

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°30

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-030>

Gestion du document

Référence	CERTA-2004-ACT-030
Titre	Bulletin d'actualité N°30
Date de la première version	23 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 09 et le 16 décembre 2004. Aucune évolution significative n'a été remarquée.

2 Problèmes liés aux serveurs mutualisés

Le CERTA a récemment traité des incidents comportant des défigurations multiples de sites web. Les incidents de ce type affectent souvent des serveurs mutualisés, c'est-à-dire, des serveurs hébergeant plusieurs sites web, n'ayant aucun rapport les uns avec les autres.

Il suffit qu'un seul de ces sites comporte une vulnérabilité pour que la sécurité de tous les autres sites du serveur ne soit plus assurée. L'exploitation d'une vulnérabilité affectant un site (par exemple une vulnérabilité php) permet donc par exemple de modifier le contenu de tous les sites du serveur.

Les sites web comportent de plus en plus de fonctionnalités et d'applicatifs qui peuvent faire l'objet de vulnérabilités (voir la note d'information CERTA-2004-INF-001). La sécurisation des applications web est donc une tâche de plus en plus complexe, et il n'est pas rare de voir des sites mal sécurisés.

L'actualité fournit une illustration de ce phénomène, avec l'exploitation d'une faille concernant les forums phpBB (ver Santy) : le CERTA a traité plusieurs cas de défiguration de site liés à la présence d'un tel forum sur un autre site web localisé sur le même serveur.

Il est donc important de bien évaluer le type d'hébergement lorsque l'on opte pour cette solution. Le choix de la mutualisation limite sans doute les coûts de l'hébergement d'un site web, mais rend donc sa sécurité dépendante de celle des sites web colocalisés.

3 Rappel des avis et des mises à jour émis

Durant la période du 13 au 17 décembre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-392 : Vulnérabilités dans WordPad
- CERTA-2004-AVI-393 : Vulnérabilité dans le service DHCP de Microsoft Windows
- CERTA-2004-AVI-394 : Vulnérabilité dans HyperTerminal de Microsoft
- CERTA-2004-AVI-395 : Vulnérabilité dans le noyau Windows et LSASS
- CERTA-2004-AVI-396 : Vulnérabilité dans Kerio WinRoute Firewall
- CERTA-2004-AVI-397 : Vulnérabilité de Adobe Acrobat Reader
- CERTA-2004-AVI-398 : Vulnérabilité de Adobe Acrobat Reader sous Unix
- CERTA-2004-AVI-399 : Vulnérabilité dans ISAKMPD sous OpenBSD
- CERTA-2004-AVI-400 : Multiples vulnérabilités dans Ethereal
- CERTA-2004-AVI-401 : Vulnérabilité du pare-feu Microsoft Windows XP SP2
- CERTA-2004-AVI-402 : Vulnérabilité de Samba
- CERTA-2004-AVI-403 : Vulnérabilité d'eTrust Antivirus de Computer Associates
- CERTA-2004-AVI-404 : Vulnérabilité de LiveUpdate pour les produits Symantec

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

- CERTA-2004-AVI-384-001 : Vulnérabilité du service WINS de Microsoft (Ajout du bulletin de sécurité Microsoft et de la section Solution)
- CERTA-2004-AVI-389-001 : Vulnérabilité de nfs-utils (ajout du bulletin de sécurité Gentoo)
- CERTA-2004-AVI-352-001 : Vulnérabilité dans PostgreSQL (Mention de la référence CVE et de l'annonce PostgreSQL. Ajout références aux bulletins de sécurité de Debian, Mandrake et FreeBSD)
- CERTA-2004-AVI-376-001 : Vulnérabilité de libXpm, XFree86 et X.Org (ajout référence au bulletin de sécurité de Debian)
- CERTA-2004-AVI-368-003 : Multiples vulnérabilités de Samba (ajout de la référence au bulletin de sécurité SGI)
- CERTA-2004-AVI-388-002 : Vulnérabilité dans imlib (Ajout de la référence CVE CAN-2004-1025. Ajout référence au bulletin de sécurité de Red Hat)

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.

6 Documentation

- Note d'information CERTA-2004-INF-001 : Sécurité des applications Web et vulnérabilité de type « injection de données »

<http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001>

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	4
3	Paquets rejetés	5

Gestion détaillée du document

23 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	29,46
135/tcp	27,65
139/tcp	8,63
137/udp	3,61
1026/udp	3,45
80/tcp	3,23
4899/tcp	3,15
1433/tcp	3,03
5554/tcp	2,37
1027/udp	2,34
9898/tcp	2,34
1434/udp	2,20
1023/tcp	2,14
2745/tcp	1,33
22/tcp	0,93
3127/tcp	0,82
6129/tcp	0,75
21/tcp	0,67
111/tcp	0,43
443/tcp	0,37
1080/tcp	0,36
3128/tcp	0,20
23/tcp	0,17
42/tcp	0,15
5000/tcp	0,14
3389/tcp	0,09
10080/tcp	0,01

TAB. 3 – *Paquets rejetés*