Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 septembre 2009
N° CERTA-2009-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-36

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-036

Gestion du document

Référence	CERTA-2009-ACT-036
Titre	Bulletin d'actualité 2009-36
Date de la première version	04 septembre 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-036.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-036/

1 Vulnérabilité dans le service FTP de IIS

Cette semaine le CERTA a publié l'alerte CERTA-2009-ALE-015 relative à une vulnérabilité non corrigée dans le service `FTP` de `Microsoft Internet Information Services` (`IIS`). Cette faille entraîne différentes conséquences selon les versions :

- une exécution de code arbitraire à distance est possible sur la version `IIS 5.0` ;
- un déni de service à distance est possible pour les versions `IIS 5.1`, `6.0` et `7.0`.

Cette vulnérabilité nécessite, pour son exploitation, un compte utilisateur avec les droits en écriture et la possibilité de créer un répertoire sur le serveur cible. Afin de limiter les risques afférents à cette vulnérabilité, le CERTA recommande les actions suivantes :

- désactiver le support de l'écriture de fichiers dans la configuration du serveur `FTP` de `Microsoft IIS` pour les utilisateurs non identifiés (compte *anonymous*) ;
- supprimer la permission *NTFS* de créer des répertoires pour les utilisateurs du service `FTP` ;
- restreindre l'accès du serveur `FTP` aux seules personnes de confiance ;
- désactiver le service `FTP` si ce dernier n'est pas nécessaire.

Documentation

- Alerte CERTA CERTA-2009-ALE-015 du 02 septembre 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-015
- Bulletin de sécurité Microsoft 975191 du 01 septembre 2009 :
  http://www.microsoft.com/technet/security/advisory/975191.mspx

2 Incidents de la semaine

Attaques par dictionnaire sur POP3

Cette semaine, plusieurs correspondants nous ont informés, après avoir dépouillé leurs journaux de connexion, d'attaques par dictionnaire sur leurs serveurs `POP3` (port `110/tcp`). Le rythme d'une des attaques était relativement lent, avec une tentative environ toutes les 9 secondes. Les autres essais, provenant tous de la même source, avaient une cadence plus soutenue, comparable à celle des attaques visant les serveurs `SSH`.

Le CERTA recommande donc aux administrateurs de vérifier dans leurs journaux les tentatives d'accès au service `POP3`, et de s'assurer que les mots de passe utilisés ne sont pas triviaux. En période de rentrée scolaire, de nombreux comptes de messagerie sont souvent créés. Il est conseillé d'éviter les mots de passe prévisibles, notamment ceux basés sur le nom du compte. Il est également possible de mettre en place des mécanismes automatiques de mise en quarantaine et ou d'interdiction définitive de connexion lorsqu'une adresse fait trop de tentatives de connexion infructueuses dans un délai préalablement défini.

3 Attaque du chiffrement TKIP

En 2008, lors d'une célèbre conférence de sécurité, deux chercheurs allemands, *Martin Beck* et *Eric Tews*, ont démontré des faiblesses sur le chiffrement *TKIP* utilisé pour assurer la sécurité dans les réseaux sans fil *WiFi 802.11*. L'attaque décrite permettait d'envoyer des paquets légitimes à une station *WiFi*, pour peu que certaines conditions soient présentes (notamment le support de la *QoS 802.11e*, et un temps d'une quinzaine de minutes nécessaires pour obtenir les éléments permettant l'attaque). L'attaque avait beaucoup fait parler d'elle, car bien que non critique (*TKIP* n'étant pas à proprement parlé « cassé »), elle ouvrait cependant la porte à une attaque réelle sur ces mécanismes de sécurité.

Début août 2009, deux chercheurs japonais, *Toshihiro Ohigashi* et *Masakatu Morii* ont publié un nouveau document améliorant l'attaque de *Beck* et *Tews*. Ils expliquent comment reproduire la même attaque, mais avec des conditions nécessaires plus simples (*QoS* non active, durée de la phase de préparation de l'attaque plus courte, de l'ordre d'une minute). Encore une fois, la réalisation de l'attaque présente encore une complexité forte, et ne « casse » pas totalement *TKIP*. Cependant, ce type de publication démontre que la sécurité de *TKIP* s'effrite peu à peu. Le CERTA recommande, si l'utilisation du *WiFi* est indispensable, de migrer rapidement vers les nouvelles solutions de sécurité intégré dans la norme *802.11i*, notamment l'utilisation de *CCMP* comme méthode de sécurité.

Documentation

- Recommandation CERTA CERTA-2002-REC-002 Sécurité des réseaux sans fil (Wi-Fi) :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002
- Bulletin d'actualité du CERTA CERTA-2008-ACT-045 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045
- Bulletin d'actualité du CERTA CERTA-2008-ACT-047 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047

4 Mise à jour et régression

Cette semaine `Apple` a publié la dernière version de son système d'exploitation : `Mac OS X version 10.6` aussi appelée *Snow Leopard*. Cette sortie implique donc que la version 10.4 ou *Tiger* ne sera bientôt plus maintenue. Il faudra donc envisager une mise à jour des machines sous ce système d'exploitation vers une version plus récente : 10.5 ou 10.6.

En outre, il a été découvert cette semaine, suite à cette sortie, que le système était livré en standard avec une version vulnérable du logiciel `Adobe Flash Player`. En effet, la version du lecteur `Flash` présente sur les supports d'installation est la 10.0.23.1 alors que la version à jour à la date de cet article est la 10.0.32.18.

