

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-21

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-021>

Gestion du document

Référence	CERTA-2010-ACT-021
Titre	Bulletin d'actualité 2010-21
Date de la première version	28 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-021.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-021/>

1 Le référentiel général de sécurité (RGS) entre en application

Dans le cadre du développement de l'administration électronique, un référentiel général de sécurité a été élaboré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en liaison avec la Direction générale de la modernisation de l'État (DGME). La sécurité des procédures dématérialisées est en effet un enjeu crucial tant pour les autorités administratives elles-mêmes que pour leurs usagers, et la confiance de ces derniers est essentielle à l'essor de l'administration électronique.

L'arrêté du Premier ministre portant approbation du RGS a été publié au *Journal Officiel* le 18 mai 2010. Il fait entrer en application ce référentiel qui définit les règles de sécurité et les bonnes pratiques pour dématérialiser les procédures administratives en garantissant leur fiabilité et la sécurité des données échangées.

Le RGS s'adresse à toutes les autorités administratives (administrations de l'État, collectivités territoriales, établissements publics à caractère administratif, organismes gérant des régimes de protection sociale et autres organismes chargés de la gestion d'un service public administratif), en particulier à la maîtrise d'ouvrage (MOA), à la maîtrise d'œuvre (MOE) et aux responsables de sécurité des systèmes d'information (RSSI). Au-delà des autorités administratives, ce document intéresse également les éditeurs de services de sécurité et les prestataires de services de confiance.

Le corps du document donne des lignes directrices d'une politique de sécurité pour chaque système d'information. D'un point de vue technique, le *RGS* examine et donne les règles à suivre concernant notamment les différentes fonctions de sécurité, les politiques de certification ou encore le choix des mécanismes cryptographiques, la gestion de clés et l'authentification.

Les règles et recommandations du *RGS* devront être appliquées dans un délai de trois ans pour les téléservices et systèmes en service, dans un délai d'un an pour ceux en cours de réalisation, et d'emblée pour les téléservices et systèmes déployés après octobre 2010. Nombre de ces règles et recommandations sont d'ores et déjà mises en œuvre par des autorités administratives dans le cadre de téléservices existants.

Documentation :

- Brève et communiqué de presse de l'ANSSI :
http://www.ssi.gouv.fr/site_article228.html
- Référentiel général de sécurité : document de présentation, documents concernant l'utilisation de certificats électroniques dans les fonctions de sécurité, documents concernant l'utilisation de mécanismes cryptographiques dans les fonctions de sécurité :
<http://www.ssi.gouv.fr/rgs>
- Contacter l'ANSSI au sujet du RGS : rgs@ssi.gouv.fr

2 Qu'est ce que le tabnabbing ?

Cette semaine, un employé de la société Mozilla a publié sur son *blog* une nouvelle approche pour le filoutage accompagnée d'une preuve de faisabilité.

Cette nouvelle méthode, baptisée « *tabnabbing* », permet de profiter de la navigation par onglet de certains navigateurs afin de tromper la vigilance de l'utilisateur.

Le principe de cette attaque est le suivant :

- un utilisateur navigue sur un site malveillant via un onglet de son navigateur ;
- l'utilisateur change d'onglet afin d'aller visiter un autre site ;
- le site malveillant profite que l'utilisateur n'est pas actif sur son site ou ne visionne plus la page pour déclencher un *JavaScript* et complètement refondre l'aspect visuel de la page qui était visitée ;
- cette modification se fait afin de tromper l'utilisateur et usurper l'apparence d'un site filouté (webmail, site bancaire, de commerce en ligne, réseau sociaux, ...) ;
- l'utilisateur peu attentif, revenant sur l'onglet malveillant précédemment ouvert, peut ainsi être trompé et penser que sa session a expiré ou qu'il a oublié de se connecter au site filouté ;
- il ne reste plus à l'attaquant qu'à intercepter les données saisies par la victime, les enregistrer et éventuellement rediriger le malheureux visiteur vers le véritable site.

