Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2006
N° CERTA-2006-ACT-003

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-03

Gestion du document

Référence	CERTA-2006-ACT-003
Titre	Bulletin d'actualité 2006-03
Date de la première version	20 janvier 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-003.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-003/

1 Activité en cours

1.1 Incidents traités

Un cas de déni de service par `mail bombing` (envoi massif de messages électroniques) sur un serveur de messagerie a été signalé. Il est assez difficile de déterminer si le but était vraiment de saturer le serveur ou bien s'il s'agissait de l'envoi d'un `spam` adressé à de très nombreux destinataires, inexistants pour la plupart.

1.2 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 29 décembre 2005 et le 05 janvier 2006.

1.2.1 Activité sur le port 106/tcp

Le CERTA constate depuis quelques semaines une importante activité sur le port 106/tcp. Cette activité a été confirmée par de très nombreux correspondants. Les adresses IP à l'origine de ce trafic ne sont pas nombreuses. Le

CERTA ne connaît pas la raison de cette activité. Une vulnérabilité affectant `Rockliffe MailSite Email Server` et permettant de récupérer la liste des utilisateurs en envoyant des requêtes sur le port 106/tcp a récemment été dévoilée (le 05 janvier 2006), mais nous ne pouvons pas affirmer que le trafic observé reflète des tentatives d'exploitation de cette vulnérabilité. Même si le nombre de rejets est assez bas (certains de nos correspondants constatent toutefois plusieurs milliers de paquets de ce type), il reste inhabituel pour ce port.

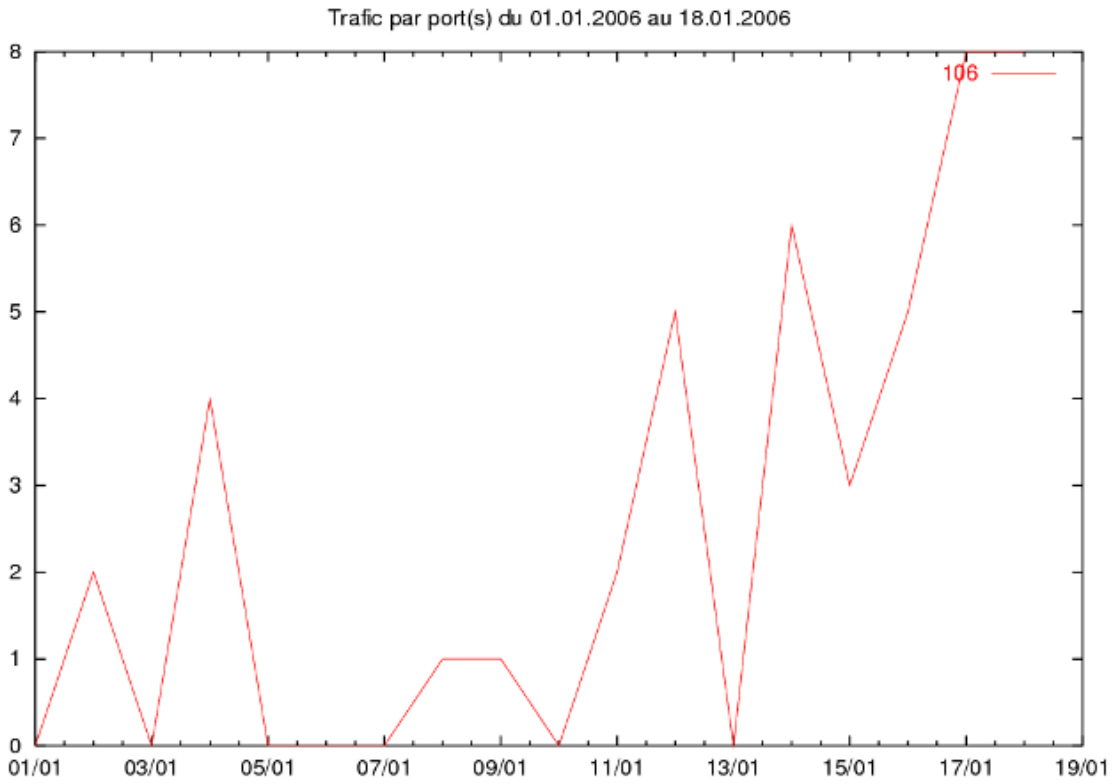

FIG. 1: Évolution des rejets sur le port 106/tcp depuis le 01/01/06

1.2.2 Activité sur le port 13701/tcp

Un outil permettant d'exploiter automatiquement une vulnérabilité de `Veritas NetBackup` (voir CERTA-2005-AVI-447) a récemment été mis à disposition sur l'Internet. Il en résulte l'apparition de trafic à destination du port 13701/tcp.

