

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-45

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-2007-ACT-045>

Gestion du document

Référence	CERTA-2007-ACT-045
Titre	Bulletin d'actualité 2007-45
Date de la première version	09 novembre 2007
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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-045.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-045/>

1 Problèmes liés à des relais HTTP

Les incidents de sécurité informatique affectant les serveurs laissent parfois des traces sur l'Internet. C'est le cas par exemple avec les défigurations, qui sont généralement revendiquées sur des sites spécialisés et/ou qui restent dans les caches des moteurs de recherche, ou encore lorsque la machine sert de relais de *phishing* ou de rebond d'attaque (les messages électroniques ou journaux relatifs à ces problèmes sont parfois publiés sur des sites web). Il est un cas que nous n'abordons quasiment jamais : les *proxies* ouverts.

Un *proxy* est un service qui relaie une requête, le cas le plus fréquent étant avec HTTP. L'utilisation d'un *proxy* HTTP (parfois appelé serveur mandataire) permet ainsi de naviguer plus ou moins anonymement sur des sites ou forums. Ils sont parfois utilisés pour déposer des messages tout en indiquant l'adresse IP du *proxy* en lieu et place de celle de l'internaute. Un serveur peut être un *proxy* suite à une action volontaire de l'administrateur, mais aussi à cause d'une erreur de configuration ou d'une intrusion frauduleuse. Des listes de serveurs mandataires publics sont maintenues sur certains sites spécialisés.

Lorsqu'un serveur figure sur une liste de *proxies* ouverts, sa fréquentation peut brutalement augmenter. Cela se traduit entre autres par une augmentation significative de la taille des journaux. Par exemple, dans le cas d'un *proxy* HTTP, de nombreuses connexions au serveur auront pour but de demander des pages externes au site web.

Une des conséquences directes peut être la saturation de la bande passante du serveur. En effet, toute page externe demandée transitera deux fois par le *proxy* : une première fois entre le serveur HTTP réellement interrogé et le *proxy* et une seconde fois entre le *proxy* et le client.

Le CERTA a récemment traité le cas d'un serveur en « déni de service » parce que le mode *proxy* était activé. Cependant, la désactivation de celui-ci ne résoud pas tous les problèmes. En effet, l'adresse IP de ce serveur est référencée dans des listes de *proxies* ouverts. La bande passante est largement moins saturée mais les journaux d'accès au serveur HTTP sont pollués par des demandes de pages externes, ce qui se traduit par des erreurs 404 en grand nombre. Dans ce cas, seul un changement d'adresse IP permet d'alléger les systèmes.

2 Des vulnérabilités associées aux navigateurs

2.1 Introduction

Les navigateurs offrent de manière générale des surfaces d'attaques intéressantes pour les attaquants. Ils se limitent souvent à quelques modèles, partageant des moteurs de rendus. La tendance est actuellement à les complexifier en multipliant les services Web au cours des diverses navigations.

Cette semaine, plusieurs vulnérabilités ont été publiées sur l'Internet. Bien que l'exploitation de ces dernières aient été testées sur Mozilla Firefox, d'autres navigateurs peuvent avoir les mêmes particularités. Elles illustrent cependant que ces applications restent un point de fragilité des machines connectées sur l'Internet.

2.2 Les documents téléchargeables

2.2.1 Présentation

L'en-tête HTTP permet au serveur de préciser différents comportements au niveau du navigateur du poste client.

Le standard MIME permet ainsi d'encapsuler plusieurs types de données dans un même document Internet (courriel ou page Web par exemple).

C'est le cas de l'option `Content-Disposition`. Cette option est définie dans le RFC 2183 (remplaçant du RFC 1806), et permet de définir quelques paramètres pour la récupération d'objets attachés, comme :

- le nom de l'objet ;
- le type ;
- la date de création ou de de modification ;
- la taille en octets. Le standard précise même que cette valeur est indicative, et peut être estimée.

Un exemple visible dans un en-tête de réponse HTTP peut être de la forme :

```
Content-type = application/octet-stream
Content-disposition = attachment; filename=certa.txt
```

L'utilisateur va donc voir une fenêtre qui lui propose d'ouvrir le fichier *certa.txt*, ou de l'enregistrer sur le poste.

Le problème souligné cette semaine par des personnes est que la page ouverte (sans ou après avoir été enregistrée) est interprétée par le navigateur Firefox dans le contexte local de la machine, et non le contexte du site sur lequel la page est prise. Des scripts insérés dans la page téléchargée peuvent ainsi accéder à des données locales.

