



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 05 novembre 2004  
N° CERTA-2004-ACT-024

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité N°24**

---

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-2004-ACT-024>

---

### Gestion du document

Référence	CERTA-2004-ACT-024
Titre	Bulletin d'actualité N°24
Date de la première version	05 novembre 2004
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 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.

## 2 Activité en cours

Durant la semaine du 21 au 28 octobre 2004, les rejets constatés concernaient essentiellement les ports 135/tcp, 445/tcp et 139/tcp.

L'incident remonté par un ministère concernant la très forte augmentation des rejets sur le port 445/tcp a été analysé et est en voie de résolution : les 180 adresses IP les plus agressives appartenaient tous au même fournisseur d'accès français.

<b>port</b>	<b>pourcentage</b>
135/tcp	30,20
445/tcp	23,12
139/tcp	12,38
137/udp	4,41
1026/udp	3,58
1027/udp	3,17
80/tcp	3,06
1433/tcp	2,63
9898/tcp	2,41
5554/tcp	2,38
1023/tcp	2,26
1080/tcp	1,81
2745/tcp	1,57
3127/tcp	1,38
1434/udp	1,26
21/tcp	1,06
4899/tcp	1,03
6129/tcp	0,85
22/tcp	0,51
443/tcp	0,35
23/tcp	0,16
111/tcp	0,14
3128/tcp	0,11
3389/tcp	0,10
5000/tcp	0,05
6112/tcp	0,01
10080/tcp	0,01

TAB. 2 – *Paquets rejetés*

D'autre part, le CERTA a récemment traité différents cas de compromission par exploitation de mots de passe faibles sur SSH. Bien que très peu sophistiquée, la technique utilisée pour compromettre les machines est efficace. Les machines ainsi compromises recherchent des serveurs SSH ayant des comptes avec des mots de passe triviaux. Si vous voyez de telles tentatives dans vos journaux (caractérisées par des tentatives de connexion avec de nombreux comptes), il ne faut surtout pas hésiter à nous le faire savoir, car l'adresse IP attaquant est probablement une machine piratée.

## **3 Actions suggérées**

### **3.1 Respecter la politique de sécurité**

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.

### **3.2 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.

### **3.3 Appliquer les correctifs de sécurité**

Le tableau 3 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

### **3.4 Utiliser un pare-feu**

L'application des correctifs sur un parc informatique important n'est probablement pas immédiat. 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.

### **3.5 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.

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

Durant la période du 18 au 29 octobre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-348 : Vulnérabilité de Squid
- CERTA-2004-AVI-349 : Vulnérabilité dans plusieurs antivirus

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-179 CERTA-2003-AVI-131
80	TCP	HTTP	–	CERTA-2004-AVI-050 CERTA-2004-AVI-195 CERTA-2004-AVI-210 CERTA-2004-AVI-239 CERTA-2004-AVI-313 CERTA-2004-AVI-315
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	–	CERTA-2003-AVI-168 CERTA-2003-AVI-144 CERTA-2004-AVI-126
389	TCP	LDAP	–	CERTA-2004-AVI-045 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-095 CERTA-2004-AVI-126 CERTA-2004-AVI-178 CERTA-2004-AVI-247 CERTA-2004-AVI-301 CERTA-2004-AVI-313 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2003-AVI-038 CERTA-2004-AVI-126
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
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
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	–
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–

