

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-04

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-004>

Gestion du document

Référence	CERTA-2010-ACT-004
Titre	Bulletin d'actualité 2010-04
Date de la première version	29 janvier 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-004.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-004/>

1 Incident de la semaine

1.1 Conficker : appliquer le correctif MS08-067 nécessaire et insuffisant

1.1.1 Faits

Cette semaine le CERTA a été contacté pour une infection récente par *Conficker*, ver apparu il y a plus d'un an. Le ver s'est propagé sur l'ensemble du réseau, ralentissant fortement les activités de l'entité.

Les administrateurs informatiques se sont étonnés de l'ampleur de la propagation car le correctif MS08-067 de *Microsoft*, corrigeant une vulnérabilité du service *Server* de *Windows*, avait été appliqué sur tous les ordinateurs du parc, postes de travail et serveurs. Ce problème est l'objet de l'avis CERTA-2008-AVI-523 du 23 octobre 2008.

En fait, le ver a évolué entre la fin 2008 et le premier trimestre 2009 et a diversifié ses modes de propagation.

Outre l'attaque exploitant la vulnérabilité mentionnée précédemment, le ver se propage :

- par les supports amovibles dont les clefs USB, en exploitant l'exécution automatique (*Autorun*) activée par défaut sur les versions 2000, XP et 2003 de *Microsoft Windows* ;
- par les partages réseau, en volant un jeton d'authentification ou en réalisant une attaque par dictionnaire sur la base d'une liste d'une centaine de mots de passe.

Dans l'incident, le correctif désactivant l'Autorun n'avait pas été appliqué, permettant une première infection. Ensuite, les partages réseau ont servi à la propagation rapide du ver.

1.1.2 Recommandations

Des recommandations contre le ver Conficker sont généralisables au maintien d'un niveau de sécurité minimal :

- appliquer les correctifs de sécurité, tous les correctifs, dans un délai le plus court possible, après qualification ;
- cloisonner le système d'information (réseau, partages, applications) et isoler très fortement les ordinateurs pour lesquels la mise à jour n'est pas possible ou différée ;
- utiliser des mots de passe robustes mais facilement mémorisables par leurs détenteurs ;
- utiliser au quotidien des comptes utilisateur aux droits restreints ;
- éviter de se connecter sur un ordinateur compromis en tant qu'administrateur, local ou du domaine. Préférer la connexion en utilisateur ordinaire et la fonction `runas` ou `Exécuter` comme ;
- surveiller les différents journaux disponibles (pare-feu, relais HTTP, serveurs, etc.) pour réagir rapidement aux anomalies ;
- se méfier des supports amovibles.

1.1.3 Documentation

- Avis du CERTA CERTA-2008-AVI-523 du 23 octobre 2008 *Vulnérabilité dans Windows Service Server* : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-523/>
- Avis du CERTA CERTA-2009-AVI-064 du 11 février 2009 *Vulnérabilité dans l'Autorun sur Windows* : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-064/>
- Bulletin d'actualité du CERTA CERTA-2009-ACT-007 du 13 février 2009 : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-007/>
- Note d'information du CERTA CERTA-2005-INF-001 du 12 avril 2007 *Les mots de passe* : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information du CERTA CERTA-2006-INF-006 du 11 février 2009 *Risques associés aux clés USB* : <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>

2 Qualification de vulnérabilité et liste de changements

Il y a deux semaines, était publié sur l'Internet les détails d'une vulnérabilité affectant le noyau Linux. On trouve également la preuve de faisabilité associée. En substance cette faille permet à un utilisateur local d'élever ses privilèges sous certaines conditions pour devenir *root*. Cette vulnérabilité a été prise en compte par les développeurs et corrigée à partir de la version 2.6.32.4 du noyau.

