



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 24 décembre 2009  
N° CERTA-2009-ACT-052

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2009-52**

---

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-052>

---

### Gestion du document

Référence	CERTA-2009-ACT-052
Titre	Bulletin d'actualité 2009-52
Date de la première version	24 décembre 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-052.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-052/>

## 1 Attaques ciblant *phpMyVisites*

L'application *phpMyVisites* a fait l'objet d'une très importante mise à jour de sécurité le 16 décembre 2009 (avis CERTA-2009-AVI-560). Ce correctif fait suite à l'exploitation d'une vulnérabilité d'un module tiers, appelé *Clickheat*, fourni avec *phpMyVisites*. La nouvelle version du logiciel n'intègre plus cette extension vulnérable.

De plus, les développeurs de *phpMyVisites* ont publié une page dédiée à des attaques constatées début décembre 2009. En particulier, un serveur compromis pourrait contenir les fichiers suivants :

- *phpmv2/datas/thumbs.php* ;
- *styles.css.php* ;
- *fotter.php* ;
- *s.php* ;
- un fichier PHP ayant pour nom une série de chiffres, par exemple *8475875.php*.

La compromission est susceptible de s'étendre à tout le serveur, pas uniquement au répertoire de *phpMyVisites*. Un des correspondants du CERTA a déjà signalé une telle compromission, survenue le 5 décembre 2009. L'intrus n'a pas défiguré le site Web, donc l'attaque ne laisse pas de traces évidentes (en dehors des journaux). Par contre,

l'attaquant a déposé de nombreuses portes dérobées et a peut-être exploité des vulnérabilités du noyau pour élever ses privilèges et devenir administrateur du serveur.

Le CERTA recommande à tous les administrateurs de sites fonctionnant avec *phpMyVisites* de rechercher dans les journaux d'accès les appels au module `Clickheat` (par exemple à l'aide de la commande `grep -i clickheat access.log`). De tels accès, notamment à l'aide de requêtes `POST`, sont caractéristiques d'une compromission. Tout administrateur constatant une telle activité dans ses journaux est invité à contacter le CERTA.

## 2 Attaquer le serveur DNS plutôt que le site Web cible

*Twitter*, le célèbre site de *microblogging* (<http://www.twitter.com>) a subi une attaque le 18 décembre 2009. Dans la matinée de cette journée, la majorité des internautes qui tentaient de se connecter sur le site Web de Twitter arrivaient sur un site affichant une page de revendication anti-américaine, signée par « l'Iranian Cyberarmy ».

À la lumière des éléments publics de l'attaque, le site Web de Twitter n'a vraisemblablement subi aucune agression. Les pirates ont en fait visé le système DNS de *Twitter*. La société *Twitter* utilise une offre externalisée de DNS, qui a pour rôle de résoudre les requêtes. Ainsi, lorsqu'un internaute souhaite se connecter à *Twitter*, son navigateur Web va émettre une demande de résolution DNS, afin de transformer le nom `www.twitter.com` en adresse IP, par exemple `168.143.162.36`. Les attaquants ont réussi, en se connectant à l'interface d'administration du DNS, à modifier cette résolution, pour la faire pointer vers le site de leur choix. La suite est connue...

Cet incident peut amener quelques réflexions.

Tout d'abord, commençons par la revendication du piratage. Même si la page visible des internautes contenait des propos anti-américains, reprochant notamment l'ingérence des États-Unis envers l'Iran, aucun élément ne permet à l'heure actuelle d'identifier avec certitude les auteurs de l'attaque. Les conclusions rapides sont donc à éviter dans ce genre d'affaire, d'autant plus que le fameux groupe « Iranian Cyberarmy » ne bénéficie d'aucun historique dans les sources d'informations ouvertes...