Recommandation :

Il est fortement recommandé de filtrer le port 13701/tcp qui est associé à `Veritas NetBackup` et d'appliquer le correctif conformément à votre politique de sécurité.

2 Hébergement mutualisé et traitement d'incident

Le CERTA a une nouvelle fois mis en évidence cette semaine, à l'occasion d'un traitement d'incident, le problème de l'hébergement mutualisé des serveurs web. Dans le cas traité, certains sites Internet d'un de nos correspondants étaient co-hébergés avec plus de 40 autres sites, ce qui a compliqué la résolution de l'incident. Il est plus difficile de faire procéder à une modification de configuration ou d'accéder aux journaux du serveur en cas de co-hébergement. A cette occasion, il est à nouveau observé à quel point l'aspect sécurité n'est pas toujours pris en compte contractuellement dans ces hébergements. Ainsi, les conditions d'hébergements risquent parfois d'être en totale incohérence avec les exigences opérationnelles portées par ces sites. Il ne s'agit pas de remettre en cause la notion d'hébergement mutualisé, mais que chacun prenne conscience des risques et des conséquences d'un tel choix. A ce propos, le CERTA a diffusé une note d'information (CERTA-2005-INF-005) en décembre

2005 fournissant un ensemble de bonnes pratiques dans la relation avec les hébergeurs. Cette note à disponible à l'adresse :

http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html

3 Liens utiles

- Mémento sur les virus ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf
- Note d'information sur l'acquisition de correctifs ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information pour 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
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien)
  http://www.auscert.org.au/render.html?it=1935

4 Rappel des avis et mises à jour émis

Durant la période du 13 au 19 janvier 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-024 : Vulnérabilité de PostgreSQL pour Windows
- CERTA-2006-AVI-025 : Vulnérabilité dans les produits Aironet Access Points de Cisco
- CERTA-2006-AVI-026 : Vulnérabilité de Solaris 10
- CERTA-2006-AVI-027 : Vulnérabilité dans Solaris
- CERTA-2006-AVI-028 : Vulnérabilité de grsecurity
- CERTA-2006-AVI-029 : Vulnérabilité des téléphones IP Cisco
- CERTA-2006-AVI-030 : Mutliples vulnérabilités sur PHP
- CERTA-2006-AVI-031 : Vulnérabilité du serveur de fax HylaFAX
- CERTA-2006-AVI-032 : Multiples vulnérabilités sur Oracle
- CERTA-2006-AVI-033 : Vulnérabilité de FreeBSD
- CERTA-2006-AVI-034 : Vulnérabilité de Cisco IOS
- CERTA-2006-AVI-035 : Multiples vulnérabilités des logiciels antivirus F-Secure
- CERTA-2006-AVI-036 : Multiples vulnérabilités dans Kerio WinRoute Firewall
- CERTA-2006-AVI-037 : Vulnérabilité dans le produit Enterprise Server Remote Manager de Novell

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2005-AVI-483-006 : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées
  (ajout des références aux bulletins de sécurité Debian DSA-938, DSA-940 et Mandriva MDKSA-2006:012)
- CERTA-2005-AVI-487-004 : Vulnérabilité de Ethereal
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-499-001 : Vulnérabilité dans la bibliothèque libavcodec
  (ajout des références aux bulletins de sécurité Mandriva et Gentoo)
- CERTA-2005-AVI-500-001 : Vulnérabilité dans VMware
  (ajout de la référence au bulletin de sécurité Gentoo et la référence CVE)
- CERTA-2006-AVI-012-001 : Vulnérabilité dans ClamAV
  (ajout des références aux bulletins de sécurité Gentoo, FreeBSD, SUSE et de la référence CVE)
- CERTA-2006-AVI-020-001 : Vulnérabilité dans mod_auth_pgsql pour Apache
  (ajout des références aux bulletins de sécurité Mandriva et Gentoo)
- CERTA-2005-AVI-474-003 : Multiples vulnérabilités dans la machine virtuelle Java de Sun
  (ajout des références aux bulletins de sécurité SUSE et Gentoo et des références CVE)
- CERTA-2005-AVI-486-003 : Vulnérabilité de Perl
  (ajout de la référence au bulletin de sécurité Debian DSA-943)

