Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 septembre 2006
N° CERTA-2006-ACT-039

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2006-39**

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-2006-ACT-039`

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2006-ACT-039 |
| Titre | Bulletin d'actualité 2006-39 |
| Date de la première version | 29 septembre 2006 |
| Date de la dernière version | – |
| Source(s) | |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – *Gestion du document*

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

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-039.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-039/

## 1 Bulletins de sécurité Microsoft

### 1.1 Vulnérabilité VML de la librairie VGX.DLL

Microsoft a publié de manière exceptionnelle un correctif décrit dans le bulletin MS06-055, mardi 26 septembre 2006. L'application de ce dernier corrige une vulnérabilité affectant la bibliothèque `vgx.dll` (CVE-2006-4868). Cette bibliothèque est utilisée pour prendre en compte le format `VML` (pour *Vector Markup Language*).

Un vecteur d'attaque consiste à construire et à publier des pages HTML qui exploitent la faille par l'intermédiaire d'Internet Explorer. Cependant, toute application faisant appel à cette bibliothèque peut être considérée comme vulnérable (messagerie électronique Outlook, visionneuse d'images, etc.).

Plusieurs codes malveillants circulent déjà dans l'Internet, les noms attribués variant selon les marques des produits de sécurité :

- HTML/Levem.C (Microsoft)
- Trojan.Vimalov (Symantec)
- Exploit.HTML.VML.a (F-Secure, Kaspersky)
- Exploit-VMLFill (McAfee)
- Troj/Dloadr-ANO, Troj/Goldun (Sophos)

– JS/Veemyfull!exploit (CA)

Le CERTA recommande vivement d'appliquer le correctif associé au bulletin MS06-055, et a publié l'avis CERTA-2006-AVI-410 le 27 septembre 2006 à ce sujet.

### 1.2 Mise à jour du bulletin MS06-049

Microsoft a mis à jour le 26 septembre 2006 le correctif correspondant au bulletin de sécurité MS06-049. Le bulletin initial corrigeait une vulnérabilité dans le noyau Windows. Celle-ci permettrait à un utilisateur local au système vulnérable d'élever ses privilèges et d'en prendre le contrôle.

L'application du correctif initial peut entraîner certaines erreurs pour les systèmes utilisant de la compression de fichiers NTFS. Les fichiers compressés dont la taille excède 4ko peuvent être corrompus au cours de leur manipulation. Il est donc recommandé aux utilisateurs de Windows 2000 SP4 employant la compression de fichiers NTFS d'appliquer la mise à jour du correctif.

## 2 Vulnérabilité non corrigée dans Microsoft Office Powerpoint

Une vulnérabilité concernant Microsoft Office a été publiée, ainsi qu'un code pour l'exploiter. Elle impliquerait les différentes versions de l'application Powerpoint.

Un utilisateur malveillant peut construire un document au format Powerpoint de façon particulière. Ce dernier permettrait d'exécuter du code arbitraire dans tout système vulnérable sur lequel le document serait ouvert.

Il est fortement recommandé de n'accepter que les documents provenant de sources de confiance.

Un contournement consiste aussi à convertir ses propres documents Powerpoint en `.pdf` (pour *Portable Document Format* et de n'accepter que les transparents sous ce même format. Ceux-ci peuvent être lu par plusieurs lecteurs et visualiser en mode `diaporama`.

– Avis de sécurité Microsoft 925984 du 27 septembre 2006 :
  http://www.microsoft.com/technet/security/advisory/925984.mspx
– Référence CVE associée CVE-2006-4694 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4694
– Alerte du CERTA CERTA-2006-ALE-011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-011/

## 3 OpenSSH

Le CERTA a publié l'avis de sécurité CERTA-2006-AVI-411 au sujet d'une vulnérabilité dans OpenSSH concernant la possibilité de réaliser un déni de service via un paquet SSH spécialement construit. Il convient de noter que cette vulnérabilité ne concerne que la version 1 du protocole SSH. Cette version de protocole était déjà considérée comme non sûre. Il est important de vérifier que vos serveurs SSH ne concervent pas le support de cette version. Ils devront être impérativement configurer pour ne supporter que la version 2 du prototole. Pour s'en assurer, il suffit de vérifier que la directive `Protocol` est fixée uniquement à 2 dans le fichier `sshd_config`.

