Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 septembre 2004
N° CERTA-2004-ACT-018

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N18

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2004-ACT-018

Gestion du document

Référence	CERTA-2004-ACT-018
Titre	Bulletin d'actualité N18
Date de la première version	17 septembre 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

Durant la semaine du 02 au 09 septembre 2004, l'activité constatée sur les ports surveillés était principalement composée de rejets sur les ports 445/tcp, 135/tcp et 137/udp. Le trafic à destination du port 22/tcp (ssh) représente toujours une menace particulière pour les comptes mal protégés.

Par ailleurs, un de nos correspondants nous a signalés la compromission d'un serveur sous Sun Solaris 2.6 ou 2.7, vraisemblablement par l'exploitation d'une faille rpc ou de dtspcd. L'exploitation de telles failles correspond au

trafic observé sur les ports 6112/tcp et 111/tcp, qui, même s'il est de faible intensité, est particulièrement dangereux pour les machines non mises à jour. L'analyse du disque dur de cette machine devrait être prochainement réalisé par le CERTA. Nous rappelons qu'il est très important de nous signaler ce type de compromission.

port	pourcentage
445/tcp	30,08
135/tcp	23,47
137/udp	14,93
1026/udp	3,66
139/tcp	3,10
80/tcp	2,90
1433/tcp	2,83
5554/tcp	2,71
9898/tcp	2,60
1023/tcp	2,35
1027/udp	2,31
2745/tcp	1,62
1434/udp	1,60
3127/tcp	1,06
6129/tcp	1,02
4899/tcp	0,82
1080/tcp	0,75
22/tcp	0,61
21/tcp	0,59
443/tcp	0,34
3128/tcp	0,23
23/tcp	0,16
3389/tcp	0,14
6112/tcp	0,08
5000/tcp	0,02
111/tcp	0,02
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

Le tableau 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. Unpare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-20 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-17 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-21 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-00 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-11 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-03
139	TCP	NetBios-ssn	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-16 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-14 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-00 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-09 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-17 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-30 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-03 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-15
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-18 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-21
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-16
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-21
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*

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.

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 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 Rappel des avis et des mises à jour émis

Pendant la période du 06 au 10 septembre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-299 : Vulnérabilité de xv
- CERTA-2004-AVI-300 : Vulnérabilité de IBM DB2
- CERTA-2004-AVI-301 : Vulnérabilité dans le module mod_ssl du serveur web Apache
- CERTA-2004-AVI-302 : Vulnérabilité du serveur DNS de Sun Solaris 8
- CERTA-2004-AVI-303 : Vulnérabilité de cdrecord
- CERTA-2004-AVI-304 : Vulnérabilité de mpg123
- CERTA-2004-AVI-305 : Vulnérabilité de OpenCA
- CERTA-2004-AVI-306 : Vulnérabilité de Usermin
- CERTA-2004-AVI-307 : Vulnérabilité de Samba
- CERTA-2004-AVI-308 : Vulnérabilité dans OpenSSH
- CERTA-2004-AVI-309 : Multiples vulnérabilités dans Mac OS X
- CERTA-2004-AVI-310 : Vulnérabilité de F-Secure anti-virus pour Microsoft Exchange et F-secure Internet Gatekeeper

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

- CERTA-2004-AVI-286-002 : Vulnérabilités de MIT Kerberos V (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-292-001 : Vulnérabilités de imlib et imlib2 (ajout de la référence à la mise à jour de sécurité NetBSD)
- CERTA-2004-AVI-106-006 : Vulnérabilités de tcpdump (ajout de la référence au bulletin de sécurité Apple)
- CERTA-2004-AVI-153-006 : Vulnérabilité de Rsync (ajout de la référence au bulletin de sécurité Apple)
- CERTA-2004-AVI-178-006 : Vulnérabilité du module Apache mod_ssl (ajout de la référence au bulletin de sécurité Apple)
- CERTA-2004-AVI-180-006 : Vulnérabilité de MIT Kerberos 5 (ajout de la référence au bulletin de sécurité Apple et modification de la référence au bulletin de sécurité Sun)
- CERTA-2004-AVI-210-006 : Vulnérabilité du serveur HTTP Apache (ajout de la référence au bulletin de sécurité Apple)
- CERTA-2004-AVI-259-001 : Vulnérabilité de KAME Racoon (ajout de la référence au bulletin de sécurité Apple)

- CERTA-2004-AVI-263-001 : Multiples vulnérabilités dans SquirrelMail (ajout de la référence au bulletin de sécurité Apple)
- CERTA-2004-AVI-272-001 : Vulnérabilités du serveur tnftpd (ajout de la référence au bulletin de sécurité Apple et de la référence CVE)
- CERTA-2004-AVI-281-002 : Multiples vulnérabilités dans gaim (ajout de la référence au bulletin de sécurité de Red Hat)
- CERTA-2004-AVI-282-003 : Vulnérabilité de la bibliothèque zlib (ajout de la référence au bulletin de sécurité de Mandrake)
- CERTA-2004-AVI-286-003 : Vulnérabilités de MIT Kerberos 5 (ajout de la référence à la mise à jour de sécurité NetBSD)
- CERTA-2004-AVI-292-002 : Vulnérabilités de imlib et imlib2 (ajout de la référence aux bulletins de sécurité de Mandrake et Gentoo)
- CERTA-2004-AVI-295-001 : Vulnérabilité dans ImageMagick (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-301-001 : Vulnérabilité dans le module mod_ssl du serveur (ajout de la référence à la mise à jour de sécurité NetBSD)
- CERTA-2004-AVI-269-001 : Vulnérabilité de gaim (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2004-AVI-294-001 : Vulnérabilité de lha (ajout de la référence au bulletin de sécurité Gentoo)

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

17 septembre 2004 version initiale.