



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 septembre 2010
N° CERTA-2010-ACT-035

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-36

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-036>

Gestion du document

Référence	CERTA-2010-ACT-035
Titre	Bulletin d'actualité 2010-36
Date de la première version	10 septembre 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-035.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-035/>

1 Vulnérabilité non corrigée dans Adobe Acrobat et Adobe Reader

Cette semaine, le CERTA a publié un bulletin d'alerte, CERTA-2010-ALE-014, portant sur une vulnérabilité dans Adobe Reader et Adobe Acrobat.

Cette vulnérabilité présente dans le module de traitement des polices de caractère d'Adobe Reader et Adobe Acrobat (*CoolType.dll*) permet l'exécution de code arbitraire à distance au moyen d'un document PDF spécialement construit.

Un code d'exploitation est déjà diffusé sur l'Internet et semble fonctionner sur de nombreuses plateformes, incluant Microsoft Windows 7 et Vista. De plus, il a la capacité de contourner les mécanismes de protection de type ASLR (*Address Space Layout Randomization*) et DEP (*Data Execution Prevention*).

Dans l'attente d'un correctif de sécurité de la part de l'éditeur le CERTA préconise certaines recommandations dans le bulletin d'alerte CERTA-2010-ALE-014, afin de limiter l'impact et l'exploitation de cette vulnérabilité.

Documentation

– Avis CERTA-2010-ALE-014 :

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-014/>

2 Nouveau ver « Here you have »

Depuis ces dernières 24 heures, un nouveau ver se propage par les courriels. Ce type de ver n'est pas nouveau, le virus « I love you » avait utilisé la même technique de propagation il y a plus de dix ans.

Ce ver se propage donc principalement via la messagerie en parcourant le carnet d'adresses du client de messagerie et envoyant un courriel à tous les contacts. Le message envoyé peut notamment avoir comme titre « Here you have » mais d'autres variantes sont déjà apparues. Le contenu du message utilise l'ingénierie sociale pour inciter l'utilisateur à cliquer sur un lien qui semble pointer sur un document de type PDF (principalement mais d'autres versions existent avec d'autres types de documents). Le document en question n'est pas un PDF mais un fichier exécutable avec l'extension « .SCR ».

Le ver se répand aussi en utilisant le mécanisme des fichiers `Autorun.inf` via des supports amovibles ou des disques réseau.

Une fois installé le virus peut notamment (liste non exhaustive) :

- désactiver le *Centre de Sécurité Windows* et *Windows Update* ;
- modifier des paramètres de sécurité de Windows ;
- désactiver le pare-feu ou en changer la configuration ;
- bloquer l'exécution de nombreux antivirus et utilitaires de nettoyage ;
- télécharger des fichiers arbitraires depuis l'Internet ;
- désactiver certains utilitaires de gestion des périphériques USB ;
- supprimer le fichier `HOSTS`.

De par son activité de « *mass mailing* » le ver peut provoquer des dysfonctionnements des serveurs de messagerie à cause de la charge induite. Pour les serveurs Exchange, Microsoft a publié une entrée de blog décrivant les procédures à suivre pour purger les messages malveillants, créer des règles de filtrage et identifier les stations de travail à l'origine de l'envoi massif de messages (Cf. la section « Documentation »).

Plusieurs mesures peuvent limiter l'impact de ce type de vers (liste non exhaustive) :

- informer les utilisateurs du type de message qu'ils pourraient recevoir ;
- mettre à jour les antivirus ;
- contacter votre éditeur si vous utilisez des solutions de sécurité sur vos serveurs de messagerie (mise à jour de signatures, de règles, etc) ;
- filtrer les liens ou fichiers « .SCR » sur les proxies/pare-feux/filtres de messagerie ;
- désactiver l'*Autorun* ;
- utiliser un compte avec des droits limités.

