objectif que certains considèrent, un peu hâtivement, comme déjà acquis.

## 4 Une application Android indiscreète

Après un module additionnel malveillant pour *Firefox* et l’application *iPhone* « lampe de poche » aux fonctionnalités cachées, c’est maintenant au tour d’Android d’être visé par une application indiscreète. En effet, lors de la même conférence que dans les articles précédents, une présentation a pointé du doigt une application de fond d’écran qui envoyait les données de l’appareil (agenda, contacts, *IMSI*, ...) vers un serveur à l’étranger. Cette application a été retirée par Google de l’« *Android Market* » une fois signalée comme malveillante.

Ces trois affaires ont en commun qu’elles reposent sur la décision de l’utilisateur d’installer une application. Cette opération étant grandement simplifiée par l’utilisation de *fournisseurs officiels* avec des procédures automatisées et qui apportent un sentiment de confiance, l’utilisateur a tendance à faire moins attention à ce qu’il installe.

Le CERTA recommande la plus grande prudence lors de l’installation de modules tiers, comme pour l’installation de tout logiciel. Une mesure de prudence est de n’installer que les programmes nécessaires et de suivre les mises à jour et publications les concernant, et, si possible, d’attendre avant d’installer une application nouvellement disponible, qu’elle soit évaluée par la communauté des utilisateurs.

## 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 23 au 29 juillet 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-335 : Vulnérabilité dans Mozilla Firefox
- CERTA-2010-AVI-336 : Vulnérabilité dans JBoss ESB
- CERTA-2010-AVI-337 : Vulnérabilités dans Google Chrome

- CERTA-2010-AVI-338 : Vulnérabilités dans IBM Lotus Notes
- CERTA-2010-AVI-339 : Multiples vulnérabilités dans les produits Symantec
- CERTA-2010-AVI-340 : Vulnérabilité dans Nessus Web Server Plugin
- CERTA-2010-AVI-341 : Vulnérabilité dans GnuPG
- CERTA-2010-AVI-342 : Multiples vulnérabilités dans Apple Safari
- CERTA-2010-AVI-343 : Vulnérabilité de Dovecot
- CERTA-2010-AVI-344 : Multiples vulnérabilités dans SAP NetWeaver

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

- CERTA-2009-AVI-482-009 : Vulnérabilité du protocole SSL/TLS (ajout des bulletins de sécurité HP)
- CERTA-2010-AVI-044-001 : Vulnérabilité dans BIND avec DNSSEC (ajout de la référence au bulletin IBM)

## **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\\_rubrique67.html](http://www.ssi.gouv.fr/site_rubrique67.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.

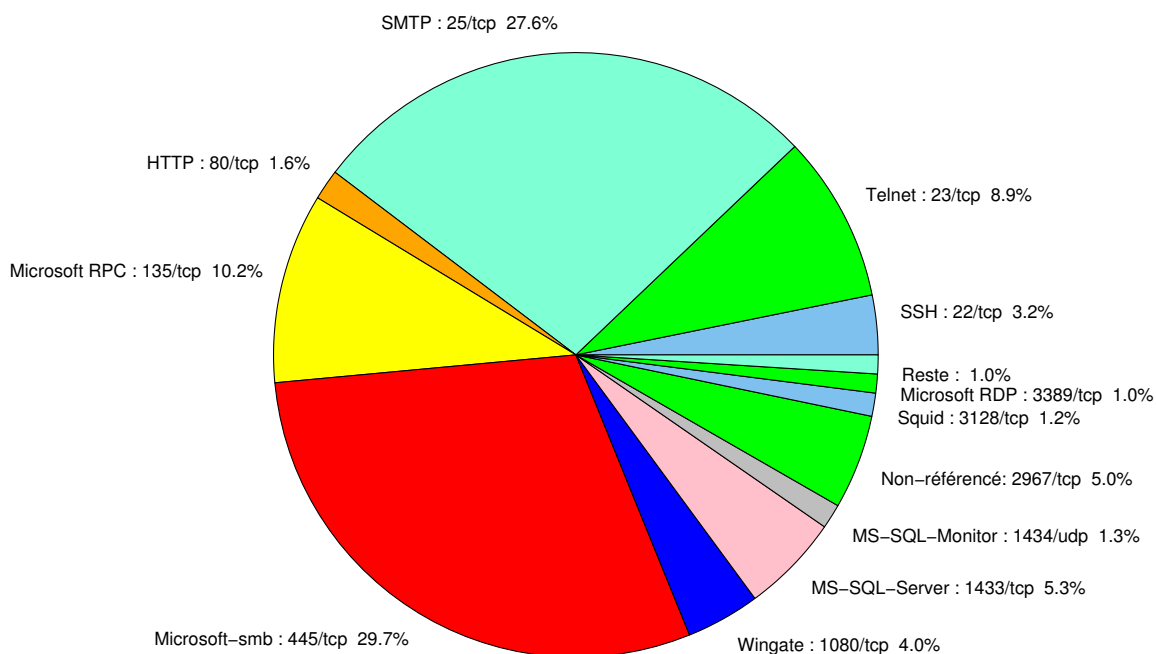


FIG. 1: Répartition relative des ports pour la semaine du 23 au 29 juillet 2010

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
445/tcp	29.65
25/tcp	27.56
135/tcp	10.17
23/tcp	8.92
1433/tcp	5.27
2967/tcp	5.04
1080/tcp	3.95
22/tcp	3.18
80/tcp	3.02
1434/udp	1.31
3128/tcp	1.24
3389/tcp	1
21/tcp	0.46
4899/tcp	0.31
3306/tcp	0.23
143/tcp	0.07

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	7
3	Paquets rejetés . . . . .	8

## Gestion détaillée du document

30 juillet 2010 version initiale.