

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2008-02

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-002>

---

### Gestion du document

Référence	CERTA-2008-ACT-002
Titre	Bulletin d'actualité 2008-02
Date de la première version	11 janvier 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-002.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-002/>

## 1 Les lecteurs multimédia

Les lecteurs multimédia ont fait l'objet de beaucoup d'attention ces derniers jours, avant la publication de ce bulletin d'actualité. Un chercheur en sécurité a travaillé sur le protocole RTSP mis en œuvre dans différents lecteurs multimédia et a publié certains codes d'exploitation pour les vulnérabilités découvertes. Voici un récapitulatif des différents risques et vulnérabilités récents relatifs à ces lecteurs.

### 1.1 QuickTime

Le CERTA a publié une alerte CERTA-2008-ALE-001 relative à une vulnérabilité dans Apple QuickTime. Cette vulnérabilité permet à un individu malveillant d'exécuter du code arbitraire à distance. Cette vulnérabilité peut être exploitée via un lien du type `rtsp://serveur_malveillant/fichier.mp3`. Le serveur de flux étant indisponible QuickTime bascule en HTTP et une page d'erreur spécialement conçue permet l'exploitation de la vulnérabilité du lecteur. Ces codes d'exploitation étant en circulation sur l'Internet, le CERTA recommande de vérifier que l'option de gestion des flux RTSP est bien désactivée dans QuickTime. Cette action permet d'éviter l'ouverture de QuickTime via un lien malveillant mais ne corrige aucunement la vulnérabilité. Un autre palliatif est d'utiliser un lecteur alternatif pour la lecture de ces flux.

## 1.2 RealPlayer

Une nouvelle vulnérabilité a été publiquement révélée cette semaine. Cette vulnérabilité de RealPlayer permet d'exécuter du code arbitraire à distance par un individu malveillant. Le code d'exploitation de cette vulnérabilité est disponible sur l'internet. Il est recommandé de ne pas ouvrir de fichier multimédia dont la provenance est incertaine. Une autre vulnérabilité, découverte en octobre 2007, est aussi en cours d'exploitation par des individus malveillants. Cette dernière a été corrigée provisoirement par un correctif additionnel pour la version 10.5, il est donc nécessaire d'installer ce correctif afin de limiter les risques de compromission. La version stable n'est pas corrigée, à la date de rédaction de ce bulletin.

## 1.3 la bibliothèque `xine-lib`

La bibliothèque `xine-lib` est elle aussi victime d'une vulnérabilité non corrigée de type exécution de code arbitraire à distance. L'exploitation de cette vulnérabilité peut s'effectuer via un serveur de diffusion de flux vidéo. Il est recommandé de ne pas se connecter à des serveurs non sûrs. Cette bibliothèque est entre autres utilisée par les lecteurs : `xine`, `totem` ou `VLC`.

## 1.4 Flash Cross Site Scripting

### 1.4.1 L'injection de code indirecte

Un attaque par injection de code indirecte, ou *cross site scripting* (XSS), consiste à faire exécuter du script sur le navigateur d'un internaute, et cela dans le contexte d'une page web tierce.

Le CERTA a publié à ce sujet la note d'information CERTA-2002-INF-001 :

<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/>

### 1.4.2 Pourquoi le Flash est potentiellement vulnérable aux XSS ?

Les interfaces Flash, pour être plus que de simples animations, doivent offrir de l'interactivité. Pour cela elles utilisent sur un langage de script permettant de traiter et de réagir aux actions des internautes. Ce langage est `Actionscript`. Les programmes flash, en fonction de leur finalité et réalisation, peuvent accepter des arguments, passables via l'adresse (URL) d'appel. Par exemple :

```
http://mon_site/afficher_text_en_gros.swf?var=le_texte_a_afficher
```

Si la variable `le_texte_a_afficher` n'est pas vérifiée, il est possible d'y passer du script qui sera exécuté dans le contexte de l'application `afficher_texte_en_gros.swf`

### 1.4.3 La problématique

La majorité des outils d'édition de sites Web, lors de la création de fichiers flash, y insèrent automatiquement de l'`Actionscript`. Ces fonctions, inconnues de la personne réalisant l'animation flash, sont identiques pour tout les programmes ayant été créés à l'aide du même outil, voire communes à plusieurs outils. Ces fonctions acceptant des paramètres, elles rendent de nombreux sites vulnérables. Une recherche sur Google permet d'identifier plusieurs milliers de sites hébergeant des fichiers Flash vulnérables à une attaque par injection de code indirecte.