Pour obtenir un peu plus d'informations sur cette faille et sur la nature du correctif, on peut s'intéresser à la liste de changements apportés à cette version du noyau : `Changelog-2.6.32.4`. On cherche alors la fonction vulnérable (`do_mremap()`) et la correction associée. Voici ce que l'on peut lire :

```
commit 1f51eb3a881359e97dc2c228e55c83fba598e349
Author: Al Viro <viro@zeniv.linux.org.uk>
Date: Thu Jan 14 11:39:39 2010 -0800

    untangle the do_mremap() mess

This backports the following upstream commits all as one patch:
54f5de709984bae0d31d823ff03de755f9dcac54
ecc1a8993751de4e82eb18640d631dae1f626bd6
1a0ef85f84feb13f07b604fcf5b90ef7c2b5c82f
f106af4e90eadd76cfc0b5325f659619e08fb762
097eed103862f9c6a97f2e415e21d1134017b135
935874141df839c706cd6cdc438e85eb69d1525e
0ec62d290912bb4b989be7563851bc364ec73b56
c4caa778157dbbf04116f0ac2111e389b5cd7a29
2ea1d13f64efdf49319e86c87d9ba38c30902782
570dcf2c15463842e384eb597a87c1e39bead99b
564b3bffc619dcbdd160de597b0547a7017ea010
```

```
0067bd8a55862ac9dd212bd1c4f6f5bff1ca1301
f8b7256096a20436f6d0926747e3ac3d64c81d24
8c7b49b3ecd48923eb64ff57e07a1cdb74782970
9206de95b1ea68357996ec02be5db0638a0de2c1
2c6a10161d0b5fc047b5bd81b03693b9af99fab5
05d72faa6d13c9d857478a5d35c85db9adada685
bb52d6694002b9d632bb355f64daa045c6293a4e
e77414e0aad6a1b063ba5e5750c582c75327ea6a
aa65607373a4daf2010e8c3867b6317619f3c1a3
```

Backport done by Greg Kroah-Hartman. Only minor tweaks were needed.

```
Cc: David S. Miller <davem@davemloft.net>
Cc: Hugh Dickins <hugh.dickins@tiscali.co.uk>
Cc: Paul Mundt <lethal@linux-sh.org>
Cc: Russell King <rmk+kernel@arm.linux.org.uk>
Cc: Linus Torvalds <torvalds@linux-foundation.org>
Signed-off-by: Al Viro <viro@zeniv.linux.org.uk>
Signed-off-by: Greg Kroah-Hartman <gregkh@suse.de>
```

À la simple lecture de ce rapport de changement, il est quasiment impossible d'évaluer si ceci correspond à une vulnérabilité et, si tel était le cas, quelle en serait la nature. Ainsi, comment être sûr que ce descriptif correspond bien à la vulnérabilité en question. Comme cela a déjà été précisé par le CERTA, il est indispensable pour un éditeur de publier des bulletins de sécurité clairs et précis concernant ses produits. Ceci aide le travail quotidien de veille des CSIRT comme le CERTA mais également celui des responsables sécurité soucieux du niveau de mise à jour de leur parc informatique.

3 Des petites causes pour de grandes conséquences

Parfois, des éléments paraissant anodins peuvent être à l'origine de grandes problématiques. Un exemple concret nous est parvenu ces derniers temps.

Suite à une réorganisation minimale, un service a dû changer de nom. Jusque là, rien de bien difficile et surtout rien qui ne concerne la sécurité informatique a priori. Seulement, si on se penche un peu sur les effets de bords d'un changement de nom, on s'aperçoit que le nom d'un service ou d'une entité est utilisé dans plusieurs mécanismes, notamment de sécurité :

- certains noms de domaine intègrent le nom du service ou de l'entité. Il faut alors revoir toute la configuration du système de nommage, ce qui n'est pas anodin. C'est aussi le cas pour les domaines *Active Directory* et, par extension, pour tous les systèmes utilisant le nom du service comme identification d'un noeud ;
- le nom d'un service intervient aussi fréquemment dans les infrastructures de gestion de clefs. Ainsi, le changement du nom d'un ou plusieurs services oblige à changer toute la branche de l'IGC. Ceci a un coût en termes de ressources humaines, mais aussi financier (achat éventuel des nouveaux certificats, changement des cartes à puces, etc.) ;
- d'autres effets de bords peuvent être à prévoir dans des applications métier.

