Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2008
N° CERTA-2008-ACT-038

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-38

Gestion du document

Référence	CERTA-2008-ACT-038
Titre	Bulletin d'actualité 2008-38
Date de la première version	19 septembre 2008
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-2008-ACT-038.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-2008-ACT-038/

1 Incidents traités cette semaine

1.1 Effets de bord et incident de sécurité

Cette semaine, le CERTA a traité un incident affectant les routeurs d'une infrastucture réseau. Les routeurs présentaient des problèmes dans le traitement de trames *IGMP*. Ces dernières provoquaient un déni de service des routeurs. Ne comprenant pas l'origine de ces trames, l'organisme victime a demandé au CERTA d'étudier une machine afin d'identifier la provenance des communications *IGMP* et de déterminer si ces dernières étaient d'origine malveillante ou non.

Après analyse, il s'est avéré que les trames *IGMP* pouvaient avoir différentes origines. En effet, un service activé par défaut, ainsi que deux applications installées sur la machine étaient susceptibles de créer du trafic *IGMP* sur le réseau. Toutes ces origines étaient a priori légitimes.

Après une analyse plus fine, les trames provoquant le dysfonctionnement des routeurs étaient probablement dues à une application de *ToIP* (téléphonie sur IP). Le CERTA profite de cet incident, qui n'était pas lié à un problème de sécurité, pour attirer l'attention des lecteurs sur l'intérêt d'effectuer une bonne étude des applications avant de les intégrer dans un système d'information. Il est primordial d'identifier correctement, au préalable, toutes les communications et les effets de bords que l'installation d'une application peut entraîner. Une étude de cette

application de *TOIP* aurait permis de découvrir ces modes de communication et d'éviter la panne des routeurs ainsi que les doutes sur la provenance malveillante ou non de ces trames indisposantes pour l'architecture réseau.

– Bulletin d'actualité CERTA-2008-ACT-005, « MS08-001 et protocole IGMPv3 » du 01 février 2008 : http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-005/

1.2 Pages indiscrètes - suite

Cette semaine, le CERTA a traité un incident relatif à l'affichage d'une page indiscrète sur un site de l'administration. La page en question affichait le contenu d'un répertoire car il n'y avait pas de page d'index par défaut. Ce sujet a été abordé dans le bulletin d'actualité CERTA-2008-ACT-037 du 12 septembre 2008. Dans ce cas précis, le répertoire contenait plusieurs documents `Word` non destinés au public.

Le CERTA rappelle qu'il est conseillé de désactiver par défaut l'affichage du contenu des répertoires (cf. bulletin d'actualité CERTA-2008-ACT-037). En plus de divulguer la présence de fichiers qui peuvent être sensibles, cela peut renseigner une personne malintentionnée sur la version du serveur et des applications utilisées. Il est également fortement déconseillé de mettre sur l'Internet des documents qui ne sont pas destinés au grand public. Le CERTA rappelle aussi à cette occasion qu'il est important de convertir et nettoyer tout document avant de le mettre en ligne. Des informations peuvent être accessibles via les vicissitudes des différents formats et des propriétés du document.

1.2.1 Documentation

– Bulletin d'actualité CERTA-2008-ACT-037, « Pages indiscrètes » : http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-037.pdf

2 Vulnérabilité dans l'application *phpMyAdmin*

2.1 Présentation

Le CERTA a publié cette semaine l'avis CERTA-2008-AVI-464 concernant une vulnérabilité de l'application Web *phpMyAdmin*.

Dans la version 3.0.0-rc1 ainsi que certaines antérieures, un mauvais traitement des paramètres permet d'injecter du code `PHP`. Pour réussir l'injection, l'attaquant doit disposer d'un jeton d'identification valide, et donc s'identifier en premier lieu. Dans le cas d'un serveur mutualisé, il suffit de se créer un compte ou d'obtenir les identifiants d'un des administrateurs de sites par une attaque en filoutage ou en ingénierie sociale.

Le code injecté peut lancer des commandes sur le serveur, avec les droits de l'utilisateur du service Web, à l'aide de commandes `PHP` telles que *exec()*. Il peut, par exemple, recopier les fichiers de configuration locaux en changeant l'extension afin de les rendre lisibles , effacer les fichiers du serveur, accéder à la configuration de la machine, etc.

