Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 août 2004
N° CERTA-2004-ACT-014

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N14

Gestion du document

Référence	CERTA-2004-ACT-014
Titre	Bulletin d'actualité N14
Date de la première version	18 août 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

Dans la semaine du 05 août au 12 août 2004, plus de 60% des rejets constatés correspondent à l'activité sur les ports 445/tcp et 135/tcp. L'activité sur les ports 21/tcp (ftp) et 23/tcp (telnet) est relativement élevée alors qu'il n'y pas eu de failles récentes concernant ces services. Il peut s'agir de tentatives de connexion sur des comptes particuliers, avec des mots de passe faibles, comme pour le cas de ssh (voir Section Activité Particulière).

port	pourcentage
445/tcp	32,84
135/tcp	29,71
139/tcp	7,28
2745/tcp	3,83
80/tcp	3,45
9898/tcp	2,95
5554/tcp	2,59
1023/tcp	2,45
1433/tcp	2,38
1434/udp	2,08
4899/tcp	2,04
137/udp	1,93
3127/tcp	1,80
6129/tcp	1,54
21/tcp	0,74
23/tcp	0,73
1080/tcp	0,46
22/tcp	0,26
3128/tcp	0,25
5000/tcp	0,22
111/tcp	0,14
3389/tcp	0,14
10080/tcp	0,11
443/tcp	0,06
6112/tcp	0,04

TAB. 2 – *Paquets rejetés*

3 Activité particulière

Depuis quelques semaines, les rejets sur le port 22/tcp (ssh) ont augmenté. Cette augmentation des rejets n'est pas liée à la découverte d'une nouvelle vulnérabilité du serveur `ssh`, mais à l'utilisation d'un outil qui essaie de se connecter au serveur en utilisant les comptes `guest`, `user`, `test`, `admin` et `root` avec des mots de passe triviaux.

Cette activité laisse des traces caractéristiques dans les journaux :

```
Jul 29 22:12:35 serveur-ssh sshd[8456]: Illegal user guest
Jul 29 22:12:35 serveur-ssh sshd[8456]: Failed password for illegal user guest
```

Sur une machine compromise récemment analysée par le CERTA, de nombreux comptes avaient des mots de passe triviaux. Parfois, ce mot de passe était le nom du compte. Ces comptes faiblement protégés peuvent être visés par les tentatives de connexion sur les ports 21/tcp, 22/tcp et 23/tcp. Même s'il ne s'agit généralement pas de comptes avec des privilèges élevés, il est possible pour un intrus d'obtenir les droits de l'administrateur en exploitant une vulnérabilité locale, notamment une affectant `ptrace` (voir avis CERTA-2002-AVI-016, CERTA-2001-AVI-124).

Afin de se protéger de ce type d'attaque, il convient de s'assurer qu'il n'y a pas de mots de passe faibles sur vos machines, et de supprimer les comptes qui ne sont plus utilisés, et d'appliquer des règles de filtrage strictes au niveau du pare-feu pour les ports 21/tcp et 22/tcp. Il est par ailleurs fortement déconseillé d'utiliser le service `telnet` sur l'Internet, puisque les communications et la phase d'authentification ne sont pas chiffrées.

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 relatifsaux 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. 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.

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 09 au 13 août 2004, le CERTA a émis la mise à jour suivante :

– CERTA-2004-AVI-266-004 : Multiples Vulnérabilités de la bibliothèque libpng (ajout des références aux bulletins de sécurité Sun et Apple)

6 Documentation

– Avis CERTA-2001-AVI-124 : Vulnérabilités dans le noyau linux (2.2.x et 2.4.x)
http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-124
– Avis CERTA-2002-AVI-016 : Vulnérabilité de ptrace dans les systèmes BSD
http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-016

Liste des tableaux

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 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-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 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-247
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*

Gestion détaillée du document

18 août 2004 version initiale.