Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 août 2010
N° CERTA-2010-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-32

Gestion du document

Référence	CERTA-2010-ACT-032
Titre	Bulletin d'actualité 2010-32
Date de la première version	13 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-032.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-032/

1 Mise à jour de sécurité mensuelle de Microsoft

Microsoft a publié 14 bulletins de sécurité pour le mois d'août 2010. Ces mises à jour de sécurité couvrent toutes les versions de Windows et corrigent des vulnérabilités dont les plus critiques permettant d'exécuter du code arbitraire à distance sans action de l'utilisateur ou encore d'élever ses privilèges.

Parmi les vulnérabilités corrigées, on peut citer les avis CERTA-2010-AVI-363 et CERTA-2010-AVI-364 qui portent sur des vulnérabilités dans le noyau ou des pilotes en mode noyau qui peuvent être exploitées afin de réaliser une élevation de privilèges.

Les avis CERTA-2010-AVI-367 et CERTA-2010-AVI-369 couvrent des vulnérabilités présentes dans Internet Explorer ou exploitable via le navigateur. Ainsi, une personne malveillante peut exécuter du code arbitraire à distance, notamment au moyen d'un fichier au format HTML spécialement construit.

L'avis CERTA-2010-AVI-370 sera le dernier cité dans cet article. Il porte sur une vulnérabilité dans le serveur SMB de Windows qui permet à un utilisateur distant non-authentifié d'exécuter du code arbitraire. Cette vulnérabilité rappelle celle décrite dans le bulletin de sécurité *Microsoft* MS08-067 du 11 novembre 2008 largement exploitée par le code malveillant Conficker.

L'application de ces correctifs est donc impérative pour élever le niveau de sécurité des systèmes d'information fonctionnant sous Windows.

2 «Patch tuesday», Adobe également

Si le mardi 11 août 2010 était attendu pour les correctifs *Microsoft*, il était également l'occasion pour l'éditeur *Adobe* de publier des correctifs de sécurité, repris dans trois avis du CERTA (voir documentation).

Le CERTA attire l'attention sur deux points :

- la vulnérabilité CVE-2010-2862 affectant Adobe Reader et Acrobat, liée aux police de caractères, et traitée dans l'alerte CERTA-2010-ALE-012, n'est toujours pas corrigée à l'heure de la rédaction de cet article ;
- concernant Flash Media Player, tous les greffons des différents navigateurs utilisés sur l'ordinateur doivent être mis à jour, manuellement si besoin.

2.1 Documentation

- Avis du CERTA CERTA-2010-AVI-377, Vulnérabilités dans Adobe AIR et Flash Player, du 11 août 2010 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-377/
- Avis du CERTA CERTA-2010-AVI-378, Vulnérabilité dans ColdFusion, du 11 août 2010 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-378/
- Avis du CERTA CERTA-2010-AVI-379, Vulnérabilités dans Adobe Flash Media Server, du 11 août 2010 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-379/
- Alerte du CERTA CERTA-2010-ALE-012, Vulnérabilité dans Adobe Reader et Adobe Acrobat, du 06 août 2010 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-012/

3 Mise à jour de sécurité importante pour l'Apple iOS

Dans le bulletin d'actualité de la semaine dernière, nous avions mentionné des deux failles de sécurité activement utilisées pour réaliser le *Jailbreak* de l'Apple iOS à distance, l'une permettant de s'introduire dans le système par le biais d'un document au format PDF spécialement construit et l'autre permettant d'élever ses privilèges. Comme nous l'avions écrit, ces vulnérabilités sont critiques et pourraient être exploitées par des codes malveillants (voir l'alerte CERTA-2010-ALE-011).

Apple a corrigé cette semaine ces deux vulnérabilités, l'avis du CERTA correspondant est référencé CERTA-2010-AVI-380. Le CERTA recommande vivement de mettre à jour les appareils fonctionant sous iOS. Cette mise à jour est manuelle, et peut être faite par le biais d'un ordinateur équipé du logiciel iTunes.

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 06 août 2010 au 12 août 2010, le CERTA a émis les avis suivants :

