

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité n° 2005-40**

---

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-040>

---

### Gestion du document

Référence	CERTA-2005-ACT-040
Titre	Bulletin d'actualité n° 2005-40
Date de la première version	07 octobre 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 29 septembre et le 06 octobre 2005.

### 1.2 Incident traité

Le CERTA a traité un cas d'infection de 4 machines par un cheval de Troie. La détection de cet incident a été rendue possible par l'analyse de journaux de routeur. En effet, le cheval de troie en question tentait d'établir des connexions vers des adresses réticulaires bien identifiées par ailleurs. Un examen du trafic «sortant» à destination de ces adresses a permis l'identification des machines compromises.

## 2 De l'utilité du filtrage des flux sortants

Le pare-feu est un élément incontournable de la sécurité périmétrique des réseaux. Il assure un rôle évident de protection d'un milieu dit «de confiance» vis-à-vis de l'extérieur (souvent de l'Internet). Il est d'ailleurs souvent uniquement configuré de telle sorte qu'il ne filtre que les flux entrants. Cependant notre expérience montre presque quotidiennement que cela ne suffit pas. Une machine ou un ensemble de machines infectées par un virus ou un cheval de Troie ne pourra être détecté qu'en appliquant également un filtrage des flux sortant. En effet, si une

machine d'un réseau local tente de se connecter à un serveur afin d'y envoyer des informations compromettantes (identifiants de connexion, mots de passe. . .), une discrimination des flux sortants préviendra sans doute cette fuite d'information. Elle permettra, en outre, une identification plus rapide de la machine compromise en examinant les journaux du pare-feu.

#### **Recommandation :**

Il convient donc d'appliquer, dans la mesure du possible, une politique de filtrage pour les flux sortants. Comme pour les flux entrants, une bonne démarche consiste à n'autoriser que les flux définis comme légitimes par la PSSI en vigueur. Cela se traduira certainement par un gain en terme de sécurité au quotidien mais aussi en terme de rapidité de détection et de réponse à un incident. Si toutefois, en examinant vos journaux de pare-feux, vous identifiez ce type de comportement anormal de la part d'une ou de plusieurs de vos machines, veuillez en avvertir le CERTA.

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

Durant la période du 26 au 30 septembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-364 : Vulnérabilité de Courier-SqWebMail ;
- CERTA-2005-AVI-365 : Vulnérabilité dans Xsun et Xprt sous Solaris ;
- CERTA-2005-AVI-366 : Mauvaise interprétation des règles dans des produits Check Point ;
- CERTA-2005-AVI-367 : Multiples vulnérabilités dans le navigateur Opera ;
- CERTA-2005-AVI-368 : Vulnérabilité des systèmes d'exploitation AIX ;
- CERTA-2005-AVI-369 : Vulnérabilité dans Mozilla Thunderbird.

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

- CERTA-2005-AVI-280-004 : Vulnérabilités de Apache (ajout des bulletins IBM HMC)
- CERTA-2005-AVI-314-001 : Vulnérabilité d'Evolution (ajout des références aux bulletins de sécurité Mandriva MDKSA-2005:141, RedHat RHSA-2005:743 et SUSE SUSE-SA:2005:054 ainsi qu'aux références CVE CAN-2005-2549 et CAN-2005-2550.)
- CERTA-2005-AVI-345-003 : Vulnérabilité dans Xfree86/X11/Xorg (ajout de la référence au bulletin de sécurité SUSE SUSE-SA-2005:056.)
- CERTA-2005-AVI-348-002 : Multiples vulnérabilités dans ClamAV (ajout des références aux bulletins de sécurité FreeBSD et SUSE)
- CERTA-2005-AVI-356-001 : Vulnérabilité de Webmin et Usermin (ajout du lien vers les changements Usermin ainsi que des références aux bulletins de sécurité SNS No. 83, Gentoo GLSA 200509-17 et CVE CAN-2005-3042.)
- CERTA-2005-AVI-276-005 : Vulnérabilité sur la bibliothèque zlib (ajout de la référence au bulletin de sécurité Gentoo GLSA 200509-18)
- CERTA-2005-AVI-336-004 : Vulnérabilité du moteur d'expressions régulières PCRE (ajout de la référence au bulletin de sécurité Debian DSA-821)
- CERTA-2005-AVI-207-001 : Vulnérabilité de GNU wget (ajout du Bulletin Red Hat)
- CERTA-2005-AVI-348-003 : Multiples vulnérabilités dans ClamAV (ajout de la référence aux bulletin de sécurité Debian)
- CERTA-2005-AVI-355-001 : Vulnérabilités dans le client de messagerie d'Opera (ajout des références CVE, de la page de mise à jour Opera et de la mise à jour de Suse)

