

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-47

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-047>

Gestion du document

Référence	CERTA-2009-ACT-047
Titre	Bulletin d'actualité 2009-47
Date de la première version	20 novembre 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-047.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-047/>

1 Incident de la semaine

Le contrat d'hébergement ralentit la résolution d'un incident

Cette semaine le CERTA a traité le cas d'un serveur de l'administration ayant subi une intrusion. Afin d'effectuer une première analyse, le CERTA a demandé à la victime les journaux d'événement de la machine. Malheureusement, la victime s'est aperçue que les clauses du contrat d'hébergement souscrit avec le prestataire ne prévoient pas la communication au client des journaux de connexion au site web en cas de problème. Le CERTA n'a donc pas été en mesure d'analyser les journaux et donc d'identifier les causes de l'intrusion, ce qui ralentit le retour à la normale.

Le CERTA rappelle qu'il est crucial de prévoir les mesures permettant la résolution des incidents informatiques dans les contrats d'hébergement. Les clauses du contrat doivent prévoir différentes situation comme :

- l'accès inconditionnel aux journaux d'événements ;
- la désignation d'une équipe technique d'intervention ;
- l'accès à la machine physique si une copie de disque doit être effectué ;
- le respect de la PSSI ...

2 Vulnérabilité dans Windows 7 et Windows Server 2008 R2

Une vulnérabilité dans Windows 7 et Windows Server 2008 R2 a été récemment rendue publique. Le CERTA a donc publié une nouvelle alerte afin d'avertir les utilisateurs de ces deux systèmes d'exploitation des risques résultant de cette faille. Il est en effet possible pour un individu malintentionné de provoquer un déni de service à distance par le biais du protocole *SMB*.

Dans l'attente d'un correctif officiel, le CERTA rappelle l'impérative nécessité de filtrer l'utilisation des ports TCP/139 et TCP/445 ou de les bloquer complètement s'ils sont inutiles. De telles mesures peuvent nuire au fonctionnement de certains services ou applications comme le partage de fichiers et d'imprimantes ou le système de fichiers *Distributed File System (DFS)*.

Le CERTA rappelle que les ports TCP/139 et TCP/445 ne doivent en aucun cas être ouverts sur l'Internet et qu'un filtrage sur les équipements périphériques du système d'information doit être mis en place.

Documentation

- Alerte du CERTA CERTA-2009-ALE-019 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-019/>
- Bulletin de sécurité Microsoft 977544 du 13 novembre 2009 :
<http://www.microsoft.com/technet/security/advisory/977544.msp>
- Référence CVE CVE-2009-3676 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3676>

3 Invitations en nombre limité et malveillance

Lors du lancement commercial d'une nouvelle application sur le Web, certains éditeurs utilisent un système d'invitations pour permettre à un groupe réduit d'utilisateurs d'accéder à leur dernière création. Outre les retours d'expérience des utilisateurs ayant été invités, ces invitations présentent, pour l'éditeur, l'avantage de créer un phénomène d'attente auprès du grand public et de créer l'événement.

Le problème étant que lorsqu'un utilisateur demande une invitation, ou se fait inviter par un autre ayant à sa disposition des invitations à distribuer, l'attente peut parfois durer plusieurs jours. Et c'est lors de cette période d'attente que l'utilisateur est particulièrement vulnérable aux attaques informatiques usurpant l'identité de l'éditeur en question.

Il existe aujourd'hui des logiciels qui font croire à l'utilisateur qu'il aura accès à une invitation, alors qu'ils installent un cheval de Troie sur le système. Il existe également des attaques de type *phishing*, l'agresseur se faisant passer pour la société émettrice de l'invitation, afin de récupérer des mots de passe de messagerie, par exemple.

Le CERTA recommande la plus grande vigilance face à ces offres d'invitation. C'est-à-dire de s'assurer que l'URL du site dont émane l'invitation correspond bien à l'éditeur officiel de l'application.

4 Routeurs grand public et identification

4.1 Les faits

La plupart des routeurs dits « grand public » sont administrables et configurables via une interface web. Celle-ci permet généralement de configurer, entre autre, les paramètres réseau des interfaces internes : *Wi-Fi* ou filaire, les fonctionnalités de redirections de port (*NAT/PAT*) ou de filtrage. Bien entendu, tous ces paramètres influent sur le niveau de sécurité proposé par le routeur. L'authentification pour accéder à l'interface d'administration de ces équipements est donc quasi systématique.

Une première recommandation, sur laquelle l'utilisateur est pleinement acteur, est de changer d'emblai le mot de passe fixé par défaut, souvent d'une bien piètre robustesse et largement documenté sur l'Internet. Pour aider dans le choix d'un bon mot de passe, il est possible de s'appuyer sur la note d'information CERTA-2005-INF-005.

Cependant, l'utilisateur peut être contraint par les limitations techniques de l'équipement. Ainsi, le CERTA a rencontré récemment un routeur sur lequel l'interface limitait grandement le jeu de caractères utilisables pour le mot de passe. En effet, on ne pouvait le construire qu'à partir de caractères alphanumériques ! Ceci est très clairement insuffisant et se justifie techniquement assez mal. La plupart des équipements de ce type sont généralement capables de supporter l'utilisation de la table *IA5* soit 256 caractères au moins dans le but d'offrir un bon rendu des pages de l'interface et ce dans plusieurs langues. On trouve normalement déjà suffisamment de caractères dans cet

ensemble pour construire des mots de passe robustes. Il est donc pour le moins incongru qu'une telle limitation existe.

