

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité N°2005-09**

---

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-009>

---

### Gestion du document

Référence	CERTA-2005-ACT-009
Titre	Bulletin d'actualité N°2005-09
Date de la première version	04 mars 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

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 17 et le 24 février 2005. Un cas de défiguration de site web a été traité par le CERTA.

## 2 Les « PHPWorms »

Dans le bulletin d'actualité N°2005-08, nous avons abordé le « Google Hacking ».

En résumé, il s'agit de la possibilité de réaliser des requêtes habilement construites afin d'accéder à des informations sensibles sur les serveurs web telles que des applications vulnérables, des documents confidentiels, des ressources en accès restreint, etc.

Le PHP (Personal Home Page) est un langage permettant la construction de sites web dynamiques. De très nombreux sites utilisent ce langage. Parmi les applications web construites avec ce langage on peut citer des forums Internet, des outils de statistiques, des jeux en ligne, etc. L'avantage indéniable du langage est sa grande souplesse et sa facilité d'apprentissage. Cependant, de nombreux problèmes de sécurité sont découverts tous les jours dans les applications basées sur PHP. Alors que ce langage semble facilement accessible, il nécessite pourtant des programmeurs expérimentés. Parmi les vulnérabilités courantes engendrées par l'utilisation du langage PHP sur un site web, on peut citer la possibilité pour un pirate d'inclure des fichiers (CERTA-2003-ALE-003), de traverser des répertoires, d'exécuter des commandes à distance, etc. De nombreuses failles récentes ont été publiées par le CERTA, par exemple sur phpBB (CERTA-2005-AVI-086 et CERTA-2005-AVI-096).

Une nouvelle vague de vers apparaissent aujourd'hui utilisant une combinaison de la technique de « Google Hacking » et de l'exploitation des problèmes de sécurité engendrés par l'utilisation du langage PHP. Ils sont généralement appelés « PHPWorms ». Une fois une machine infectée par le biais d'une vulnérabilité quelconque, le ver est installé. Le code malveillant va alors effectuer du Google Hacking afin de rechercher des serveurs vulnérables. Ensuite, le code malveillant va explorer ces sites à la recherche de vulnérabilités, PHP par exemple. Enfin, le ver va effectuer différentes actions malicieuses telles la défiguration de sites Internet (en modifiant par exemple tous les fichiers index.html trouvés sur la machine), l'exécution de code arbitraire à distance, etc.

Avec plusieurs vulnérabilités critiques dans des applications PHP très répandues et l'activité certaine autour des techniques de « Google Hacking », il est très important de mettre à jour ses services exposés sur l'Internet, et de surcroît, porter une attention particulière à celles utilisant du PHP. Ceci d'autant plus que les PHPWorms sont de plus en plus rapidement développés et mis en circulation suite à la découverte d'une vulnérabilité. Ils sont également de plus en plus répandus et sophistiqués. Comme mentionné dans le bulletin d'actualité N°2005-08, les pare-feux ne sont d'aucune aide dans ce cas, dans la mesure où les flux considérés sont généralement des flux autorisés (port 80/tcp). Une revue méthodique et systématique des journaux des serveurs web est indispensable afin de détecter au plus vite tout incident de sécurité.

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

Durant la période du 21 au 25 février 2005, le CERTA a émis l'avis suivant :

- CERTA-2005-AVI-083 : Vulnérabilité dans PuTTY
- CERTA-2005-AVI-084 : Vulnérabilité dans Squid
- CERTA-2005-AVI-085 : Vulnérabilité de unace
- CERTA-2005-AVI-086 : Vulnérabilités de phpBB

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

- CERTA-2005-AVI-023-001 : Multiples vulnérabilités du noyau Linux (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:092-14)
- CERTA-2005-AVI-068-002 : Vulnérabilité dans vim (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-069-002 : Vulnérabilité de cpio (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-082-001 : Vulnérabilité de gFTP (ajout des références aux bulletins de sécurité Gentoo et FreeBSD)
- CERTA-2004-AVI-257-005 : Vulnérabilité de SoX (ajout de la référence au bulletin de sécurité Fedora)
- CERTA-2004-AVI-289-002 : Vulnérabilité de gnome-vfs (ajout référence au bulletin de sécurité Fedora)
- CERTA-2004-AVI-303-002 : Vulnérabilité de cdrecord (ajout référence au bulletin de sécurité de Fedora)
- CERTA-2005-AVI-083-001 : Vulnérabilité dans PuTTY (ajout des références aux bulletins de sécurité Gentoo et FreeBSD)
- CERTA-2004-AVI-377-005 : Vulnérabilité dans la machine virtuelle Java de SUN (ajout de la référence au bulletin de sécurité Apple MacOS X)
- CERTA-2005-AVI-044-001 : Vulnérabilité de ClamAV (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-046-006 : Vulnérabilité de Perl (ajout de la référence au correctif de sécurité IBM)
- CERTA-2005-AVI-048-001 : Vulnérabilité dans UW-Imapd (ajout du site Internet de UW-Imap et des références aux bulletins de sécurité Gentoo GLSA 200502-02 et RedHat RHSA-2005:128)
- CERTA-2005-AVI-072-002 : Vulnérabilité du module Apache mod\_python (ajout de la référence au bulletin de sécurité Debian)

- CERTA-2005-AVI-084-001 : Vulnérabilité dans Squid  
(ajout du site Internet Squid, des références aux bulletins de sécurité Debian et SUSE ainsi que de la référence CVE)
- CERTA-2005-AVI-067-005 : Vulnérabilité de Emacs et XEmacs  
(ajout des références aux bulletins de sécurité NetBSD)
- CERTA-2005-AVI-084-002 : Vulnérabilité dans Squid  
(ajout de la référence au bulletin de sécurité Mandrake)

## **4 Actions suggérées**

### **4.1 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.

### **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 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.

### **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.

### **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.

## 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.

### 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

04 mars 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
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
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
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
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	–
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
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	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

<b>port</b>	<b>pourcentage</b>
445/tcp	72,23
139/tcp	6,03
137/udp	4,48
1433/tcp	3,22
1026/udp	2,73
4899/tcp	2,52
1027/udp	2,11
15118/tcp	1,52
6129/tcp	1,46
5554/tcp	0,78
9898/tcp	0,55
1434/udp	0,37
80/tcp	0,31
2745/tcp	0,29
3306/tcp	0,22
22/tcp	0,21
3127/tcp	0,17
1080/tcp	0,15
1023/tcp	0,11
42/tcp	0,11
6101/tcp	0,11
11768/tcp	0,11
443/tcp	0,07
21/tcp	0,04
3128/tcp	0,03
5000/tcp	0,03
3389/tcp	0,02
111/tcp	0,02
23/tcp	0,01

TAB. 3 – *Paquets rejetés*