Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 septembre 2008
N° CERTA-2008-ACT-037

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2008-37**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2008-ACT-037 |
| Titre | Bulletin d'actualité 2008-37 |
| Date de la première version | 12 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-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-2008-ACT-037/

## 1 Incidents traités cette semaine

### 1.1 Données oubliées

Cette semaine, le CERTA a eu l'occasion de traiter un incident dû à un oubli de l'administrateur d'un site Internet. Lors d'une modification de son site web, l'administrateur avait placé dans un répertoire temporaire une sauvegarde des informations contenues dans une base de données. Une fois son travail effectué, la personne a oublié de nettoyer les données présentes dans le répertoire et ces dernières se sont retrouvées sur l'Internet, accessible à tous. Le CERTA rappelle qu'il est important de vérifier régulièrement le contenu des sites Internet afin de détecter ce type d'oubli ou une éventuelle modification du site. Il existe pour cela différents outils permettant de vérifier l'arborescence d'un site ou de contrôler l'intégrité des pages. Dans le cas présent, les fichiers laissés dans le répertoire temporaire se sont retrouvés indexés par les moteurs de recherche facilitant ainsi les divulgations. Le CERTA insiste également sur la nécessité de régulièrement inspecter les journaux d'événements afférant à l'activité des visiteurs du site web. Cette analyse peut permettre de détecter des comportements suspects et de révéler des données disponibles depuis l'Internet alors que ces dernières devraient être inaccessibles ou tout simplement effacées.

# 2 Un comportement de MySQL : "la troncature des données"

Lors de l'insertion d'une chaine de caractères de longueur supérieure à celle d'une colonne de taille fixe (ex: *char(10)*), la chaîne est tronquée avant d'être insérée et l'avertissement (*warning*) 1265 est levée. Dans la pratique cet avertissement est tout simplement ignoré. Ce comportement mal contrôlé est utilisé dans une exploitation de vulnérabilité mise en ligne cette semaine et visant `WordPress`.

Il est possible de modifier la configuration de la base pour que l'erreur bloquante 1405 soit levée plutôt qu'un avertissement. Pour cela il faut ajouter le mode "`STRICT_ALL_TABLES`" au serveur.

Le CERTA recommande que les variables soient vérifiées avant toute utilisation. Ce contrôle doit avoir lieu au niveau du code du serveur et ne pas reposer sur des limitations de formulaires (taille de champs) ou des scripts de la page, ceux-ci pouvant être facilement contournés.

## 2.1 Exemple de troncature et de configuration

```
mysql> create table coltrunc(nom char(5));
mysql> insert into coltrunc(nom) values("12345");
Query OK, 1 row affected (0.00 sec)

mysql> insert into coltrunc(nom) values("123456");
Query OK, 1 row affected, 1 warning (0.00 sec)
```

On remarque ici l'alerte qui est consultable avec *show warnings*

```
mysql> show warnings ;
+---------+------+-----------------------------------------+
| Level   | Code | Message                                 |
+---------+------+-----------------------------------------+
| Warning | 1265 | Data truncated for column 'nom' at row 1 |
+---------+------+-----------------------------------------+

mysql> select * from coltrunc ;
+-------+
| nom   |
+-------+
| 12345 |
| 12345 |
+-------+
```

Effectivement la consultation de la table retourne bien deux valeurs identiques. On modifie alors le mode du serveur et en essayant d'insérer une donnée trop grande, on obtient une erreur.

```
mysql> set sql_mode='STRICT_ALL_TABLES';
mysql> insert into coltrunc(nom) values("123456");
ERROR 1406 (22001): Data too long for column 'nom' at row 1
```

Dans le cas des vulnérabilités identifiées et corrigées cette semaine, le principe est identique à l'exemple mais s'applique aux tables utilisateur. L'exploitation de cette faille permet d'ajouter de nouvelles entrées pour l'utilisateur `admin` illégitimes (l'exploitation dépendant fortement de l'index et des clés primaires utilisés pour la table).

