



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 06 août 2010
N° CERTA-2010-ACT-031

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-31

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-031>

Gestion du document

Référence	CERTA-2010-ACT-031
Titre	Bulletin d'actualité 2010-31
Date de la première version	06 août 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-031.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-031/>

1 Correction de la vulnérabilité du shell de Microsoft Windows

Cette semaine, Microsoft a publié une mise à jour corrigeant la vulnérabilité du *shell* Windows. Cette faille dans la gestion des fichiers de raccourcis .lnk permet l'exécution de code arbitraire à distance. Elle est activement exploitée, notamment par le code malveillant dénommé *Stuxnet*.

L'application du correctif dès que possible est fortement recommandée. Pour rappel, les systèmes Windows 2000 et Windows XP Service Pack 2 ne sont plus supportés par Microsoft. Ils seront donc toujours vulnérables à cette faille et il est nécessaire de migrer vers une version plus récente du système d'exploitation.

Documentation

- Avis CERTA-2010-AVI-353 du 03 août 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-353>
- Alerte CERTA-2010-ALE-009 du 03 août 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-009>

2 Alerte concernant l'Apple iOS

Cette semaine le CERTA a publié l'alerte CERTA-2010-ALE-011 concernant l'Apple iOS, le système d'exploitation des *iPhones*, *iPad* et *iPod*.

Elle traite de deux vulnérabilités, l'une permettant l'exécution de code arbitraire à distance et l'autre une élévation de privilèges. Elles sont actuellement utilisables en ligne pour débloquer (*jailbreaker*) les différents appareils concernés. Cette action demande une validation de l'utilisateur mais pourrait être automatisée et utilisée à des fins malveillantes. La portée de cette action est d'ailleurs mal connue. Il est certain que des logiciels sont installés, au moins *cydia* (gestionnaire de paquets alternatifs à *AppStore*), et que pour cela des droits élevés sont obtenus. Il n'y a aucune garantie que cela ne fasse pas autre chose. De plus, l'utilisateur ayant accès au compte administrateur, le modèle de sécurité est cassé, or ce modèle est là pour protéger l'utilisateur contre des attaques, mais aussi contre lui même et les erreurs de manipulations. L'un des objectifs du « *jailbreak* » est de pouvoir installer des applications quelconques.

Pour ce qui est des attaques exploitant les vulnérabilités de l'alerte, le CERTA recommande la plus grande prudence avec les fichiers *PDF*, que cela soit par courriel, en naviguant voire par *MMS*.

Pour ce qui est du déblocage des appareils, d'un point de vue de la sécurité des systèmes d'information, le CERTA recommandant de ne pas installer des applications d'origine peu contrôlée et au suivi aléatoire, mais également de ne pas briser les modèles de sécurité, il est conseillé, bien sûr, de ne pas le faire.

Pour les directeurs et responsables de la sécurité des services d'information, le CERTA recommande la plus grande vigilance quant à l'usage des ces appareils dans leur SI. Il est essentiel de communiquer et sensibiliser sur l'importance de ne pas traiter d'informations sensibles dessus, et s'il s'agit d'appareil professionnels, d'être clair sur les limites d'utilisation .

Documentation

- Alerte CERTA-2010-ALE-011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-011/>

3 Vulnérabilité non corrigée dans les produits Adobe

Cette semaine, Adobe a confirmé la présence d'une vulnérabilité non corrigée dans Adobe Reader et Adobe Acrobat. Cette faille, révélée lors du conférence de sécurité informatique, réside dans l'interprétation de police de caractère au sein d'un fichier au format *PDF* spécialement conçu.

Le CERTA a donc publié une alerte afin d'avertir ses lecteurs et recommande l'utilisation d'un logiciel alternatif dans l'attente du correctif annoncé pour le 16 août 2010.

Documentation

- Alerte CERTA-2010-ALE-012 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-012/>
- Bulletin de sécurité Adobe APSB10-17 du 05 août 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-17.html>

4 La sécurité des applications utilisant VxWorks mise à mal

Un problème de sécurité important touche le répandu système d'exploitation temps-réel *VxWorks*.

Ce système d'exploitation spécialisé pour faire fonctionner les systèmes embarqués est très utilisé, notamment dans un grand nombre de projets de défense et à destination du grand public : aérospatiale, transport aérien civil et militaire, armes de guerre, équipements informatiques (routeurs, box Internet, ...), télécommunication, automobile...

De par sa nature c'est un système d'exploitation destiné à fonctionner sur des architectures différentes des ordinateurs personnels (*MIPS*, *SH-4*, ...), ce qui implique que les développeurs travaillant sur cette plate-forme utilisent un compilateur croisé couplé à un émulateur de l'architecture cible, au moins dans les premières étapes du développement. Aussi, pour pouvoir déboguer plus facilement l'application une fois installée sur l'architecture cible, *VxWorks* fournit un service de débogage accessible à distance écoutant sur le port UDP/17185. Ce

service permet d'effectuer plusieurs actions sur le système embarqué, notamment la lecture et l'écriture de la mémoire physique.

Le problème réside dans le fait que beaucoup d'intégrateurs n'ont pas désactivé ce service de débogage lors de la mise en production de leur système. Il apparaît que beaucoup de ces systèmes sont stratégiques et sont connectés à Internet. À noter que ce service utilise le protocole *ONC RPC* (plus connu sous le nom de *SunRPC*) qui est un *RPC* léger n'ayant de toute façon pas vocation à être déployé sur des *WAN*, contrairement à *CORBA* ou *SOAP* par exemple.

