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 juillet 2004
N° CERTA-2004-ACT-008

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N8

Gestion du document

Référence	CERTA-2004-ACT-008
Titre	Bulletin d'actualité N8
Date de la première version	09 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

L'activité entre le 24 juin 2004 et le 01 juillet 2004 a été marquée par les recherches des ports 135/tcp et 445/tcp, qui représentent 60% des rejets sur nos dispositifs de filtrage, malgré les mesures de filtrage déployées par certains fournisseurs d'accès.

L'activité liée aux recherches de services vulnérables sous Linux et SunOS (ports 22/tcp, 111/tcp, 443/tcp et 6112/tcp) est non négligeable.

port	pourcentage
135/tcp	31,27
445/tcp	29,20
137/udp	10,16
139/tcp	8,99
80/tcp	4,86
1433/tcp	3,29
2745/tcp	2,86
1434/udp	1,61
3127/tcp	1,47
9898/tcp	1,12
5554/tcp	1,06
6129/tcp	1,03
4899/tcp	0,86
21/tcp	0,59
5000/tcp	0,38
443/tcp	0,31
1080/tcp	0,29
23/tcp	0,21
3128/tcp	0,18
3389/tcp	0,16
111/tcp	0,07
6112/tcp	0,02
22/tcp	0,01
389/tcp	0,01

TAB. 2 – *Paquets rejetés*

3 La pertinence des journaux

Certains dispositifs de filtrage ne fournissent que quelques éléments sur les paquets enregistrés dans les journaux, en se limitant souvent à l'horodatage, l'adresse IP source, l'adresse IP destination, le protocole, ainsi qu'aux ports source et destination (dans le cas des protocoles TCP et UDP). Si ces informations donnent un aperçu de l'activité sur le réseau, elles sont insuffisantes dans le cadre du traitement d'un incident.

Dans le cas du protocole à états TCP, les en-têtes des paquets contiennent des `flags` qui permettent de déterminer l'état de la communication : établissement ou fin de la connexion, envoi ou acquittement des données, etc. Lorsqu'un paquet TCP est rejeté, l'examen des `flags` permet de qualifier la nature du rejet (recherche de services, paquets arrivés en retard, déni de service, etc).

Le numéro de séquence des paquets est un paramètre qui peut fournir des informations sur la source des paquets.

L'en-tête IP contient également des paramètres importants, comme par exemple, le paramètre `TTL` (`Time To Live`) qui représente le nombre de routeurs traversés. A chaque passage de routeur, cette valeur est décrémentée de 1. La valeur de départ est généralement de 64, 128 ou 255 (suivant le système d'exploitation qui a émis le paquet, et le protocole utilisé). Le `TTL` permet, dans certains cas, de déterminer si la source du paquet est plausible ou ou si l'adresse a été usurpée (`IP spoofing`).

La synchronisation des horloges des dispositifs de filtrage (à l'aide du protocole `NTP -Network Time Protocol-` par exemple) est aussi un élément à prendre en compte. La corrélation des événements survenus sur plusieurs machines distinctes ne peut se faire que si les horloges sont cohérentes. Il peut donc être utile de synchroniser les différents équipements du réseau.

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

La table 3 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 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.

5 Rappel des avis et des mises à jour émis

Pendant la semaine du 28 juin 2004 au 02 juillet 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-209 : Vulnérabilités de BEA WebLogic
- CERTA-2004-AVI-210 : Vulnérabilité du serveur HTTP Apache
- CERTA-2004-AVI-211 : Vulnérabilité dans XFree86
- CERTA-2004-AVI-212 : Vulnérabilité dans la bibliothèque libpng
- CERTA-2004-AVI-213 : Vulnérabilité dans Directory Services de Mac OS X
- CERTA-2004-AVI-214 : Vulnérabilité sur Novell iChain
- CERTA-2004-AVI-215 : Vulnérabilité de HP-UX ARPA Transport
- CERTA-2004-AVI-216 : Vulnérabilité de pavuk
- CERTA-2004-AVI-217 : Vulnérabilités dans MPlayer
- CERTA-2004-AVI-218 : Vulnérabilité dans Cisco Collaboration Server
- CERTA-2004-AVI-219 : Multiples vulnérabilités de rlpr

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-050 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-195 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-210
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-00 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-111 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-127
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-126
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-045 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-126
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-156 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-095 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126 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-105 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-038 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-126
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-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-186
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-165
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-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*

Les mises à jour suivantes ont été publiées :

- CERTA-2004-AVI-195-002 : Vulnérabilité du module mod_proxy du serveur HTTP Apache (ajout référence au bulletin de sécurité Debian)
- CERTA-2003-AVI-201-001 : Vulnérabilité sur le moteur de recherche SPIRIT de la société Technologie (précision sur la disponibilité de la version corrigée)
- CERTA-2004-AVI-204-002 : Multiples vulnérabiltés du service ISC DHCP (ajout référence au bulletin de sécurité de FreeBSD)
- CERTA-2004-AVI-180-005 : Vulnérabilité de MIT Kerberos 5 (ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2004-AVI-167-002 : Multiples vulnérabilités sur le serveur HTTP Apache (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2004-AVI-178-004 : Vulnérabilité du module Apache mod_ssl (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2004-AVI-195-003 : Vulnérabilité du module mod_proxy du serveur HTTP Apache (ajout référence au bulletin de sécurité Mandrake)
- CERTA-2004-AVI-210-001 : Vulnérabilité du serveur HTTP Apache (ajout référence au bulletin de sécurité de Mandrake)
- CERTA-2004-AVI-216-001 : Vulnérabilité de pavuk (ajout de la référence CVE et de la version impactée)
- CERTA-2004-ALE-009-001 : Vulnérabilités d'Internet Explorer (prise en compte de la vulnérabilité ADODB.Stream et ajout du lien pour la désinstallation du composant)

6 Documentation

Liste des tableaux

Gestion détaillée du document

09 juillet 2004 version initiale.