

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°22

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-022>

Gestion du document

Référence	CERTA-2004-ACT-022
Titre	Bulletin d'actualité N°22
Date de la première version	15 octobre 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 30 septembre au 07 octobre 2004, le CERTA a constaté sur deux dispositifs de filtrage que la majorité des rejets étaient dûs à du trafic à destination du port 135/tcp. L'activité sur le port 445/tcp a également été élevée, représentant près de 20% des rejets pour les ports sous surveillance. En revanche, l'activité sur le port 137/udp est particulièrement faible en comparaison avec ce qui avait pu être observé les semaines précédentes.

Un ministère nous a transmis ses observations particulières sur le port 445/tcp. Les rejets ont été multipliés par 10 en l'espace d'un mois, avec un pic particulièrement important pour le 06 octobre 2004. Les adresses IP source

port	pourcentage
135/tcp	35,38
445/tcp	19,28
139/tcp	9,05
137/udp	6,28
5554/tcp	4,51
1026/udp	3,20
1433/tcp	2,85
2745/tcp	2,71
9898/tcp	2,55
80/tcp	2,54
1023/tcp	2,26
1027/udp	2,06
1080/tcp	1,89
1434/udp	1,23
6129/tcp	0,76
4899/tcp	0,74
3127/tcp	0,64
21/tcp	0,37
443/tcp	0,36
22/tcp	0,34
3389/tcp	0,22
5000/tcp	0,21
111/tcp	0,19
3128/tcp	0,16
23/tcp	0,14
10080/tcp	0,05
6112/tcp	0,02

TAB. 2 – *Paquets rejetés*

de la majorité de ces paquets font partie de deux classes C qui se trouvent dans le bloc 212.234.0.0/16. Le ministère qui reçoit ce trafic possède également des adresses dans le bloc 212.234.0.0/16.

Le CERTA a besoin de vos journaux sur ce port afin de comprendre la nature de cette activité. N'hésitez pas à nous appeler pour déterminer le moyen de nous les faire parvenir.

Les rejets sur les ports 135/tcp et 445/tcp, bien que souvent associés respectivement aux vers Blaster et Sasser, peuvent aussi être liés à l'activité de personnes mal intentionnées cherchant à exploiter des failles des services rpc-dcom et lsass de Microsoft Windows. Dans ce cas, les conséquences de la compromission peuvent être plus graves, car les actions entreprises par l'intrus sur la machine compromise sont totalement imprévisibles (destruction volontaire ou non de fichiers, vol de données bancaires, attaques en déni de service par saturation, etc).

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. 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.

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. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2004-AVI-066 CERTA-2004-AVI-064 CERTA-2003-AVI-132
22	TCP	SSH	–	CERTA-2003-AVI-152
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-179 CERTA-2003-AVI-131
80	TCP	HTTP	–	CERTA-2004-AVI-050 CERTA-2004-AVI-195 CERTA-2004-AVI-210 CERTA-2004-AVI-239 CERTA-2004-AVI-313 CERTA-2004-AVI-315
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn	–	CERTA-2003-AVI-168 CERTA-2003-AVI-144 CERTA-2004-AVI-126
389	TCP	LDAP	–	CERTA-2004-AVI-045 CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-095 CERTA-2004-AVI-126 CERTA-2004-AVI-178 CERTA-2004-AVI-247 CERTA-2004-AVI-301 CERTA-2004-AVI-313
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2003-AVI-038 CERTA-2004-AVI-126
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	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

4 Rappel des avis et des mises à jour émis

Durant la semaine du 04 au 08 octobre, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-330 : Vulnérabilités dans RealPlayer
- CERTA-2004-AVI-331 : Multiples vulnérabilités dans Mac OS X
- CERTA-2004-AVI-332 : Vulnérabilité de Samba

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

- CERTA-2004-AVI-313-002 : Vulnérabilités du serveur http Apache 2.0.x (Ajout de la référence au bulletin de sécurité Debian)
- CERTA-2004-AVI-325-002 : Vulnérabilités de XFree86 et de libXpm (LessTif est prise en compte. Ajout de la référence au bulletin de sécurité de Red Hat (RHSA-2004-078) et Debian (DSA-560))
- CERTA-2004-AVI-329-001 : Vulnérabilité dans Subversion (ajout référence au bulletin de sécurité de Gentoo)

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	2
3	Correctifs correspondant aux ports destination des paquets rejetés	4

Gestion détaillée du document

15 octobre 2004 version initiale.