



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juillet 2004
N° CERTA-2004-ACT-011

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N11

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-011>

Gestion du document

Référence	CERTA-2004-ACT-011
Titre	Bulletin d'actualité N11
Date de la première version	27 juillet 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 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.

2 Activité en cours

Nous constatons toujours un bruit de fond sur les ports 135/tcp, 445/tcp, 139/tcp et 137/tcp.
De plus, l'activité sur le port 5554/tcp dû au ver Sasser est toujours visible cette semaine.

port	pourcentage
135/tcp	26,84
445/tcp	25,72
139/tcp	12,67
137/udp	10,83
5554/tcp	5,71
80/tcp	3,40
2745/tcp	3,13
1433/tcp	1,94
1434/udp	1,87
9898/tcp	1,56
3127/tcp	1,55
4899/tcp	1,11
1023/tcp	1,08
6129/tcp	0,86
21/tcp	0,67
443/tcp	0,28
1080/tcp	0,19
3128/tcp	0,13
111/tcp	0,13
5000/tcp	0,12
22/tcp	0,06
23/tcp	0,05
3389/tcp	0,04
6112/tcp	0,04
10080/tcp	0,01

TAB. 2 – *Paquets rejetés*

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.

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

La table 3 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.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-066 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-064 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-132
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-152
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-209 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-179 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-131
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-051 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-193 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-210 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-052
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-001 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-111 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-127 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-253
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-031
139	TCP	NetBios-ssn	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-168 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-144 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-120
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-043 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-102 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-068 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-041 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-004 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-120
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-150 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-093 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-120 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-178
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-053 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-103 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-038 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-120
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-001
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-157
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-062 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-180
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-163
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-214
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–

TAB. 3 – Correctifs correspondant aux ports destination des paquets rejetés

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.

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 inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité.

4 Rappel des avis et des mises à jour émis

Du 18 juillet 2004 au 24 juillet 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-248 : Vulnérabilité de l2tpd
- CERTA-2004-AVI-249 : Vulnérabilité de Solaris Volume Manager
- CERTA-2004-AVI-250 : Vulnérabilités dans Cisco ONS 15000
- CERTA-2004-AVI-251 : Vulnérabilité de Samba
- CERTA-2004-AVI-252 : Vulnérabilité de Courier MTA, Courier-IMAP et Courier SqWebMail
- CERTA-2004-AVI-253 : Vulnérabilité du service RPC DCE

Les mises à jour suivantes ont été publiées :

- CERTA-2004-AVI-228-003 : Vulnérabilités dans Ethereal (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2004-AVI-234-001 : Faille dans le serveur SSLtelnet (ajout des références aux bulletins de sécurité Debian et FreeBSD)
- CERTA-2004-AVI-244-003 : Vulnérabilité de PHP (ajout de la référence au bulletin de sécurité OpenBSD)
- CERTA-2004-AVI-247-001 : Vulnérabilité du module Apache mod_ssl (ajout de la référence à la mise à jour NetBSD pour ap-ssl)
- CERTA-2004-AVI-244-004 : Vulnérabilité de PHP (ajout des références aux bulletins de sécurité Red Hat)
- CERTA-2004-AVI-231-001 : Vulnérabilité de plusieurs navigateurs (ajout du bulletin de sécurité Gentoo)
- CERTA-2004-AVI-244-005 : Vulnérabilité de PHP (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2004-AVI-225-002 : Multiples vulnérabilités du noyau Linux (ajout de la référence au second bulletin de sécurité Gentoo GLSA 200407-16 ainsi que la description de la vulnérabilité CVE CAN-2004-0447)
- CERTA-2004-AVI-247-002 : Vulnérabilité du module Apache mod_ssl (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-248-001 : Vulnérabilité de l2tpd (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-247-003 : Vulnérabilité du module Apache mod_ssl (ajout de la référence au bulletin de sécurité Debian. Ajout référence CVE)
- CERTA-2004-AVI-251-001 : Vulnérabilité de Samba (ajout de la référence au bulletin de sécurité SUSE)

5 Documentation

Liste des tableaux

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

Gestion détaillée du document

27 juillet 2004 version initiale.