

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°31

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-031>

Gestion du document

Référence	CERTA-2004-ACT-031
Titre	Bulletin d'actualité N°31
Date de la première version	30 décembre 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 Activité en cours

Le tableau 3 montre les rejets sur deux dispositifs de filtrage entre le 16 et le 23 décembre 2004. L'actualité a été marquée par la propagation du ver *Santy*. Cette activité ne se remarque pas dans les rejets des dispositifs de filtrage puisque ce ver effectue une recherche sur Google ou Yahoo (du moins pour les versions du ver que nous avons analysées) afin de trouver des serveurs http.

2 Le ver *Santy*

Le ver *Santy*, évoqué dans l'alerte CERTA-2004-ALE-014, exploite une vulnérabilité de phpBB.

Ce ver a une caractéristique très particulière : il utilise des moteurs de recherche connus (Google et Yahoo) pour trouver des sites web utilisant les scripts php, ce qui rend plus efficace sa propagation tout en le rendant quasiment invisibles dans les journaux des pare-feux (pas de recherche aveugle du port 80/tcp).

Si son activité n'est pas détectable dans les journaux des pare-feux, elle l'est dans les journaux des serveurs web. En effet, une simple recherche sur le motif `highlight=%2527` met en évidence la tentative de compromission du serveur. Par exemple, pour un serveur apache sous Linux :

```
grep highlight=%2527' access_log error_log
```

Si vous détectez de telles lignes dans vos journaux, contactez le CERTA.

Le code exécuté par le ver sur les serveurs vulnérables provoque le téléchargement de quatre programmes, ainsi que l'effacement de nombreux fichiers sur le serveur. Trois de ces programmes sont des scripts écrits en

perl utilisés pour la propagation du ver. Le quatrième est un robot irc qui semble avoir des fonctionnalités pour sonder des réseaux.

Cet incident illustre une fois de plus l'importance des filtres en sortie : une machine vulnérable ainsi compromise ne pourrait pas provoquer des dégâts à l'extérieur de son périmètre de sécurité. En revanche, ces filtres ne préservent pas la machine des éventuels effacements de fichiers.

NB : Ce que fait Santy automatiquement peut être fait à la main par un utilisateur mal intentionné avec n'importe quel navigateur. Cette technique permet d'exécuter n'importe quelle commande en l'écrivant dans une URL malicieusement constituée.

3 Rappel des avis et des mises à jour émis

Durant la période du 20 au 24 décembre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-405 : Multiples vulnérabilités de PHP
- CERTA-2004-AVI-406 : Vulnérabilité de KDE
- CERTA-2004-AVI-407 : Vulnérabilité de la commande file
- CERTA-2004-AVI-408 : Vulnérabilité de la commande newgrp sous HP-UX
- CERTA-2004-AVI-409 : Nombreuses failles du noyau Linux
- CERTA-2004-AVI-410 : Plusieurs vulnérabilités sur AIX
- CERTA-2004-AVI-411 : Vulnérabilité de MIT Kerberos 5
- CERTA-2004-AVI-412 : Vulnérabilité dans le service FTP sous HP-UX
- CERTA-2004-AVI-413 : Multiples vulnérabilité dans Konqueror
- CERTA-2004-AVI-414 : Vulnérabilités dans MPlayer
- CERTA-2004-AVI-415 : Vulnérabilité dans a2ps
- CERTA-2004-AVI-416 : Vulnérabilités dans Xine
- CERTA-2004-AVI-417 : Vulnérabilité dans mpeg123

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

- CERTA-2004-AVI-347-004 : Vulnérabilités dans MySQL
(ajout de la référence aux bulletins de sécurité FreeBSD du 16 décembre 2004)
- CERTA-2004-AVI-360-005 : Vulnérabilité de la bibliothèque gd
(ajout de la référence aux bulletins de sécurité de Red Hat et FreeBSD)
- CERTA-2004-AVI-361-004 : Multiples vulnérabilités de libxml2
(ajout de la référence au bulletin de sécurité Red Hat (RHSA-2004:650) relatif à libxml)
- CERTA-2004-AVI-398-001 : Vulnérabilité de Adobe Acrobat Reader sous Unix
(ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2004-AVI-400-001 : Multiples vulnérabilités dans Ethereal
(Ajout référence au bulletin de sécurité de Gentoo. Ajout références CVE)
- CERTA-2004-AVI-402-001 : Vulnérabilité de Samba
(ajout référence aux bulletins de sécurité de Red Hat et Gentoo)
- CERTA-2004-AVI-391-001 : Vulnérabilité de zip
(ajout référence au bulletin de sécurité de Red Hat)
- CERTA-2004-AVI-377-004 : Vulnérabilité dans la machine virtuelle Java de SUN
(ajout de la référence au bulletin de sécurité HP HPSBUX01100)
- CERTA-2004-AVI-372-001 : Vulnérabilité des noyaux Linux 2.4 et 2.6
(ajout des références CVE CAN-2004-1070, CAN-2004-1071, CAN-2004-1072 et CAN-2004-1073, des bulletins des éditeurs RedHat et SuSE et du statut de la distribution Gentoo)
- CERTA-2004-AVI-206-002 : Vulnérabilité de Aspell
(ajout référence au bulletin de sécurité de Mandrake. Ajout référence CVE)
- CERTA-2004-AVI-352-002 : Vulnérabilité dans PostgreSQL
(ajout référence au bulletin de sécurité de Red Hat)
- CERTA-2004-AVI-376-002 : Vulnérabilité de libXpm, XFree86 et X.Org
(ajout référence aux bulletins de sécurité de Red Hat)