Documentation

- Analyse technique du virus par le MMPC :
<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm:Win32/Visal.B>
- Blog Microsoft concernant les actions spécifiques pour les serveurs Exchange :
<http://social.technet.microsoft.com/wiki/contents/articles/worm-win32-visual-b.aspx>

3 RIPE et perturbation de BGP

Malgré plusieurs précautions (audit de code et routeur *BGP* en coupure du routeur expérimental), une expérience visant à valider une version sécurisée du protocole *BGP* (*Border Gateway Protocol*) a engendré une petite perturbation de l'Internet le jeudi 27 août 2010 pour une durée estimée de 30 minutes à 1 heure.

Dans le cadre de cette expérience, le RIPE NCC (Réseaux IP Européens Network Coordination Centre : organisme en charge de la gestion et de la coordination technique de l'infrastructure de l'Internet pour l'Europe) a effectué des annonces *BGP* expérimentales depuis Amsterdam en utilisant un attribut non défini dans les *RFC* de *BGP*. Il est important de souligner que d'après ces *RFC*, ces annonces expérimentales devaient être sans conséquence sur les implémentations existantes de *BGP*.

Un bug dans les routeurs Cisco a été l'origine de la panne. Face à cet attribut inconnu, certaines versions d'implémentation du protocole *BGP* embarquées dans des routeurs Cisco modifiaient les annonces *BGP* expérimentales en les rendant incompatibles avec les *RFC*, donc avec les implantations des autres constructeurs. Par voie de conséquence, ces annonces invalides étaient rejetées par les voisins des routeurs Cisco incriminés. Le rejet de ces annonces invalides a eu pour conséquence de couper les sessions *BGP* entre les routeurs de certains opérateurs.

Plusieurs impacts sur l'Internet ont rapidement été identifiés :

- la disparition de certains préfixes (0.04% à 0.13%) donc l'inaccessibilité des IP correspondantes ;
- l'instabilité de certaines annonces BGP (1.4% - 4500 préfixes).

En France, cette inaccessibilité a touché deux serveurs *DNS* gérant la zone « FR », cinq d'entre eux n'ont pas été touchés du tout. L'AFNIC a par ailleurs indiqué que cela n'a absolument pas perturbé le service global de résolution sur la zone « FR ».

Ce bogue et ses conséquences ont rapidement été identifiés grâce à la grande réactivité du RIPE NCC et des différents acteurs de l'Internet. Le bogue a par ailleurs été corrigé par Cisco via un patch pour ses routeurs (Cf. l'avis CERTA-2010-AVI-410). Ce bogue d'implémentation aurait pu être déclenché par n'importe quel opérateur utilisant *BGP* et demeure similaire au bogue Cisco de février 2009 (<http://www.renesys.com/blog/2009/02/longer-is-not-better.shtml>).

Documentation

- Avis CERTA-2010-AVI-410 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-410/>

4 Problème avec SPIP 2.1

Selon les développeurs de SPIP, un bogue a été introduit il y a environ 10 mois dans la version 2.1 de leur produit. Cela a eu pour conséquence, le 3 septembre 2010, de donner le sentiment que les articles des sites sous SPIP avaient disparu. Alors qu'en fait, il ne s'agissait que d'un problème d'affichage.

Les développeurs proposent deux façons de corriger ce problème :

- en remplaçant, dans le fichier *ecrire/public/quete.php*, ligne 82, la valeur 10000 par 365*2 ;
- ou bien en installant la version 2.1.2 de SPIP.

Le problème n'existe que sur les architectures 32 bits, pour lesquelles la date excède la valeur maximale.

Le CERTA n'a pas publié d'avis de sécurité concernant cette nouvelle version de SPIP, le problème n'étant pas une atteinte à l'intégrité des données.

