Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 septembre 2006
N° CERTA-2006-ACT-037

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-37

Gestion du document

Référence	CERTA-2006-ACT-037
Titre	Bulletin d'actualité 2006-37
Date de la première version	15 septembre 2006
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-2006-ACT-037.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-2006-ACT-037/

1 Activité en cours

1.1 Données insérées dans une base de données

Le CERTA a traité cette semaine un incident concernant une base de données. Celle-ci est accessible par le biais d'un formulaire d'une page web. les utilisateurs, en enregistrant différentes informations, remplissent à distance des champs de la base.

De manière générale, plusieurs services peuvent s'appuyer sur une même base de données. Ils interrogent celle-ci par différentes requêtes qui leur sont propres. Il est donc important de vérifier, avant toute nouvelle entrée dans une base de données :

- la *syntaxe* des données introduites : il s'agit ici de vérifier le format des variables, ainsi que leur longueur, et leur contenu (interdiction de caractères spéciaux) ;
- la *sémantique* des données introduites : il s'agit de vérifier ici que les données introduites gardent un sens. Dans le cas de dates de naissance par exemple, il faut donc limiter la valeur du champ 'jour' (1 à 31), du 'mois' (1 à 12), voire de l'année (supérieure à 1890). Une seconde illustration concerne les codes postaux associés aux noms de ville.

Ce contrôle doit se faire côté serveur avant l'insertion des nouvelles données dans la base. Celle-ci doit être aussi construite de manière à anticiper de mauvaises entrées ou des entrées incohérentes (rôle des clés primaires et droits sur les tables).

1.2 Configuration de *Webdav*

Dans le cadre d'un traitement d'incident, le CERTA recommande d'être vigilant dans l'usage de `Webdav`.

Webdav est une extension du protocole `HTTP` permettant la mise à jour de contenu `HTML` sur un serveur web sans utiliser d'autres services (ftp, sftp, samba) que le serveur web. Il convient de prendre garde à l'utilisation qui peut être faite d'un tel protocole. En effet l'utilisation de Webdav revient à autoriser la méthode `PUT` sur le serveur web. Celle-ci permet la dépose de fichiers sur un serveur web, parfois sans autorisation préalable. Un serveur web offrant des fonctionnalités webdav mal configurées permet à un éventuel attaquant de modifier un site web. De manière générale, il est fortement déconseillé d'utiliser webdav sur un serveur de production. Il est préférable de réserver cette technologie à un serveur interne de test ou de développement.

1.3 Publication concernant IPv6

Le CERTA a publié cette semaine une note d'information concernant les enjeux liés à la sécurité lors d'un déploiement vers IPv6. Cette note reprend quelques principes associés à ce nouveau protocole, et en explique différents risques. Elle présente aussi un ensemble de recommandations à considérer, que le déploiement soit envisagé ou pas.

La note est accessible à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html

1.4 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 07 et le 14 septembre 2006.

2 Mises à jour Microsoft du mois de septembre 2006

2.1 Récapitulatif

Microsoft a publié mardi 12 septembre 2006 trois nouveaux bulletins de sécurité, concernant :

1. une vulnérabilité du protocole de diffusion (`PGM`) sur les systèmes d'exploitation Windows XP. Ce protocole n'est pas activé par défaut. (CERTA-2006-AVI-387)
2. une vulnérabilité du service d'indexage concernant la majorité des systèmes d'exploitation Windows. Cependant cette vulnérabilité n'est exploitable que sous certaines conditions, avec l'utilisation sur le même système d'un serveur Web IIS. (CERTA-2006-AVI-388)
3. une vulnérabilité jugée critique dans Microsoft Publisher. Une personne malveillante pourrait construire un fichier exploitant celle-ci, afin d'exécuter du code arbitraire sur le système où le document est ouvert. (CERTA-2006-AVI-389)

