

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-50

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-050>

Gestion du document

Référence	CERTA-2009-ACT-050
Titre	Bulletin d'actualité 2009-50
Date de la première version	11 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-050.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-050/>

1 Incident de la semaine

Cette semaine le CERTA a traité un incident somme toute assez banal. Il s'agit de la modification de la page d'accueil de 13 sites, hébergés sur le même serveur. La modification consistait à rajouter un lien pointant vers un site externe. Quand un client du site naviguait sur la page d'accueil, ce script chargeait et exécutait un code malveillant à son insu.

Pour une fois, le problème ne venait pas spécialement de la mutualisation de l'hébergement. Les 13 sites appartiennent à la même entité et sont gérés de manière homogène. En revanche, l'hébergeur utilise un CMS (gestionnaire de contenu ou *Content Management System*) pour la gestion courante des sites et a succombé à la tentation de l'installation de plusieurs greffons (*plug-ins*) afin de faciliter les tâches d'administration courante.

Malheureusement, un de ces greffons s'avérait présenter une faille de sécurité permettant d'accéder en écriture aux pages des sites administrés. Le pirate n'a donc eu qu'à utiliser des codes d'exploitation existant afin de modifier toutes les pages d'accueil des 13 sites.

Cela prouve une fois de plus (s'il en était besoin) que la maîtrise précise et complète de tout le système d'information, quelque soit la granularité, reste la fondation du processus de sécurisation d'un système d'information. Il est parfois tentant d'utiliser des outils tiers, mais une grande vigilance doit être de mise. Dans le doute, il vaut

certainement mieux se passer d'outils plutôt que d'abaisser le niveau de sécurité de son système. Et quelque soit les outils utilisés, il est primordial de suivre les mises à jour et de les appliquer dès que possible.

2 Alertes de la semaine

Cette semaine le CERTA a publié deux alertes :

- CERTA-2009-ALE-021 : Vulnérabilité dans Adobe Illustrator : Une vulnérabilité affecte Adobe Illustrator CS3 et Adobe Illustrator CS4 lors du traitement des fichiers au format eps (*Encapsulated Postscript*). Elle permet l'exécution de code arbitraire à distance.
- CERTA-2009-ALE-022 : Vulnérabilité dans le produit de visioconférence TANDBERG MXP : Une vulnérabilité affecte les produits TANDBERG MXP lors du traitement du flux H.225 RAS (*Registration, Administration and Status*). Elle permet à une personne malveillante distante de provoquer un déni de service.

2.1 Documentation

- Bulletin d'alerte du CERTA CERTA-2009-ALE-021 du 10 décembre 2009 : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-021/index.html>
- Bulletin d'alerte du CERTA CERTA-2009-ALE-022 du 11 décembre 2009 : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-022/index.html>

3 L'actualité Microsoft

3.1 Les bulletins de sécurité Microsoft du mois de décembre

Cette semaine, Microsoft a publié les 6 derniers bulletins de sécurité de l'année dans le cadre de son *patch Tuesday*. Les vulnérabilités corrigées sont les suivantes :

- une vulnérabilité dans le service LSASS de Microsoft Windows lors du traitement de certains messages ISAKMP permet de provoquer un déni de service à distance ;
- deux vulnérabilités présentes dans ADFS (*Active Directory Federation Service*) ont été publiées et permettent d'exécuter du code arbitraire à distance ou de contourner la politique de sécurité ;
- des vulnérabilités ont été découvertes dans le service d'authentification Internet de Microsoft et permettent, entre autre, d'exécuter du code arbitraire à distance.
- plusieurs vulnérabilités concernant Microsoft Internet Explorer ont été corrigées. Certaines permettent à un utilisateur malveillant distant d'exécuter du code arbitraire au moyen d'une page Web spécialement écrite.
- une vulnérabilité dans Microsoft WordPad et Microsoft Office Word permet à un utilisateur d'exécuter du code arbitraire à distance par le biais d'un document Word 97 spécialement conçu ;
- une vulnérabilité a été identifiée dans Microsoft Office Project et permet d'exécuter du code arbitraire à distance en incitant une victime à ouvrir un fichier Project spécialement conçu.