– CERTA-2006-AVI-012-002 : Vulnérabilité dans ClamAV
(ajout de la référence au bulletin de sécurité Mandriva)
– CERTA-2005-AVI-490-003 : Vulnérabilité sur le module mod_imap d'Apache
(ajout du bulletin de sécurité Mandriva)
– CERTA-2005-AVI-447-001 : Vulnérabilité de VERITAS NetBackup
(ajout de la référence au bulletin de sécurité iDEFENSE et d'une section contournement provisoire)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

6 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

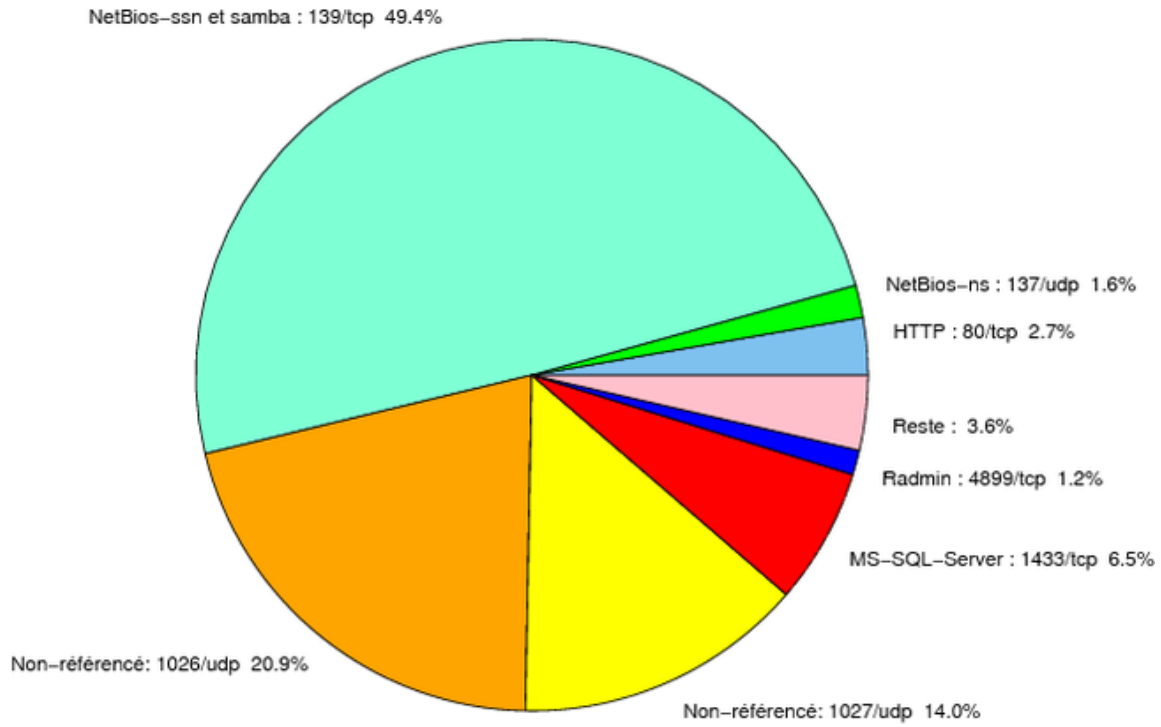

FIG. 2: Répartition relative des ports pour la semaine du 12.12.2005 au 19.01.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERT
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERT
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERT
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERT
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CERT

6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	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
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	–
11768	TCP	–	Netdepix	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	49,44
1026/udp	20,93
1027/udp	13,97
1433/tcp	6,53
80/tcp	2,74
137/udp	1,57
4899/tcp	1,19
1080/tcp	0,59
1434/udp	0,58
22/tcp	0,39
3128/tcp	0,24
10000/tcp	0,22
15118/tcp	0,18
9898/tcp	0,17
443/tcp	0,15
5554/tcp	0,13
6129/tcp	0,09
1023/tcp	0,08
2100/tcp	0,07
10080/tcp	0,05
3306/tcp	0,04
42/tcp	0,03
11768/tcp	0,02
6101/tcp	0,01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

20 janvier 2006 version initiale.