D'autre part, cet incident n'est en soit pas nouveau, d'autres sites ont subi les mêmes types d'attaques dans le passé. L'élément intéressant ici est de bien identifier la chaîne globale de confiance. Assurer la sécurité et la disponibilité d'un site Web est une tâche souvent bien plus complexe qu'il n'apparaît à première vue, car de nombreux éléments doivent être pris en compte... Depuis les routeurs d'accès, les équipements de partage de charge, le réseau d'administration, les serveurs de *middleware* et bases de données, sans oublier les serveurs DNS et le maintien des noms de domaine, tous les maillons de la chaîne ont leurs importances, et il suffit parfois d'un simple grain de sable mal placé pour que tout s'effondre.

## 3 Cadeaux de fin d'année malveillants

La période des fêtes de fin d'année est toujours propice à la propagation de codes malveillants. Il est en effet dans la tradition de s'échanger de nombreux cadeaux et autres cartes de vœux. Ces dernières, développement durable oblige, ont maintenant pris un format électronique et permettent à certains individus malintentionnés de profiter de la situation.

Il existe, en effet, de nombreux sites permettant la création et l'envoi de cartes de vœux virtuelles. Certains sites peuvent avoir de nombreuses façons de détourner la gentille attention en cadeau empoisonné, outre la collecte d'informations personnelles comme l'adresse électronique. Il est également envisageable d'intégrer dans la carte de vœux des *JavaScript* et autres codes dynamiques (comme *Flash* par exemple) afin d'exploiter des vulnérabilités dans les interpréteurs et ainsi compromettre la machine du destinataire.

En cette fin d'année, nombreuses sont les personnes qui commandent leurs cadeaux via l'Internet ou qui font livrer les cadeaux chez leurs proches. Il est ainsi aisé de profiter de cette situation afin d'émettre de faux avis de passage ou de réception de colis et ainsi pousser les utilisateurs à ouvrir des pièces jointes malveillantes.

Le CERTA rappelle qu'il existe une vulnérabilité non corrigée dans les produits Adobe Acrobat et Adobe Reader permettant d'exécuter du code arbitraire à distance et que celle-ci est susceptible d'être exploitée, sous la forme d'une carte de vœux par exemple. Il est fortement recommandé d'appliquer les contournements provisoires détaillés dans l'alerte CERTA-2009-ALE-023 afin de limiter les risques de compromission.

### Documentation

- Alerte CERTA-2009-ALE-023 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-023>

## 4 Vulnérabilités des produits Citrix

La semaine dernière, l'éditeur Citrix a publié deux bulletins de sécurité :

- CTX123649, relatif aux produits NetScaler et Access Gateway Enterprise Edition, fait référence à la vulnérabilité détaillée dans CVE-2009-4609. Cette vulnérabilité a fait l'objet d'une alerte CERTA-2009-ALE-017 puis de plusieurs avis pour les éditeurs ayant corrigé leurs produits : CERTA-2009-AVI-372, CERTA-2009-AVI-376, CERTA-2009-AVI-377 et CERTA-2009-AVI-422. Le CERTA n'a pas publié d'avis de sécurité relatif à ce bulletin Citrix car il ne constitue qu'un contournement provisoire détaillant les éléments de configuration à prendre en compte pour rendre une attaque inopérente.
- CTX123610, relatif aux produits Clientless SSL VPN, détaille une vulnérabilité dans l'implémentation de la couche SSL de ces produits. Dans ce cas également, le CERTA n'a pas produit d'avis car la vulnérabilité dont il est question n'est pas corrigée dans ces produits Citrix mais fait simplement l'objet de contournements provisoire.

En tout état de cause, ces recommandations sont évidemment à appliquer si vous disposez de ces équipements ou si vous mettez en œuvre ce type de technologies.

