

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-20

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-020>

Gestion du document

Référence	CERTA-2010-ACT-020
Titre	Bulletin d'actualité 2010-20
Date de la première version	21 mai 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-020.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-020/>

1 Incidents de la semaine

1.1 Un réseau isolé ?

Cette semaine le CERTA a traité un incident dans lequel l'analyse portait sur un réseau d'administration déconnecté de l'Internet pour des raisons de sécurité. L'entité en charge de l'administration de ce réseau, que ce soit pour les serveurs, les clients ou bien encore les équipements réseau, a donc bâti ses procédures de maintenance sur cet état de fait.

Ainsi, les gestionnaires du SI sont partis du principe que l'infrastructure étant isolée, les menaces inhérentes à l'Internet ne s'y appliquaient pas. À leurs yeux, il n'était donc pas nécessaire, par exemple, de définir une politique de mise à jour systématique ou de mettre en place une gestion de droits d'accès pour certains utilisateurs. Ceci donne un réseau contenant des systèmes non à jour et sur lesquels les utilisateurs s'identifient uniquement avec le compte administrateur...

Clairement, les seules menaces retenues étaient la fuite d'information ou la prise de contrôle à distance. Or, après une rapide analyse, il est apparu que, régulièrement, un utilisateur particulier introduisait dans le SI un certain nombre d'éléments par le biais de supports amovibles. En l'occurrence, il s'agissait d'une clef ou un disque externe USB en fonction du volume à transférer. Cet utilisateur particulier n'était autre que l'agent chargé

de la maintenance de certains serveurs. Pour réaliser cette opération, aucune consigne ou procédure particulière ne lui avait été donnée.

Or un de ces supports a, semble-t-il, été infecté par un code malveillant utilisant un fichier *autorun.inf* sur le support mais également les ressources du réseau. Après insertion de la clef, le code s'est rapidement propagé à l'ensemble du SI entraînant un déni de service général en saturant le réseau. Malheureusement, ce réseau « isolé » servait à contrôler un certain nombre d'automates et d'éléments de contrôle d'accès. . .

Recommandations :

Quelque soit le SI, les d'interaction avec l'extérieur peuvent exister. Une imperméabilité totale est quasiment impossible. Il est donc indispensable de toujours appliquer une politique de défense en profondeur. En l'espèce, des pratiques simples ici auraient suffi à éviter le problème :

- application des mises à jour des systèmes ;
- utilisations de comptes à droits limités pour les opérations courantes ;
- désactivation du support de l'*autorun* ;
- désactivation des services inutiles sur les systèmes ;
- passage systématique à un ou plusieurs antivirus des supports amovibles avant insertion.

1.2 Maîtriser son système d'information. . .

Lors de ce même traitement d'incident, le CERTA a pu constater que le réseau utilisé pour relier les différents équipements était d'un type un peu particulier : il s'agissait d'une infrastructure de type industriel et propriétaire. Ceci n'est pas sans poser certains problèmes. Le fait d'utiliser un protocole propriétaire a empêché l'analyse des trames réseau et des éventuels problèmes liés aux éléments de communication. Il aurait fallu disposer d'outils spécifiques (matériels et logiciels) fournis uniquement par le constructeur des équipements. De plus, le fait de ne pas connaître précisément la façon dont l'information est véhiculée a été également très problématique. Ainsi, le fournisseur de la solution n'a pas pu indiquer quelle topologie était utilisée, quels protocoles étaient mis en jeu et pour quelles raisons. Ceci a été un frein à la bonne compréhension du problème.

Recommandations :

Lorsque l'on a à mettre en œuvre un système d'information, il est indispensable d'avoir une vision claire de l'infrastructure et des protocoles mis en jeu. Si toutefois, une partie de ces derniers n'étaient pas correctement documentés, il en résulterait une impossibilité de diagnostic en cas de panne.