2.2 Correctifs de mises à jour

En complément des trois bulletins précédents, Microsoft a réédité deux bulletins :

- `MS06-040` : il s'agit d'un correctif lié au service Serveur. Le précédent correctif pouvait entraîner certains dysfonctionnements des systèmes d'exploitation Windows Server 2003 SP1 et Windows XP Professionnel Edition x64.
- `MS06-042` : il s'agit d'une deuxième mise à jour du bulletin (la première datant du 24 août 2006) lié à Internet Explorer. La précédente version introduirait une nouvelle vulnérabilité dans les navigateurs Internet Explorer 6 (version SP 1) et Internet Explorer 5.01 SP 4.

Le CERTA recommande, dans la mesure du possible, d'appliquer de nouveau les correctifs fournis par les précédents bulletins `MS06-040` et `MS06-042`.

2.3 Problèmes liés à *ActiveX*

Une nouvelle vulnérabilité ciblant un contrôleur `ActiveX` (`DirectAnimation Path`) est actuellement exploitée, mais n'est pas corrigée par les bulletins Microsoft de septembre (http://www.microsoft.com/technet/security/advisory/925444.mspx). Ce contrôleur se trouve dans le module nommé `Daxctle.ocx`. Cette vulnérabilité non corrigée liée à ActiveX s'ajoute à celles dévoilées en juillet (cf. les bulletins d'actualité du CERTA du mois de juillet 2006).

Le CERTA recommande donc vivement de vérifier que les options `ActiveX` sont désactivées par défaut dans le navigateur Internet Explorer. Elles ne doivent être utilisées que ponctuellement, au cours de la visite de pages web de confiance.

Pour désactiver `ActiveX` sous Internet Explorer :

- Ouvrir Internet Explorer
- Cliquer sur le menu «Outils»
- Choisir «Options Internet»
- Afficher l'onglet «Sécurité»
- Cliquer sur «Personnaliser le niveau»
- Sélectionner *Désactiver* pour les lignes suivantes :
  - 'Contrôles ActiveX et Plugins'
  - 'Contrôles ActiveX reconnus sûrs pour l'écriture de scripts'
  - 'Contrôles d'initialisation et de script ActiveXnon marqués comme sécurisés'
  - 'Exécuter les contrôles ActiveX et les plugins'
  - 'Télécharger les contrôles ActiveX' (signés et non signés)

3 Pourriels

3.1 Remarques concernant les pourriels

Des abonnés du CERTA ont signalé une recrudescence d'un pourriel à caractère antisémite très largement distribué. Ces courriers électroniques avaient déjà étaient diffusés par le passé. Les messages contiennent une diatribe de plus de 60 pages. L'objet du message est «Trop c'est trop...».

Il est rappelé de ne jamais répondre aux messages non sollicités et de s'appuyer sur la note d'information du CERTA sur le Spam (http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/index.html). Vous trouverez aussi sur le site Signal-spam (http://www.signal-spam.fr) des informations et des moyens de lutter contre le spam.

3.2 Protection des machines personnelles

Le CERTA a été informé dans le cadre de la coopération internationale entre CSIRTs d'un nombre conséquent de machines compromises par un cheval de Troie connu (`Haxdoor`). Ce cheval de Troie est muni d'une fonctionnalité de capture des frappes clavier (*keylogger*). Ainsi de nombreux internautes se connectant sur des sites (institutionnels, marchands, bancaires, etc) laissent fuir à leur insu les informations confidentielles saisies sur les pages web. Cette fuite a lieu que la connexion soit sécurisée ou pas.