## 4 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 21 et le 28 septembre 2006.

**Documentation :**

– Alerte CERTA-2006-ALE-011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-011
– Bulletin de sécurité 925568 de Microsoft du 21 septembre 2006 :
  http://www.microsoft.com/technet/security/advisory/925568.mspx
– Bulletin de sécurité VU#416092 de l'US-CERT du 21 septembre 2006 :
  http://www.kb.cert.org/vuls/id/416092

# 5 Liens utiles

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

# 6 Rappel des avis et mises à jour émis

Durant la période du 15 au 21 septembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-406 : Vulnérabilités d'Apple AirPort
- CERTA-2006-AVI-407 : Vulnérabilités dans HP-UX
- CERTA-2006-AVI-408 : Vulnérabilités dans HP-UX
- CERTA-2006-AVI-409 : Vulnérabilités dans CA
- CERTA-2006-AVI-410 : Vulnérabilité du système Microsoft Windows
- CERTA-2006-AVI-411 : Vulnérabilité dans OpenSSH
- CERTA-2006-AVI-412 : Vulnérabilité dans GnuTLS
- CERTA-2006-AVI-413 : Multiples vulnérabilités dans gzip

Pendant cette même période, l'alerte suivante a été mise à jour :

- CERTA-2006-AVI-222-001 : Vulnérabilités de cURL
  (ajout des références aux bulletins de sécurité SuSE, Ubuntu et Mandriva)
- CERTA-2006-AVI-301-002 : Multiples vulnérabilités dans Ethereal/Wireshark
  (ajout des références aux bulletins de sécurité Avaya, SuSE et Red Hat)
- CERTA-2006-AVI-332-001 : Multiples vulnérabilités dans PHP
  (ajout des références aux bulletins de sécurité Red Hat et Mandriva)
- CERTA-2006-AVI-347-001 : Vulnérabilité du noyau de Windows 2000
  (ajout de la référence CVE et de la nouvelle mise à jour du bulletin MS06-049)
- CERTA-2006-AVI-351-003 : Vulnérabilité de SquirrelMail
  (ajout des bulletins de sécurité SuSE et Red Hat)
- CERTA-2006-AVI-361-002 : Vulnérabilité dans ImageMagick
  (ajout de la référence au bulletin de sécurité de Gentoo)
- CERTA-2006-AVI-391-002 : Multiples vulnérabilités dans les produits Mozilla
  (ajout des références aux bulletins de sécurité Ubuntu, Red Hat)
- CERTA-2006-AVI-411-001 : Vulnérabilité dans OpenSSH
  (ajout de la section `Contournement provisoire`)

# 7 Actions suggérées

## 7.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

## 7.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

## 7.3 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.

## 7.4 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.

## 7.5 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.

## 7.6 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.

### 7.7 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

## 8 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.

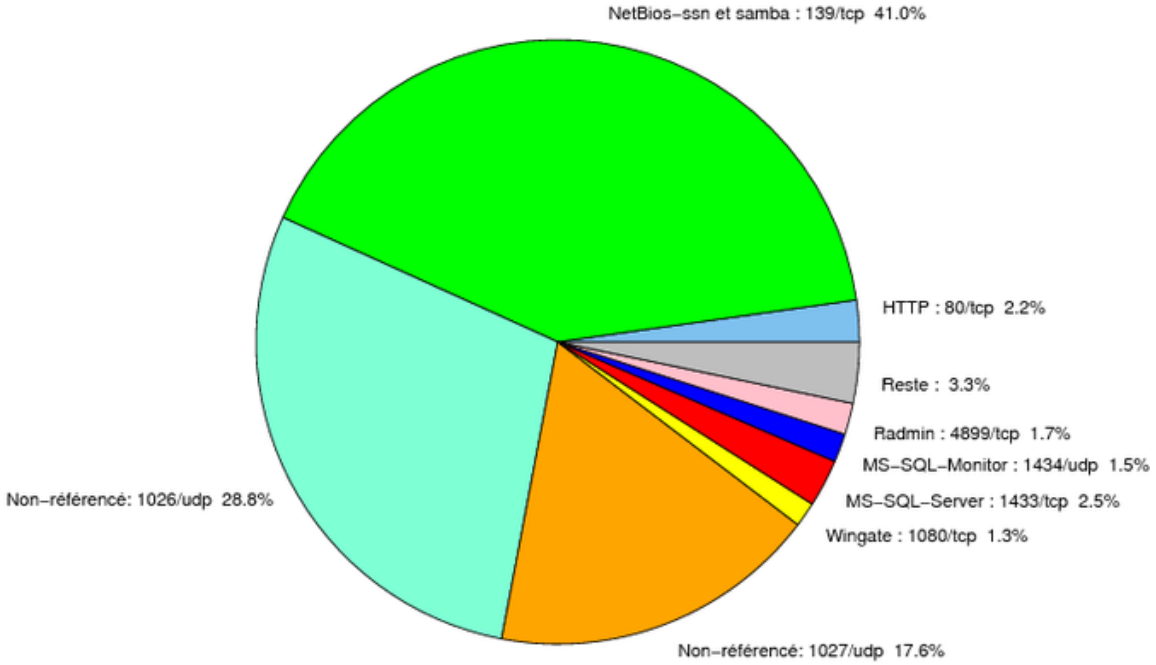


FIG. 1: Répartition relative des ports pour la semaine du 21.09.2006 au 28.09.2006