Dans le même esprit, il est indispensable de toujours disposer d'outils de contrôle couvrant l'intégralité du SI de ses couches les plus basses jusqu'aux plus hautes. Seule une bonne maîtrise et une bonne vision globale du fonctionnement d'un système d'information permettent une réponse rapide et efficace à un problème. Dans ce contexte et de manière générale, l'utilisation de protocoles ouverts, normalisés et correctement documentés, doit être la règle.

2 Vulnérabilité dans Windows 7 64-bits et dans Windows Server 2008 R2

Une vulnérabilité a été découverte dans *Windows 7* et dans *Windows Server 2008 R2* pour les systèmes 64-bits. Plus précisément, elle affecte la bibliothèque *cdd.dll* (*Canonical Display Driver*) lorsque le thème *Windows Aero* est installé (ce qui est le cas par défaut dans *Windows 7* mais pas dans *Windows Server 2008 R2*). L'exploitation de cette vulnérabilité se fait par l'intermédiaire d'une image spécifiquement constituée et provoque un déni de service à distance (redémarrage du système). L'exécution de code arbitraire est possible, mais l'utilisation d'*ASLR* (*Address Space Layout Randomization*) rend cette opération plus difficile.

L'éditeur *Microsoft* travaille actuellement sur un correctif pour cette vulnérabilité. En l'attente de celui-ci, il est possible de se prémunir contre toute tentative d'exploitation de cette faille en désactivant le thème *Windows Aero* (voir bulletin de l'éditeur).

Documentation

- Bulletin de sécurité Microsoft #2028859 du 18 mai 2010 :
<http://www.microsoft.com/technet/security/advisory/2028859.msp>
- Référence CVE-2009-3678 :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3678>

3 Courriels malveillants ciblant les boîtes électroniques publiques

Cette semaine, un éditeur de solution de sécurité a fait état d'une campagne de courriels malveillants ciblant les boîtes aux lettres de service des ressources humaines. Ce courriel fait la demande de l'examen d'un *curriculum vitae* fourni en pièce jointe.

Cette pièce jointe, au format *zip* et contenant un exécutable, est bien évidemment malveillante, provoque une fausse alerte antivirusale et pousse la victime au téléchargement d'une fausse solution antivirusale.

Le CERTA profite de cette actualité pour rappeler à ses lecteurs que les courriels malveillants sont de mieux en mieux élaborés afin d'inciter au maximum le destinataire à ouvrir les pièces jointes ou cliquer sur un lien. De plus, cette campagne cible des adresses qui sont largement diffusées sur l'Internet car destinées à être publique par le biais de diverses offres d'emploi.

Il est donc important d'accorder une attention toute particulière aux adresses électroniques publiques et surtout à la façon dont les courriels reçus sont gérés. Il est, en effet, préférable de lire les courriers reçus sur un poste dédié et isolé afin de limiter les risques de fuite d'information et la propagation d'un code malveillant si ce poste se retrouvait compromis. Le CERTA recommande que seuls les services d'envoi et de réception de courrier soient autorisés et la gestion des pièces jointes rigoureuses surtout lors de leurs diffusions et ouvertures. Et comme toujours, l'application des correctifs du système d'exploitation et des mises à jour applicatives reste une pratique essentielle à la sécurité des systèmes d'information.

4 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/>

5 Rappel des avis émis

Dans la période du 14 au 20 mai 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-210 : Multiples vulnérabilités dans Cisco PGW Softswitch
- CERTA-2010-AVI-211 : Vulnérabilités dans le serveur HTTP d'IBM
- CERTA-2010-AVI-212 : Vulnérabilité dans HP Systems Insight Manager
- CERTA-2010-AVI-213 : Multiples vulnérabilités dans HP OpenView Network Node Manager (OV NNM)
- CERTA-2010-AVI-214 : Multiples vulnérabilités dans PostgreSQL