Ces mises à jour ont permis de corriger l'alerte CERTA-2009-ALE-020.

3.2 Mise à jour de sécurité concernant le codec Indeo

Cette semaine, Microsoft a émis l'avis de sécurité n°954157 concernant le codec Intel Indeo41. La mise à jour ne corrige pas de vulnérabilité dans le codec mais empêche son chargement depuis Internet Explorer et Windows Media Player. L'ouverture d'un fichier spécialement conçu exploitant une faille dans le codec peut en effet provoquer l'exécution de code arbitraire sur le système vulnérable. Par cette mise à jour, Microsoft a donc réduit la surface d'attaque possible et bloque les vecteurs d'infection les plus utilisés.

Les systèmes d'exploitation concernés sont Microsoft Windows 2000, Windows XP et Windows Server 2003. La mise à jour est proposée en téléchargement automatique.

Cela ne corrigeant pas le codec vulnérable, le CERTA recommande, dans la mesure du possible, de désinscrire complètement le codec. Cela peut toutefois avoir des effets de bord sur certaines applications. La démarche pour désinscrire le codec est disponible sur le site internet de Microsoft (kb954157).

3.3 Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de décembre 2009 : <http://www.microsoft.com/france/technet/security/bulletin/ms09-dec.msp>
- Avis de sécurité Microsoft 954157 du 08 décembre 2009 : <http://support.microsoft.com/kb/954157>

4 Google DNS ?

Le 3 décembre 2009, Google a annoncé son nouveau service : Google Public DNS (<http://code.google.com/speed/public-dns/>). Google élargit donc son offre, et propose maintenant un service universel de résolution de nom. La chose n'est en soit pas si nouvelle : des offres de DNS externes existent depuis plusieurs années, citons par exemple OpenDNS (<http://www.opendns.com>) ou DynDNS (<http://www.dyndns.org>)...

Néanmoins, l'offre de Google mérite probablement un peu plus d'attention, ne serait-ce que par le battage médiatique qu'elle soulève, et l'importance qu'elle pourrait prendre si, comme pour beaucoup de services Google, elle rencontre un succès fort.

4.1 Le DNS

Tout d'abord, il est important de comprendre de quoi il s'agit. Le DNS est un service critique de l'Internet qui a pour rôle d'établir une correspondance entre une adresse IP et un nom de domaine. Ainsi, les ordinateurs connectés à un réseau IP possèdent tous une adresse IP (en IPv4, elle est de la forme `www.xxx.yyy.zzz`, en base 255). Ce quadruplet étant difficile à retenir, un mécanisme permet d'associer à une adresse IP un nom intelligible, appelé nom de domaine (ex : le nom de domaine `www.certa.ssi.gouv.fr` est associé à l'adresse IP 213.56.176.2).

Généralement, le fournisseur d'accès met à disposition de ses abonnés ses propres serveurs DNS. Dans le cadre de réseaux plus importants, le DNS est un service directement mis en place en interne. Pourquoi donc utiliser un service DNS alternatif ? Plusieurs raisons peuvent être invoquées :

- le service DNS de votre opérateur ne fonctionne pas de façon optimale. Cela peut en effet parfois arriver, même si un opérateur digne de ce nom devrait savoir que le DNS est un élément critique du réseau ;
- un service DNS externe propose plus de fonctions (sécurité, performance, analyse et journalisation, ...).

4.2 Des fonctions DNS avancées ?

Cette deuxième raison peut en effet être séduisante. Les offres DNS externes fournissent parfois plusieurs fonctions qui intéressent tant le gestionnaire réseau que l'utilisateur final :

- un service de liste noire, c'est-à-dire que le DNS va refuser de résoudre des domaines jugés non conformes à votre politique de sécurité (par exemple, sites non professionnels, sites dangereux ou infectés par des maliciels, voir contrôle parental...);
- des tableaux de bord, permettant de connaître l'activité de vos utilisateurs (domaines les plus consultés, top 10...);
- des fonctions « avancées », par exemple de meilleures performances par une optimisation de la gestion des caches, et/ou par une distribution géographique des serveurs ;
- l'utilisation de techniques visant à éviter les attaques de type « empoisonnement de cache ». Suite aux événements sur le DNS de l'été 2008, la sécurité des requêtes DNS est devenue un enjeu fort. Des techniques d'amélioration de l'entropie des requêtes sont donc conseillées. Il est ainsi souhaitable de s'assurer d'une bonne entropie sur le port source utilisé par le serveur DNS lors de requêtes récursives, voir même de l'utilisation de techniques « avancées ».

