Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 avril 2010
N° CERTA-2010-ACT-017

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2010-17**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2010-ACT-017 |
| Titre | Bulletin d'actualité 2010-17 |
| Date de la première version | 30 avril 2010 |
| Date de la dernière version | – |
| Source(s) | – |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-017.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-017/

## 1 Vulnérabilité Microsoft Sharepoint

Microsoft a publié le 29 Avril 2010 un avis Sharepoint concernant une vulnérabilité non corrigée de type injection de code indirecte.

La vulnérabilité permet à un attaquant d'exécuter du code *JavaScript* dans le contexte de la session Sharepoint de l'utilisateur. L'exploitation de cette vulnérabilité nécessite que l'utilisateur ait une session ouverte sur un site Sharepoint vulnérable, et que dans le même temps, il clique sur un lien malveillant.

Les versions de Sharepoint affectées sont :

- Microsoft Office SharePoint Server 2007 Service Pack 1 et 2 ;
- Microsoft Windows SharePoint Services 3.0 Service Pack 1 et 2.

En attendant un correctif, une solution de contournement est documentée dans l'avis Microsoft 983438 :
http://www.microsoft.com/technet/security/advisory/983438.mspx

# 2 ZFS et enjeux de sécurité

ZFS (Z File System) est le système de fichiers utilisé par défaut sur les systèmes d'exploitation Sun Solaris et OpenSolaris. Il est distribué sous licence CDDL (Common Development and Distribution License) Il est également supporté par FreeBSD nativement et par Linux via FUSE (File System in Userland). Ce système dans sa conception et dans son mode de fonctionnement est totalement à part des autres systèmes de fichiers plus traditionnels comme NTFS, ext3 ou même le récent ext4.

En effet, d'un point de vue fonctionnalité, il présente un certain nombre d'avantages non-négligeables. Par exemple, les fonctionnalités de type LVM (Logical Volume Manager) sont intégrées directement au système. Il est ainsi possible d'agréger plusieurs volumes physiques dans un seul et même *pool* (équivalent à un *Volume Group* pour LVM). Mais ce concept est poussé encore plus loin car ce *pool* n'est pas découpé en partitions de tailles fixes. Le *pool* constitue lui même le système dans le lequel on va créer différentes « découpages » se partageant l'espace total disponible.

Par exemple, on aura un *pool* principal que l'on nommera *lepool* découpé en différentes parties : racine , usr, home, var. Pour chaque découpage, on pourra attribuer un point de montage :

- lepool/racine -> /
- lepool/usr -> /usr
- lepool/home -> /home
- lepool/var -> var

L'intérêt est de partager l'espace dynamiquement entre les différents découpages. Il est ainsi aisé de rajouter dans un *pool* un disque supplémentaire pour étendre l'espace disponible.

D'autres fonctionnalités intéressantes sont intégrées dans ZFS. Dans les principales, on pourra citer :

- des technologies de RAID 1, 5 et 6 intégrées nativement ;
- une capacité de prise d'instantanés : *snapshots* ;
- des fonctionnalités de réplication : *cloning*.

En matière de fonctionnalités et de souplesse d'utilisation, ZFS est vraiment très intéressant mais lors d'une analyse *a posteriori*, il peut poser un certain nombre de problèmes.

Ainsi, le fait d'agréger plusieurs volumes physiques ou encore le partage dynamique de l'espace disponible entres différentes « partitions » peut poser des problèmes de fragmentation d'information lorsque l'on voudra récupérer des données en faisant abstraction du système de fichiers. Comme dans le cas de disques en RAID 5 ou 6 , il est nécessaire d'avoir une copie de l'intégralité des disques (ou au moins *n-1* en fait) même s'ils sont loin d'être pleins pour disposer de données exploitables.

Ceci ne facilite pas forcément la phase d'acquisition des données surtout avec de gros volumes. En particulier la récupération des données dans des blocs désalloués sera sans doute délicate.

*À contrario*, le fait de disposer de fonctionnalités de *snapshot* et de *clone* peut aider à préserver des traces en attendant une copie ultérieure des données.

### Recommandations :

Dans le cas d'une compromission et surtout lorsque les volumes de stockage sont très importants, la réalisation d'un snapshot dès la détection du problème peut être une solution pour conserver les traces et indices même si une copie reste la solution à privilégier. En effet, le fait de réaliser ainsi un instantané engendrera de nombreuses écritures sur les disques pouvant altérer d'éventuelles traces dans des blocs désalloués.

# 3 Snort 2.8.6

Une nouvelle version de l'outil de détection d'intrusion Snort a été publiée le 26 avril 2010.

Outre quelques améliorations mineures et un changement de nom du fichier des règles, elle apporte trois nouveautés, présentées brièvement ci-dessous.

