Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 avril 2010
N° CERTA-2010-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-15

Gestion du document

Référence	CERTA-2010-ACT-015
Titre	Bulletin d'actualité 2010-15
Date de la première version	16 avril 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-015.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-015/

1 Bulletins Microsoft du mois d'avril

Cette semaine, Microsoft a publié son lot de correctifs de sécurité pour le mois d'avril dans le cadre de son cycle mensuel.

En tout, onze bulletins ont ainsi été publiés. Cinq sont considérés comme critiques, cinq comme importants et un comme modéré par l'éditeur. Les logiciels touchés sont :

- le client SMB de Microsoft Windows ;
- Microsoft Windows Media Services ;
- le codec Microsoft MPEG Layer-3 ;
- le lecteur Windows Media ;
- le noyau de Windows ;
- VBScript ;
- Microsoft Office Publisher ;
- Microsoft Visio ;
- le composant ISATAP de Windows ;
- la vérification de signature Authenticode.

La mise à jour concernant VBScript corrige l'alerte CERTA-2010-ALE-003. Il est recommandé d'appliquer les correctifs dans les plus brefs délais.

2 Fin de vie de la version 0.94.x de ClamAV

Cette semaine ClamAV a publié sur son site Internet un article faisant part de la fin de vie de la version 0.94.x de son antivirus.

Il est expliqué dans cette annonce qu'un bogue affecte toutes les versions antérieures à la 0.95 empêchant d'intégrer des signatures de plus de 980 octets dans les mises à jour incrémentielles. Cette limite diminue les capacités de l'antivirus dans son traitement de signature antivirale complexe. À partir du 15 avril 2010, ClamAV va donc propager une signature particulière désactivant toutes les installations de l'antivirus antérieures à la version 0.95.

ClamAV prévoit le début de la diffusion de base de signatures supérieure au mois de mai 2010. Le CERTA recommande donc aux utilisateurs de ce logiciel de migrer le plus rapidement possible vers la dernière version au risque de voir la protection antivirale totalement désactivée.

Documentation

Annonce de fin de vie de ClamAV :
http://www.clamav.net.lang/fr/2009/10/05/eol-clamav-094/

3 Durcissement de la configuration des systèmes Windows 8/8 : désactivation des services inutiles

Afin de réduire la surface d'attaque des systèmes Windows utilisés en tant que serveurs ou que postes de travail, les services applicatifs qui ne sont pas utilisés doivent être désactivés. La liste des services applicatifs et leur état (en cours d'exécution, arrêté, désactivé, exécution automatique ou manuelle, etc.) est récupérable grâce au composant enfichable `services.msc` ou *via* l'utilitaire en ligne de commande `sc`.

Ainsi, dans la mesure où ils ne sont pas utilisés, les services suivants devraient être désactivés. La plupart sont activées par défaut lors d'une installation standard, mais ces services peuvent affaiblir la sécurité du système. L'établissement de cette liste prend en compte l'historique des services en termes de vulnérabilités, la divulgation d'informations qu'ils entraînent ainsi que l'absence usuelle d'utilité fonctionnelle.

Browser (Explorateur d'ordinateur): ce service met en œuvre le protocole *Browser*[1] utilisé pour la résolution des noms *NetBios*. Son exécution entraîne la divulgation d'informations sur le réseau ainsi que des risques de rebond RPC.

Alerter (Avertissement): ce service implémente la notification des alertes dites « administratives » aux utilisateurs ou aux ordinateurs. Ce service a été désactivé par défaut à partir de Windows XP Service Pack 2.

Messenger (Affichage des messages): ce service permet de transporter sur le réseau les alertes du service Alerter ci-dessus. La commande « `net send` » repose sur ce mécanisme. Ce service a également été désactivé par défaut à partir de Windows XP Service Pack 2.

SSDPSRV (Service de découvertes SSDP): à partir de Windows XP, ce service met en œuvre le protocole SSPD (*Simple Service Discovery Protocol*) qui permet de découvrir automatiquement sur un réseau les différents équipements, ainsi que les services offerts par ces derniers. Ce protocole se base sur des envois en *multicast* sur le port 1900/UDP.

upnphost (Hôte de périphérique universel Plug-and-Play): à partir de Windows XP, ce service gère les différents mécanismes de la norme UPnP (*Universal Plug and Play*) offerts par le système. Les services UPnP permettent de simplifier et d'automatiser les configurations réseau au moyen de différents protocoles, mais restent très peu utilisés, a fortiori dans un environnement professionnel.

WebClient (WebClient): à partir de Windows XP, ce service implémente l'accès distant à des fichiers via les protocoles HTTP et WebDAV (*Web-based Distributed Authoring and Versioning*).