## 2.2 Documentation

- Configuration des modes de Mysql :
  http://dev.mysql.com/doc/refman/5.0/fr/server-sql-mode.html
- Avis CERTA concertant WordPress:
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-453/index.html
- Article traitant de ce comportement de MySQL :
  http://www.suspekt.org/2008/08/18/mysql-and-sql-column-truncation-vulnerabilities/

# 3 Pages indiscrètes

Cette semaine, le CERTA a prévenu plusieurs administrations que certains de leurs sites contenaient des pages indiscrètes. Dans ce cas précis, il s'agissait de contenus de répertoires visibles, ce qui peut se produire lorsqu'il n'y a pas de fichier d'index (fichier défini par `DirectoryIndex` dans Apache et « document par défaut » dans l'onglet « Documents » de IIS).

Si, dans la plupart des cas, la possibilité de visualisation du contenu des répertoires ne pose pas un grand risque pour un site, une bonne pratique est toutefois de la désactiver. En effet, cela peut faciliter la découverte par une personne malintentionnée des éléments suivants :

- serveur utilisé et version ;
- applications utilisées sur le serveur et leurs versions ;
- date de dernière mise à jour des pages, et donc éventuellement des applications.

D'une manière générale, les serveurs doivent être configurés pour cacher un maximum d'informations sur leur fonctionnement.

Pour désactiver l'affichage du contenu des répertoires (et provoquer l'affichage d'une erreur HTTP 403) dans Apache, il faut désactiver l'option `Indexes` :

```
<Directory monrépertoire/>
  Options -Indexes
  ...
</Directory>
```

Les options des répertoires sont héritées et celle-ci n'est pas désactivée par défaut.

Dans IIS 6.0, il faut décocher la case « Exploration du répertoire » (ou « Directory Browsing ») dans les options de sites Internet, ce qui semble être le cas par défaut.

# 4 Traitement d'un rootkit sous Windows

Cette semaine, le CERTA a traité le cas d'une machine sous Windows XP SP3 sur laquelle était installée un *rootkit* (ensemble d'outils modifiant le comportement du système, typiquement pour camoufler l'activité d'un intrus). L'objet de cet article est de présenter deux approches différentes pour nettoyer la machine, avec leurs avantages et inconvénients.

## 4.1 Réinstallation complète du système

Lorsqu'une machine est compromise, le CERTA préconise généralement une réinstallation complète du système. Cette méthode présente l'avantage de faire disparaître tous les éléments susceptibles de modifier le système. Elle est particulièrement bien adaptée aux systèmes Linux, mais elle présente quelques inconvénients sous Windows :

- le système Windows s'appuie sur une base appelée registre qui peut être vue comme un gros fichier de configuration (le registre est en fait composé de plusieurs fichiers). La réinstallation complète du système réinitialise cette base. Or, la plupart des logiciels installés sous Windows inscrivent des informations essentielles dans le registre. La réinitialisation du registre implique donc la nécessité de réinstaller tous les logiciels, ce qui est une opération très fastidieuse. De plus, il est nécessaire de remettre à jour toutes les applications ;
- lors de l'installation du système, il faut créer un compte utilisateur. Si l'on réutilise le même nom d'utilisateur que lors de l'installation précédente, cela crée un doublon, avec une deuxième arborescence. Par exemple, si, avant compromission, le système n'avait qu'un utilisateur `Alice` et que l'on décide de recréer l'utilisateur `Alice` lors de la réinstallation, le système contiendra les répertoires suivants (sous Windows XP) :
  `\Documents and Settings\Alice\`
  et
  `\Documents and Settings\Alice.`*nom_ordi*
  Certains utilisateurs stockent leurs documents dans le répertoire `Mes Documents` qui est une sous-arborescence du compte utilisateur. Par conséquent, il faut penser à recopier les fichiers dans le nouveau compte utilisateur. Après plusieurs installations, si le compte utilisateur est toujours le même, de nombreux comptes utilisateurs sont créés, ce qui peut engendrer de la confusion.

### 4.2 Nettoyage du système en supprimant le rootkit

La suppression simple des codes malveillants semble être une solution séduisante (mais déconseillée) car relativement rapide. Toutefois, elle se heurte à quelques problèmes. En effet, le *rootkit* découvert dans cette affaire modifiait le comportement des routines `Zw`*xXx*, ce qui avait pour effet d'empêcher la désinstallation des fichiers concernés, ainsi que des clés de registre. La méthode choisie consiste donc à redémarrer sur un autre système. Plusieurs possibilités s'offrent à nous, notamment :

- redémarrer en mettant le disque dur en esclave d'un autre Windows. L'avantage est que NTFS (le système de fichiers typiquement utilisé avec Windows XP) est reconnu. L'inconvénient en revanche est que toute mauvaise manipulation est susceptible de propager un code malveillant sur le système sain utilisé lors de l'opération ;
- redémarrer depuis un Linux (par exemple avec une distribution telle que *Knoppix*). La difficulté consiste à pouvoir effectuer des opérations d'écriture sur un système NTFS depuis Linux, ce qui n'est pas toujours possible nativement. Cette opération est réalisable par exemple en utilisant `ntfs-3g`.