4.3 Quels risques ?

Cependant, l'utilisation d'un DNS externe non maîtrisé soulève plusieurs problèmes.

En premier lieu, la question de la confidentialité se pose. En effet, connaître vos requêtes DNS, c'est savoir ce que vous faites sur l'Internet ! Toutes consultations ou utilisations de l'Internet reposent sur l'utilisation du DNS... Si en plus, le fournisseur du service DNS possède déjà de nombreuses informations sur les utilisateurs (par exemple parce qu'il opère aussi un service de messagerie, un moteur de recherche...), alors la somme des connaissances auxquelles il accède peut devenir très importante.

Ensuite, le DNS est véritablement la clef de voûte en termes de confiance sur l'Internet. Ainsi, une personne mal intentionnée qui maîtriserait votre DNS aurait un contrôle complet sur votre usage de l'Internet, avec la possibilité de contrôler la vision même du réseau, vous rediriger sur des serveurs de son choix... Tout devient possible.

D'autres pratiques non souhaitables sont aussi envisageables. Par exemple, la substitution de « NX Domain » (cf. le bulletin d'actualité CERTA-2009-ACT-049).

Enfin, l'externalisation du DNS implique que les requêtes vont alors transiter sur le réseau Internet, entre le client et le DNS. Toute personne malintentionnée sur le chemin de connexion devient alors en mesure de réaliser les actions décrites précédemment.

L'utilisation d'un service externe de résolution de nom doit donc être un acte murement réfléchi, et il convient de bien peser les avantages, et les inconvénients, que cette décision entraînera.

5 La gestion des correctifs de sécurité Mozilla

Lors d'un bulletin d'actualité précédent (<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-032/index.html>), nous avons déjà parlé de la différence de traitement entre les différents produits Mozilla en matière de sécurité. Régulièrement, Thunderbird affiche un retard sur Firefox dans la publication des correctifs de sécurité, qui concernent pourtant des vulnérabilités communes aux deux logiciels.

Cette semaine a vu la sortie de Thunderbird 3.0. Cette nouvelle mouture du client de messagerie Mozilla offre un certain nombre d'évolutions notamment, au niveau de l'interface utilisateur. Ces changements sont présentés sur le site de Thunderbird :

<http://www.mozillamessaging.com/en-US/thunderbird/3.0/releasenotes>

Le CERTA a publié une alerte sur Thunderbird 2 le 7 août 2009 concernant plusieurs vulnérabilités critiques non corrigées. Plusieurs de ces vulnérabilités ne sont toujours pas corrigées à ce jour dans la version 2. Il est donc surprenant de voir Mozilla sortir une version 3.0 de son client de messagerie sans avoir corrigé les vulnérabilités critiques de la version 2.

Mozilla ne fournit pas d'informations quant aux vulnérabilités potentielles de cette dernière mouture, Thunderbird 3.0 n'étant pas encore suivi officiellement par les bulletins de sécurité de Mozilla.

Le CERTA recommande d'utiliser les mêmes contournements provisoires pour Thunderbird 3.0 que ceux indiqués dans l'alerte CERTA-2009-ALE-014 pour Thunderbird 2.

Documentation

- Alerte CERTA-2009-ALE-014 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-014/>
- Page de téléchargement de Thunderbird 3
<http://fr.www.mozillamessaging.com/fr/>

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=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/>

7 Rappel des avis émis

Dans la période du 04 au 10 décembre 2009 , le CERTA a émis les avis suivants :