WZCSVC (Configuration automatique sans fil): à partir de Windows XP, ce service fournit deux fonctionnalités :

- la gestion des réseaux sans-fil : énumération des différents points d'accès, traitement des phases d'authentification et stockage des clefs ;

[1] `http://support.microsoft.com/kb/188001`

– le protocole 802.1x (authentification auprès d'un équipement réseau).

ERSvc (Service de rapport d'erreurs): à partir de Windows XP, ce service offre la possibilité en cas d'arrêt intempestif d'une application d'envoyer un rapport d'erreur à Microsoft.

PolicyAgent (Services IPSEC): ce service implémente le protocole `IKE` en charge de la négociation des associations de sécurité dans le cadre des communications IPsec.

Les noms des services applicatifs peuvent varier selon la version de Windows. De plus, de nouveaux services ont été ajoutés dans les systèmes récents, par exemple WinHttpAutoProxySvc.

Cette liste de services n'est pas exhaustive et doit être adaptée selon le contexte d'utilisation de la machine concernée. Il faudra notamment prendre en compte la présence de programmes spécifiques d'administration à distance ou requérant des fonctionnalités particulières. À titre d'exemple, d'autres services peuvent être désactivés : accès du périphérique d'interface utilisateur, acquisition d'image Windows (WIA), agent de protection d'accès réseau, assistance TCP/IP NetBIOS, audio Windows, client DHCP, gestionnaire de connexion automatique d'accès distant, gestionnaire de l'album, etc.

Enfin, la désactivation d'un service peut avoir des conséquences, il est donc nécessaire de valider l'absence d'impact dans un environnement de qualification avant de mettre en production une configuration dans laquelle les services activés sont réduits.

Conclusion

Cet article termine une série de recommandations sur le durcissement de la configuration des systèmes Windows. Bien d'autres éléments peuvent être configurés par GPO (grâce aux composants enfichables `gpedit.msc` et `secpol.msc`) et d'autres fonctionnalités peuvent être désactivées (support des protocoles IPX, IPv6, interface FireWire, mode débogage noyau, etc.) ou activées (DEP, pare-feu local, signature des échanges RPC, ordre de chargement des fichiers de type DLL, etc.). Microsoft fournit des guides de sécurisation détaillant la configuration conseillée d'une grande partie des GPO disponibles. Il est également nécessaire de réaliser une veille technique pour se tenir informé de nouveaux éléments de durcissement (contenus par exemple dans les contre-mesures temporaires des bulletins de sécurité Microsoft).

D'autre part, un travail identique de durcissement de la configuration doit être effectué sur les différents programmes installés sur les postes de travail (navigateurs, suite bureautique, Acrobat Reader, etc.) et sur les différents services offerts par les serveurs (Exchange, serveurs Web, serveurs de gestion de base de données, etc.).

Enfin, des audits réguliers de configuration doivent être réalisés, de façon manuelle ou automatique, pour vérifier que les éléments configurés n'ont pas subît de régression ou d'erreurs de configuration.

4 Du problème de configuration à l'incident de sécurité

De très nombreux sites fonctionnant avec *WordPress* ont récemment fait l'objet d'attaques. Celles-ci ont consisté, pour l'essentiel, à modifier la valeur `siteurl` dans la base de données pour rediriger les visiteurs vers un site malveillant.

A priori, ce n'est pas une vulnérabilité du logiciel qui a été exploitée, mais un défaut de configuration du serveur. En effet, les sites *WordPress* attaqués étaient presque tous hébergés chez le même prestataire. Or, les paramétrages des droits de fichier des différents serveurs du prestataire permettaient d'accéder en lecture au fichier de configuration de *WordPress*, ce dernier contenant en clair les identifiants de connexion à la base de données.

Cet incident est loin d'être un cas isolé. De nombreux administrateurs (ou webmestres) commettent l'erreur de positionner des droits trop permissifs pour des fichiers sensibles, notamment ceux contenant des identifiants de connexion. Ces informations sont généralement facilement retrouvées à l'aide de moteurs de recherche, et font parfois l'objet de publications sur des sites spécialisés.

D'une manière générale, il est fortement recommandé aux administrateurs et aux webmestres de vérifier que les fichiers de configuration des sites ne sont pas accessibles depuis l'Internet. La lecture régulière des journaux d'accès donne également des indications quant à la fuite éventuelle d'informations sensibles.

