

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité n° 2005-46

---

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-2005-ACT-046>

---

### Gestion du document

Référence	CERTA-2005-ACT-046
Titre	Bulletin d'actualité n° 2005-46
Date de la première version	18 novembre 2005
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.

## 1 Activité en cours

### 1.1 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 03 et le 10 novembre 2005.

### 1.2 Incidents traités

#### 1.2.1 Multiples compromissions

Le CERTA traite actuellement la compromission de plusieurs serveurs sous Linux. La faille exploitée n'est pas encore connue. Ces compromissions ont été découvertes suite au dysfonctionnement des serveurs `sshd` qui étaient activés sur ces machines.

#### 1.2.2 Ver Lupper

Le CERTA traite un cas de compromission d'un serveur par le ver Lupper, en collaboration avec le CERT-Renater. L'analyse des journaux de cette machine a permis de déterminer qu'elle était régulièrement compromise par l'exploitation d'une faille de `AWStats.pl`. Les différentes compromissions ont conduit à l'installation de nombreux `bots irc` (robots qui peuvent recevoir des instructions par `irc`). Ces installations n'ont été possibles que parce que le serveur était autorisé à effectuer des connexions sortantes. Un filtrage en sortie (pour empêcher

le serveur http d'établir une quelconque connexion) et une lecture régulière des journaux des pare-feux auraient permis de détecter la compromission du serveur plus tôt.

#### **Recommandations :**

Il est conseillé d'appliquer les correctifs de sécurité pour vos applicatifs web et de réfléchir à la mise en place d'un filtrage en sortie aussi bien qu'en entrée.

#### **1.2.3 Spam massif**

De nombreux correspondants nous ont informés de la réception de nombreux messages non sollicités incitant à cliquer sur un lien vers une recherche Google.

Le lien renvoie vers le site [www.standartza.com](http://www.standartza.com) qui n'est plus joignable pour le moment, mais qui pourrait l'être de nouveau prochainement.

#### **Recommandation :**

Il peut être souhaitable d'ajouter un filtre temporaire sur ce site au niveau des proxies http.

## **2 Vulnérabilité sur Flash**

Le CERTA a publié l'avis CERTA-2005-AVI-438 concernant le logiciel Macromedia Flash Player. Un outil exploitant automatiquement cette vulnérabilité a été mis à disposition sur l'Internet.

#### **Recommandation :**

Il est urgent de mettre à jour le logiciel Macromedia Flash Player.

## **3 Rappel des avis et mises à jour émis**

**Note :** Suite à une erreur de notre part dans la numérotation des avis, il n'y a pas d'avis CERTA-2005-AVI-450. Par ailleurs, plusieurs avis ont été envoyés dans le cadre d'un exercice (ces messages portent la mention EXE dans le numéro), ils ne sont pas rappelés ici.

Durant la période du 07 au 10 novembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-437 : Multiples vulnérabilités dans ClamAV
- CERTA-2005-AVI-438 : Vulnérabilité du logiciel Macromedia Flash Player
- CERTA-2005-AVI-439 : Vulnérabilité dans fetchmail
- CERTA-2005-AVI-440 : Multiples vulnérabilités dans la bibliothèque libungif/giflib
- CERTA-2005-AVI-441 : Multiples vulnérabilités dans la bibliothèque libgda
- CERTA-2005-AVI-442 : Vulnérabilité dans divers produits F-Secure
- CERTA-2005-AVI-443 : Vulnérabilité dans Computer Associates iGateway
- CERTA-2005-AVI-444 : Vulnérabilité dans KOffice/KWord
- CERTA-2005-AVI-445 : Multiples vulnérabilités dans le moteur de rendu graphique de Microsoft
- CERTA-2005-AVI-446 : Vulnérabilité dans IBM Tivoli Directory Server
- CERTA-2005-AVI-447 : Vulnérabilité de VERITAS NetBackup
- CERTA-2005-AVI-448 : Vulnérabilité de VERITAS Cluster Server pour UNIX
- CERTA-2005-AVI-449 : Multiples vulnérabilité dans IBM Lotus Domino
- CERTA-2005-AVI-451 : Vulnérabilité de HP-UX remshd
- CERTA-2005-AVI-452 : Vulnérabilité des clients de messagerie Sylpheed et Sylpheed-Claws
- CERTA-2005-AVI-453 : Vulnérabilité de HP-UX envd

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

- CERTA-2005-AVI-400-002 : Faiblesse dans OpenSSL 0.9.x  
(ajout des références aux bulletins de sécurité Debian DSA-888 et Ubuntu)

