Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2005
N° CERTA-2005-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-32

Gestion du document

Référence	CERTA-2005-ACT-032
Titre	Bulletin d'actualité n° 2005-32
Date de la première version	12 août 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 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 04 et le 11 août 2005.

1.2 Correctifs de sécurité Microsoft du 9 août 2005 :

Suite à la parution des correctifs Microsoft du 9 août 2005, des outils exploitant ces vulnérabilités ont été rendus publics. C'est le cas en particulier pour la vulnérabilité décrite dans l'avis CERTA-2005-AVI-302 concernant les fonctions `plug and play` de Microsoft Windows. Nous avons la confirmation qu'il existe au moins un outil fonctionnel capable de compromettre un système vulnérable.

1.2.1 Recommandations :

Il est recommandé d'appliquer sans tarder les correctifs de sécurité mis à disposition par Microsoft pour chacune des vulnérabilités concernées.

1.3 Activité anormale sur le port `6101/tcp` :

Nous constatons depuis cette semaine une activité croissante sur le port `6101/tcp` comme le montre la figure 1. Cette activité est sans doute liée à la mise à disposition d'outils malveillants visant à exploiter des vulnérabilités du logiciel de sauvegarde `Veritas Backup Exec` décrites dans l'avis CERTA-2005-AVI-229 du 23 juin 2005.

1.3.1 Recommandations :

Il est encore une fois recommandé d'appliquer les correctifs de sécurité associés à ces vulnérabilités. Il est également conseillé de filtrer les flux à destination du port `6101/tcp` et provenant de l'Internet.

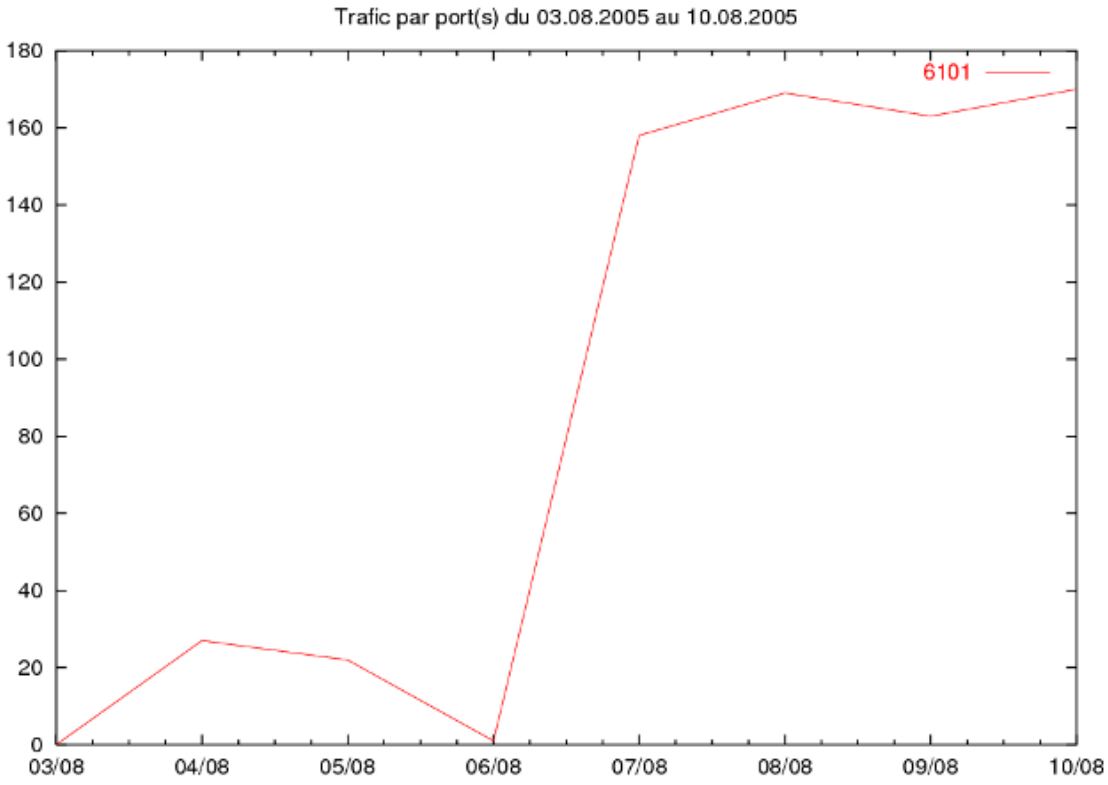

FIG. 1 – *Trafic sur le port 6101/tcp pour la semaine du 04.08.2005 au 11.08.2005*

2 Rappel des avis et mises à jour émis

Durant la période du 01 au 05 août 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-293 : Vulnérabilité dans BrightStor ARCserve/Enterprise Backup
- CERTA-2005-AVI-294 : Vulnérabilité de HP NonStop DCE Core Services
- CERTA-2005-AVI-295 : Vulnérabilité dans SAP R/3 Internet Graphic Server
- CERTA-2005-AVI-296 : Vulnérabilité de apt-cacher
- CERTA-2005-AVI-297 : Vulnérabilité de Business Objects Enterprise et Crystal Reports
- CERTA-2005-AVI-298 : Multiples Vulnérabilités dans Oracle for Openview (OfO)