- CERTA-2010-AVI-215 : Vulnérabilité dans Pidgin
- CERTA-2010-AVI-216 : Multiples vulnérabilités dans Invision Power Board
- CERTA-2010-AVI-217 : Multiples vulnérabilités Java de Mac OS X
- CERTA-2010-AVI-218 : Vulnérabilités dans HP Insight Control Server Migration
- CERTA-2010-AVI-219 : Vulnérabilité dans MIT Kerberos
- CERTA-2010-AVI-220 : Multiples vulnérabilités dans HP Performance Manager
- CERTA-2010-AVI-221 : Vulnérabilité dans HP-UX
- CERTA-2010-AVI-222 : Vulnérabilité dans les produits Palo Alto Networks

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

- CERTA-2009-AVI-482-008 : Vulnérabilité du protocole SSL/TLS (ajout des bulletins de sécurité HP)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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

7 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.

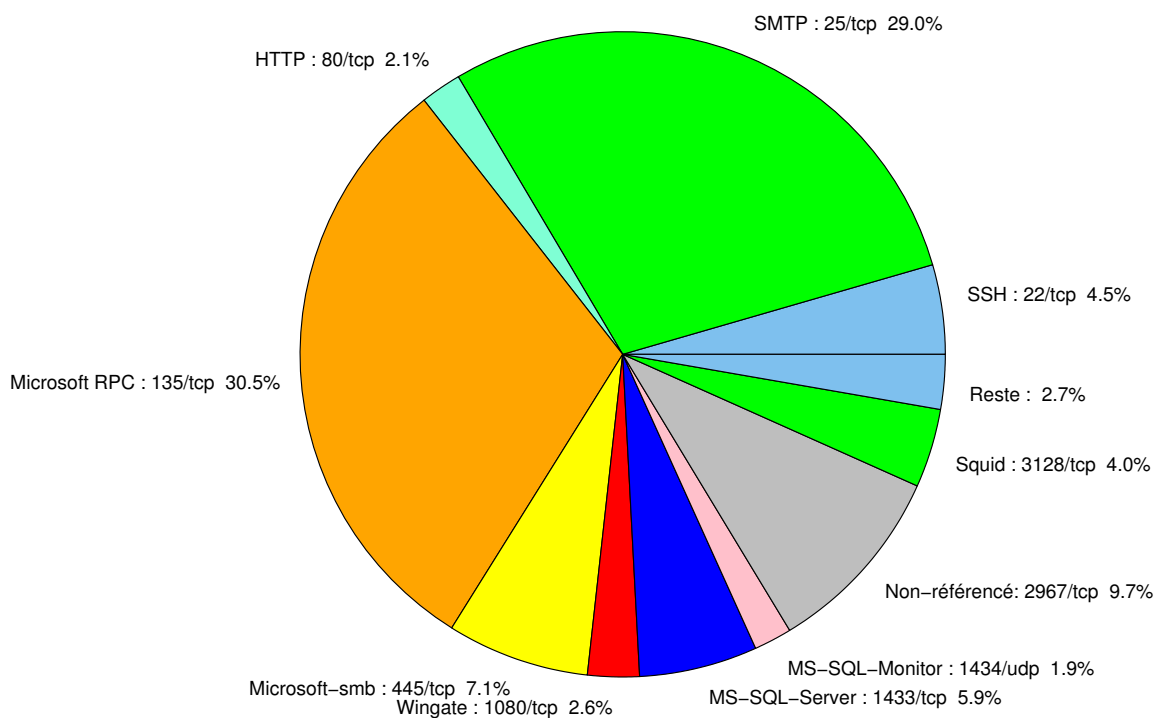


FIG. 1: Répartition relative des ports pour la semaine du 14 au 20 mai 2010

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	30.54
25/tcp	29.02
2967/tcp	9.65
445/tcp	7.14
1433/tcp	6.07
22/tcp	4.48
3128/tcp	3.95
1080/tcp	2.58
80/tcp	2.5
1434/udp	1.89
3389/tcp	0.6
4899/tcp	0.53
15118/tcp	0.3
1026/udp	0.15
42/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

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

Gestion détaillée du document

21 mai 2010 version initiale.