Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 mai 2005
N° CERTA-2005-ACT-020

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°2005-20

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-2005-ACT-020`

Gestion du document

Référence	CERTA-2005-ACT-020
Titre	Bulletin d'actualité N°2005-20
Date de la première version	20 mai 2005
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 Activité en cours

1.1 Ports observés

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 05 et le 12 mai 2005.

2 Les flux multimédia

Avec la banalisation des connexions haut débit, est apparu la possibilité de recevoir des flux multimédia « en temps réel » plus couramment appelés *Streaming*. On pourra citer à titre d'exemple : RTSP (`Real Time Streaming Protocol`) ou MMS (`Microsoft Multimedia Server`).

On peut distinguer essentiellement deux types de flux : video et audio. Ils sont bien souvent composés de simples paquets de type UDP. Mais parfois, ils utilisent des ports prévus à un tout autre usage comme le `80/tcp`.

Il peut arriver que l'utilisation abusive en interne de ce type de technologie induise l'administrateur en erreur. En effet, les flux multimedia sont généralement par essence très consommateurs en bande passante. Ce que l'administrateur pourrait prendre pour une attaque par saturation (`flood`) depuis l'extérieur n'est, en fait, due qu'à des utilisateurs de son propre réseau qui écoutent ou regardent une radio ou une vidéo en ligne. De plus, certains logiciels utilisant le port `80/tcp` sont capables d'utiliser les serveurs mandataires (`proxy`). Il peut arriver dans

ce cas que ces derniers ne soient pas dimensionnés pour accepter ce type d'utilisation et se retrouvent en état de déni de service.

Recommandation :

Si vous constatez une consommation excessive de votre bande passante, il convient donc d'examiner l'orientation des flux et de s'assurer que le phénomène n'est pas dû à ces types de flux. En particulier, la consultation des journaux du serveur mandataire est souvent révélatrice. Une parade possible à ce déni de service consiste à filtrer les sites qui distribuent ce type de flux via le serveur mandataire. Cependant, ce n'est qu'une explication parmi d'autres pour une consommation excessive de bande passante. Si vous constatiez ce type de phénomène, veuillez en informer le CERTA.

3 Rappel des avis et mises à jour émis

Durant la période du 09 au 13 mai 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-159 : Multiples vulnérabilités dans Mac OS X
- CERTA-2005-AVI-160 : Vulnérabilité d'iTunes
- CERTA-2005-AVI-161 : Vulnérabilité dans phpBB
- CERTA-2005-AVI-162 : Vulnérabilité de l'explorateur Windows
- CERTA-2005-AVI-163 : Multiples vulnérabilités de gaim

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

- CERTA-2005-AVI-104-006 : Vulnérabilité de libXpm
  (ajout références aux bulletins de sécurité Mandriva et Debian relatifs à XFree86)
- CERTA-2005-AVI-147-002 : Vulnérabilité dans OpenOffice
  (ajout référence au bulletin de sécurité Mandriva)
- CERTA-2005-AVI-104-007 : Vulnérabilité de libXpm
  (ajout référence au bulletin de sécurité Red Hat relatif à openmotif)

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. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

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

Le tableau 2 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 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.

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 4
3 Paquets rejetés 5

Gestion détaillée du document

20 mai 2005 version initiale.

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-131
25	TCP	SMTP	–	CERTA-2005-AVI-133
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
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 et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051
389	TCP	LDAP	–	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-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051
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
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
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	–
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
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	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

TAB. 2 – *Correctifs correspondant aux ports destination des paquets rejetés*

port	pourcentage
1433/tcp	21,69
1026/udp	15,20
139/tcp	14,71
137/udp	12,96
1027/udp	11,54
4899/tcp	5,63
445/tcp	4,40
15118/tcp	3,68
1434/udp	2,37
9898/tcp	0,88
2745/tcp	0,79
5554/tcp	0,72
80/tcp	0,67
3306/tcp	0,64
1080/tcp	0,59
6129/tcp	0,56
22/tcp	0,46
25/tcp	0,46
23/tcp	0,41
42/tcp	0,34
21/tcp	0,26
1023/tcp	0,16
11768/tcp	0,16
2100/tcp	0,16
111/tcp	0,15
443/tcp	0,13
3127/tcp	0,10
135/tcp	0,08
5000/tcp	0,03
3389/tcp	0,02
8866/tcp	0,02
6101/tcp	0,02

TAB. 3 – *Paquets rejetés*