Il est donc indispensable après une installation de `Mac OS X 10.6`, et ce dans les plus brefs délais, de mettre à jour le lecteur, cette version obsolète présentant un risque d'attaque certain. Plus généralement, avant tout usage d'un système d'exploitation, il est impératif de le mettre à jour ainsi que les logiciels qui y sont installés.

5 Publications de vulnérabilités non corrigées

Certaines sociétés sur l'Internet commercialisent des vulnérabilités de type *0-day* ainsi que les méthodes d'-exploitation. Cette constatation démontre, s'il en était en besoin, qu'il n'existe pas de solution ou de système d'information sûr à 100%. Le CERTA rappelle donc que, même si un système est complètement à jour, il est important d'y appliquer quelques bonnes pratiques :

- appliquer les principes de défense en profondeur et multiplier les couches de protection, de filtrage et journalisation ;
- journaliser au maximum les événements ;
- consulter régulièrement les journaux afin d'y détecter toute activité anormale ou suspecte ;
- former et sensibiliser les utilisateurs ;

Ces recommandations sont rappelées chaque semaine dans la partie « statique » du bulletin d'actualité au format *PDF* du CERTA (voir les sections suivantes). De plus, le CERTA met à disposition sur son site Internet de nombreuses notes d'information permettant d'obtenir des recommandations sur différents sujets.

Documentation

- Les notes d'information du CERTA :
  http://www.certa.ssi.gouv.fr/site/index_inf.html

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=1936
- 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 28 août au 03 septembre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-359 : Vulnérabilité dans Norton AntiVirus et Symantec Client Security Email
- CERTA-2009-AVI-360 : Multiples vulnérabilités dans Opera
- CERTA-2009-AVI-361 : Vulnérabilité dans Dnsmasq
- CERTA-2009-AVI-362 : Vulnérabilités dans OpenOfficeorg
- CERTA-2009-ALE-015 : Vulnérabilité du serveur FTP de Microsoft IIS
- CERTA-2009-AVI-363 : Vulnérabilité de wget
- CERTA-2009-AVI-364 : Vulnérabilité dans Qt
- CERTA-2009-AVI-365 : Vulnérabilités dans IBM Java

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 règlementaire, 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 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.

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.

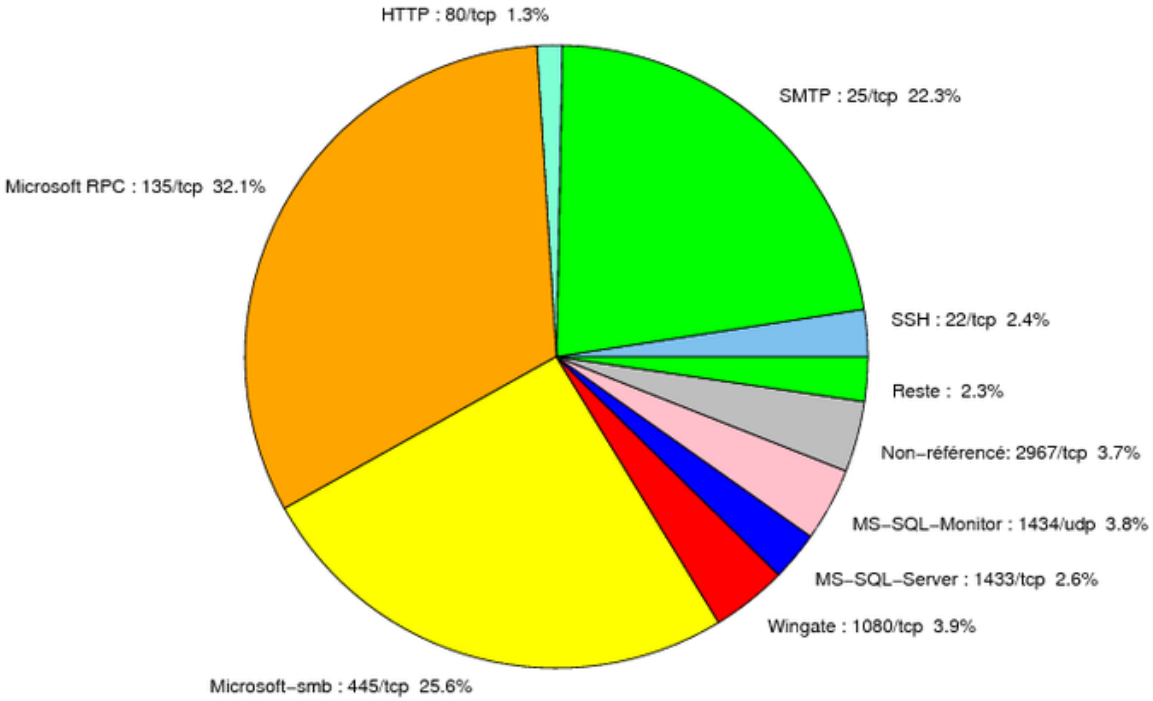

FIG. 1: Répartition relative des ports pour la semaine du 28 août au 04 septembre 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	32.1
445/tcp	25.62
25/tcp	22.25
1080/tcp	3.92
1434/udp	3.8
2967/tcp	3.67
1433/tcp	2.55
22/tcp	2.43
80/tcp	1.37
21/tcp	0.56
3128/tcp	0.43
4899/tcp	0.37
23/tcp	0.31
9898/tcp	0.06

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

04 septembre 2009 version initiale.