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 09 au 15 avril 2010, le CERTA a émis les avis suivants :
– CERTA-2010-AVI-162 : Multiples vulnérabilités dans les produits VMware
– CERTA-2010-AVI-163 : Vulnérabilité dans TYPO3
– CERTA-2010-AVI-164 : Vulnérabilité dans TheGreenBow
– CERTA-2010-AVI-165 : Multiples vulnérabilités dans les produits VMware
– CERTA-2010-AVI-166 : Vulnérabilité dans F-Secure
– CERTA-2010-AVI-167 : Vulnérabilités dans Microsoft Windows Authenticode Verification
– CERTA-2010-AVI-168 : Vulnérabilités dans le client SMB de Microsoft
– CERTA-2010-AVI-169 : Vulnérabilités dans le noyau Windows
– CERTA-2010-AVI-170 : Vulnérabilité dans Microsoft VBScript
– CERTA-2010-AVI-171 : Vulnérabilité dans Microsoft Office Publisher
– CERTA-2010-AVI-172 : Multiples vulnérabilités dans Microsoft Exchange et Windows SMTP
– CERTA-2010-AVI-173 : Vulnérabilité dans Microsoft Windows Media Services
– CERTA-2010-AVI-174 : Vulnérabilité du Codec Microsoft MPEG Layer-3
– CERTA-2010-AVI-175 : Vulnérabilité dans Windows Media Player
– CERTA-2010-AVI-176 : Multiples vulnérabilités dans Microsoft Visio
– CERTA-2010-AVI-177 : Vulnérabilités dans Microsoft Windows ISATAP
– CERTA-2010-AVI-178 : Multiples vulnérabilités dans Adobe Reader et Adobe Acrobat
– CERTA-2010-AVI-179 : Multiples vulnérabilités dans les produits Oracle
– CERTA-2010-AVI-180 : Vulnérabilité dans Cisco Secure Desktop
– CERTA-2010-AVI-181 : Vulnérabilité dans Apple Mac OS X
– CERTA-2010-AVI-182 : Multiples vulnérabilités dans CUPS
– CERTA-2010-AVI-183 : Vulnérabilité dans IBM WebSphere Portal

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 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.

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.

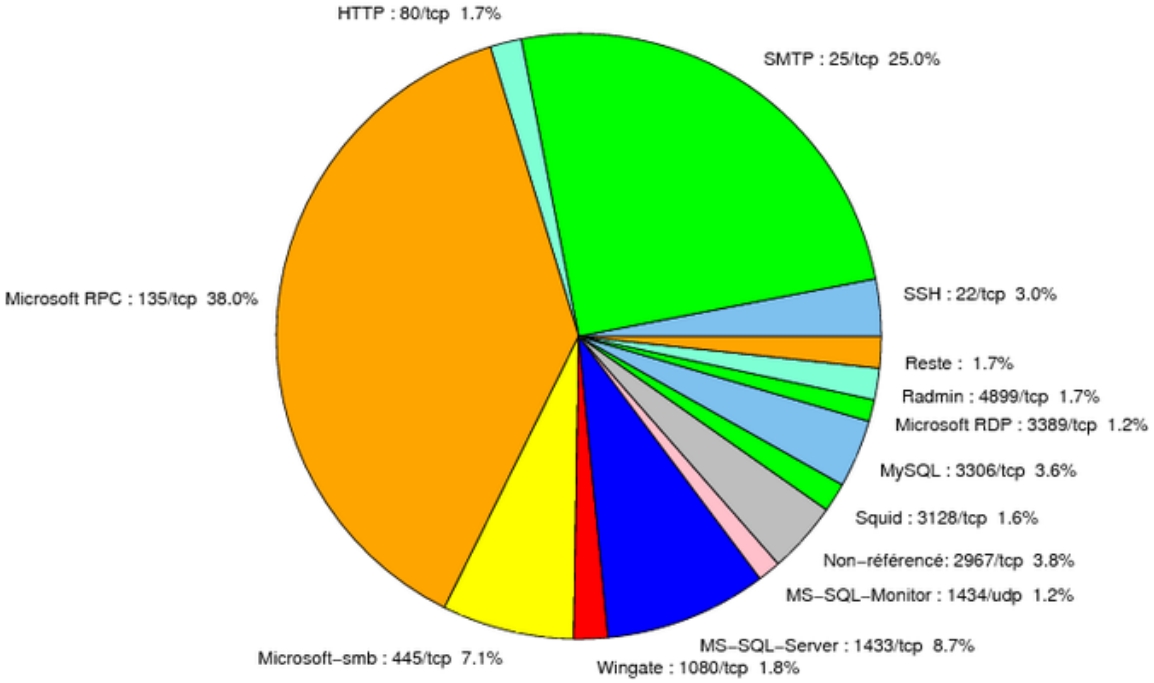

FIG. 1: Répartition relative des ports pour la semaine du 09 au 15 avril 2010

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
135/tcp	38.01
25/tcp	25
1433/tcp	8.67
445/tcp	7.05
2967/tcp	3.82
3306/tcp	3.62
22/tcp	3.04
80/tcp	2.33
1080/tcp	1.81
4899/tcp	1.68
3128/tcp	1.55
3389/tcp	1.29
1434/udp	1.23
21/tcp	0.71
3127/tcp	0.45
15118/tcp	0.25
23/tcp	0.12
2100/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

16 avril 2010 version initiale.