Il faut que l'utilisateur ouvre, à un moment ou un autre, la page proposée en téléchargement, pour que l'action malveillante réussisse.

La page peut inciter cette action d'une manière ou une autre.

Il faut enfin noter que Microsoft précise bien dans un document de sa base de connaissances (KB279667) que plusieurs méthodes existent pour contourner la demande présentée à l'utilisateur pour enregistrer ou ouvrir le document. Il cite les contrôles ActiveX ou une applet Java.

2.2.2 Recommandations

Les recommandations classiques s'appliquent ici : l'utilisateur doit naviguer sur des sites de confiance, et ne doit pas activer l'interprétation de codes dynamiques (Javascript, ActiveX, etc.) par défaut.

Cette rigueur dans la configuration du navigateur doit s'appliquer pour tout document ouvert avec celui-ci, même s'il est ouvert à partir d'un fichier téléchargé et enregistré sur la machine.

2.3 Les URI de type jar:

2.3.1 Présentation

Le CERTA a mentionné dans de précédents bulletins d'actualité des problèmes issus de l'interprétation par le navigateur de certains champs protocolaires, comme `res:`, `data:`, etc. Des personnes ont rappelé cette semaine qu'un bogue subsiste et concerne `jar:`. Ce bogue a été mentionné dans le site de suivi de bogues de Mozilla, dès février 2007, mais n'est toujours pas corrigé à la date de rédaction de cet article.

Le protocole `jar:` a une syntaxe particulière, et peut être inséré dans une page HTML pour indiquer une archive via une adresse réticulaire URL (chemin absolu), ainsi que le fichier à extraire de cette archive.

```
...
jar:http://serveur_victime_xss/fichier.jar!/mon_fichier
...
```

L'URL peut être de forme quelconque : `http://`, comme dans l'exemple ci-dessus, ou `https://`, `file://`, `ftp://`, `chrome://`, etc.

Cette propriété peut aussi être exploitée via tout site offrant la possibilité de charger de tels fichiers d'archives, qu'ils soient aux formats traditionnels JAR ou ZIP, ou sous des formes plus complexes, comme les formats OpenOffice OpenDocument (ODT) ou Microsoft OpenXML.

Un tel site est alors exploité pour lancer une attaque par injection de code indirecte (XSS).

2.3.2 Recommandations

Plusieurs actions peuvent être entreprises :

- pour l'administrateur :
 - surveiller au niveau d'une passerelle Web les contenus de type `jar:URL!fichier` ;
 - limiter les chargements possibles par les utilisateurs via un site Web, et contrôler l'accès de ceux-ci ;
 - mettre en place éventuellement des mesures de conversion des fichiers.
- pour l'utilisateur :
 - naviguer sur des sites de confiance ;
 - ne pas interpréter par défaut de codes dynamiques au niveau du navigateur ;
 - utiliser un système d'exploitation et des applications (navigateur et antivirus notamment) à jour.

2.4 Documentation associée

- RFC 2183, "Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field", août 1997 :
<http://www.ietf.org/rfc/rfc2183.txt>
- Documentation Java.net, "Class JarURLConnection" :
<http://java.sun.com/j2se/1.4.2/docs/api/java/net/JarURLConnection.html>
- Bug de référence 369814 de Bugzilla, concernant Mozilla Firefox :
https://bugzilla.mozilla.org/show_bug.cgi?id=369814

3 Vulnérabilité sur Macrovision SafeDisc

Macrovision SafeDisc est un mécanisme de vérification de l'authenticité de certains jeux sur Microsoft Windows. Il utilise le pilote `secdrv.sys` et il est installé par défaut sur les systèmes Windows XP, Windows Server 2003 et Windows Vista.

Le CERTA a publié le 06 novembre 2007 l'avis CERTA-2007-AVI-480 portant sur ce pilote. La vulnérabilité est un débordement de mémoire causé par une erreur dans le traitement de certains paramètres de configuration du pilote. L'exploitation de cette faille par une personne malveillante permet une élévation de privilèges maximale. Toutefois, elle nécessite auparavant que l'attaquant soit connecté au système d'exploitation (via un code malveillant ou en local, par exemple).