### Documentation :

<http://support.citrix.com/article/CTX123649>

<http://support.citrix.com/article/CTX123610>

## 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 18 au 24 décembre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-548 : Vulnérabilité dans VMware vCenter Lab Manager
- CERTA-2009-AVI-549 : Multiples vulnérabilités dans Drupal

- CERTA-2009-AVI-550 : Multiples vulnérabilités dans Cisco WebEx WRF Player
- CERTA-2009-AVI-551 : Multiples vulnérabilités dans IBM WebSphere
- CERTA-2009-AVI-552 : Vulnérabilité dans des produits Horde
- CERTA-2009-AVI-553 : Multiples vulnérabilités de PHP
- CERTA-2009-AVI-554 : Multiples vulnérabilités dans Wireshark
- CERTA-2009-AVI-555 : Vulnérabilités dans Adobe Flash Media Server
- CERTA-2009-AVI-556 : Multiples vulnérabilités dans IBM AIX
- CERTA-2009-AVI-557 : Vulnérabilités dans OSSIM
- CERTA-2009-AVI-558 : Vulnérabilité dans IBM WebSphere Application Server Feature Pack for CEA
- CERTA-2009-AVI-559 : Vulnérabilités dans Winamp
- CERTA-2009-AVI-560 : Vulnérabilité dans phpMyVisites

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

- CERTA-2009-AVI-149-001 : Vulnérabilité dans mod\_perl pour Apache (ajout des bulletins de sécurité Sun Solaris et Mandriva )
- CERTA-2009-AVI-508-001 : Multiples vulnérabilités dans GIMP (ajout du bulletin de sécurité Sun Solaris)

## **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](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.

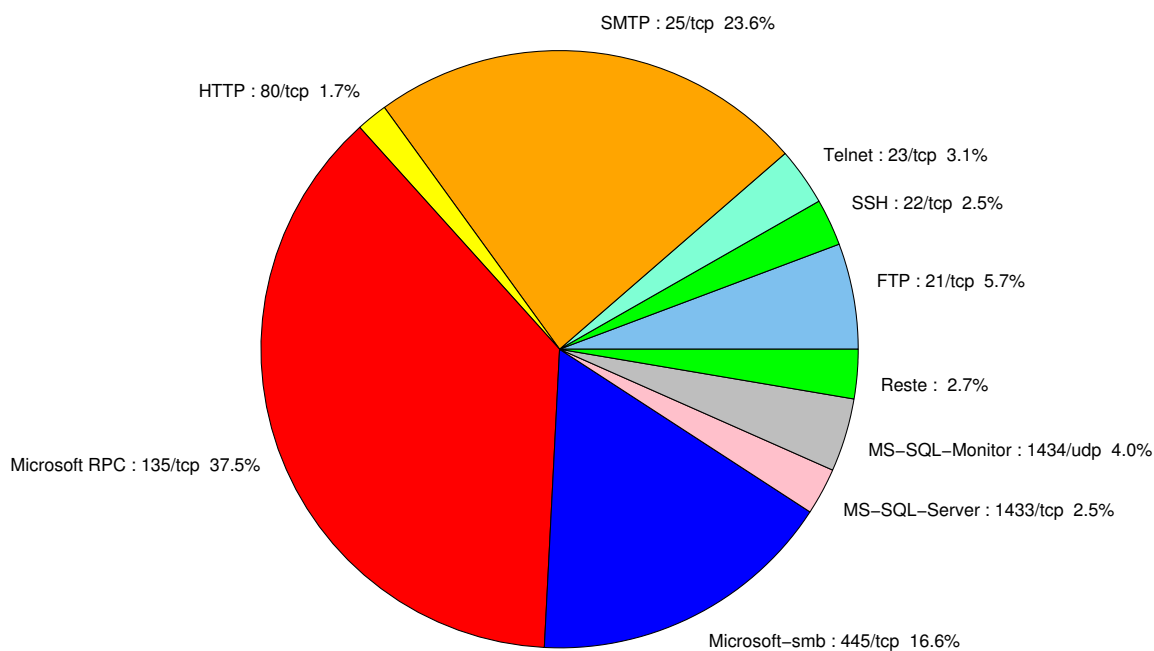


FIG. 1: Répartition relative des ports pour la semaine du 18 au 24 décembre 2009

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	37.51
25/tcp	23.6
445/tcp	16.64
21/tcp	5.72
1434/udp	3.96
23/tcp	3.31
22/tcp	2.6
1433/tcp	2.53
80/tcp	2.21
1080/tcp	0.71
4899/tcp	0.58
3389/tcp	0.32
143/tcp	0.13

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

24 décembre 2009 version initiale.