4 HTML5

La version 4 de HTML datant de décembre 1997 et le « Web 2.0 » commençant déjà à dater, la presse spécialisée parle régulièrement du HTML5 comme étant l'avenir de la toile. Mais en réalité, de quoi s'agit-il ? Il s'agit d'un nouveau standard coécrit par les membres du WHATWG (*Web Hypertext Application Technology Working Group*) et du W3C *HTML Working Group*. Elle n'est pas attendue en version finie avant 2012 mais son implémentation et son utilisation ont déjà commencé.

4.1 Qu'est ce qui change ?

Si les principes restent globalement inchangés, cette nouvelle version du langage Web apporte son lot de renouvellement de balises. On voit, entre autres, apparaître les balises *audio* et *video* qui devraient simplifier l'intégration du multimédia. En effet, jusque là, pour qu'une page ait un contenu multimédia, il fallait y insérer un lecteur sous forme d'appel à un module externe avec comme paramètre le contenu désiré. L'utilisation de ces nouvelles balises est similaire à celle de *IMG*. Qu'elle soit au format PNG, JPEG ou GIF importe peu, à charge du

navigateur de l'afficher. Il en ira de même pour les balises multimédia, le navigateur devra gérer ses *codecs* afin de pouvoir jouer les contenus. Le choix de ces *codecs* est en cours de discussion. Chaque éditeur voulant mettre en avant son format, il se pose des problèmes légaux, car certains ne sont pas libres d'utilisation en fonction des pays. Ainsi, les navigateurs qui voudraient être compatibles avec le format H. 264 devront acheter une licence, au risque sinon de ne pas pouvoir afficher le contenu de certaines pages. Ce nouveau langage aura aussi la particularité de respecter, contrairement à la version 4, la double syntaxe HTML et XML.

4.2 Quand pourra-t-on l'utiliser ?

Si la version finale de ce nouveau langage n'est pas attendue avant plusieurs années, HTML5 commence déjà à être intégré et pris en compte dans les nouvelles versions des navigateurs. Cette semaine, par exemple, on peut lire dans la liste des changements apportés à *Firefox 3.6* l'ajout de l'API `File`. Sur le bloc-notes français concernant *Internet Explorer*, on trouve qu'IE 8 prend actuellement en compte la norme la plus répandue (CSS 2.1) et une partie du HTML5 et qu'IE 9 vise l'excellence sur HTML5 et CSS.

4.3 Où en est-on ?

Le standard et son implémentation dans les navigateurs évoluant en parallèle, il faut à la fois suivre l'actuelle version de travail disponible sur le site du *W3C Working Group* qui date du 25 août 2009 (cf. Documentation) et les listes de fonctionnalités et de changements apportés aux navigateurs. Il existe aussi quelques sites qui référencent les différents niveaux d'avancement de certains moteurs de rendu HTML tel que *Trident*, *Gecko* et *WebKit*. (cf. Documentation)

4.4 Et la sécurité ?

Les nouvelles fonctionnalités apportant toujours leur lot de bogues, leur utilisation doit être faite avec une certaine prudence. Un autre problème apparaît avec certaines nouvelles balises, telle que la *video* nécessitant des *codecs*. En effet, qui aura en charge de les maintenir à jour ? Pourra-t-on les désactiver facilement ?

4.5 En conclusion

La migration entre les différentes versions de langage va se faire petit à petit, les navigateurs tentant de rester le plus possible compatibles, et ne devrait pas poser de problème aux utilisateurs. Le CERTA recommande bien sur la mise à jour régulière des navigateurs mais aussi de se tenir informé des impacts, au niveau des risques et de la sécurité, des nouvelles fonctionnalités intégrées.