- CERTA-2004-AVI-389-002 : Vulnérabilité de nfs-utils
(ajout du bulletin de sécurité Red Hat)
- CERTA-2004-AVI-400-002 : Multiples vulnérabilités dans Ethereal
(Ajout référence au bulletin de sécurité de Mandrake)
- CERTA-2004-AVI-402-002 : Vulnérabilité de Samba
(ajout référence au bulletin de sécurité de FreeBSD)
- CERTA-2004-AVI-398-002 : Vulnérabilité de Adobe Acrobat Reader sous Unix
(ajout référence au bulletin de sécurité de FreeBSD)
- CERTA-2004-AVI-400-003 : Multiples vulnérabilités dans Ethereal
(Ajout référence au bulletin de sécurité de Debian)
- CERTA-2004-AVI-402-003 : Vulnérabilité de Samba
(ajout référence au bulletin de sécurité Red Hat RHSA-2004-681)
- CERTA-2004-AVI-405-001 : Multiples vulnérabilités de PHP
(ajout références aux bulletins de sécurité Red Hat et OpenBSD (PHP5))
- CERTA-2004-AVI-398-003 : Vulnérabilité de Adobe Acrobat Reader sous Unix
(ajout référence au bulletin de sécurité d'OpenBSD)
- CERTA-2004-AVI-400-004 : Multiples vulnérabilités dans Ethereal
(Ajout référence au bulletin de sécurité de FreeBSD)
- CERTA-2004-AVI-402-004 : Vulnérabilité de Samba
(ajout référence au bulletin de sécurité SuSE SUSE-SA:2004:045)
- CERTA-2004-AVI-407-001 : Vulnérabilité de la commande file
(ajout référence CVE)
- CERTA-2004-AVI-409-001 : Nombreuses failles du noyau Linux
(ajout référence au bulletin de sécurité SUSE SuSE-SA:2004:044)
- CERTA-2004-AVI-411-001 : Vulnérabilité de MIT Kerberos 5
(ajout référence au bulletin de sécurité Mandrake MDKSA-2004:156)
- CERTA-2004-AVI-413-001 : Multiples vulnérabilité dans Konqueror
(ajout référence au bulletin de sécurité Mandrake MDKSA-2004:154)
- CERTA-2004-AVI-414-001 : Vulnérabilités dans MPlayer
(ajout références aux bulletins de sécurité Mandrake, FreeBSD et OpenBSD. Ajout références CVE)
- CERTA-2004-AVI-409-002 : Nombreuses failles du noyau Linux
(deuxième mise-à-jour : ajout référence CVE CAN-2004-1144 et bulletin de sécurité SUSE associé)

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 Documentation

- Bulletin d'alerte CERTA-2004-ALE-014 : Exploitation massive d'une faille du forum phpBB
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-014>

6 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

30 décembre 2004 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-2003-AVI-144 CERTA-2004-AVI-126
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-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. 2 – Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
445/tcp	34,66
135/tcp	19,04
80/tcp	8,41
139/tcp	4,59
1433/tcp	4,20
1026/udp	4,12
1434/udp	3,60
137/udp	3,54
1027/udp	3,17
4899/tcp	2,51
9898/tcp	2,32
5554/tcp	2,31
1023/tcp	2,23
2745/tcp	1,00
21/tcp	0,87
6129/tcp	0,72
3127/tcp	0,65
22/tcp	0,52
443/tcp	0,40
1080/tcp	0,35
111/tcp	0,25
3128/tcp	0,19
3389/tcp	0,13
42/tcp	0,12
10080/tcp	0,04
5000/tcp	0,04
6112/tcp	0,03

TAB. 3 – *Paquets rejetés*