D'une façon générale, le CERTA rappelle les bonnes pratiques suivantes en matière de protection de son ordinateur personnel :

- l'Internet est une rue : il faut rester vigilant lorsque l'on s'y déplace;
- être vigilant lors de l'ouverture des pièces jointes aux messages électroniques. Ces pièces jointes sont traditionnellement un moyen facile pour compromettre un ordinateur;
- mettre à jour régulièrement ses logiciels (système d'exploitation, navigateur Internet, messagerie, anti virus, etc.) : les codes malveillants profitent souvent des logiciels non corrigés pour se propager;
- utiliser un pare-feux pour filtrer ce qui entre et sort de votre ordinateur;
- ne jamais répondre aux messages non sollicités (spam);
- ne jamais ouvrir des messages dont l'origine est inconnue ou l'objet douteux.

Pour comprendre les termes techniques de la sécurité des systèmes d'information, nous vous invitons à consulter le document suivant :

http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html

Pour de plus amples informations sur la façon de se protéger contre les codes malveillants, nous vous recommandons de lire le mémento du CERTA à ce sujet, disponible à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/index.html

3.3 Signalement au CERTA de courriers électroniques anormaux

Dans le cas où vous souhaiteriez demander l'avis technique du CERTA concernant des courriers électroniques reçus, il est important de lui envoyer l'ensemble des informations disponibles. Cela inclut l'en-tête du message dans son intégralité, celle-ci contenant des indications de l'origine (adresses IPs). Attention, quand vous utilisez `Transférer` sous Outlook, l'intégralité du message d'origine n'est pas transmise, et en particulier l'en-tête.

Concernant Outlook (versions 2000 et XP), une en-tête complète peut se récupèrer de la façon suivante :

1. Sélectionner le message
2. Cliquer sur le menu «Affichage»
3. Choisir «Options»
4. Copier-coller l'en-tête complète qui s'affiche dans la fenêtre

Concernant Mozilla Thunderbird :

1. Sélectionner le message
2. cliquer sur le menu «Affichage»
3. Choisir «Source du message»
4. Copier-coller le texte qui s'affiche dans une nouvelle fenêtre

4 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
  http://www.auscert.org.au/render.html?it=1935

5 Rappel des avis et mises à jour émis

Durant la période du 08 au 14 septembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-386 : Vulnérabilité des IOS Cisco
- CERTA-2006-AVI-387 : Vulnérabilité du protocole PGM dans Microsoft Windows
- CERTA-2006-AVI-388 : Vulnérabilité dans le service d'indexage de Microsoft Windows
- CERTA-2006-AVI-389 : Vulnérabilité dans Microsoft Publisher
- CERTA-2006-AVI-390 : Multiples vulnérabilités dans Apple QuickTime
- CERTA-2006-AVI-391 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2006-AVI-392 : Vulnérabilités dans Avast!
- CERTA-2006-AVI-393 : Multiples vulnérabilités dans CISCO IOS
- CERTA-2006-AVI-394 : Multiples vulnérabilités de l'antivirus Symantec

– CERTA-2006-AVI-395 : Vulnérabilité du logiciel Ipswitch IMail server
– CERTA-2006-AVI-396 : Vulnérabilité dans HP-UX
– CERTA-2006-AVI-397 : Plusieurs vulnérabilités dans Xorg X11 et XFree86
– CERTA-2006-AVI-398 : Vulnérabilité dans Adobe Flash Player

Pendant cette même période, les mises à jour suivantes ont été publiées :

– CERTA-2006-AVI-300-001 : Vulnérabilité dans Gnu GCC
(ajout de la référence au bulletin de sécurité Debian)
– CERTA-2006-AVI-315-003 : Vulnérabilité dans Apache httpd
(ajout de la référence à la mise à jour Debian)
– CERTA-2006-AVI-338-001 : Vulnérabilité dans le Service Serveur de Microsoft Windows
(ajout de la mise à jour du bulletin MS06-040 par Microsoft)
– CERTA-2006-AVI-340-002 : Multiples vulnérabilités dans Internet Explorer
(modification liée à la mise à jour du bulletin MS06-042)
– CERTA-2006-AVI-361-001 : Vulnérabilité dans ImageMagick
(ajout des références CVE et des bulletins de sécurité de RedHat, Mandriva, Debian, Ubuntu, SuSE1.)
– CERTA-2006-AVI-373-001 : Multiples vulnérabilités dans Wireshark (Ethereal)
(ajout de la référence à la mise à jour Debian)
– CERTA-2006-AVI-377-001 : Vulnérabilité dans XOrg X11 et des bibliothèques associées
(ajout de la référence à la mise à jour Ubuntu)
– CERTA-2006-AVI-384-002 : Vulnérabilité dans OpenSSL
(ajout de la référence aux bulletins de sécurité Debian et OpenBSD)
– CERTA-2006-AVI-385-002 : Vulnérabilités de BIND
(ajout des bulletins de sécurité Debian, OpenBSD et Mandriva)