4.2 Les recommandations

Autant que faire ce peut, il convient d'éviter d'utiliser des équipements présentant de telles limitations. Si toutefois cela était impossible, une solution envisageable est de rallonger la taille du mot de passe pour compenser le faible nombre de caractères disponibles. On gardera ainsi un nombre de possibilités suffisant améliorant la robustesse du mot de passe.

4.3 Documentation

- Note d'information CERTA-2005-INF-005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>

5 Wi-Fi, PDA et smartphones

Cette semaine plusieurs articles ont parlé de possibles attaques en *man in the middle* sur les téléphones communicants. Voilà l'occasion pour le CERTA de rappeler que ces appareils sont des ordinateurs à part entière, exposés aux mêmes risques techniques, et qu'il est nécessaire que leurs utilisateurs en aient conscience afin d'avoir au moins les mêmes comportements sécuritaires. En effets, la majorité des attaques décrites ne sont pas propres aux terminaux mobiles, mais elles sont simplifiées par la différence de comportement des utilisateurs de ces terminaux.

Le CERTA recommande donc aux possesseurs de terminaux mobiles la plus grande prudence. Il convient par exemple de ne pas autoriser les connexions automatiques aux points d'accès et d'appliquer les bonnes pratiques générales. La note de recommandation CERTA-2002-REC-002 sur la sécurité des réseaux sans fil peut aider à la mise en place de bonnes pratiques.

Documentation

- Note de recommandation CERTA-2002-REC-002 :
<http://www.certa.ssi.gouv.fr/site/CERTA-200-REC-002/>

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 13 au 19 novembre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-498 : Vulnérabilités dans Wordpress
- CERTA-2009-AVI-499 : Vulnérabilité dans Netgear WNDAP330
- CERTA-2009-AVI-500 : Vulnérabilité dans Google Chrome
- CERTA-2009-AVI-501 : Vulnérabilité dans IBM WebSphere
- CERTA-2009-AVI-502 : Vulnérabilité dans XOOPS
- CERTA-2009-AVI-503 : Vulnérabilité dans libexif
- CERTA-2009-AVI-504 : Vulnérabilité dans Bugzilla
- CERTA-2009-AVI-505 : Vulnérabilité dans HP Discovery & Dependency Mapping Inventory
- CERTA-2009-AVI-506 : Vulnérabilité dans HP OpenView Network Node Manager

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

- CERTA-2009-AVI-420-001 : Multiples vulnérabilités dans Samba (ajout de la référence au bulletin Sun Solaris)

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.

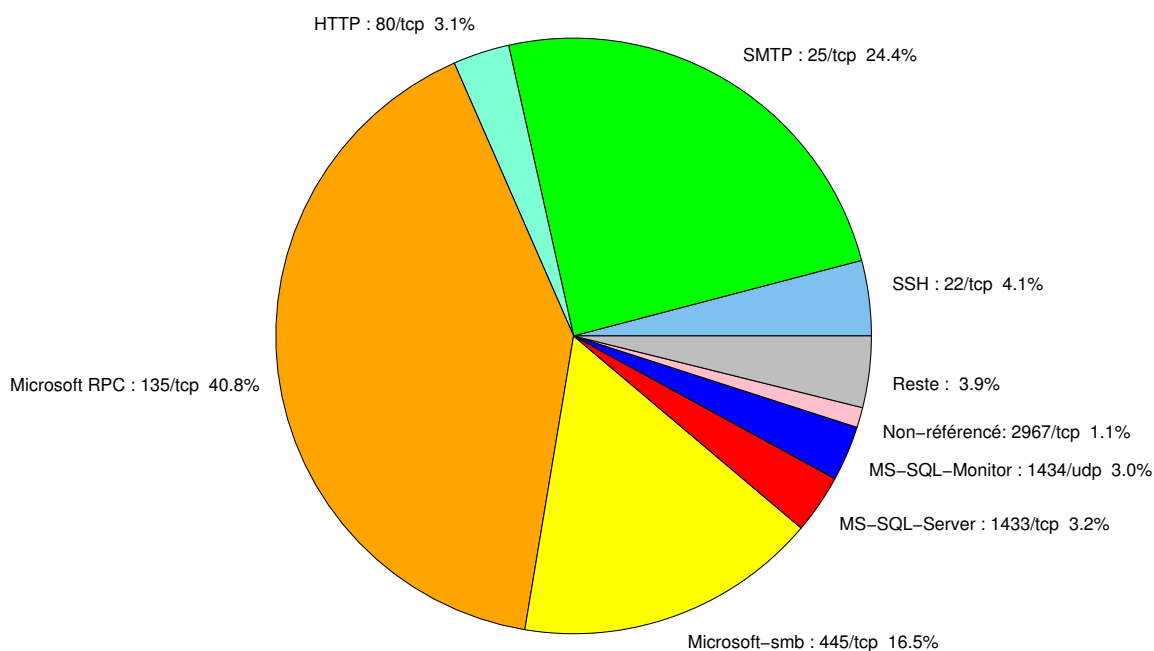


FIG. 1: Répartition relative des ports pour la semaine du 13 au 19 novembre 2009

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	40.81
25/tcp	24.42
445/tcp	16.46
80/tcp	4.89
22/tcp	4.08
1433/tcp	3.19
1434/udp	2.99
2967/tcp	1.08
137/udp	0.81
3128/tcp	0.74
21/tcp	0.61
4899/tcp	0.54
3389/tcp	0.47
1080/tcp	0.27

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

20 novembre 2009 version initiale.