Le CERTA recommande de :

– mettre à jour les applications et le système d'exploitation du serveur ;
– éviter si possible de mettre en ligne ce genre d'interfaces d'administration et surtout ne pas les laisser accessibles à tous. Leur accès doit être restreint et contrôlé.
– désactiver autant que possible les interactions entre le site Web et le système local en désactivant les fonctions à l'aide de la primitive *disable_functions* contenue dans le fichier de configuration *php.ini* ;
– limiter les droits de l'utilisateur exécutant le service Web ;
– utiliser un serveur mandataire inverse pour filtrer les requêtes contenant des chaînes de caractères dangereuses telles que *exec(*)* ;

2.2 Documentation

– Site officiel du projet *phpMyAdmin* : http://www.phpmyadmin.net/home_page/index.php
– Avis CERTA-2008-AVI-464 du 16 septembre 2008, « Vulnérabilité dans phpMyAdmin » : http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-464/

3 Filtrage et cloisonnement des zones de confiance

3.1 Présentation générale

Le CERTA a mentionné dans sa note d'information CERTA-2006-INF-001 traitant du filtrage la nécessité de cloisonner proprement les flux dans le réseau entre les différentes zones de confiance.

Prenons le cas d'une zone dans laquelle est placée un serveur web. Celui-ci peut être en communication avec :

- des machines quelconques de l'Internet, car il offre au public un service en ligne ;
- des machines du réseau Intranet, qui souhaitent y accéder pour des raisons de maintenance, de mises à jour et d'accès au service.

Voici deux hypothèses :

1. un code a pu être inséré sur le site en ligne, du fait d'une compromission ou d'un script de téléchargement et de stockage offerte par le site (zone pour « *uploader* »). Ce script peut être écrit en PHP, en ASP, en JSP, etc. ;
2. les règles de filtrage entre cette DMZ et l'Intranet sont relativement laxistes, offrant certains accès du serveur Web à des services internes. Pour les machines de l'Internet, la politique est plus rigoureuse : seules les communications en HTTP associées au port 80/TCP depuis l'extérieur sont autorisées à destination du serveur Web (cf. figure 1).

Que se passe-t-il alors ? Le réseau Intranet est potentiellement exposé. Le serveur Web peut être utilisé pour construire un tunnel depuis des machines externes pour accéder à des ressources internes.

3.2 Fonctionnement de l'attaque

Le principe de l'attaque est identique à celui mis en place dans le cas d'une machine offrant un service SSH et autorisant la construction de tunnels (directive `PermitTunnel=yes` dans le fichier de configuration de `sshd` par exemple). Ce dernier peut être volontaire afin d'inciter les utilisateurs à construire un tunnel chiffré pour communiquer avec certains serveurs depuis l'extérieur du réseau.

Dans le cas de l'attaque, un client « tunnelise » certaines requêtes adressées à un port en boucle locale (127.0.0.1) en lançant une commande de la forme :

```
$create_tunnel 1234:machine_interne_cible:XXX
```

Un tunnel se construit et permet à l'utilisateur externe d'accéder au port XXX de la machine interne. Le script inséré sur le serveur Web permet d'ouvrir de nouvelles connexions vers des machines internes. Cette opération fonctionne donc si les communications entre le site Web de la DMZ et la machine interne sur le port XXX ne sont pas bloquées. Le scénario permet également d'accéder aux interfaces internes des équipements réseau (routeurs, commutateurs, etc.).

Des outils sont disponibles sur l'Internet afin de mettre en place une telle activité.

3.3 Recommandations

Les recommandations consistent à éviter que les hypothèses faites ne soient satisfaites et à limiter les actions de l'attaque si celle-ci se produit. Il s'agit donc essentiellement de bonnes pratiques courantes :

- configurer avec précaution les applications et les services ;
- filtrer de manière très restrictive les échanges entre les zones ;
- vérifier régulièrement l'intégrité du serveur et ne pas laisser télécharger n'importe quel code depuis n'importe quelle machine sur un serveur ;
- analyser régulièrement les journaux des équipements réseau, des systèmes et des applications.

Les machines dans une zone démilitarisée (DMZ) doivent être cloisonnées entre elles et des règles de filtrage rigoureuses doivent être établies pour leurs communications aussi bien externes qu'internes.