### **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**

À 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 :

## 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.

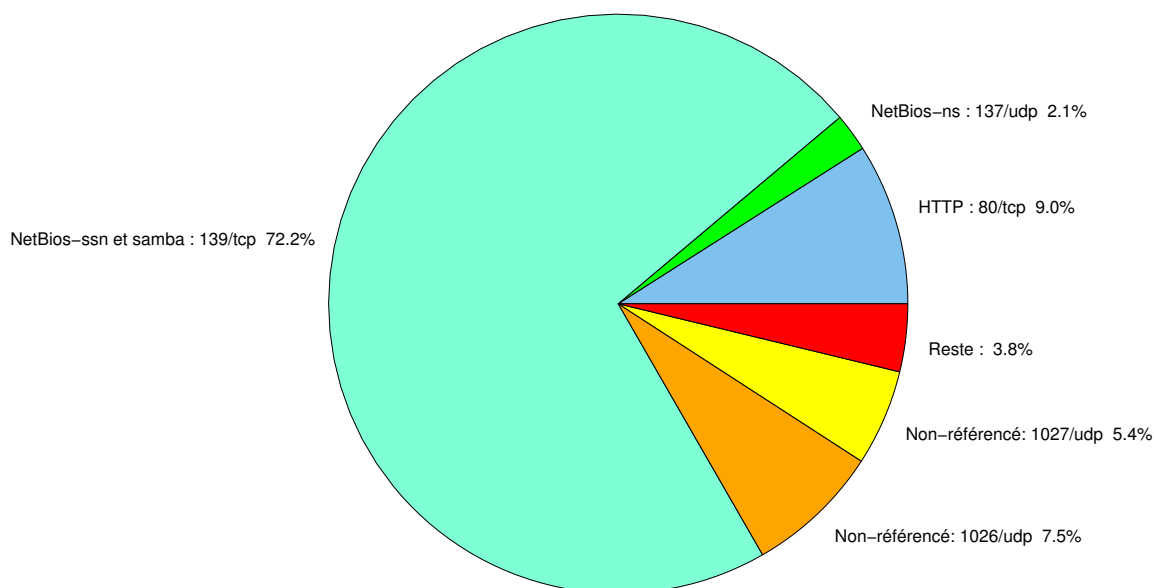


FIG. 1: Répartition relative des ports pour la semaine du 29.09.2005 au 06.10.2005

### Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	5
3	Paquets rejetés	6

### Gestion détaillée du document

07 octobre 2005 version initiale.

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
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	–

<b>port</b>	<b>pourcentage</b>
139/tcp	72.17
80/tcp	9.01
1026/udp	7.54
1027/udp	5.36
137/udp	2.11
1433/tcp	0.96
4899/tcp	0.79
1080/tcp	0.42
1434/udp	0.4
15118/tcp	0.3
22/tcp	0.2
6101/tcp	0.15
6129/tcp	0.14
3306/tcp	0.04
10000/tcp	0.03
9898/tcp	0.01

TAB. 3: Paquets rejetés