Cette méthode permet d'effacer les codes malveillants, mais il faut encore effectuer une étape supplémentaire qui consiste à purger la base de registre de toute référence aux fichiers effacés.

### 4.3 Conclusion

La suppression du code malveillant semble être très séduisante de prime abord, car elle permet de s'affranchir des diverses réinstallations. Elle se révèle toutefois plus compliquée car elle nécessite de disposer d'un second système sain, et que l'on ne peut jamais être sûr que le code malveillant est intégralement désinstallé. Au final, la réinstallation complète du système ne prend pas forcément beaucoup plus de temps, mais est en revanche susceptible d'engendrer une confusion importante dans le système de fichiers, notamment au niveau des comptes utilisateur.

## 5 La problématique des mises à jour automatiques

Le CERTA rappelle très souvent qu'il est important d'appliquer des correctifs de sécurité afin d'avoir un système et des applications à jour. Cette remarque avait également fait l'objet d'une note d'information CERTA-2001-INF-004, « Acquisition des correctifs ».

L'objet de cet article n'est pas de rappeler une nouvelle fois ce bon principe, mais de souligner qu'il est important de bien maîtriser cette étape dans le cadre d'une gestion d'un parc informatique.

Les composants physiques vendus dans le commerce, tout comme les applications installées sur les machines, offrent souvent la possibilité de faire des mises à jour automatiques.

Citons à valeur d'exemple : des points d'accès sans-fil, des applications de bureautique, des navigateurs, des lecteurs de fichiers PDF, etc.

Ce choix de mise à jour automatique est proposé par défaut dans plusieurs installations. Il est également choisi par l'administrateur car il permet de s'affranchir de la vérification périodique d'annonces de mises à jour.

Derrière cette apparente simplification des tâches se cache un problème de sécurité plus important : ce processus de mise à jour doit être compris et maîtrisé.

Pour chacune des mises à jour, il faut pouvoir répondre aux questions suivantes :

- quelles sont les informations échangées avec le serveur de mise à jour distant ?
- par quel protocole s'effectuent les communications avec le serveur distant ?
- les échanges sont-ils chiffrés afin de garantir la confidentialité des informations échangées (version, état des machines, etc.) ?
- les mises à jour sont-elles authentifiées ?

Comment faire pour parvenir à répondre aux questions précédentes ? Voici quelques éléments de réponse :

- lire la documentation associée ;
- demander directement aux éditeurs/producteurs/vendeurs ;
- contrôler par des captures d'activités réseau et système le processus de mise à jour depuis une plate-forme de test.

Si ces différentes approches ne permettent pas de répondre, alors il faut considérer l'étape de mise à jour comme une tâche obscure sur et depuis le système. La plus grande méfiance doit être accordée à ce dernier. Il ne peut plus être considéré comme un système de confiance au sein du réseau.

# 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 04 et le 11 septembre 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 05 au 11 septembre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-437 : Vulnérabilité dans ClamAV
- CERTA-2008-AVI-438 : Vulnérabilité dans IBM AIX
- CERTA-2008-AVI-439 : Vulnérabilité du noyau de FreeBSD pour plateforme amd64
- CERTA-2008-AVI-440 : Multiples vulnérabilités dans VLC
- CERTA-2008-AVI-441 : Multiples vulnérabilités des équipements Cisco ASA et PIX
- CERTA-2008-AVI-442 : Multiples vulnérabilités dans Novell eDirectory
- CERTA-2008-AVI-443 : Vulnérabilité dans OpenOffice.org
- CERTA-2008-AVI-444 : Multiples vulnérabilités dans Wireshark
- CERTA-2008-AVI-445 : Multiples vulnérabilités dans les produits VMware
- CERTA-2008-AVI-446 : Vulnérabilité dans Cisco Secure ACS
- CERTA-2008-AVI-447 : Vulnérabilité dans libtiff
- CERTA-2008-AVI-448 : Multiples vulnérabilités dans IBM DB2
- CERTA-2008-AVI-449 : Vulnérabilités dans la bibliothèque Microsoft Windows GDI+
- CERTA-2008-AVI-450 : Vulnérabilité dans Windows Media Encoder 9 Series
- CERTA-2008-AVI-451 : Vulnérabilité dans Windows Media
- CERTA-2008-AVI-452 : Vulnérabilité dans Microsoft Office
- CERTA-2008-AVI-453 : Vulnérabilités de WordPress