Documentation :

- Article du 3 septembre 2010 sur le site de SPIP :
http://www.spip.net/fr_article5248.html

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 03 au 09 septembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-415 : Multiples vulnérabilités dans Apple iTunes
- CERTA-2010-AVI-416 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-417 : Vulnérabilité dans Squid
- CERTA-2010-AVI-418 : Vulnérabilités dans MantisBT
- CERTA-2010-AVI-419 : Multiples vulnérabilités dans Mozilla Thunderbird
- CERTA-2010-AVI-421 : Vulnérabilités dans Apple Safari
- CERTA-2010-AVI-422 : Multiples vulnérabilités dans les produits Cisco Wireless LAN
- CERTA-2010-AVI-423 : Multiples vulnérabilités dans Apple iOS
- CERTA-2010-AVI-424 : Vulnérabilité dans RSA Access Manager Server
- CERTA-2010-AVI-425 : Vulnérabilité dans RSA Access Manager Agent

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

- CERTA-2010-AVI-420 : Multiples vulnérabilités dans Mozilla Firefox et Mozilla SeaMonkey (Ajout de Mozilla SeaMonkey dans les systèmes affectés)

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

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.

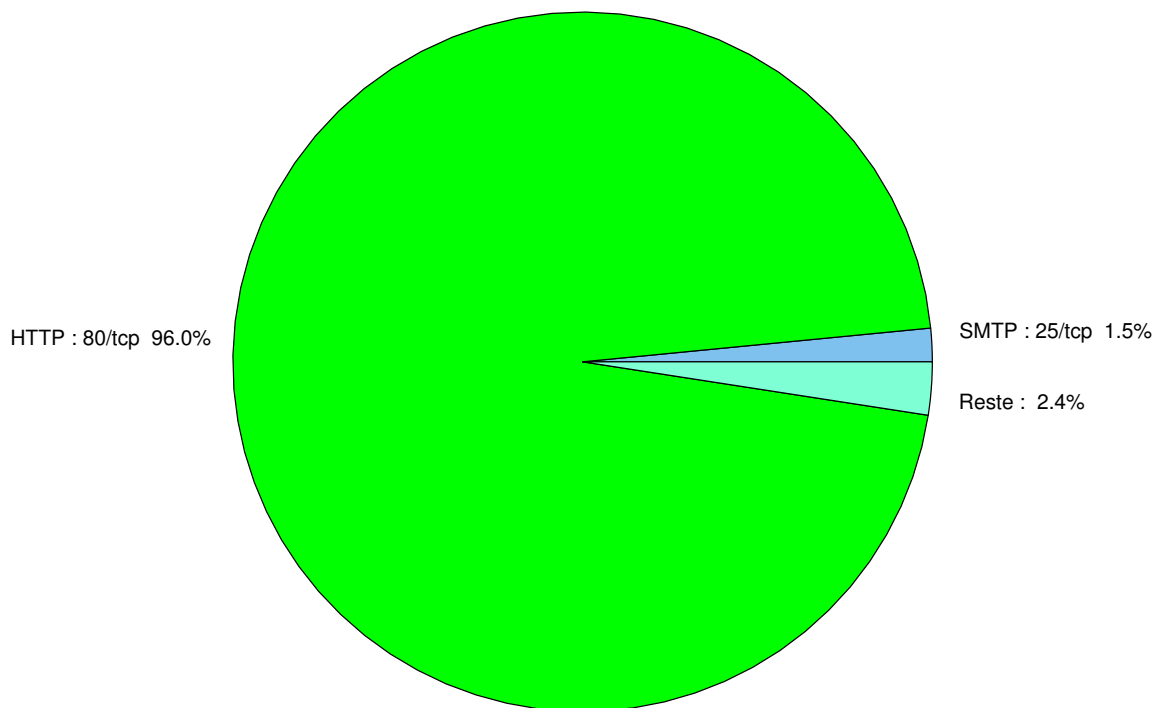


FIG. 1: Répartition relative des ports pour la semaine du 03 au 09 septembre 2010

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
80/tcp	96.05
25/tcp	1.54
2967/tcp	0.39
1433/tcp	0.35
445/tcp	0.34
135/tcp	0.28
1080/tcp	0.26
22/tcp	0.2
3389/tcp	0.12
1434/udp	0.09
21/tcp	0.06
4899/tcp	0.03

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

10 septembre 2010 version initiale.