Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 septembre 2004
N° CERTA-2004-ACT-019

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N19

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-019

Gestion du document

Référence	CERTA-2004-ACT-019
Titre	Bulletin d'actualité N19
Date de la première version	24 septembre 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

Les rejets constatés sur deux dispositifs de filtrage pendant la semaine du 09 au 16 septembre 2004 étaient principalement composés de paquets à destination des ports 445/tcp, 135/tcp et 137/udp. L'importance en volume du trafic sur le port 137/udp n'est pas expliquée.

port	pourcentage
137/udp	26,66
445/tcp	22,06
135/tcp	19,74
139/tcp	3,74
1433/tcp	3,44
1026/udp	3,00
9898/tcp	2,74
80/tcp	2,50
5554/tcp	2,42
1023/tcp	2,37
1027/udp	2,21
2745/tcp	2,19
1434/udp	1,72
3127/tcp	0,85
4899/tcp	0,81
1080/tcp	0,80
21/tcp	0,59
6129/tcp	0,49
22/tcp	0,44
443/tcp	0,43
23/tcp	0,29
111/tcp	0,22
5000/tcp	0,14
3128/tcp	0,08
3389/tcp	0,04
10080/tcp	0,02

TAB. 2 – *Paquets rejetés*

3 Vulnérabilité de la bibliothèque gdiplus.dll sous Windows

La vulnérabilité concernant la bibliothèque `gdiplus.dll` sous Windows a fait l'objet d'un avis du CERTA (CERTA-2004-AVI-312) ainsi que d'une alerte (CERTA-2004-ALE-011).

Quelques précisions s'imposent au sujet de cette vulnérabilité.

La bibliothèque `gdiplus.dll` est installée par défaut par certaines versions de Windows (Windows XP ou Windows Server 2003) et/ou par certaines applications (suite Office et Internet Explorer 6 par exemple). Elle est utilisée pour le traitement des images au format JPEG (type le plus répandu sur l'Internet). Il est tout à fait possible que plusieurs versions de cette bibliothèque soient installées sur une même machine. Les applications n'utilisent pas forcément la bibliothèque `gdiplus.dll` qui se trouve dans l'arborescence système de Windows. C'est la raison pour laquelle l'application du correctif de Microsoft peut sembler confuse. Il s'agit, dans un premier temps, de corriger le fichier qui aurait pu être créé par l'installation de Windows, puis de mettre les correctifs pour chaque applicatif tiers pouvant avoir installé cette bibliothèque. Enfin, il est possible que d'autres applications non référencées par Microsoft utilisent leur propre bibliothèque `gdiplus.dll` vulnérable.

Il existe des outils permettant de rechercher des versions vulnérables du fichier `gdiplus.dll`. Le CERTA a testé ces outils, mais les résultats ne sont pas satisfaisants. Il est préférable de rechercher manuellement les fichiers `gdiplus.dll`, et de vérifier leur version.

Les versions suivantes sont connues comme étant vulnérables :

- toutes les versions antérieure à la version `5.1.3102.1355` ;
- la version `5.2.3790.0` ;
- la version `6.0.3260.0`.

Les versions suivantes ne sont pas vulnérables :

- la version `5.1.3102.1355` ;
- la version `5.1.3102.1360` ;
- la version `5.1.3102.2180` ;
- la version `5.2.3790.136` ;
- les versions `6.0.3264.0` et postérieures.

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.

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 3 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. Unpare-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.

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-17 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-21 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
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	–	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-2004-AVI-04 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-09 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-17 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-30 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31
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
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	–
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	–

TAB. 3 – *Correctifs correspondant aux ports destination des paquets rejetés*

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 Rappel des avis et des mises à jour émis

Pendant la période du 13 au 17 septembre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-310 : Vulnérabilité de F-Secure anti-virus pour Microsoft Exchange et F-secure Internet Gatekeeper
- CERTA-2004-AVI-311 : Multiples vulnérabilités de Samba
- CERTA-2004-AVI-312 : Vulnérabilité de GDI+ de Microsoft
- CERTA-2004-AVI-313 : Vulnérabilités du serveur http Apache 2.0.x
- CERTA-2004-AVI-314 : Vulnérabilité dans le composant WordPerfect Converter de Microsoft
- CERTA-2004-AVI-315 : Vulnérabilité du module mod_rewrite
- CERTA-2004-AVI-316 : Vulnérabilité dans Squid
- CERTA-2004-AVI-317 : Vulnérabilité de CUPS
- CERTA-2004-AVI-318 : Vulnérabilité d'OpenOffice et StarOffice
- CERTA-2004-AVI-319 : Multiples vulnérabilités dans gdk-pixbuf
- CERTA-2004-AVI-320 : Multiples vulnérabilités sur les logiciels Mozilla
- CERTA-2004-AVI-321 : Multiples vulnérabilités dans BEA WebLogic

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

- CERTA-2004-AVI-306-001 : Vulnérabilité de Usermin (ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2004-AVI-304-001 : Vulnérabilité de mpg123 (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2004-AVI-306-002 : Vulnérabilité de Usermin (ajout de la référence au bulletin de sécurité de FreeBSD)
- CERTA-2004-AVI-272-002 : Vulnérabilité du serveur tnftpd (ajout de la référence au bulletin de sécurité Heimdal et à la mise à jour de sécurité du paquetage NetBSD heimdal)
- CERTA-2004-AVI-303-001 : Vulnérabilité de cdrecord (ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2004-AVI-306-003 : Vulnérabilité de Usermin (ajout de la référence au bulletin de sécurité de Debian)
- CERTA-2004-AVI-291-001 : Vulnérabilités dans les produits Mozilla (ajout des références aux deux bulletins de sécurité FreeBSD)
- CERTA-2004-AVI-292-003 : Vulnérabilités de imlib et imlib2 (ajout de la référence au bulletins de sécurité de Red Hat)
- CERTA-2004-AVI-297-001 : Vulnérabilité de Squid (ajout référence au bulletin de sécurité de Mandrake. Ajout référence CVE)
- CERTA-2004-AVI-292-004 : Vulnérabilités de imlib et imlib2 (ajout de la référence au bulletins de sécurité de Debian)
- CERTA-2004-AVI-295-002 : Vulnérabilité dans ImageMagick (ajout de la référence au bulletin de sécurité Debian)

– CERTA-2004-AVI-304-002 : Vulnérabilité de mpg123 (ajout de la référence au bulletin de sécurité Gentoo)
– CERTA-2004-AVI-319-001 : Multiples vulnérabilités dans gdk-pixbuf (ajout référence au bulletin de sécurité de Debian)
– CERTA-2004-AVI-313-001 : Vulnérabilités du serveur http Apache 2.0.x (Prise en compte de la sortie de la version 2.0.51 d'Apache : ajout des vulnérabilités CVE CAN-2004-0786, CAN-2004-0747 et CAN-2004-0748. Ajout des références aux bulletins de sécurité Gentoo, Mandrake, RedHat et FreeBSD)

6 Documentation

– Avis CERTA-2004-AVI-312 :
http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-312
– Alerte CERTA-2004-ALE-011 :
http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-011

Liste des tableaux

Gestion détaillée du document

24 septembre 2004 version initiale.