## 3.1 Détection de données dites « sensibles »

Par l'intermédiaire du préprocesseur *sensitive_data* et du mot clé *sd_pattern*, le système peut émettre une alerte quand il voit transiter des données sensibles. Par exemple, une alerte peut être déclenchée quand deux numéros de carte bancaire apparaissent dans une session. Pour l'instant, il y a un nombre limité de types de données sensibles (dont les adresses de messagerie), reconnues grâce à des expression régulières. Il existe cependant la possibilité de définir ses propres types avec une expression régulière dédiée.

Il reste à voir sur quels flux appliquer ce préprocesseur et quel est le taux de faux-positifs. Afin de réduire ce taux, les numéros de carte banquaire sont vérifiés par l'algorithme de Luhn (tests sur les sommes et les divisions par 10 des chiffres du numéro).

```
Fichier dynamic-preprocessors/sdf/spp_sdf.h
(...)
/* Keywords for SDF built-in option */
#define SDF_CREDIT_KEYWORD "credit_card"
#define SDF_CREDIT_PATTERN "\\d{15}\\d?"
#define SDF_CREDIT_PATTERN2 "\\d{4} \\d{4} \\d{4} \\d{4}"
#define SDF_CREDIT_PATTERN_AMEX "\\d{4} \\d{6} \\d{5}"

/* This pattern matches Visa/Mastercard/Amex, with & without spaces or dashes.
   The pattern alone would match other non-credit patterns, but the function
   SDFLuhnAlgorithm() does stricter checking. */
#define SDF_CREDIT_PATTERN_ALL "\\d{4} ?-?\\d{4} ?-?\\d{2} ?-?\\d{2} ?-?\\d{3}\\d?"
(...)
```

Une alerte proposée par défaut dans le fichier `sensitive_data.rules` est par exemple :

```
alert $HOME_NET any -> $EXTERNAL_NET [80,20,25,143,110] (
msg:"SENSITIVE-DATA Credit Card Numbers";
metadata:
service http,
service smtp,
service ftp-data,
service imap,
service pop3;
sd_pattern:2,credit_card;
classtype:sdf; sid:2; gid:138; rev:1;)
```

Cette alerte signifie simplement que les caractéristiques des expressions régulières précédentes sont cherchées dans les flux *HTTP*, *SMTP*, *FTP*, *IMAP* et *POP3* (pour les ports associés renseignés). Les fonctions de recherche sont propres à ce préprocesseur.

De manière générale, il est important de bien comprendre le fonctionnement des processus de détection afin de pouvoir interpréter la remontée (ou l'absence de remontée) des alertes. Ainsi, par exemple, le lecteur comprendra que toute donnée correspondant à ces expressions régulières et étant conforme selon les quelques tests de validité effectués, pourra engendrer une alerte. De la même manière, toute transmission masquée d'un numéro de carte ne sera probablement pas prise en compte.

## 3.2 Optimisation de la reconnaissance de motifs

On peut obtenir un gain de performances par l'ajout judicieux du nouveau mot-clé `fast-pattern` dans les règles adaptées. Ce mot-clé existait déjà mais il comprend maintenant plus d'options.

C'est une bonne nouvelle qu'il faut toutefois nuancer.

Le moteur de reconnaissance de motifs n'est pas fondamentalement changé. Ainsi, les performances ne seront améliorées que si des règles le sont. De plus, seulement certaines règles peuvent être optimisées (elles doivent contenir au moins deux motifs) et il faut une certaine expertise humaine pour que cette modification entraîne un gain de performance.

En effet, le mot-clé `fast-pattern` permet de choisir manuellement plutôt qu'automatiquement le premier motif cherché. Seulement, dans les cas où ce motif est trouvé, les autres conditions de la règle seront testées. Ce motif doit donc être le plus restrictif possible. En règle générale, Snort prendra le plus long motif mais il ne fait pas toujours le meilleur choix. Cette nouvelle option permet d'outrepasser le comportement par défaut, d'écrire des règles plus intelligemment et finalement d'obtenir un gain de performances qui reste à quantifier.

La société `Sourcefire` devrait passer en revue l'ensemble des règles actives pour voir celles qui peuvent être optimisées.

### 3.3 Nouveau préprocesseur HTTP

Plusieurs améliorations ont été apportées au préprocesseur *HTTP*.

Tout d'abord, la compression gzip (couramment utilisée) est supportée sur plusieurs paquets. Toutefois, les contenus décompressés sont inspectés individuellement.

De plus, le préprocesseur sépare les requêtes (et les réponses) en 5 composants : méthode, URI, en-tête, cookie et corps. Il est alors possible d'écrire des règles avec des options relatives uniquement au contenu de ces composants (motif fixe ou expression régulière). La normalisation de ces différents champs est configurable au niveau du préprocesseur mais une règle peut l'outrepasser.

