Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 juillet 2005
N° CERTA-2005-ACT-027

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité n° 2005-27**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2005-ACT-027 |
| Titre | Bulletin d'actualité n° 2005-27 |
| Date de la première version | 08 juillet 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 23 et le 30 juin 2005.

Nous pouvons constater l'apparition de rejets sur le port 10000/tcp. Ces connexions correspondent à des tentatives d'exploitation d'une faille de `Veritas Backup Exec` (voir CERTA-2005-AVI-229).

### 1.2 Incidents traités

Le CERTA a traité plusieurs cas de défiguration de site web. Pour l'un de ces incidents, c'est l'exploitation d'une faille d'`autologin` du forum `phpBB` qui a été exploitée (voir avis CERTA-2005-AVI-096). Elle permet à un utilisateur mal intentionné de se connecter avec les droits de l'administrateur du forum. Ceci se traduit généralement par des modifications mineures du forum (changement du nom des modérateurs, remplacement des bannières, etc).

Dans un autre cas, c'est la dernière faille de `phpBB` qui a été exploitée (voir avis CERTA-2005-AVI-237). Cette faille affecte le paramètre `highlight` du fichier `viewtopic.php`, et est très proche de la vulnérabilité massivement exploitée en décembre 2004 (voir CERTA-2005-ALE-014). Son exploitation est très critique, puisqu'elle permet de prendre totalement le contrôle du serveur web à distance. Un outil permettant d'exécuter n'importe quelle commande en exploitant cette vulnérabilité a été mis à disposition sur l'Internet le 30 juin. De nombreuses

remontées de nos correspondants ont permis de montrer que des attaques s'appuyant sur cet outil avaient débuté dans l'après-midi du 30 juin. Il est possible qu'un ver fasse bientôt son apparition, sur le même modèle que `Santy` (voir CERTA-2005-ALE-014).

**Recommandation :**

Il est conseillé de déterminer si le produit `phpBB` est utilisé sur vos réseaux, et de le mettre à jour le cas échéant.

# 2 Rappel des avis et mises à jour émis

Durant la période du 27 juin au 01 juillet 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-231 : Multiples vulnérabilités dans le noyau Linux
- CERTA-2005-AVI-232 : Vulnérabilité dans SGI IRIX
- CERTA-2005-AVI-233 : Vulnérabilité dans la base de données DB2
- CERTA-2005-AVI-234 : Vulnérabilité de ClamAV
- CERTA-2005-AVI-235 : Multiples vulnérabilités des produits Adobe pour Mac OS X
- CERTA-2005-AVI-236 : Vulnérabilité du chargeur ld.so sous Solaris
- CERTA-2005-AVI-237 : Vulnérabilité dans phpBB
- CERTA-2005-AVI-238 : Vulnérabilité de RADIUS Authentication sous CISCO IOS
- CERTA-2005-AVI-239 : Multiples vulnérabilité dans heimdal telnetd server
- CERTA-2005-AVI-240 : Vulnérabilités FreeBSD (ipfw)
- CERTA-2005-AVI-241 : Vulnérabilités dans la pile TCP de FreeBSD
- CERTA-2005-AVI-242 : Vulnérabilités dans PHP PEAR