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 42 | TCP | WINS | – | http://www.certa.ssi.gouv.fr/site/CE |
| 80 | TCP | HTTP | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 106 | TCP | MailSite Email Server | – | – |
| 111 | TCP | Sunrpc-portmapper | – | http://www.certa.ssi.gouv.fr/site/CE |
| 119 | TCP | NNTP | – | http://www.certa.ssi.gouv.fr/site/CE |
| 135 | TCP | Microsoft RPC | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 137 | UDP | NetBios-ns | – | http://www.certa.ssi.gouv.fr/site/CE |
| 139 | TCP | NetBios-ssn et samba | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 143 | TCP | IMAP | – | http://www.certa.ssi.gouv.fr/site/CE |
| 389 | TCP | LDAP | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 443 | TCP | HTTPS | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 1023 | TCP | – | Serveur ftp de Sasser.E | – |
| 1080 | TCP | Wingate | MyDoom.F | http://www.certa.ssi.gouv.fr/site/CE |
| 1433 | TCP | MS-SQL-Server | – | http://www.certa.ssi.gouv.fr/site/CE |
| 1434 | UDP | MS-SQL-Monitor | – | http://www.certa.ssi.gouv.fr/site/CE |
| 2100 | TCP | Oracle XDB FTP | – | http://www.certa.ssi.gouv.fr/site/CE |

| | | | | |
|---|---|---|---|---|
| 2381 | TCP | – | HP System Management | http://www.certa.ssi.gouv.fr/site/CE |
| 2745 | TCP | – | Bagle | – |
| 2967 | TCP | – | Symantec Antivirus | http://www.certa.ssi.gouv.fr/site/CE |
| 3127 | TCP | – | MyDoom | – |
| 3128 | TCP | Squid | MyDoom | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 3306 | TCP | MySQL | – | – |
| 3389 | TCP | Microsoft RDP | – | http://www.certa.ssi.gouv.fr/site/CE |
| 4899 | TCP | Radmin | – | – |
| 5000 | TCP | Universal Plug and Play | Bobax, Kibuv | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 5554 | TCP | SGI ESP HTTP | Serveur ftp de Sasser | – |
| 5900 | TCP | VNC | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 6070<br>6101 | TCP<br>TCP | BrightStor ARCserve/Enterprise Backup<br>Veritas Backup Exec | –<br>– | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 6112 | TCP | Dtspcd | – | http://www.certa.ssi.gouv.fr/site/CE |
| 6129 | TCP | Dameware Miniremote | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 8866 | TCP | – | Porte dérobée Bagle.B | – |
| 9898 | TCP | – | Porte dérobée Dabber | – |
| 10000 | TCP | Webmin, Veritas Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CE<br>http://www.certa.ssi.gouv.fr/site/CE |
| 10080 | TCP | Amanda | MyDoom | – |
| 13701 | TCP | Veritas NetBackup | – | http://www.certa.ssi.gouv.fr/site/CE |
| 18264 | TCP | CheckPoint interface | – | http://www.certa.ssi.gouv.fr/site/CE |

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

| port | pourcentage |
|---|---|
| 139/tcp | 41.01 |
| 1026/udp | 28.78 |
| 1027/udp | 17.63 |
| 1433/tcp | 2.54 |
| 80/tcp | 2.22 |
| 4899/tcp | 1.67 |
| 1434/udp | 1.52 |
| 1080/tcp | 1.32 |
| 137/udp | 0.91 |
| 3128/tcp | 0.63 |
| 3306/tcp | 0.54 |
| 25/tcp | 0.43 |
| 22/tcp | 0.34 |
| 21/tcp | 0.1 |
| 11768/tcp | 0.08 |
| 3389/tcp | 0.04 |
| 111/tcp | 0.02 |

TAB. 3: Paquets rejetés

# Liste des tableaux


1 Gestion du document . . . . . 1
2 Correctifs correspondant aux ports destination des paquets rejetés . . . . . 7
3 Paquets rejetés . . . . . 8


# Gestion détaillée du document

**29 septembre 2006** version initiale.