### 3.4 Références

- Site officiel de Snort :
  http://www.snort.org
- Bloc-notes Sourcefire, "Using Snort fast patterns wisely for fast rules" :
  http://vrt-sourcefire.blogspot.com/2010/04/using-snort-fast-patterns-wisely-for.html

## 4 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information du CERTA sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
- Note d'information du CERTA sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
- Note d'information du CERTA sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
  http://www.auscert.org.au/render.html?it=1937
- Note d'information du CERTA sur les risques associés aux clés USB :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
- Note d'information du CERTA sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA sur la gestion des noms de domaine :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information du CERTA sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

## 5 Rappel des avis émis

Dans la période du 23 au 29 avril 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-195 : Vulnérabilité dans les routeurs 3Com H3C SR6600
- CERTA-2010-AVI-196 : Multiples vulnérabilités de IBM DB2
- CERTA-2010-AVI-197 : Multipes vulnérabilités dans Google Chrome

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

- CERTA-2010-AVI-020-001 : Vulnérabilité dans BIND DNSSEC (ajout de la référence au bulletin Oracle (Sun))
- CERTA-2010-AVI-164-001 : Vulnérabilité dans TheGreenBow (révision de l'impact)

# 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'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.

## 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 oeuvre (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 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique67.html

## 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.

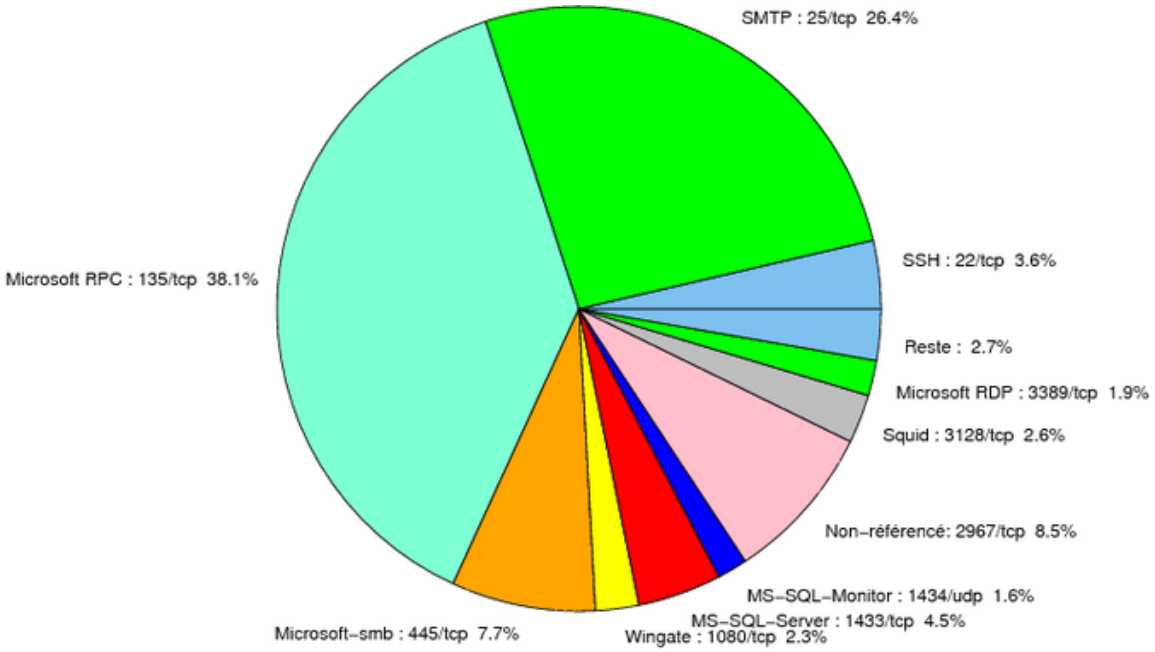


FIG. 1: Répartition relative des ports pour la semaine du 23 au 29 avril 2010

| 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 | 38.14 |
| 25/tcp | 26.36 |
| 2967/tcp | 8.48 |
| 445/tcp | 7.71 |
| 1433/tcp | 4.48 |
| 22/tcp | 3.64 |
| 3128/tcp | 2.59 |
| 1080/tcp | 2.31 |
| 3389/tcp | 1.89 |
| 1434/udp | 1.61 |
| 80/tcp | 0.7 |
| 3127/tcp | 0.56 |
| 4899/tcp | 0.42 |
| 3306/tcp | 0.28 |
| 1026/udp | 0.14 |
| 111/tcp | 0.07 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**30 avril 2010** version initiale.