Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 juillet 2005
N° CERTA-2005-ACT-029

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-29

Gestion du document

Référence	CERTA-2005-ACT-029
Titre	Bulletin d'actualité n° 2005-29
Date de la première version	22 juillet 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

Le CERTA observe de plus en plus fréquemment le déploiement de réseaux sans fil en environnement de production. Le réseau sans fil séduit par sa facilité de déploiement ainsi que le coût d'investissement faible. Parfois, le réseau sans fil est la seule solution en regard de contraintes particulières.
Comme il est mentionné dans la recommandation du CERTA CERTA-2002-REC-002 du 26 octobre 2004, un certain nombre de points de sécurité sont à prendre en compte.
L'architecture du réseau, lors de l'introduction de matériels sans fil doit être revue avec attention. Un travail de réflexion en amont sur l'intégration du réseau sans fil dans un réseau existant doit être effectuée. Il est fréquent de trouver un réseau sans fil directement raccordé à un réseau (intranet par exemple) sans prise en compte de la sécurité, chose dramatique du point de vue de la sécurité. Les réseaux sans fils doivent être traités à la manière d'une DMZ (zone démilitarisée).
Le chiffrement du lien sans fil est le point le plus médiatisé, non sans raisons.
En l'absence de chiffrement, les données sont directement visibles, d'aussi loin que la portée du réseau sans fil le permet. Le WEP (`Wired Equivalent Privacy`), mécanisme de chiffrement initial, est aujourd'hui très largement insuffisant pour assurer un minimum de sécurité. Des outils et techniques publiques sont disponibles permettant de trouver une clef WEP (64 ou 128 bits) en moins de 3 minutes.
Du matériel compatible WPA ou WPA2 est aujourd'hui nécessaire. La norme WPA resoud les faiblesses largement discutées du WEP (authentification, intégrité, chiffrement). La norme WPA2 ajoute un chiffrement ayant recourt à l'AES. En tout état de cause, IPSEC ou n'importe quelle technique de VPN doit être utilisée si l'on désire un niveau de confidentialité robuste.

Il faut noter que les réseaux sans fil restent toujours vulnérables à des attaques de type déni de service (attaques de la couche 1 par brouilleurs actifs, attaques sur la couche 2 par désassociation par exemple). Il est difficile de se pémunir contre ces attaques. Le réseau sans fil ne doit donc pas être utilisé si le réseau est critique en terme de disponibilité.
Cependant, la sécurité des réseaux sans fils ne doit pas se limiter à la seule sécurité du lien. La sécurité des points d'accès (désactivation de services non nécessaires, mises à jour de firmwares), des serveurs d'authentification ainsi que des clients doit être au centre des préoccupations.
Dans toutes ces problématiques, le CERTA peut vous apporter une assistance opérationnelle.

1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 06 et le 13 juillet 2005.

2 Rappel des avis et mises à jour émis

Durant la période du 11 juillet au 15 juillet 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-249 : Vulnérabilité de Ruby ;
- CERTA-2005-AVI-250 : Vulnérabilité de dhcpd ;
- CERTA-2005-AVI-251 : Vulnérabilité de cpio ;
- CERTA-2005-AVI-252 : Vulnérabilité dans IBM Tivoli Management Framework ;
- CERTA-2005-AVI-253 : Vulnérabilité dans Microsoft Word ;
- CERTA-2005-AVI-254 : Vulnérabilité dans le module de gestion des couleurs de Microsoft ;
- CERTA-2005-AVI-255 : Multiples vulnérabilités dans les produits Oracle ;
- CERTA-2005-AVI-256 : Multiples vulnérabilité dans les produits Mozilla ;
- CERTA-2005-AVI-257 : Vulnérabilité de MIT Kerberos 5 ;
- CERTA-2005-AVI-258 : Multiples vulnérabilités dans Mac OS X ;
- CERTA-2005-AVI-259 : Vulnérabilités dans CISCO Call Manager ;
- CERTA-2005-AVI-260 : Vulnérabilités dans IBM AIX ftpd ;
- CERTA-2005-AVI-261 : Multiples vulnérabilités dans Bugzilla ;
- CERTA-2005-AVI-262 : Vulnérabilité de SquirrelMail ;
- CERTA-2005-AVI-263 : Vulnérabilité dans Cisco Security Agent (CSA) ;
- CERTA-2005-AVI-264 : Vulnérabilité dans CISCO ONS 15216 OADM ;
- CERTA-2005-AVI-265 : Vulnérabilité de IBM Lotus Notes ;
- CERTA-2005-AVI-266 : Vulnérabilité de Sophos Anti-Viru ;
- CERTA-2005-AVI-267 : Vulnérabilité dans JRun de Macromedia.