### 1.4.4 Les solutions

Plusieurs éditeurs d'outils de réalisation de site Web ont déjà corrigé leurs solutions. Cependant, cela n'est pas suffisant. Il faut que ces nouvelles versions soient installées, et surtout que les Flash mis en ligne soient tous recréés. Plus drastiquement, il suffit de ne pas utiliser cette technologie pour réaliser un site. Au niveau des navigateurs, il est possible d'interdire simplement l'interprétation des fichiers `SWF`.

Le CERTA recommande de désactiver le Javascript et de ne pas installer de module permettant la lecture de Flash, et bien sûr de ne pas naviguer avec un compte aux droits administrateurs.

## 2 Storm Worm

Le CERTA a mentionné dans plusieurs bulletins d'actualité de l'année 2007 les évolutions du vers Storm Worm.

Dans le bulletin CERTA-2007-ACT-028, il est fait mention de son fonctionnement principal, qui s'appuie sur l'envoi de courriels pointant vers des adresses réticulaires (URL) dangereuses.

Le ver a connu un nouvel essor fin décembre 2007, avec les fêtes de Noël et de nouvel an. Le fonctionnement est très semblable, avec l'envoi de courriels aguicheurs contenant des liens vers des sites malveillants.

Quelques noms de domaine ont été liés à l'activité de Storm Worm pendant ces fêtes, en hébergeant notamment des fichiers dangereux :

- merrychristmasdude.com
- uhavepostcard.com
- happycards2008.com
- newyearcards2008.com
- newyearwithlove.com
- familypostcards2008.com
- hellosanta2008.com
- happy2008toyou.com
- freshcards2008.com
- happysantacards.com
- hohoho2008.com
- parentscards.com
- postcards-2008.com
- santapcards.com
- santawishes2008.com

Toute requête vers ces domaines, avec éventuellement dans l'adresse complète la mention d'un fichier exécutable, est suspecte. Il est donc vivement recommandé de vérifier au niveau des passerelles Web si de telles connexions sortantes sont visibles. Ces connexions révéleraient des machines en cours d'infection.

Des cas de filoutage viennent plus récemment d'être signalés. Ils impliquent des sous-ensembles de machines compromises par Storm Worm et visent des organismes bancaires étrangers.

Qu'il s'agisse de Storm Worm ne présente pas vraiment d'intérêt. Il faut noter que les deux vecteurs précédents, un courriel de filoutage ou un courriel contenant un lien vers du code cherchant à compromettre la machine, restent des méthodes pour piéger l'utilisateur. La meilleure protection reste donc la méfiance absolue vis-à-vis des courriels reçus. Par ailleurs, naviguer avec des droits d'utilisateurs limités empêche le code de s'installer correctement sur le système. Ces deux précautions ont l'avantage de ne pas dépendre de bases de signatures des antivirus.

### 3 L'injection d'ordre d'impression

L'injection d'ordre d'impression ou *Cross Site Printing*, est une technique qui peut être utilisée par des personnes malveillantes afin de lancer des commandes sur une imprimante simplement en invitant un utilisateur à visualiser une page web spécialement construite. D'un premier abord cette technique d'injection peut amener à sourire, toute fois avec le déploiement d'imprimantes multifonctions, cette technique peut permettre :

- d'imprimer des documents ;
- d'envoyer des télécopies ;
- de modifier la configuration de l'imprimante ;
- d'augmenter la crédibilité d'une attaque par ingénierie sociale ;
- des fraudes à la surtaxation téléphonique ;
- ...

La plupart des imprimantes réseaux sont capables d'imprimer un document envoyé sur le port TCP 9100. La configuration par défaut de ces imprimantes n'exige pas de mot de passe lors de la connexion sur ce port. L'attaque consiste donc à amener l'utilisateur à visualiser une page spécialement construite incluant des directives de connexion sur le port 9100 de l'imprimante.

Plusieurs recommandations peuvent être appliquées pour réduire les possibilités d'attaque par injection d'ordre d'impression :

- naviguer sur des sites de confiance ;
- mettre en place un mot de passe administrateur sur les imprimantes ;
- dans la mesure du possible limiter l'accès réseau des imprimantes aux seuls serveurs d'impression ;
- dissocier les fonctions de télécopie et d'imprimante réseau en séparant les matériels.

