



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 septembre 2004
N° CERTA-2004-ACT-016

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N° 16

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-016>

Gestion du document

Référence	CERTA-2004-ACT-016
Titre	Bulletin d'actualité N° 16
Date de la première version	01 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

Durant la semaine du 19 au 26 août 2004, les rejets observés sur deux dispositifs de filtrage ont été composés, pour près de 60%, de tentatives de connexion sur les ports 135/tcp et 445/tcp.

L'activité sur le port 23/tcp (telnet) attire l'attention. Le CERTA n'est, pour le moment, pas en mesure de déterminer la nature de cette activité. Toutefois, une alerte (CERTA-2004-ALE-010) a récemment été publiée au sujet de la vulnérabilité du service telnet de certains équipements Cisco. Il est donc fortement recommandé

port	pourcentage
135/tcp	29,16
445/tcp	28,06
137/udp	9,13
139/tcp	5,76
1433/tcp	3,26
80/tcp	3,14
9898/tcp	2,92
2745/tcp	2,75
5554/tcp	2,68
1023/tcp	2,37
1434/udp	2,19
4899/tcp	1,97
3127/tcp	1,55
6129/tcp	1,33
21/tcp	0,80
22/tcp	0,66
1080/tcp	0,65
23/tcp	0,50
443/tcp	0,34
111/tcp	0,24
3128/tcp	0,19
3389/tcp	0,18
5000/tcp	0,16
6112/tcp	0,03

TAB. 2 – *Paquets rejetés*

d'appliquer les mesures de contournement provisoire décrites dans cette alerte, et d'installer les correctifs dès que ceux-ci seront disponibles.

3 L'activité que vous ne verrez pas dans les journaux des garde-barrières

Et oui, c'est la rentrée

Ceux qui ont pris l'autoroute cet été pour partir en vacances ont sûrement entendu les consignes de sécurité répétées inlassablement sur les ondes : « En cas de problème sur l'autoroute, si vous devez abandonner votre véhicule sur la bande d'arrêt d'urgence, abritez-vous derrière la barrière de sécurité. La durée de vie d'un piéton sur l'autoroute est très faible ».

Sur les autoroutes de l'information, le discours est le même : « Toute machine connectée à l'Internet sans prendre des mesures de sécurité a une durée de vie extrêmement réduite ». A peine connectée, toute machine vulnérable sera compromise, même si vous pensez quelle ne présente pas d'intérêt pour qui que ce soit (se référer à la note d'information CERTA-2002-INF-003 « Chronique d'un incident ordinaire »).

A travers les bulletins d'actualités, le CERTA met en évidence l'activité liée à la recherche de services réseau vulnérables (scan de ports). Ce « trafic non sollicité » est permanent et le CERTA rappelle régulièrement que ne pas démarrer les services réseau non utilisés, mettre en place une protection périmétrique (garde-barrières) et mettre à jour des logiciels sont des mesures indispensables.

Il faut souligner toutefois que le mois d'août a vu la publication d'un grand nombre de vulnérabilités pour lesquelles la protection périmétrique (garde-barrières) est insuffisante. Il s'agit en effet de vulnérabilités exploitables à distance visant non pas un service réseau en écoute sur une machine mais des logiciels client interprétant des données pouvant contenir une charge hostile telles des images ou des fichiers visualisables :

- CERTA-2004-AVI-275 « Vulnérabilité dans la bibliothèque Qt » : faille dans l'interprétation de fichiers au format BMP, PNG, JPEG ou GIF ;
- CERTA-2004-AVI-270 « Vulnérabilités d'Adobe Acrobat » : faille dans l'interprétation de fichiers au format PDF ;
- CERTA-2004-AVI-260 « Multiples vulnérabilités dans Internet Explorer » : faille dans l'interprétation de fichiers au format BMP et GIF ;

- CERTA-2004-AVI-266 « Multiples Vulnérabilités de la bibliothèque libpng » : faille dans l'interprétation de fichiers au format PNG ;
- CERTA-2004-AVI-257 « Vulnérabilité de SoX » : faille dans l'interprétation de fichiers au format WAV.

A ces vulnérabilités liées au traitement des données, on peut également ajouter de nombreuses vulnérabilités liées à la mise en oeuvre d'un protocole donné par un logiciel client :

- CERTA-2004-AVI-287 : « Vulnérabilité du logiciel Winamp » ;
- CERTA-2004-AVI-281 : « Multiples vulnérabilités dans gaim » ;
- CERTA-2004-AVI-277 : « Vulnérabilité de Xine » ;
- CERTA-2004-AVI-267 : « Vulnérabilité dans PuTTY » ;
- CERTA-2004-AVI-261 : « Vulnérabilité des navigateurs Netscape et Mozilla » ;
- CERTA-2004-AVI-255 : « Vulnérabilité de Pavuk ».

Il suffit pour un client de se connecter sur un serveur hostile pour qu'un code arbitraire en provenance du serveur soit exécuté sur la plate-forme client vulnérable.

Pour ces vulnérabilités du « client », seule la mise-à-jour du logiciel vulnérable ou l'utilisation d'un logiciel non vulnérable aux mêmes fonctionnalités est une réponse efficace, le garde-barrière ne filtrant pas les données issues d'un trafic légitime et ne disposant pas toujours de filtres applicatifs pour les protocoles réseau exotiques.

C'est donc l'heure des bonnes résolutions pour cette rentrée : « Non, je n'oublie pas de réaliser la mise-à-jour systématique d'un logiciel que j'utilise lorsqu'une vulnérabilité est publiée ».

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 oeuvre (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.

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.

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-179 CERTA-2003-AVI-131
80	TCP	HTTP	–	CERTA-2004-AVI-050 CERTA-2004-AVI-195 CERTA-2004-AVI-210 CERTA-2004-AVI-239
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
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	–	CERTA-2003-AVI-168 CERTA-2003-AVI-144 CERTA-2004-AVI-126
389	TCP	LDAP	–	CERTA-2004-AVI-045 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-095 CERTA-2004-AVI-126 CERTA-2004-AVI-178 CERTA-2004-AVI-247
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2003-AVI-038 CERTA-2004-AVI-126
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
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186
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	–
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	–

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

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 inexplicables 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 23 au 28 août 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-274 : Vulnérabilité de SpamAssassin
- CERTA-2004-AVI-275 : Vulnérabilité dans la bibliothèque Qt
- CERTA-2004-AVI-276 : Vulnérabilité dans Courier-IMAP
- CERTA-2004-AVI-277 : Vulnérabilité dans Xine
- CERTA-2004-AVI-278 : Vulnérabilité de la bibliothèque NSS
- CERTA-2004-AVI-279 : Multiples vulnérabilités dans Cisco Secure ACS

Durant cette même période, la mise à jour suivante a été publiée :

- CERTA-2004-AVI-270-001 : Vulnérabilités d'Adobe Acrobat (Ajout de la référence au bulletin de sécurité RedHat)

6 Documentation

- CERTA-2002-INF-003 : "Chroniques d'un incident ordinaire"
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-003>

Liste des tableaux

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

Gestion détaillée du document

01 septembre 2004 version initiale.