4 Modifications du site web du CERTA

Cette semaine, le CERTA a procédé à quelques modifications sur son site web qui, nous l'espérons, amélioreront son usage au quotidien. Ainsi, on pourra noter l'apparition dans le bandeau de gauche de nouveaux liens :

- un lien vers les alertes en cours pointant vers une page listant les alertes toujours actives et pour lesquelles il n'existe pas de correctif ;

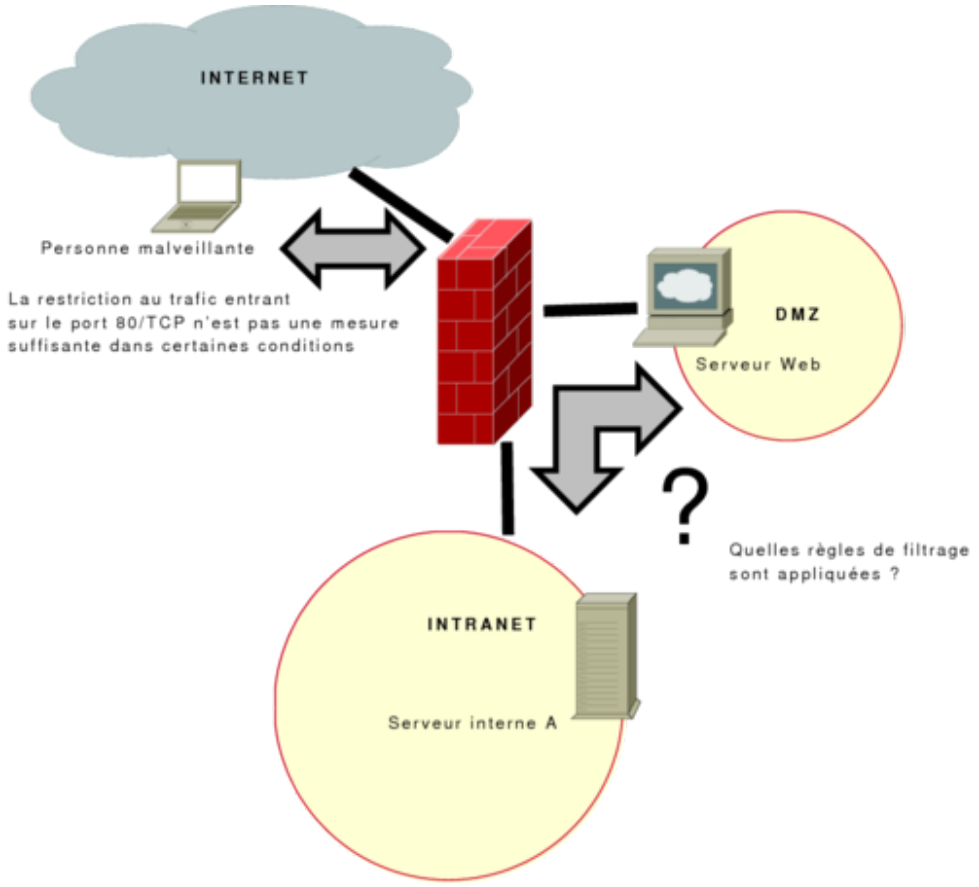

FIG. 1: Cloisonnement des zones et tunnel HTTP pour accéder à l'Intranet

– un lien vers les bulletins d'actualité de l'année en cours ;

On pourra noter également la création d'un nouveau flux RSS associé à la page des alertes en cours. Le site fournit donc désormais deux flux RSS :

– le flux « classique » des nouvelles publications ;
– le flux des alertes non-corrigées en cours.

Enfin, en terme de présentation, dans la page d'accueil, les bulletins sont maintenant situés au dessus des notes d'informations et en dessous des avis.

5 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 11 et le 18 septembre 2008.