– CERTA-2008-AVI-454 : Vulnérabilité de iTunes
– CERTA-2008-AVI-455 : Multiples vulnérabilités dans Quicktime
– CERTA-2008-AVI-456 : Vulnérabilités de Joomla!

# 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 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.

## 9.2 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.

## 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 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 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.

### 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 :

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

## 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.

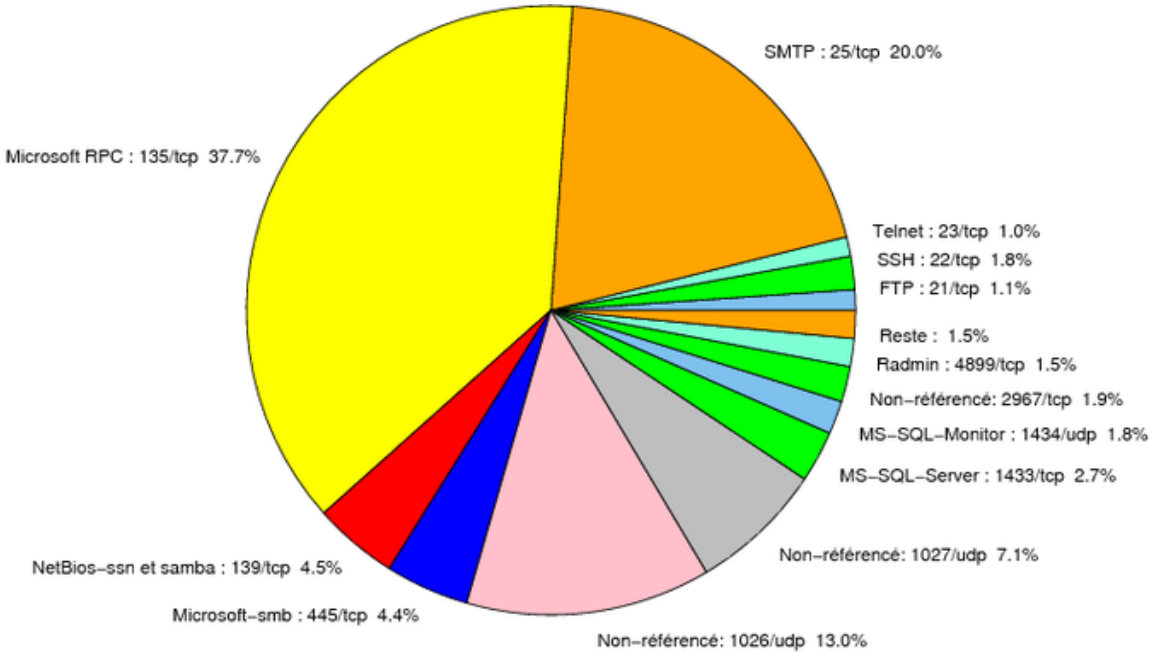


FIG. 1: Répartition relative des ports pour la semaine du 04.09.2008 au 11.09.2008

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>CERTA-2007-ALE-005-001 |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 106 | TCP | MailSite Email Server | – | –<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |

| | | | | |
|---|---|---|---|---|
| | | | | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>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<br>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<br>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 | 37.72 |
| 25/tcp | 20 |
| 1026/udp | 12.99 |
| 1027/udp | 7.12 |
| 445/tcp | 4.5 |
| 1433/tcp | 2.73 |
| 2967/tcp | 1.88 |
| 1434/udp | 1.76 |
| 4899/tcp | 1.48 |
| 23/tcp | 1.08 |
| 137/udp | 0.62 |
| 80/tcp | 0.34 |
| 1080/tcp | 0.22 |
| 3128/tcp | 0.17 |
| 3127/tcp | 0.11 |
| 3389/tcp | 0.05 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**11 septembre 2008** version initiale.