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

- CERTA-2005-AVI-165-003 : Vulnérabilité dans Squid
  (ajout de la référence au bulletin de sécurité Mandriva)
- CERTA-2005-AVI-221-001 : Vulnérabilité de gedit
  (ajout des références aux mises à jour de sécurité Fedora)
- CERTA-2005-AVI-178-003 : Multiples vulnérabilités d'Ethereal
  (ajout références aux bulletins FreeBSD et NetBSD)
- CERTA-2005-AVI-226-003 : Vulnérabilité dans l'utilitaire sudo
  (ajout de la référence au bulletin de sécurité Suse)
- CERTA-2005-AVI-230-001 : Multiples vulnérabilités des lecteurs RealPlayer
  (ajout références aux bulletins de SuSE, Red Hat, Fedora et FreeBSD. Ajout références CVE)
- CERTA-2005-AVI-203-001 : Vulnérabilité d'ImageMagick et GraphicsMagick
  (Ajout référence à la mise-à-jour Fedora. Ajout référence au bulletin de sécurité de Mandriva)
- CERTA-2005-AVI-225-005 : Vulnérabilité dans SpamAssassin
  (ajout de la référence au bulletin de sécurité Mandriva)
- CERTA-2005-AVI-226-004 : Vulnérabilité dans l'utilitaire sudo
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-234-001 : Vulnérabilité de ClamAV
  (ajout de la référence au bulletin de sécurité OpenBSD)
- CERTA-2005-AVI-225-006 : Vulnérabilité dans SpamAssassin
  (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2005-AVI-226-005 : Vulnérabilité dans l'utilitaire sudo
  (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2005-AVI-188-004 : Multiples vulnérabilités dans bzip2
  (ajout de la référence au bulletin de sécurité FreeBSD SA-05:14)

# 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. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

## 3.2 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.

## 3.3 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.

## 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.

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.

## 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 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.

# 4 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.

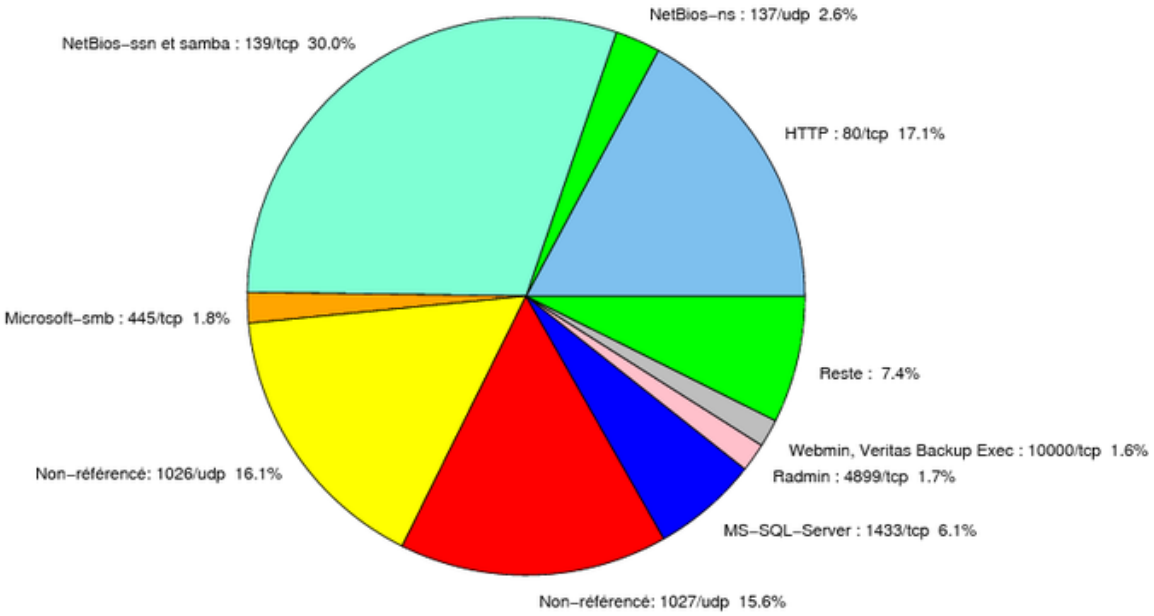


FIG. 1 – *Répartition relative des ports pour la semaine du 23.06.2005 au 30.06.2005*