Même si l'approche est tout à fait originale pour une attaque de type *phishing*, le CERTA rappelle quelques principes de base et vérification à effectuer afin de ne pas être victime de ce genre d'escroquerie :

- toujours désactiver par défaut l'interprétation des codes dynamiques (*JavaScript*, *Flash*, *ActiveX*, ...) sur des sites qui ne sont pas de confiance ;
- s'assurer que l'adresse *URL* affichée correspond bien à celle du site légitime ;
- toujours utiliser les versions sécurisées des sites Internet nécessitant une authentification ou la saisie de données personnelles et vérifier la cohérence du certificat présenté avec l'identité du site ;
- toujours utiliser un système d'exploitation, un navigateur et des modules ou extensions parfaitement à jour et un compte utilisateur aux droits limités.

3 Domotique et SSI

Cette semaine, un avis de sécurité sur un produit un peu particulier a été publié sur le site du CERTA : l'avis CERTA-2010-AVI-229 intitulé « *Multiplés vulnérabilités dans Cisco Network Building Mediator* ».

Le *Cisco Network Building Mediator* est une solution complète de domotique sur IP, permettant un contrôle via le réseau des fonctions de gestion du chauffage, de la climatisation, du contrôle d'accès, de l'éclairage... des bâtiments. Le taux de pénétration de ces solutions est en forte croissance, car les promesses sont très

intéressantes : meilleure gestion des bâtiments, pilotage centralisé, maintenance facilitée. Malheureusement, la sécurité de ces produits doit être parfaitement vérifiée, car il s'agit d'un point critique non seulement pour le bon fonctionnement, mais aussi pour la sécurité même des personnes.

L'avis de sécurité publié cette semaine est à ce titre particulièrement critique, car ce produit souffre de multiples vulnérabilités qui pourraient permettre à un attaquant une prise de contrôle totale, à distance, de ces systèmes. Il ne faut pas oublier que même si les fonctions informatiques sont enfouies ou peu visibles, comme c'est le cas dans des solutions de type informatique industrielle ou domotique, la protection contre les attaques ne doit en aucun cas être oubliée. La société Cisco a publié un avis de sécurité, il est donc indispensable d'appliquer au plus tôt le correctif adapté. D'une façon générale et quelle que soit la marque des produits utilisés, il ne faut pas les omettre dans votre politique de sécurité, et bien surveiller la bonne mise à jour et l'application des correctifs de sécurité de ces solutions.

Documentation

- Avis CERTA-2010-AVI-229 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-229/>

4 Migration vers OpenBSD 4.7

La dernière version (4.7) du système d'exploitation OpenBSD a été publiée le 19 mai 2010. Cette version apporte son lot de nouveautés parmi lesquelles on trouve une modification dans le pare-feu intégré : *Packet Filter*. En effet, la syntaxe dans le fichier de configuration *pf.conf* nécessaire aux règles de translation d'adresse ou NAT a totalement changé. Ainsi les directives : *nat*, *rdp*, et *binat* ont toutes été remplacées par une seule et nouvelle directive : *match*.

Vous pourrez trouver les exemples et les explications de sur la nouvelle syntaxe à la page : <http://openbsd.org/faq/upgrade47.html>.

Recommandations :

Si vous avez à mettre en œuvre des règles de NAT avec OpenBSD, il est indispensable de se reporter à cette documentation afin d'adapter les fichiers de configuration pour la nouvelle version. D'une manière générale, lors d'une migration quelle qu'elle soit, il est indispensable de se reporter à la documentation du produit afin d'éviter tout désagrément lié à ce genre de changements.