- CERTA-2005-AVI-435-001 : Vulnérabilité du système de réseau privé virtuel OpenVPN (ajout des références aux bulletins de sécurité Gentoo, Debian et SUSE)
- CERTA-2005-AVI-437-001 : Multiples vulnérabilités dans ClamAV (ajout des références CVE et des bulletins de sécurité Debian et Mandriva)
- CERTA-2005-AVI-440-001 : Multiples vulnérabilités dans la bibliothèque libungif/giflib (ajout de la référence au bulletin de sécurité Ubuntu USN-214)
- CERTA-2005-AVI-435-002 : Vulnérabilité du système de réseau privé virtuel OpenVPN (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:206)
- CERTA-2005-AVI-440-002 : Multiples vulnérabilités dans la bibliothèque libungif/giflib (ajout de la référence au bulletin de sécurité Debian DSA-890)
- CERTA-2005-AVI-445-001 : Multiples vulnérabilités dans le moteur de rendu graphique de Microsoft (ajout du bulletin de sécurité Avaya)
- CERTA-2005-AVI-307-003 : Vulnérabilité de AWStats (ajout du bulletin de sécurité Debian)
- CERTA-2005-AVI-439-001 : Vulnérabilité dans fetchmail (ajout de la référence au bulletin de sécurité Mandriva et Ubuntu)
- CERTA-2005-AVI-440-003 : Multiples vulnérabilités dans la bibliothèque libungif/giflib (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:207)

## 4 Actions suggérées

### 4.1 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.

### 4.2 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.

### 4.3 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.

### 4.4 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.

## 4.5 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.

## 4.6 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.

## 4.7 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>

## 5 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.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2004-AVI-066 CERTA-2004-AVI-064 CERTA-2003-AVI-132
22	TCP	SSH	–	CERTA-2003-AVI-152
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	–	CERTA-2005-AVI-133
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127

137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

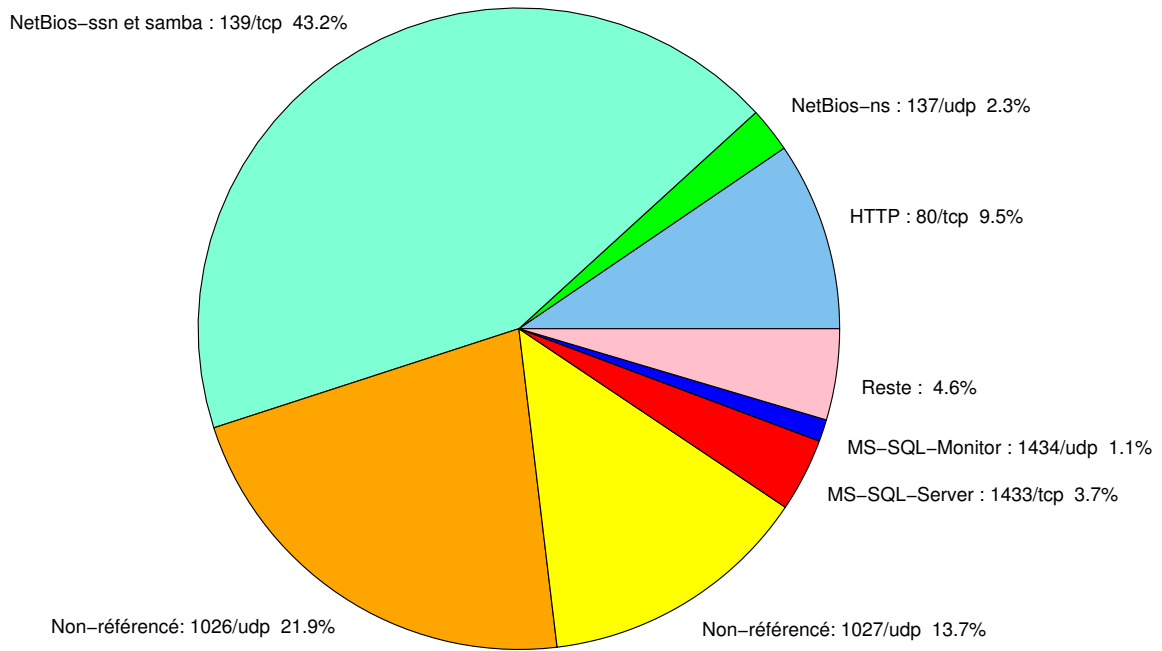


FIG. 1: Répartition relative des ports pour la semaine du 10.10.2005 au 17.11.2005

## Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	5
3	Paquets rejetés	7

## Gestion détaillée du document

18 novembre 2005 version initiale.

<b>port</b>	<b>pourcentage</b>
139/tcp	43,22
1026/udp	21,89
1027/udp	13,7
80/tcp	9,51
1433/tcp	3,69
137/udp	2,25
1434/udp	1,11
4899/tcp	0,92
1080/tcp	0,7
10000/tcp	0,46
15118/tcp	0,36
3128/tcp	0,3
22/tcp	0,29
5554/tcp	0,18
23/tcp	0,15
3306/tcp	0,13
9898/tcp	0,12
443/tcp	0,1
21/tcp	0,08
2100/tcp	0,07
143/tcp	0,06
5000/tcp	0,03
3389/tcp	0,01

TAB. 3: Paquets rejetés