# Liste des tableaux



# Gestion détaillée du document

**08 juillet 2005** version initiale.

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CERTA-2003-A |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2005-A |
| 42 | TCP | WINS | – | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 80 | TCP | HTTP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 111 | TCP | Sunrpc-portmapper | – | http://www.certa.ssi.gouv.fr/site/CERTA-2003-A |
| 119 | TCP | NNTP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 135 | TCP | Microsoft RPC | – | http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 137 | UDP | NetBios-ns | – | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 139 | TCP | NetBios-ssn et samba | – | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2005-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2005-A |
| 143 | TCP | IMAP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2005-A |
| 389 | TCP | LDAP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 443 | TCP | HTTPS | – | http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2003-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2005-A |
| 1023 | TCP | – | Serveur ftp de Sasser.E | – |
| 1080 | TCP | Wingate | MyDoom.F | – |
| 1433 | TCP | MS-SQL-Server | – | http://www.certa.ssi.gouv.fr/site/CERTA-2002-A |
| 1434 | UDP | MS-SQL-Monitor | – | http://www.certa.ssi.gouv.fr/site/CERTA-2002-A |
| 2100 | TCP | Oracle XDB FTP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2005-A |
| 2745 | TCP | – | Bagle | – |
| 3127 | TCP | – | MyDoom | – |
| 3128 | TCP | Squid | MyDoom | http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A<br>http://www.certa.ssi.gouv.fr/site/CERTA-2004-A |
| 3306 | TCP | MySQL | – | – |
| 3389 | TCP | Microsoft RDP | – | http://www.certa.ssi.gouv.fr/site/CERTA-2002-A |
| 4899 | TCP | Radmin | – | – |
| 5000 | TCP | Universal Plug and Play | Bobax, Kibuv | http://www.certa.ssi.gouv.fr/site/CERTA-2001-A |
| 5554 | TCP | SGI ESP HTTP | Serveur ftp de Sasser | – |
| 6101 | TCP | Veritas Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CERTA-2005-A |
| 6112 | TCP | Dtspcd | – | http://www.certa.ssi.gouv.fr/site/CERTA-2002-A |
| 6129 | TCP | Dameware Miniremote | – | http://www.certa.ssi.gouv.fr/site/CERTA-2003-A |
| 8866 | TCP | – | Porte dérobée Bagle.B | CERTA-2004-COM-001 |
| 9898 | TCP | – | Porte dérobée Dabber | – |
| 10000 | TCP | Webmin, Veritas Backup Exec | – | http://www.certa.ssi.gouv.fr/site/CERTA-2005-A |
| 10080 | TCP | Amanda | MyDoom | – |
| 11768 | TCP | – | Netdepix | – |
| 15118 | TCP | – | Netdepix | – |



TAB. 2 – *Correctifs correspondant aux ports destination des paquets rejetés*

| port | pourcentage |
|---|---|
| 139/tcp | 30.03 |
| 80/tcp | 17.13 |
| 1026/udp | 16.12 |
| 1027/udp | 15.56 |
| 1433/tcp | 6.13 |
| 137/udp | 2.61 |
| 445/tcp | 1.76 |
| 4899/tcp | 1.65 |
| 10000/tcp | 1.61 |
| 2745/tcp | 0.82 |
| 1080/tcp | 0.72 |
| 15118/tcp | 0.66 |
| 23/tcp | 0.57 |
| 9898/tcp | 0.49 |
| 443/tcp | 0.47 |
| 3128/tcp | 0.44 |
| 3127/tcp | 0.41 |
| 25/tcp | 0.38 |
| 5554/tcp | 0.29 |
| 5000/tcp | 0.26 |
| 10080/tcp | 0.24 |
| 22/tcp | 0.21 |
| 8866/tcp | 0.19 |
| 6129/tcp | 0.18 |
| 3306/tcp | 0.14 |
| 6101/tcp | 0.11 |
| 11768/tcp | 0.06 |
| 42/tcp | 0.05 |
| 1023/tcp | 0.04 |
| 3389/tcp | 0.03 |
| 143/tcp | 0.01 |

TAB. 3 – *Paquets rejetés*