Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 septembre 2004
N° CERTA-2004-ACT-017

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N17

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-017`

Gestion du document

Référence	CERTA-2004-ACT-017
Titre	Bulletin d'actualité N17
Date de la première version	09 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 26 août au 02 septembre 2004, près de la moitié des rejets constatés sur les ports surveillés étaient composés de tentatives de connexion sur les ports 135/tcp et 445/tcp. Nous avons ajouté les ports 1026/udp et 1027/udp dans le tableau des paquets rejetés. Ces paquets représentent près de 8% des rejets sur les ports surveillés. L'activité sur ces deux ports est assimilé à du « spam » en utilisant le service `messenger` de Windows (utilisation de la commande `NET SEND`). L'envoi abusif de messages par ce service a généralement pour but

port	pourcentage
445/tcp	26,97
135/tcp	24,97
137/udp	8,34
139/tcp	6,12
1026/udp	4,71
1027/udp	3,52
80/tcp	3,31
5554/tcp	3,22
9898/tcp	3,04
1433/tcp	2,74
1023/tcp	2,66
1434/udp	1,74
2745/tcp	1,56
3127/tcp	1,41
1080/tcp	1,25
6129/tcp	1,07
4899/tcp	0,92
21/tcp	0,65
443/tcp	0,52
22/tcp	0,37
3389/tcp	0,19
3128/tcp	0,18
23/tcp	0,18
111/tcp	0,15
5000/tcp	0,09
6112/tcp	0,08
389/tcp	0,05

TAB. 2 – *Paquets rejetés*

d'inciter les utilisateurs à consulter certains sites qui peuvent être malveillants. C'est la raison pour laquelle il est préférable de désactiver le service `messenger` de Windows et de filtrer les ports 1026/udp et 1027/udp. Pour avoir plus d'informations sur le « spam messenger », consultez le lien suivant :

http://www.msn.fr/aidemsn/antispam/messengerspam/

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 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 30 août au 03 septembre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-280 : Vulnérabilité dans divers produits Symantec
- CERTA-2004-AVI-281 : Vulnérabilité dans gaim
- CERTA-2004-AVI-282 : Vulnérabilité de la bibliothèque zlib

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
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
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
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

– CERTA-2004-AVI-283 : Vulnérabilité dans MySQL
– CERTA-2004-AVI-284 : Nombreuses vulnérabilité dans Oracle
– CERTA-2004-AVI-285 : Vulnérabilité dans l'agent de messagerie dtmail de CDE
– CERTA-2004-AVI-286 : Vulnérabilités de MIT Kerberos 5
– CERTA-2004-AVI-287 : Vulnérabilité du logiciel Winamp
– CERTA-2004-AVI-288 : Vulnérabilités dans KDE
– CERTA-2004-AVI-289 : Vulnérabilité de gnome-vfs
– CERTA-2004-AVI-290 : Vulnérabilité du serveur icecast
– CERTA-2004-AVI-291 : Vulnérabilités dans les produits Mozilla
– CERTA-2004-AVI-292 : Vulnérabilités de imlib et imlib2
– CERTA-2004-AVI-293 : Vulnérabilité de Sun xdm
– CERTA-2004-AVI-294 : Vulnérabilité de lha
– CERTA-2004-AVI-295 : Vulnérabilité dans ImageMagick
– CERTA-2004-AVI-296 : Vulnérabilité de WinZip
– CERTA-2004-AVI-297 : Vulnérabilité de Squid
– CERTA-2004-AVI-298 : Vulnérabilité dans OpenBSD

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

– CERTA-2004-AVI-265-001 : Vulnérabilité du noyau Linux (ajout référence aux bulletins de sécurité de SuSE, Gentoo et Mandrake)
– CERTA-2004-AVI-257-003 : Vulnérabilité de SoX (ajout de la référence au bulletin de sécurité FreeBSD)
– CERTA-2004-AVI-270-002 : Vulnérabilités d'Adobe Acrobat (ajout de la référence au bulletin de sécurité NetBSD et des liens vers les références CVE)
– CERTA-2004-AVI-271-002 : Vulnérabilité de rsync (ajout des références aux bulletins de sécurité FreeBSD et NetBSD)
– CERTA-2004-AVI-278-001 : Vulnérabilité de la bibliothèque NSS (ajout de la référence au bulletin de sécurité FreeBSD)
– CERTA-2004-AVI-268-001 : Vulnérabilité du navigateur Opera (ajout de la référence au bulletin de sécurité NetBSD)
– CERTA-2004-AVI-274-001 : Vulnérabilité de SpamAssassin (ajout de la référence au bulletin de sécurité NetBSD
– CERTA-2004-AVI-275-001 : Vulnérabilité dans la bibliothèque Qt (ajout des références aux bulletins de sécurité de Chris Evans, FreeBSD et NetBSD ainsi que la liste des changements dans Qt 3.3.3)
– CERTA-2004-AVI-276-001 : Vulnérabilité dans Courier-IMAP (ajout des références aux bulletins de sécurité Gentoo et FreeBSD ainsi que de la référence CVE)
– CERTA-2004-AVI-268-002 : Vulnérabilité du navigateur Opera (remplacement de Mozilla par Opera à la section Description)
– CERTA-2004-AVI-275-002 : Vulnérabilité dans la bibliothèque Qt (ajout de la référence au bulletin de sécurité de Debian)
– CERTA-2004-AVI-281-001 : Multiples vulnérabilités dans gaim (ajout de la référence au bulletin de sécurité NetBSD)
– CERTA-2004-AVI-282-001 : Vulnérabilité dans la bibliothèque zlib (ajout de la référence au bulletin de sécurité NetBSD et du site Internet de zlib)
– CERTA-2004-AVI-283-001 : Vulnérabilité dans MySQL (ajout de la référence au bulletin de sécurité OpenBSD)
– CERTA-2004-AVI-195-005 : Vulnérabilité du module mod_proxy du serveur HTTP Apache (ajout de la référence au bulletin de sécurité SUN)
– CERTA-2004-AVI-278-002 : Vulnérabilité de la bibliothèque NSS (ajout de la référence au bulletin de sécurité Sun)
– CERTA-2004-AVI-271-003 : Vulnérabilité de rsync (ajout de la référence au bulletin de sécurité RedHat)
– CERTA-2004-AVI-283-002 : Vulnérabilité dans MySQL (ajout de la référence au bulletin de sécurité Gentoo)
– CERTA-2004-AVI-286-001 : Vulnérabilités de MIT Kerberos 5 (ajout de la référence au bulletin de sécurité Cisco)

– CERTA-2004-AVI-270-003 : Vulnérabilités d'Adobe Acrobat (ajout du lien Internet de téléchargement de Adobe Acrobat Reader)
– CERTA-2004-AVI-076-001 : Python 2.2 : Débordement de variable dans la gestion des réponses du DNS (ajout des références aux bulletins de sécurité Gentoo et NetBSD)
– CERTA-2004-AVI-282-002 : Vulnérabilité de la bibliothèque zlib (ajout de la référence au bulletin de sécurité SuSE)
– CERTA-2004-AVI-284-001 : Nombreuses vulnérabilités dans les produits Oracle (ajout de détails et de documentations)

5 Documentation

Liste des tableaux

Gestion détaillée du document

09 septembre 2004 version initiale.