- CERTA-2009-AVI-529 : Vulnérabilités dans IBM WebSphere
- CERTA-2009-AVI-530 : Multiples vulnérabilités de Java pour Mac OS X
- CERTA-2009-AVI-531 : Vulnérabilité dans HP NonStop Server
- CERTA-2009-AVI-532 : Multiples vulnérabilités dans BlackBerry Attachment Service
- CERTA-2009-AVI-533 : Multiples vulnérabilités dans Sun Solaris
- CERTA-2009-AVI-534 : Multiples vulnérabilités dans Sun Java Portal Server
- CERTA-2009-AVI-535 : Vulnérabilité dans le service LSASS de Microsoft Windows
- CERTA-2009-AVI-536 : Vulnérabilités dans Microsoft ADFS
- CERTA-2009-AVI-537 : Multiples vulnérabilités du service d’authentification Internet de Microsoft
- CERTA-2009-AVI-538 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2009-AVI-539 : Vulnérabilité dans Microsoft WordPad et Microsoft Office Word
- CERTA-2009-AVI-540 : Vulnérabilité dans Microsoft Office Project
- CERTA-2009-AVI-541 : Multiples vulnérabilités dans Adobe Flash Player et Adobe Air

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

- CERTA-2009-AVI-363-002 : Vulnérabilité de wget (ajout des références aux bulletins de sécurité Sun et des systèmes affectés correspondants)

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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique63.html

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.

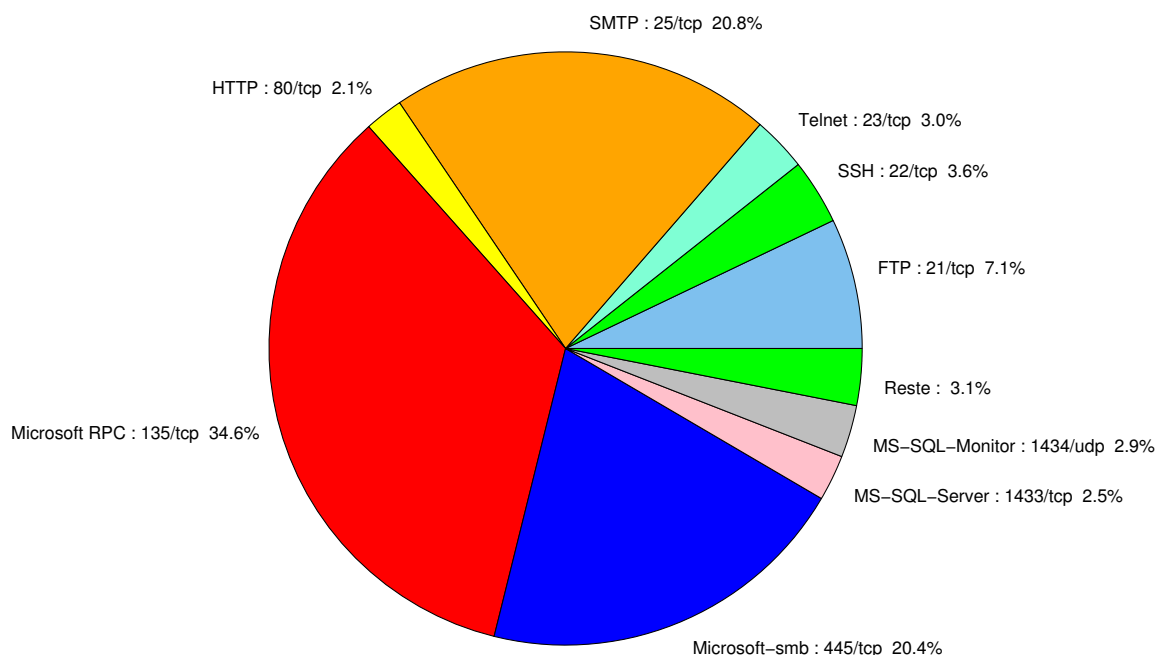


FIG. 1: Répartition relative des ports pour la semaine du 04 au 10 décembre 2009

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	34.57
25/tcp	20.83
445/tcp	20.43
21/tcp	7.1
22/tcp	3.55
23/tcp	2.96
1434/udp	2.85
1433/tcp	2.5
80/tcp	2.38
2967/tcp	0.98
3389/tcp	0.75
4899/tcp	0.52
3128/tcp	0.4
1080/tcp	0.17
3306/tcp	0.11

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

11 décembre 2009 version initiale.