Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 novembre 2005
N° CERTA-2005-ACT-045

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité n° 2005-45**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2005-ACT-045 |
| Titre | Bulletin d'actualité n° 2005-45 |
| Date de la première version | 10 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.

## 2 Ver `Lupper` et exploitation des applicatifs web

Un ver exploitant de multiples vulnérabilités de certains applicatifs web, notamment `XML-RPC` (CERTA-2005-AVI-242) et `AWStats` (CERTA-2005-AVI-035), se propage actuellement.

Les versions qui ont pu être détectées créent les fichiers `/tmp/lupii`, `/tmp/listen`, `/tmp/update.listen` et `/tmp/listen.log` et ouvrent les ports 7111/udp, 7222/udp, 27015/udp, 25555/udp.

Il est à noter que ce ver peut évoluer dans le futur pour intégrer d'autres vulnérabilités d'applicatifs web (comme par exemple `phpBB`), et que d'autres fichiers et d'autres ports que ceux indiqués peuvent être utilisés.

Ces vulnérabilités sont par ailleurs régulièrement recherchées à l'aide de méthodes comme le `Google Hacking` puis exploitées. Voici quelques exemples directement issus de nos journaux, qui montre notamment une tentative sur la page de l'avis concernant `AWStats` (il s'agit là d'un `Google Hacking` mal maîtrisé).

Tentative d'exploitation d'une faille de AWStats sans même vérifier la présence de cet applicatif :

```
xxx.xxx.xxx.xxx - - [02/Nov/2005:23:10:17 +0100]
"GET /awstats/awstats.pl?configdir=|echo;echo;id;echo;echo| HTTP/1.0"
404 212 "-" "Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.0)"
```

Tentative d'exploitation d'une faille de AWStats suite à une recherche de type Google Hacking qui a pointé vers un avis traitant de cet applicatif :

```
xxx.xxx.xxx.xxx - - [06/Nov/2005:02:05:15 +0100]
"GET /site/CERTA-2005-AVI-035/awstats.pl?configdir=|echo%20;echo%20;id;echo%20;echo|
HTTP/1.0" 404 228 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
```

Tentative d'exploitation d'une faille de AWStats sans vérification de la présence de l'applicatif, à l'aide d'un outil qui laisse la trace significative DataCha0s/2.0:

```
xxx.xxx.xxx.xxx - - [06/Nov/2005:21:20:46 +0100]
"GET /cgi-bin/awstats.pl?configdir=|echo;echo;id;%00 HTTP/1.0"
404 212 "-" "DataCha0s/2.0"
```

**Recommandations :**

Il est conseillé d'appliquer les correctifs de sécurité pour les applicatifs web et d'utiliser les techniques de Google Hacking sur votre nom de domaine pour vérifier la présence de ces applicatifs.

# 3 Rappel des avis et mises à jour émis

Durant la période du 31 octobre au 04 novembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-425 : Multiples vulnérabilité dans Mantis
- CERTA-2005-AVI-426 : Vulnérabilités de phpBB
- CERTA-2005-AVI-427 : Vulnérabilité de Apache 2.0
- CERTA-2005-AVI-428 : Multiples vulnérabilités dans PHP
- CERTA-2005-AVI-429 : Vulnérablilité dans Cisco IPS MC
- CERTA-2005-AVI-430 : Multiples vulnérabilités dans Mac OS X
- CERTA-2005-AVI-431 : Vulnérabilité dans les produits Cisco
- CERTA-2005-AVI-432 : Vulnérabilité de certains équipements de réseau sans-fil de Cisco
- CERTA-2005-AVI-433 : Vulnérabilité dans HP OpenVMS
- CERTA-2005-AVI-434 : Vulnérabilité dans l'utilitaire unzip
- CERTA-2005-AVI-435 : Vulnérabilité du système de réseau privé virtuel OpenVPN
- CERTA-2005-AVI-436 : Multiples vulnérabilités dans Quicktime