4.6 Documentation

- Liste des changements dans la version 3.6 de Firefox :
https://developer.mozilla.org/en/Firefox_3.6_for_developers
- Version de travail de la spécification HTML5 du 25 août 2009 :
<http://www.w3.org/TR/2009/WD-html5-20090825/>
- Site du « Web Hypertext Application Technology Working Group » :
<http://www.whatwg.org/>
- Bloc note français d'Internet Explorer :
<http://blogs.msdn.com/ie/archive/2009/11/18/an-early-look-at-ie9-for-developers.aspx>
- Comparaison des moteurs de rendu :
http://en.wikipedia.org/wiki/Comparison_of_layout_engines_%28HTML5%29
- Quelques informations sur le renouvellement des balises :
<http://fr.wikipedia.org/wiki/HTML5>

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 22 au 28 janvier 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-025 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2010-AVI-026 : Vulnérabilités des produits SAP
- CERTA-2010-AVI-027 : Multiples vulnérabilités dans HP Power Manager
- CERTA-2010-AVI-028 : Multiples vulnérabilités dans gzip
- CERTA-2010-AVI-029 : Vulnérabilité dans Cisco IOS
- CERTA-2010-AVI-030 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-031 : Vulnérabilité dans Citrix XenServer
- CERTA-2010-AVI-032 : Vulnérabilité dans Apache mod_proxy

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

- CERTA-2009-AVI-482-005 : Vulnérabilité du protocole SSL/TLS (ajout des bulletins de sécurité IBM du 22 et 27 janvier 2010)

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_rubrique62.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.

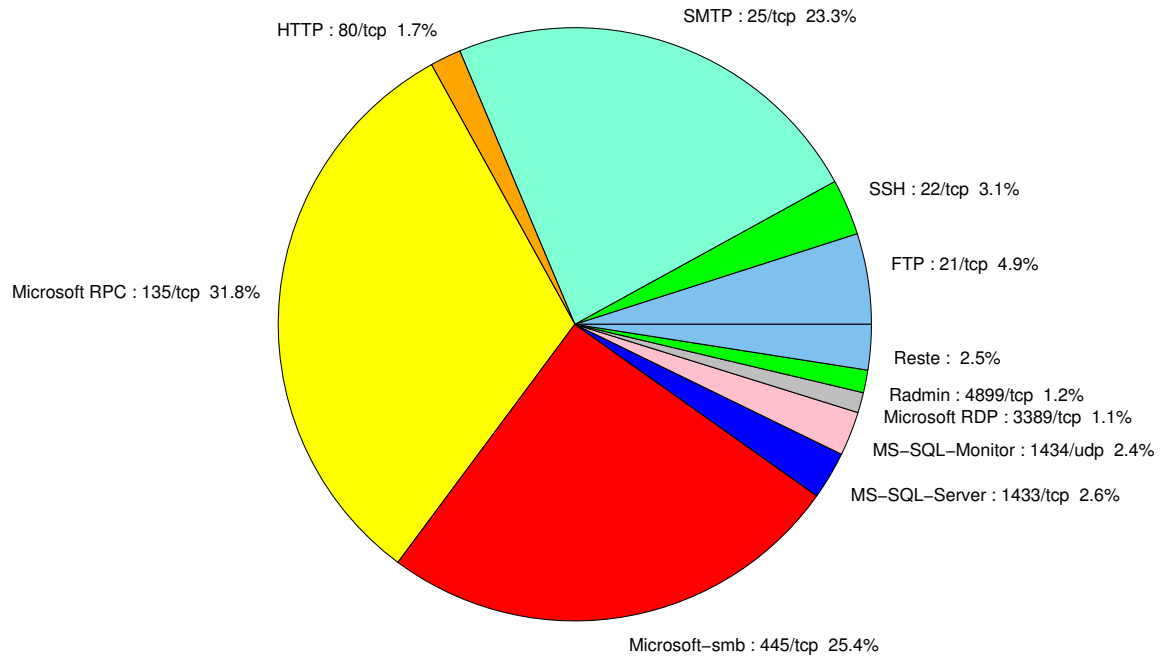


FIG. 1: Répartition relative des ports pour la semaine du 22 au 28 janvier 2010

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
135/tcp	31.79
445/tcp	25.35
25/tcp	23.34
21/tcp	4.94
22/tcp	3.05
1433/tcp	2.6
1434/udp	2.4
80/tcp	1.95
4899/tcp	1.3
3389/tcp	1.1
23/tcp	0.84
3128/tcp	0.52
3306/tcp	0.39
1080/tcp	0.26
111/tcp	0.06

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

29 janvier 2010 version initiale.