## 4 Administration à distance et VNC

### 4.1 Présentation

VNC (Virtual Network Computing) est une suite logicielle permettant la connexion à distance sur des machines sous différents systèmes d'exploitation. Cette suite est composée d'une partie « serveur » installée sur la machine à administrer et d'une partie « cliente » installée sur une machine où l'on se connecte. Le principe de VNC est de permettre une connexion graphique à distance sur une machine. Ainsi, via le protocole VNC, il est possible d'accéder à un bureau sous Windows ou à un environnement graphique type GNOME ou KDE sous GNU/Linux.

Outre le fait que VNC puisse faire l'objet de failles, le CERTA attire l'attention sur le fait que ce protocole ne prévoit pas dans ses spécifications de fonctionnalités de chiffrement. Nativement, VNC « ne sait pas » chiffrer les connexions entre le serveur et le client. Il est donc possible à un attaquant d'utiliser des techniques d'interceptions pour connaître les activités réalisées sur le « serveur ». De la même façon, l'authentification auprès du serveur VNC ne met pas en œuvre, elle non plus, de méthodes sûres garantissant la confidentialité des données de connexions. Elle ne met en œuvre qu'un couple (nom d'utilisateur, mot de passe).

### 4.2 Recommandations

Si toutefois VNC est indispensable, il est recommandé de mettre en œuvre une solution de chiffrement sous-jacente à VNC comme ssh ou IPSEC par exemple. Il est aussi envisageable de préférer une administration en ligne de commande en particulier sur les machines de type GNU/Linux ou UNIX. En tout état de cause, un serveur VNC ne devra jamais être mis en écoute sur l'Internet même pour des raisons de commodité.

Une autre recommandation est de ne pas laisser le serveur en fonctionnement permanent, si cela est possible.

## 5 Spoofing sous Mozilla Firefox

Une nouvelle vulnérabilité de type usurpation, *ouspoofing*, dans Mozilla Firefox a été publiée la semaine dernière par un chercheur. Un descriptif (le champ *realm*) spécialement conçu dans une authentification HTTP de type *basic* (identifiant / mot de passe) permet en effet de tromper un utilisateur en lui faisant croire qu'il s'authentifie sur un site légitime, alors qu'il est en fait sur un site malveillant qui peut capturer ses identifiants.

Quelques informations circulent à propos de cette faille, signalant que Firefox effectue un filtrage insuffisant en ce qui concerne les caractères espace et guillemet simple. Ces caractères sont toutefois acceptés selon la RFC2617 ; le problème est donc plutôt que Firefox présente les informations d'une mauvaise manière en insérant la source de la requête à la fin, ce qui peut être déroutant pour l'utilisateur.

La faille, proche du *phishing*, ne permet de piéger que des utilisateurs peu vigilants. Toutefois, certains vecteurs d'attaque existent, par exemple :

- l'utilisation d'un script qui dirige un utilisateur vers un site légitime sur une nouvelle page, et qui présente la fausse boîte de dialogue via la page d'origine laissée ouverte ;
- l'utilisation d'une image (envoyée à un webmail, par exemple) pointant vers le serveur réclamant l'authentification.

Le problème a été publié sur le bloc-notes (*blog*) de Mozilla et devrait être corrigé prochainement.

### Documentation

- Entrée dans le *blog* de Mozilla :  
<http://blog.mozilla.com/security/2008/01/04/basicauth-dialog-realm-value-spoofing/>
- RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication", juin 1999 :  
<http://www.ietf.org/rfc/rfc2617.txt>

## 6 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 03 et le 10 janvier 2008.

## 7 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/>

## 8 Rappel des avis émis

Dans la période du 04 au 11 janvier 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-002 : Vulnérabilité dans PHP 4
- CERTA-2008-AVI-003 : Vulnérabilité dans Novell ZENworks Endpoint Security Management
- CERTA-2008-AVI-004 : Vulnérabilité dans AIX
- CERTA-2008-AVI-005 : Vulnérabilités dans PostgreSQL
- CERTA-2008-AVI-006 : Vulnérabilité dans Asterisk
- CERTA-2008-AVI-007 : Multiples vulnérabilités dans Xerox WorkCentre
- CERTA-2008-AVI-008 : Multiples vulnérabilités dans les produits VMware
- CERTA-2008-AVI-009 : Vulnérabilités protocolaires dans Microsoft Windows
- CERTA-2008-AVI-010 : Vulnérabilité dans LSASS de Windows
- CERTA-2008-AVI-011 : Multiples vulnérabilités dans Apache
- CERTA-2008-AVI-012 : Vulnérabilité d'IBM Websphere Application Server
- CERTA-2008-AVI-013 : Vulnérabilité dans Novell Client
- CERTA-2008-AVI-014 : Vulnérabilité dans l'environnement d'exécution Java (JRE)
- CERTA-2008-AVI-015 : Vulnérabilité dans McAfee E-Business Server
- CERTA-2008-AVI-016 : Vulnérabilité dans IBM Lotus Domino

## 9 Actions suggérées

### 9.1 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 réglementaire, 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.