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

- CERTA-2005-AVI-128-001 : Vulnérabilité dans Sylpheed
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-195-002 : Vulnérabilité de libtiff
  (ajout de la référence au bulletin de sécurité FreeBSD)

- CERTA-2005-AVI-246-005 : Vulnérabilité de la bibliothèque zlib
  (ajout de la référence au bulletin de sécurité Gentoo GLSA 200508-01)
- CERTA-2005-AVI-276-004 : Vulnérabilité sur la bibliothèque zlib
  (ajout de la référence au bulletin de sécurité Gentoo GLSA 200508-01)
- CERTA-2005-AVI-284-001 : Multiples vulnérabilités dans le logiciel Ethereal
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-287-002 : Vulnérabilité de Opera
  (ajout des références aux bulletins de sécurité FreeBSD)
- CERTA-2005-AVI-292-001 : Vulnérabilité de l'éditeur Vim
  (ajout des références aux bulletins de sécurité FreeBSD)
- CERTA-2005-AVI-282-001 : Multiples vulnérabilités dans ProFTPD
  (ajout de la référence au bulletin de sécurité Gentoo GLSA 200508-02 et à la référence CVE CAN-2005-2390)

3 Actions suggérées

3.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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.

3.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres chose s, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participen t à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utili sateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

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

12 août 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERT
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERT
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERT
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERT
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070 6101	TCP TCP	BrightStor ARCserve/Enterprise Backup Veritas Backup Exec	– –	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERT
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERT
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/CERT
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

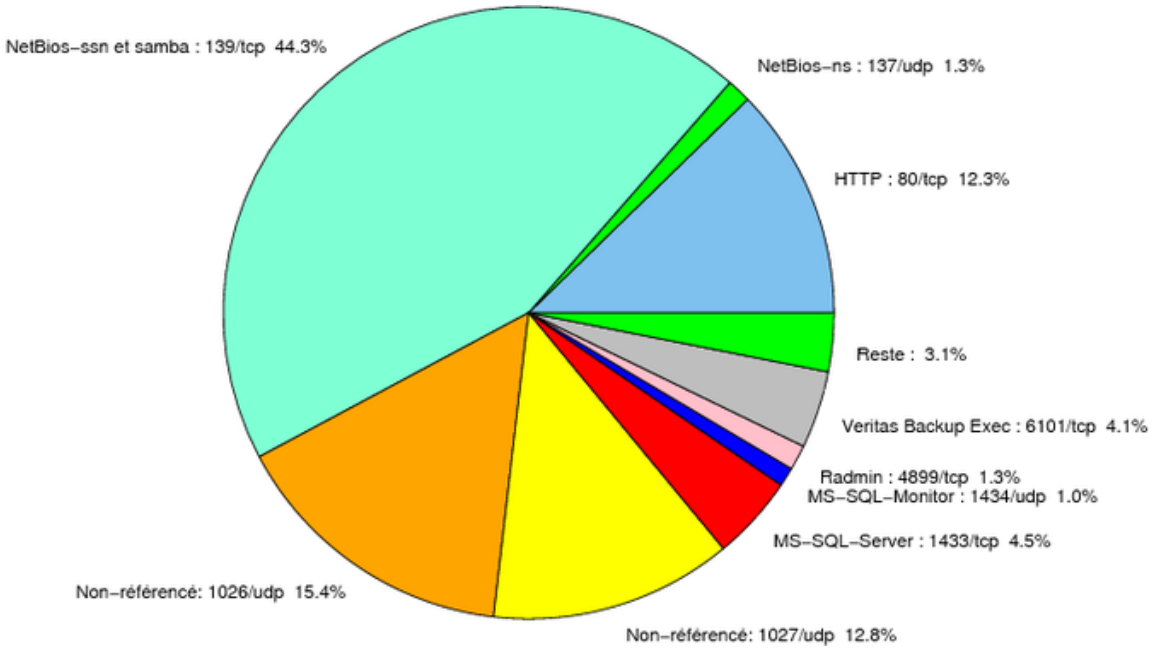

FIG. 2: Répartition relative des ports pour la semaine du 04.08.2005 au 11.08.2005

port	pourcentage
139/tcp	44,25
1026/udp	15,35
1027/udp	12,84
80/tcp	12,27
1433/tcp	4,47
6101/tcp	4,08
4899/tcp	1,32
137/udp	1,27
1434/udp	1
15118/tcp	0,55
1080/tcp	0,43
143/tcp	0,33
2745/tcp	0,28
445/tcp	0,2
3306/tcp	0,14
5554/tcp	0,13
25/tcp	0,12
9898/tcp	0,11
21/tcp	0,08
6129/tcp	0,07
10000/tcp	0,06
11768/tcp	0,04
3127/tcp	0,02
6070/tcp	0,01

TAB. 3: Paquets rejetés