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

- CERTA-2005-AVI-096-001 : Vulnérabilités dans phpBB (ajout des bulletins de sécurité iDEFENSE id=204 et id=205, du bulletin supplémentaire FreeBSD ainsi que des références CVE CAN-2005-0258 et CVE CAN-2005-0259.)
- CERTA-2005-AVI-165-004 : Vulnérabilité dans Squid (ajout de la référence au bulletin de sécurité Debian DSA-751.)
- CERTA-2005-AVI-167-001 : Multiples vulnérabilités dans CVS (ajout des références aux bulletins de sécurité SUSE et Debian.)
- CERTA-2005-AVI-192-001 : Vulnérabilité de Net-SNMP (ajout de la référence CVE CAN-2005-1740 et du bulletin de sécurité FreeBSD.)
- CERTA-2005-AVI-225-007 : Vulnérabilité dans SpamAssassin (ajout de la référence au bulletin de sécurité OpenBSD.)
- CERTA-2005-AVI-242-005 : Vulnérabilités dans PHP PEAR (ajout des références aux bulletins de sécurité RedHat RHSA-2005:564, SUSE SUSE-SA-2005:041, Debian DSA-745, Debian DSA-747, Gentoo GLSA 200507-06, Gentoo GLSA 200507-07 et Gentoo GLSA 200507-08.)
- CERTA-2005-AVI-246-003 : Vulnérabilité de la bibliothèque zlib (ajout de la référence au bulletin de sécurité OpenBSD 3.6 relatif à zlib, correctif 019.)

- CERTA-2005-AVI-247-002 : Vulnérabilités dans Adobe Reader (ajout des références aux bulletins de sécurité iDEFENSE, RedHat RHSA-2005:575 et Gentoo GLSA 200507-09.)
- CERTA-2005-AVI-153-001 : Multiples vulnérabilités de MPlayer (ajout des bulletins de sécurité MPlayer (#vuln 10 et #vuln 11) et du bulletin de sécurité Mandriva MDKSA-2005:115.)
- CERTA-2005-AVI-183-004 : Vulnérabiltés dans gzip (ajout de la référence au bulletin de sécurité Debian DSA-752.)
- CERTA-2005-AVI-234-004 : Vulnérabilité de ClamAV (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:113.)
- CERTA-2005-AVI-221-002 : Vulnérabilité de gedit (ajout de la référence au bulletin de sécurité Debian.)
- CERTA-2005-AVI-242-006 : Vulnérabilités dans PHP PEAR (ajout de la référence au bulletin de sécurité OpenBSD.)
- CERTA-2005-AVI-249-001 : Vulnérabilité de Ruby (ajout de la référence à l'annonce du correctif et des références aux bulletins de sécurité Gentoo et Mandriva.)
- CERTA-2005-AVI-250-001 : Vulnérabilité de dhcpd (ajout de la référence au bulletin de sécurité Mandriva.)
- CERTA-2005-AVI-164-005 : Multiples vulnérabilités dans tcpdump (ajout de la référence au bulletin de sécurité SUSE.)
- CERTA-2005-AVI-195-001 : Vulnérabilité de libtiff (ajout de la référence au bulletin de sécurité Debian.)
- CERTA-2005-AVI-202-005 : Multiples vulnérabilités de Gaim (ajout de la référence au bulletin de sécurité SUSE.)
- CERTA-2005-AVI-243-002 : Multiples vulnérabilités de Cacti (ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:017 et des références CVE CAN-2005-2148 et CAN-2005-2149.)
- CERTA-2005-AVI-246-004 : Vulnérabilité de la bibliothèque zlib (ajout de la référence au bulletin de sécurité SUSE.)
- CERTA-2005-AVI-250-002 : Vulnérabilité de dhcpd (ajout de la référence au bulletin de sécurité SUSE.)
- CERTA-2005-AVI-256-001 : Multiples vulnérabilité dans les produits Mozilla (suppression de Mozilla Thunderbird 1.0.2 dans les sytèmes affectées.)
- CERTA-2005-AVI-257-001 : Vulnérabilité de MIT Kerberos 5 (ajout de la référence au bulletin de sécurité SUSE.)
- CERTA-2005-AVI-256-002 : Multiples vulnérabilité dans les produits Mozilla (ajout des références aux bulletins de sécurité Mandriva MDKSA-2005:120 et Gentoo GLSA 200507-14.)
- CERTA-2005-AVI-224-003 : Vulnérabilité de SquirrelMail (ajout de la référence au bulletin de sécurité Debian.)
- CERTA-2005-AVI-242-007 : Vulnérabilités dans PHP PEAR (ajout de la référence au bulletin de sécurité Debian DSA-746.)
- CERTA-2005-AVI-247-003 : Vulnérabilités dans Adobe Reader (ajout de la référence au bulletin de sécurité SUSE.)
- CERTA-2005-AVI-257-002 : Vulnérabilité de MIT Kerberos 5 (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:119.)
- CERTA-2005-AVI-245-001 : Vulnérabilités dans OpenLDAP, nss_ldap et pam_ldap (ajout de la référence au bulletin de sécurité Gentoo 200507-13, correction de la référence CVE.)