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 21 au 27 mai 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-223 : Multiples vulnérabilités dans MySQL
- CERTA-2010-AVI-224 : Vulnérabilité dans IBM AIX
- CERTA-2010-AVI-225 : Vulnérabilités dans IBM WebSphere Application Server
- CERTA-2010-AVI-226 : Vulnérabilité dans Foxit Reader
- CERTA-2010-AVI-227 : Vulnérabilité dans ClamAV
- CERTA-2010-AVI-228 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-229 : Multiples vulnérabilités dans Cisco Network Building Mediator
- CERTA-2010-AVI-230 : Vulnérabilité dans Adobe Photoshop

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

- CERTA-2010-AVI-214-001 : Multiples vulnérabilités dans PostgreSQL (ajout du bulletin de sécurité Debian)
- CERTA-2010-AVI-219-001 : Vulnérabilité dans MIT Kerberos (ajout du bulletin de sécurité Debian)

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 inexpliqués 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.

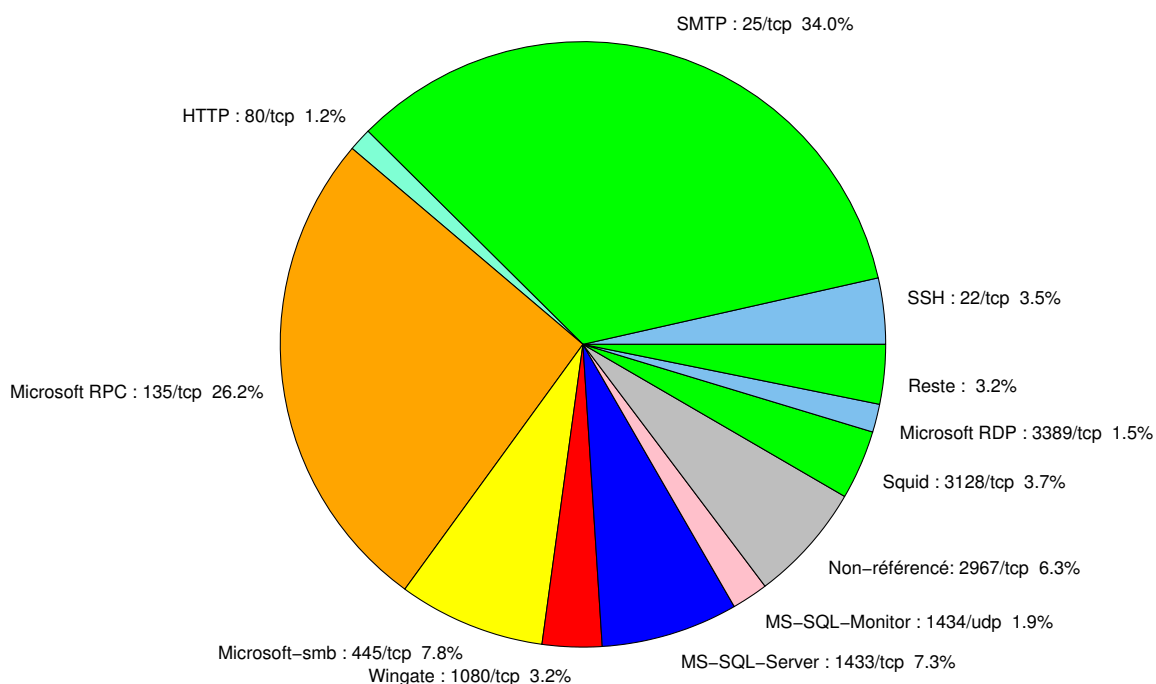


FIG. 1: Répartition relative des ports pour la semaine du 21 au 27 mai 2010

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
25/tcp	34.03
135/tcp	26.27
445/tcp	7.84
1433/tcp	7.31
2967/tcp	6.34
3128/tcp	3.7
22/tcp	3.52
1080/tcp	3.17
80/tcp	2.2
1434/udp	1.94
3389/tcp	1.49
21/tcp	0.97
4899/tcp	0.88
3127/tcp	0.79
111/tcp	0.26
3306/tcp	0.17
1026/udp	0.08

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

28 mai 2010 version initiale.