TAB. 3 – Correctifs correspondant aux ports destination des paquets rejetés

- CERTA-2004-AVI-350 : Multiples vulnérabilités de Gaim
- CERTA-2004-AVI-351 : Vulnérabilité dans Ghostscript
- CERTA-2004-AVI-352 : Vulnérabilité dans PostgreSQL
- CERTA-2004-AVI-353 : Multiples vulnérabilités dans les bibliothèques libpng
- CERTA-2004-AVI-354 : Vulnérabilité dans HP-UX
- CERTA-2004-AVI-355 : Vulnérabilité de IBM RSCT
- CERTA-2004-AVI-356 : Vulnérabilités des noyaux Linux 2.6
- CERTA-2004-AVI-357 : Vulnérabilités du lecteur PDF xpdf et de ses dérivés et du service d'impression CUPS
- CERTA-2004-AVI-358 : Vulnérabilité dans netkit-telnet et netkit-telnet-ssl
- CERTA-2004-AVI-359 : Vulnérabilité dans Cisco Secure ACS
- CERTA-2004-AVI-360 : Vulnérabilité de la bibliothèque gd
- CERTA-2004-AVI-361 : Multiples vulnérabilités de libxml2

Les mises à jour suivantes ont été publiées :

- CERTA-2004-AVI-247-005 : Vulnérabilité du module Apache mod\_ssl (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2004-AVI-345-001 : Multiples Vulnérabilités de Libtiff (ajout référence au bulletin de sécurité DSA-567 de Debian. Ajout référence CVE CAN-2004-0804)
- CERTA-2004-AVI-325-006 : Vulnérabilités de XFree86, libXpm et LessTif (ajout référence au bulletin de sécurité #57652 de Sun)
- CERTA-2004-AVI-345-002 : Multiples Vulnérabilités de Libtiff (ajout référence au bulletin de sécurité MDKSA-2004:109 de Mandrake)
- CERTA-2004-AVI-272-004 : Vulnérabilités du serveur tnftpd (ajout de la référence au bulletin de sécurité Sun #57655 pour ftpd (Heimdal) livré avec Sun Java Desktop System (JDS))
- CERTA-2004-AVI-295-006 : Vulnérabilité dans ImageMagick (ajout de la référence aux bulletins de sécurité de Red Hat)
- CERTA-2004-AVI-318-002 : Vulnérabilité d'OpenOffice et StarOffice (ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2004-AVI-325-007 : Vulnérabilités de XFree86, libXpm, LessTif, Motif et OpenMotif (Prise en compte de Motif et OpenMotif)
- CERTA-2004-AVI-348-001 : Vulnérabilité de Squid (ajout référence au bulletin de sécurité de Red Hat)
- CERTA-2004-AVI-345-003 : Multiples vulnérabilités de Libtiff (ajout référence au bulletin de sécurité MDKSA-2004:111 de Mandrake relatif à wxGTK2)
- CERTA-2004-AVI-348-002 : Vulnérabilité de Squid (ajout référence au bulletin de sécurité de Mandrake)
- CERTA-2004-AVI-264-001 : Vulnérabilité dans la machine virtuelle Java (JRE) de SUN (ajout référence au bulletin de sécurité HPSBUX01087 de HP)
- CERTA-2004-AVI-332-002 : Vulnérabilité de Samba (ajout référence au bulletin de sécurité HP (HPS-BUX01086)
- CERTA-2004-AVI-347-001 : Vulnérabilités dans MySQL (ajout du bulletin de sécurité redhat)
- CERTA-2004-AVI-283-003 : Vulnérabilité dans MySQL (ajout de la référence au bulletin de sécurité Red-Hat)
- CERTA-2004-AVI-345-004 : Multiples vulnérabilités de Libtiff (ajout référence au bulletin de sécurité de Red Hat. Ajout référence à la vulnérabilité CAN-2004-0929 ainsi qu'aux documents associés (bulletin SUSE-SA:2004:038 et bulletin d'iDEFENSE))
- CERTA-2004-AVI-350-001 : Multiples vulnérabilités de Gaim (ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2004-AVI-348-003 : Vulnérabilité de Squid (ajout référence au bulletin de sécurité de Debian)

## 5 Documentation

### Liste des tableaux

1	Gestion du document . . . . .	1
---	-------------------------------	---

2	Paquets rejetés . . . . .	2
3	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	4

## **Gestion détaillée du document**

**05 novembre 2004** version initiale.