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

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 2 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.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

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 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

Gestion détaillée du document

15 juillet 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2005-A http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2003-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
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-A
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-A
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A http://www.certa.ssi.gouv.fr/site/CERTA-2004-A
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-A
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-A
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-A
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-A
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-A
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	41.63
80/tcp	15.95
1026/udp	12.07
1027/udp	8.49
1433/tcp	7.88
137/udp	2.35
445/tcp	1.8
4899/tcp	1.1
15118/tcp	0.77
23/tcp	0.67
25/tcp	0.65
1434/udp	0.64
2745/tcp	0.63
3128/tcp	0.51
1080/tcp	0.48
443/tcp	0.46
6101/tcp	0.45
3127/tcp	0.42
9898/tcp	0.34
10000/tcp	0.33
42/tcp	0.32
5000/tcp	0.31
22/tcp	0.29
3306/tcp	0.28
5554/tcp	0.27
10080/tcp	0.2
8866/tcp	0.18
6129/tcp	0.13
21/tcp	0.06
2100/tcp	0.05
11768/tcp	0.02
119/tcp	0.01

TAB. 3 – *Paquets rejetés*

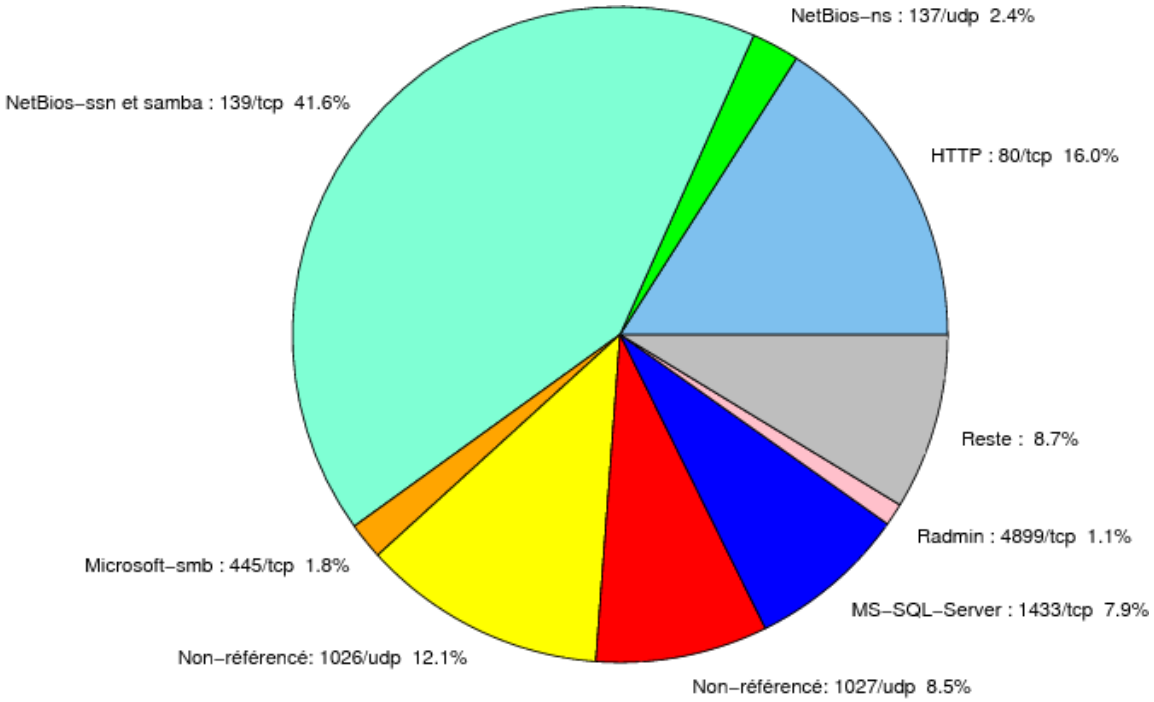

FIG. 1 – *Répartition relative des ports pour la semaine du 06.07.2005 au 13.07.2005*