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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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 œuvre (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 COSSI/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, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

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.

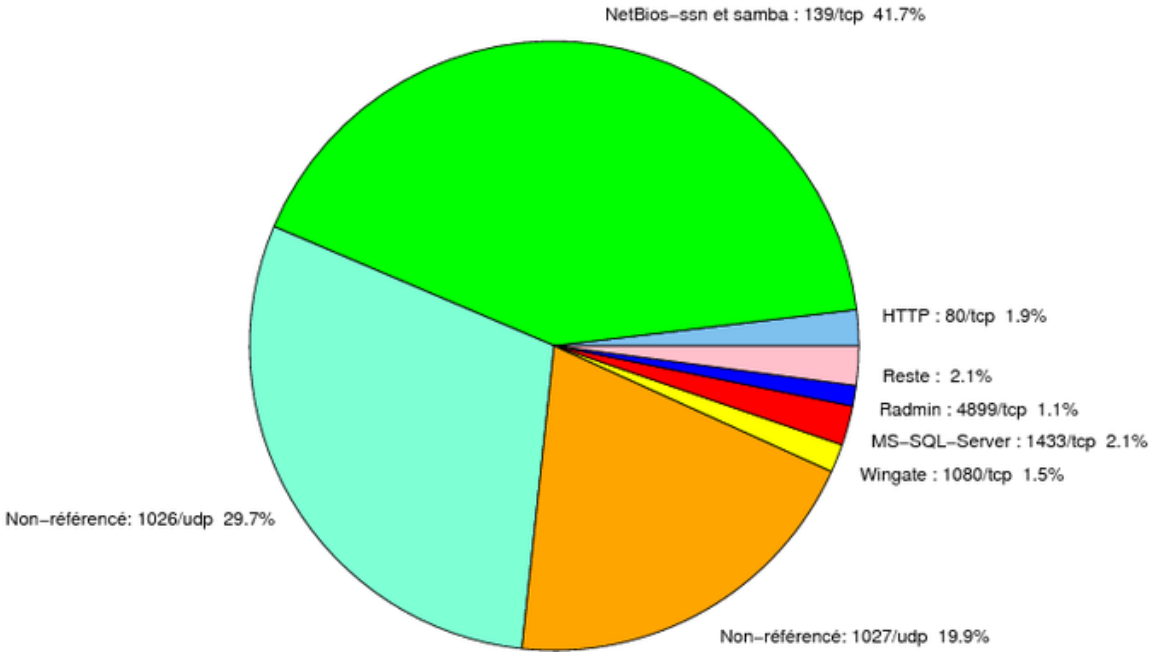

FIG. 1: Répartition relative des ports pour la semaine du 07.09.2006 au 14.09.2006

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

				http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE
2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
139/tcp	41.7
1026/udp	29.71
1027/udp	19.91
1433/tcp	2.09
80/tcp	1.89
1080/tcp	1.49
4899/tcp	1.09
1434/udp	0.62
137/udp	0.58
3128/tcp	0.28
22/tcp	0.19
25/tcp	0.16
443/tcp	0.05
15118/tcp	0.04
143/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

15 septembre 2006 version initiale.