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=1935
– 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 11 au 18 septembre 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-456 : Vulnérabilités de Joomla!
– CERTA-2008-AVI-457 : Vulnérabilité dans MySQL
– CERTA-2008-AVI-458 : Multiples vulnérabilités dans Horde
– CERTA-2008-AVI-459 : Vulnérabilité dans Trend Micro OfficeScan Server
– CERTA-2008-AVI-460 : Vulnérabilités dans DotNetNuke
– CERTA-2008-AVI-461 : Vulnérabilité de FreeBSD
– CERTA-2008-AVI-462 : Vulnérabilité dans IBM WebSphere Application Server
– CERTA-2008-AVI-463 : Multiples vulnérabilités dans Mac OS X
– CERTA-2008-AVI-464 : Vulnérabilité dans phpMyAdmin

– CERTA-2008-AVI-465 : Vulnérabilité dans libxml2
– CERTA-2008-AVI-466 : Vulnérabilité de OpenSSH pour Debian

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

– CERTA-2008-AVI-153-002 : Vulnérabilité dans bzip2
(ajout des références aux bulletins de sécurité RedHat, Gentoo, SuSE, Sun et NetBSD)
– CERTA-2008-AVI-221-001 : Vulnérabilité dans mplayer
(ajout des références aux bulletins de sécurité Gentoo et Mandriva)
– CERTA-2008-AVI-262-001 : Multiples vulnérabilités dans GnuTLS
(ajout des références aux bulletins de sécurité Gentoo, RedHat, Debian et Ubuntu)
– CERTA-2008-AVI-366-001 : Multiples vulnérabilités dans la machine virtuelle Java de Sun
(ajout des références aux bulletins SuSE et Red Hat)

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, la DCSSI dispose d'un centre de formation :

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

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.

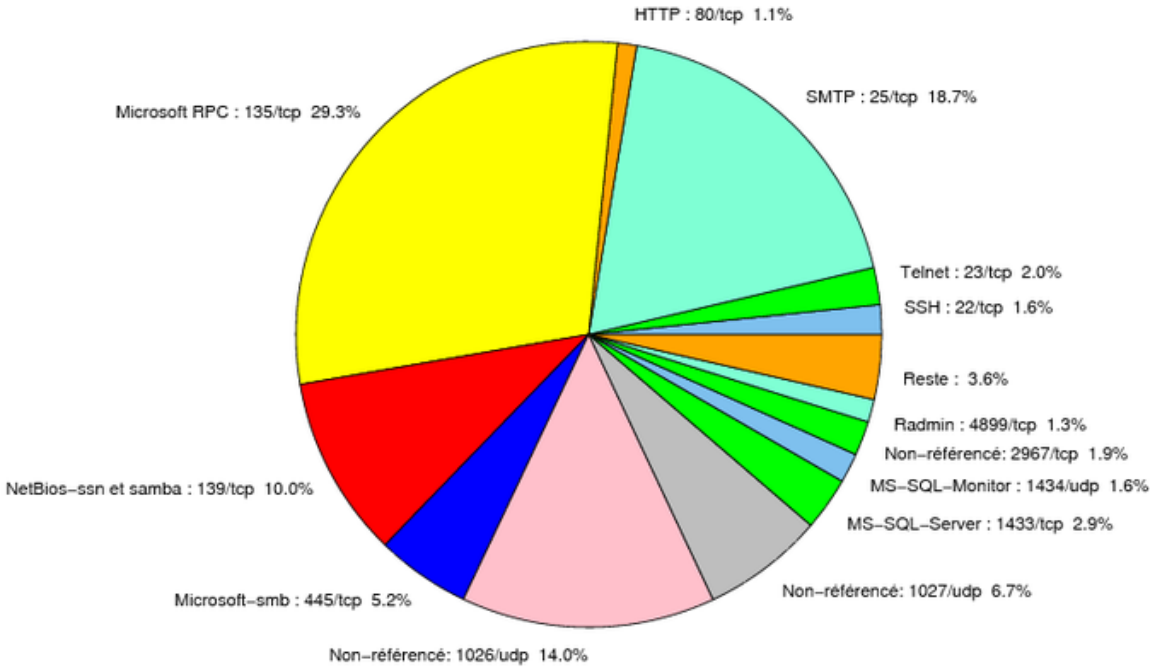

FIG. 2: Répartition relative des ports pour la semaine du 11.09.2008 au 18.09.2008

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/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT

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	29.3
25/tcp	18.69
1026/udp	14.02
139/tcp	10.03
1027/udp	6.72
445/tcp	5.19
1433/tcp	2.94
23/tcp	2.1
2967/tcp	1.89
1434/udp	1.62
4899/tcp	1.26
80/tcp	1.2
1080/tcp	0.94
3128/tcp	0.84
137/udp	0.68
3127/tcp	0.31
5554/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

19 septembre 2008 version initiale.