Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 janvier 2005
N° CERTA-2005-ACT-004

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N2005-04

Gestion du document

Référence	CERTA-2005-ACT-004
Titre	Bulletin d'actualité N2005-04
Date de la première version	28 janvier 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

Pendant la semaine du 13 au 20 janvier 2005, nous avons constaté, sur trois dispositifs de filtrage, une augmentation assez forte des rejets sur le port 15118/tcp qui sont attribués pour le moment à l'activité du cheval de Troie `Netdepix`. Ce cheval de Troie est extrêmement actif : le trafic réseau qu'il engendre est tel qu'il peut rapidement saturer les réseaux locaux et provoquer des dysfonctionnements des pare-feux.

Si vous constatez un taux de rejet anormal de paquets sortant de vos réseaux, contactez le CERTA.

Nous avons ajouté les ports 6101/tcp et 3306/tcp à notre surveillance.

Le port 6101/tcp est associé au service `Veritas Backup Exec`. Une vulnérabilité affectant ce service a fait l'objet d'un avis du CERTA (avis CERTA-2005-AVI-024). Des programmes exploitant automatiquement cette vulnérabilité ont été rendus public sur l'Internet. Les rejets indiqués dans le tableau 3 (en fin de document) montrent que le service `Veritas Backup Exec` est recherché. Par conséquent, il est urgent de vérifier l'intégrité de vos machines offrant ce service, de les mettre à jour, et de filtrer le port 6101/tcp au niveau des pare-feux.

Le port 3306/tcp correspond au serveur de base de données `MySQL`. Il est possible que l'exploitation d'un mot de passe faible soit recherchée, ce qui expliquerait les rejets que l'on constate sur ce port. Il est donc important de veiller à ce qu'un mot de passe fort soit utilisé, d'empêcher les connexions à distance en utilisant le compte de l'administrateur (typiquement `root`), et de filtrer le port 3306/tcp au niveau des pare-feux.

Dans les deux cas, si vous constatez dans vos journaux des connexions réussies à l'un de ces services, il est important d'entrer en contact avec le CERTA.

2 Rappel des avis et des mises à jour émis

Durant la période du 17 au 21 janvier 2005, le CERTA a émis l'avis suivant :

- CERTA-2005-AVI-016 : iTunes : débordement de variable dans la gestion des listes de lecture
- CERTA-2005-AVI-017 : CUPS : vulnérabilité dans l'impression de certains documents PDF
- CERTA-2005-AVI-018 : Multiples vulnérabilité dans CUPS
- CERTA-2005-AVI-019 : Vulnérabilité dans Xpdf
- CERTA-2005-AVI-020 : Vulnérabilité de ImageMagick
- CERTA-2005-AVI-021 : Vulnérabilité dans la configuration du serveur de fax HylaFAX

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

- CERTA-2004-AVI-198-001 : Multiples vulnérabilités sous IRIX
  (ajout référence au bulletin de sécurité Avaya ASA-2005-006)
- CERTA-2004-AVI-255-001 : Vulnérabilité de Pavuk
  (ajout référence au bulletin de sécurité Avaya ASA-2005-006)
- CERTA-2004-AVI-372-002 : Vulnérabilité des noyaux Linux 2.4 et 2.6
  (ajout référence au bulletin de sécurité Avaya ASA-2005-006)
- CERTA-2004-AVI-409-004 : Nombreuses failles du noyau Linux
  (ajout référence au bulletin de sécurité Avaya ASA-2005-006)
- CERTA-2004-AVI-247-006 : Vulnérabilité du module Apache mod_ssl
  (ajout de la référence aux mises à jour de sécurité VMware)
- CERTA-2004-AVI-265-002 : Vulnérabilité du noyau Linux
  (ajout référence aux mises à jour de sécurité VMware)
- CERTA-2004-AVI-343-001 : Vulnérabilité du module mod_ssl du serveur HTTP Apache
  (ajout référence aux mises à jour de sécurité VMware)
- CERTA-2004-AVI-405-002 : Multiples vulnérabilités de PHP
  (ajout références aux bulletins de sécurité Red Hat et OpenBSD (PHP5))
- CERTA-2004-AVI-418-004 : Vulnérabilité de Xpdf
  (modification du lien vers le serveur de Foolabs)
- CERTA-2005-AVI-014-001 : Multiples vulnérabailités dans Exim
  (ajout d'une nouvelle vulnérabilité découverte dans Exim)
- CERTA-2004-AVI-409-005 : Nombreuses failles du noyau Linux
  (ajout référence au bulletin de sécurité RedHat RHSA-2005:043)
- CERTA-2005-AVI-020-001 : Vulnérabilité de ImageMagick
  (ajout de la référence au bulletin de sécurité Gentoo)

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 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.

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.

5 Documentation

- Avis CERTA-2003-AVI-149 : « Vulnérabilités dans le service RPCSS sous Windows »
  http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-149

Liste des tableaux

Gestion détaillée du document

28 janvier 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-20 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-38
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
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-11 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-03
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-36 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-16 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-14 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-00 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-03 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
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-ALE-00
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-15
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-18 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-21
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-16
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-02
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-21
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
445/tcp	65,12
135/tcp	12,59
139/tcp	4,87
15118/tcp	1,89
137/udp	1,85
1026/udp	1,69
1433/tcp	1,65
1027/udp	1,55
4899/tcp	1,46
11768/tcp	0,97
5554/tcp	0,80
80/tcp	0,68
5000/tcp	0,67
6129/tcp	0,58
9898/tcp	0,55
2745/tcp	0,54
1434/udp	0,39
42/tcp	0,36
1023/tcp	0,30
6101/tcp	0,29
1080/tcp	0,26
22/tcp	0,22
21/tcp	0,20
3127/tcp	0,16
3306/tcp	0,11
23/tcp	0,09
443/tcp	0,06
111/tcp	0,05
3128/tcp	0,02
3389/tcp	0,01
10080/tcp	0,01

TAB. 3 – *Paquets rejetés*