## **9.2 Concevoir une architecture robuste**

À 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.

## **9.3 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.

## **9.4 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.

## **9.5 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.

## **9.6 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 inexplicables 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.

## **9.7 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 :

## 10 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.

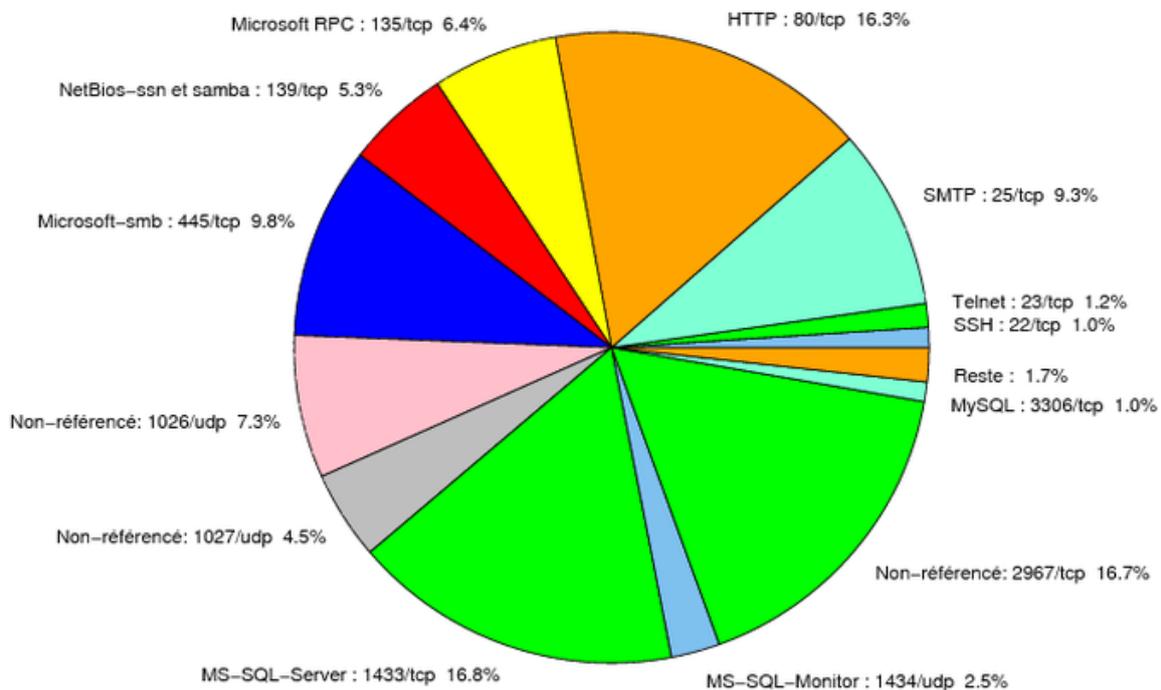


FIG. 1: Répartition relative des ports pour la semaine du 03.01.2008 au 10.01.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
22	TCP	SSH	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
23	TCP	Telnet	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> CERTA-2007-ALE-005-001
25	TCP	SMTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
42	TCP	WINS	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
69	UDP	IBM Tivoli Provisioning Manager	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
80	TCP	HTTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
106	TCP	MailSite Email Server	–	– <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
111	TCP	Sunrpc-portmapper	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
119	TCP	NNTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
135	TCP	Microsoft RPC	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
137	UDP	NetBios-ns	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
139	TCP	NetBios-ssn et samba	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
143	TCP	IMAP	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
389	TCP	LDAP	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
427	TCP	Novell Client	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
443	TCP	HTTPS	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
445	TCP	Microsoft-smb	–	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>

				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 re-  
jetés

port	pourcentage
1433/tcp	16.79
2967/tcp	16.74
80/tcp	16.31
445/tcp	9.82
25/tcp	9.26
1026/udp	7.31
135/tcp	6.41
139/tcp	5.3
1027/udp	4.54
1434/udp	2.48
23/tcp	1.21
22/tcp	1.02
3306/tcp	1
137/udp	0.71
4899/tcp	0.58
1080/tcp	0.34
21/tcp	0.07
9898/tcp	0.02

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	9
3	Paquets rejetés . . . . .	10

## Gestion détaillée du document

11 janvier 2008 version initiale.