La conséquence de ce défaut de configuration est importante. Un attaquant peut se connecter sur ce service en *UDP/17185* et lire la mémoire physique afin, par exemple, d'y chercher les mots de passe des utilisateurs. Pour contrer cette dernière attaque, *VxWorks* avait développé son propre algorithme de *hachage* pour stocker les mots de passe en mémoire, le problème étant que cet algorithme est cassable facilement, ce qui n'est pas très étonnant car il n'avait pas été testé publiquement. On ne dira jamais assez qu'en matière de cryptographie la sécurité par l'obscurité ne fonctionne pas.

Il existe donc à l'heure actuelle des outils permettant de casser les mots de passe *VxWorks* à distance sur les systèmes embarqués ayant laissé actif le service de débogage en écoute sur Internet. Et ils sont nombreux.

La solution à ce problème, c'est-à-dire de désactiver le service de débogage, est complexe à mettre en oeuvre parce qu'elle nécessite une mise à jour du système, et donc un accès direct au matériel. Par conséquent, il sera malheureusement difficile de corriger ce défaut sur tous les systèmes utilisant *VxWorks*, et le risque de trouver des systèmes encore vulnérables dans plusieurs années est important.

Dans tous les cas, si vous avez la responsabilité de systèmes utilisant *VxWorks*, il vous faut au plus vite tester si le service de débogage sur *UDP/17185* est activé. Si tel est le cas, il vous faut contacter le fournisseur de votre système au plus vite pour obtenir une mise à jour désactivant ce service.

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 30 juillet au 05 août 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-345 : Vulnérabilité dans la bibliothèque *libmsspack*

- CERTA-2010-AVI-346 : Vulnérabilités dans MediaWiki
- CERTA-2010-AVI-347 : Multiples vulnérabilités dans TYPO3
- CERTA-2010-AVI-348 : Multiples vulnérabilités dans Wireshark
- CERTA-2010-AVI-349 : Vulnérabilité dans Akamai Download Manager
- CERTA-2010-AVI-350 : Vulnérabilité dans EMC Disk Library
- CERTA-2010-AVI-351 : Vulnérabilité dans SPIP
- CERTA-2010-AVI-352 : Vulnérabilités dans Novell iPrint Client
- CERTA-2010-AVI-353 : Vulnérabilité dans le Shell de Microsoft Windows
- CERTA-2010-AVI-354 : Vulnérabilités dans JBoss Enterprise SOA
- CERTA-2010-AVI-355 : Vulnérabilité dans Linux CIFS

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

- CERTA-2010-AVI-264-002 : Multiples vulnérabilités dans Apache (ajout de la référence au bulletin de sécurité IBM)

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_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.

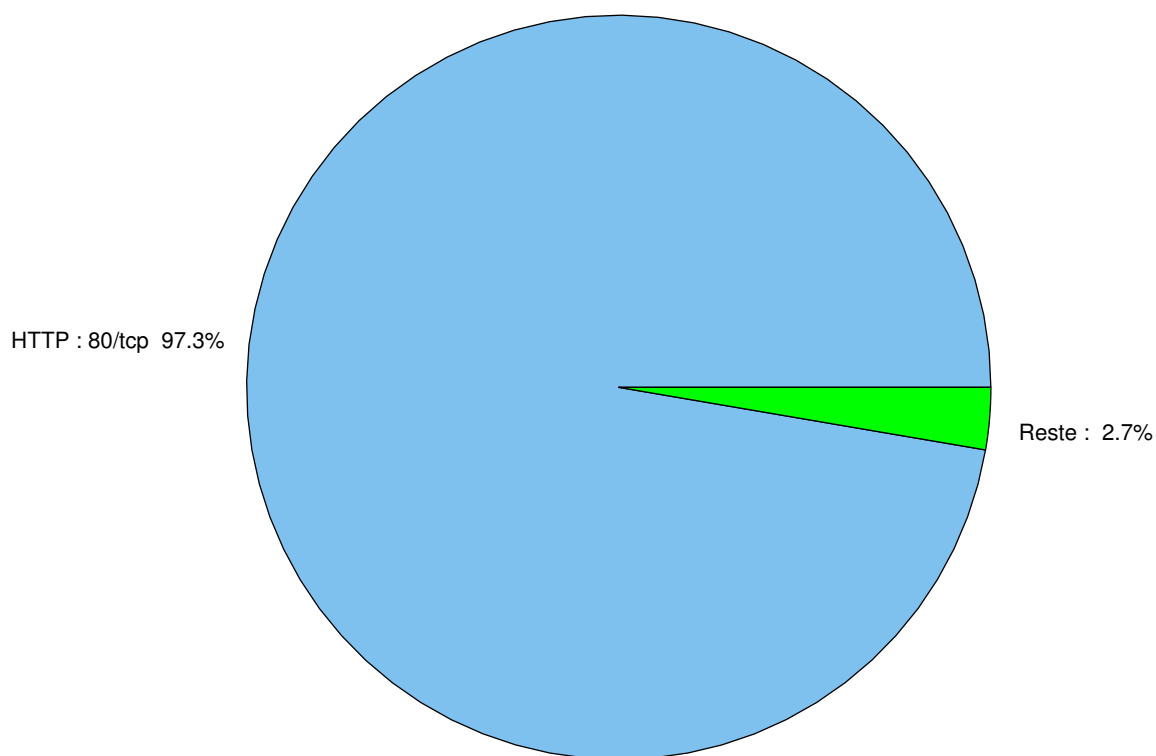


FIG. 1: Répartition relative des ports pour la semaine du 30 juillet au 05 août 2010

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
80/tcp	97.33
25/tcp	0.88
445/tcp	0.51
23/tcp	0.3
1080/tcp	0.2
1433/tcp	0.19
135/tcp	0.17
22/tcp	0.14
2967/tcp	0.09
3389/tcp	0.06
1434/udp	0.04
3128/tcp	0.02
21/tcp	0.01

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

06 août 2010 version initiale.