# 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'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.

### 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 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.

### 4.7 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.

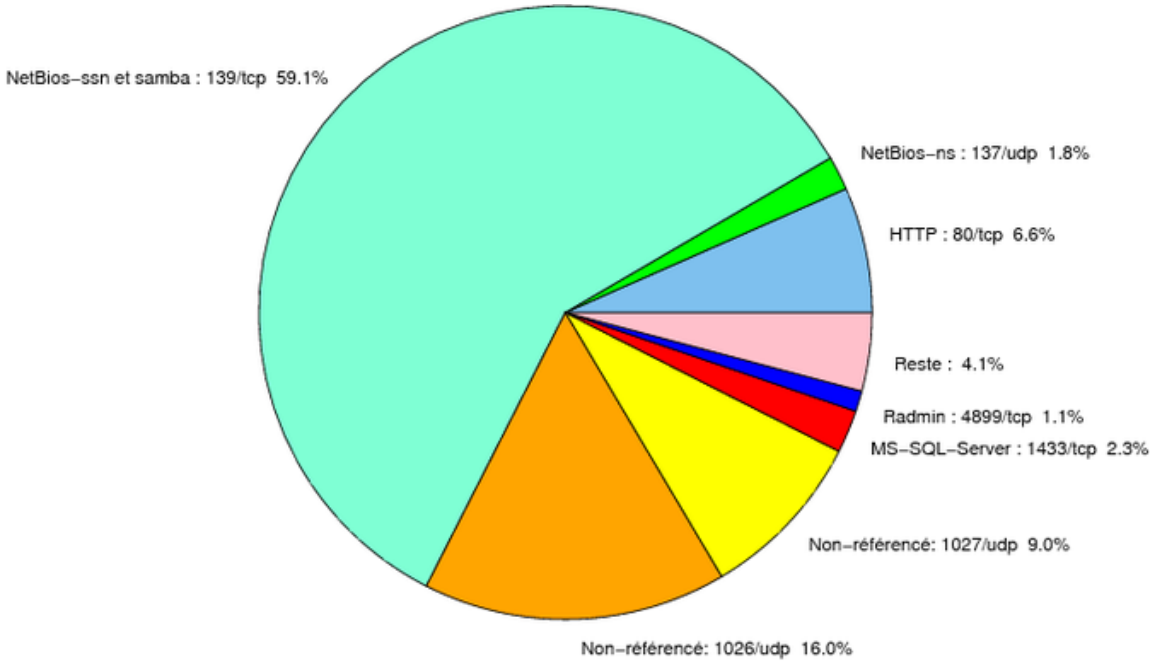


FIG. 1: Répartition relative des ports pour la semaine du 03.10.2005 au 10.11.2005

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CER |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 42 | TCP | WINS | – | http://www.certa.ssi.gouv.fr/site/CER |
| 80 | TCP | HTTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 111 | TCP | Sunrpc-portmapper | – | http://www.certa.ssi.gouv.fr/site/CER |
| 119 | TCP | NNTP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 135 | TCP | Microsoft RPC | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 137 | UDP | NetBios-ns | – | http://www.certa.ssi.gouv.fr/site/CER |
| 139 | TCP | NetBios-ssn et samba | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 143 | TCP | IMAP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 389 | TCP | LDAP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |

| | | | | |
|---|---|---|---|---|
| | | | | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 443 | TCP | HTTPS | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 1023 | TCP | – | Serveur ftp de Sasser.E | – |
| 1080 | TCP | Wingate | MyDoom.F | – |
| 1433 | TCP | MS-SQL-Server | – | http://www.certa.ssi.gouv.fr/site/CER |
| 1434 | UDP | MS-SQL-Monitor | – | http://www.certa.ssi.gouv.fr/site/CER |
| 2100 | TCP | Oracle XDB FTP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 2745 | TCP | – | Bagle | – |
| 3127 | TCP | – | MyDoom | – |
| 3128 | TCP | Squid | MyDoom | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 3306 | TCP | MySQL | – | – |
| 3389 | TCP | Microsoft RDP | – | http://www.certa.ssi.gouv.fr/site/CER |
| 4899 | TCP | Radmin | – | – |
| 5000 | TCP | Universal Plug and Play | Bobax, Kibuv | http://www.certa.ssi.gouv.fr/site/CER |
| 5554 | TCP | SGI ESP HTTP | Serveur ftp de Sasser | – |
| 6070 | TCP | BrightStor ARCserve/Enterprise Backup | – | http://www.certa.ssi.gouv.fr/site/CER |
| 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<br>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<br>http://www.certa.ssi.gouv.fr/site/CER |
| 10080 | TCP | Amanda | MyDoom | – |
| 11768 | TCP | – | Netdepix | – |
| 15118 | TCP | – | Netdepix | – |

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

| port | pourcentage |
|---|---|
| 139/tcp | 59,11 |
| 1026/udp | 16 |
| 1027/udp | 9,01 |
| 80/tcp | 6,6 |
| 1433/tcp | 2,25 |
| 137/udp | 1,79 |
| 4899/tcp | 1,08 |
| 1080/tcp | 0,97 |
| 1434/udp | 0,77 |
| 15118/tcp | 0,32 |
| 10000/tcp | 0,28 |
| 9898/tcp | 0,18 |
| 22/tcp | 0,17 |
| 5554/tcp | 0,13 |
| 443/tcp | 0,09 |
| 2100/tcp | 0,07 |
| 143/tcp | 0,06 |
| 25/tcp | 0,05 |
| 3306/tcp | 0,04 |
| 21/tcp | 0,03 |
| 11768/tcp | 0,02 |
| 6070/tcp | 0,01 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**10 novembre 2005** version initiale.