– CERTA-2010-AVI-356 : Vulnérabilités dans IBM Tivoli Directory Server
– CERTA-2010-AVI-357 : Multiples vulnérabilités dans Cisco Firewall Services Module
– CERTA-2010-AVI-358 : Vulnérabilités dans les produits Cisco ASA
– CERTA-2010-AVI-359 : Multiples vulnérabilités dans FreeType
– CERTA-2010-AVI-360 : Vulnérabilité dans Foxit Reader
– CERTA-2010-AVI-361 : Vulnérabilité dans wget
– CERTA-2010-AVI-362 : Vulnérabilités dans Bugzilla
– CERTA-2010-AVI-363 : Vulnérabilités dans le noyau Windows
– CERTA-2010-AVI-364 : Vulnérabilités de pilotes en mode noyau de Windows
– CERTA-2010-AVI-365 : Vulnérabilités dans SSL/TLS et Secure Channel de Windows
– CERTA-2010-AVI-366 : Vulnérabilité dans Windows Movie Maker
– CERTA-2010-AVI-367 : Vulnérabilité dans Microsoft XML Core Services
– CERTA-2010-AVI-368 : Vulnérabilité du Codec MicrosoftMPEG Layer-3
– CERTA-2010-AVI-369 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTA-2010-AVI-370 : Multiples vulnérabilités dans le seveur SMB de Microsoft Windows
– CERTA-2010-AVI-371 : Vulnérabilité dans Microsoft Cinepak Codec
– CERTA-2010-AVI-372 : Multiples vulnérabilités dans Microsoft Office Word
– CERTA-2010-AVI-373 : Vulnérabilité dans Microsoft Excel
– CERTA-2010-AVI-374 : Vulnérabilités dans la pile TCP/IP de Microsoft Windows
– CERTA-2010-AVI-375 : Vulnérabilités dans la fonctionnalité de suivi de services sous Microsoft Windows
– CERTA-2010-AVI-376 : Vulnérabilités dans Microsoft NET Common Language Runtime et Microsoft Silverlight
– CERTA-2010-AVI-377 : Vulnérabilités dans Adobe AIR et Flash Player
– CERTA-2010-AVI-378 : Vulnérabilité dans ColdFusion
– CERTA-2010-AVI-379 : Vulnérabilités dans Adobe Flash Media Server
– CERTA-2010-AVI-380 : Multiples vulnérabilités dans Apple iOS

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

– CERTA-2009-AVI-482-010 : Vulnérabilité du protocole SSL/TLS (ajout du bulletin de sécurité Microsoft)
– CERTA-2010-AVI-325-002 : Multiples vulnérabilités dans OpenLDAP (ajout des références aux bulletins de sécurité SuSE, Ubuntu et Debian)

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 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.

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 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.

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.

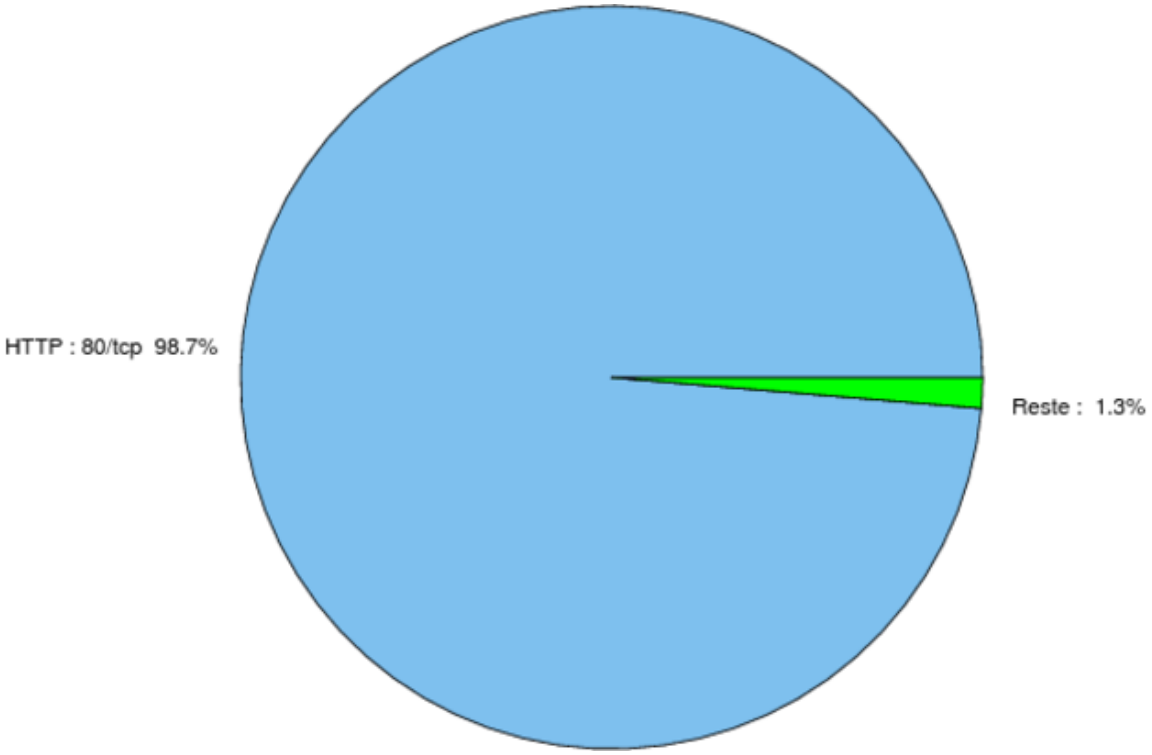

FIG. 1: Répartition relative des ports pour la semaine du 06 juillet au 12 août 2010

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
80/tcp	98.68
25/tcp	0.62
1080/tcp	0.14
445/tcp	0.11
22/tcp	0.1
135/tcp	0.09
1433/tcp	0.07
23/tcp	0.06
1434/udp	0.03
3128/tcp	0.02
3389/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

13 août 2010 version initiale.