Le CERTA insiste sur l'importance de cette vulnérabilité car elle affecte tous les utilisateurs de systèmes d'exploitation Windows XP et Windows Server 2003. Windows Vista utilise également *SafeDisc* mais n'est pas affecté par la faille. Macrovision a publié un correctif que l'on peut d'ores et déjà télécharger manuellement. Il

est également probable que Microsoft publie une mise à jour via son système des mises à jour automatiques. La vulnérabilité est actuellement exploitée et il est donc recommandé d'installer la mise à jour de Macrovision sans plus attendre.

Documentation

- Bulletin de sécurité Microsoft 944653 du 05 novembre 2007 :
<http://www.microsoft.com/technet/security/advisory/944653.msp>
- Avis CERTA-2007-AVI-480 du 07 novembre 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-480/index.html>
- Bulletin de sécurité ESB-2007-0871 de l'AusCERT du 06 novembre 2007:
<http://www.auscert.org.au/render.html?it=8310>

4 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 01 et le 08 novembre 2007.

5 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1935>
- Note d'information du CERTA sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

6 Rappel des avis émis

Dans la période du 02 au 09 novembre 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-462 : Vulnérabilité de McAfee e-Business Server
- CERTA-2007-AVI-463 : Vulnérabilités dans Symantec Mail Security
- CERTA-2007-AVI-464 : Multiples vulnérabilités dans IBM AIX
- CERTA-2007-AVI-465 : Vulnérabilité dans NuFW

- CERTA-2007-AVI-466 : Vulnérabilité dans les serveurs Sun Fire X2100/X2200 M2
- CERTA-2007-AVI-467 : Vulnérabilité dans CUPS
- CERTA-2007-AVI-468 : Vulnérabilité dans Novell BorderManager
- CERTA-2007-AVI-469 : Vulnérabilité dans IBM Lotus Domino
- CERTA-2007-AVI-470 : Vulnérabilité de Tomcat WebDAV et des applications l'utilisant
- CERTA-2007-AVI-471 : Vulnérabilité de Blue Coat Security Gateway OS
- CERTA-2007-AVI-472 : Multiples vulnérabilités de SonicWALL SSL VPN
- CERTA-2007-AVI-473 : Multiples vulnérabilités dans les extensions de Nagios
- CERTA-2007-AVI-474 : Vulnérabilité de l'antivirus Symantec
- CERTA-2007-AVI-475 : Vulnérabilité dans Avaya
- CERTA-2007-AVI-476 : Multiples vulnérabilités dans gFTP
- CERTA-2007-AVI-477 : Multiples vulnérabilités dans Apple QuickTime
- CERTA-2007-AVI-478 : Vulnérabilité dans PWLib
- CERTA-2007-AVI-479 : Vulnérabilité de GNU Emacs
- CERTA-2007-AVI-480 : Vulnérabilité dans Macrovision SafeDisc
- CERTA-2007-AVI-481 : Vulnérabilité de Perl
- CERTA-2007-AVI-482 : Vulnérabilité dans Plone
- CERTA-2007-AVI-483 : Vulnérabilité de Ghostscript

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2007-AVI-182-001 : Vulnérabilité dans ProFTPD
(ajout de la référence CVE et de la référence au bulletin de sécurité Mandriva)
- CERTA-2007-AVI-391-001 : Vulnérabilité dans GNU Tar
(ajout de la référence au bulletin de sécurité SuSE)
- CERTA-2007-AVI-424-001 : Multiples vulnérabilités dans XOrg
(ajout de la référence CVE et des références aux bulletins de sécurité Mandriva, Gentoo, SUSE et Sun.)
- CERTA-2007-AVI-425-001 : Multiples vulnérabilités dans libpng
(ajout des références CVE et des références aux bulletins de sécurité Ubuntu et Red Hat)
- CERTA-2007-AVI-463-001 : Vulnérabilités dans Symantec Mail Security
(mise à jour des produits affectés, de la solution et ajout du bulletin de sécurité de Symantec)
- CERTA-2007-AVI-467-002 : Vulnérabilité dans CUPS
(ajout de la référence au bulletin de sécurité Ubuntu)
- CERTA-2007-AVI-480 : Vulnérabilité dans Macrovision SafeDisc
(révision des risques liés à la vulnérabilité)

7 Actions suggérées

7.1 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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme 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 réglementaire, 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.

7.2 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.

7.3 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.

7.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. 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.

7.5 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.

7.6 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.

7.7 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 choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

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

8 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.

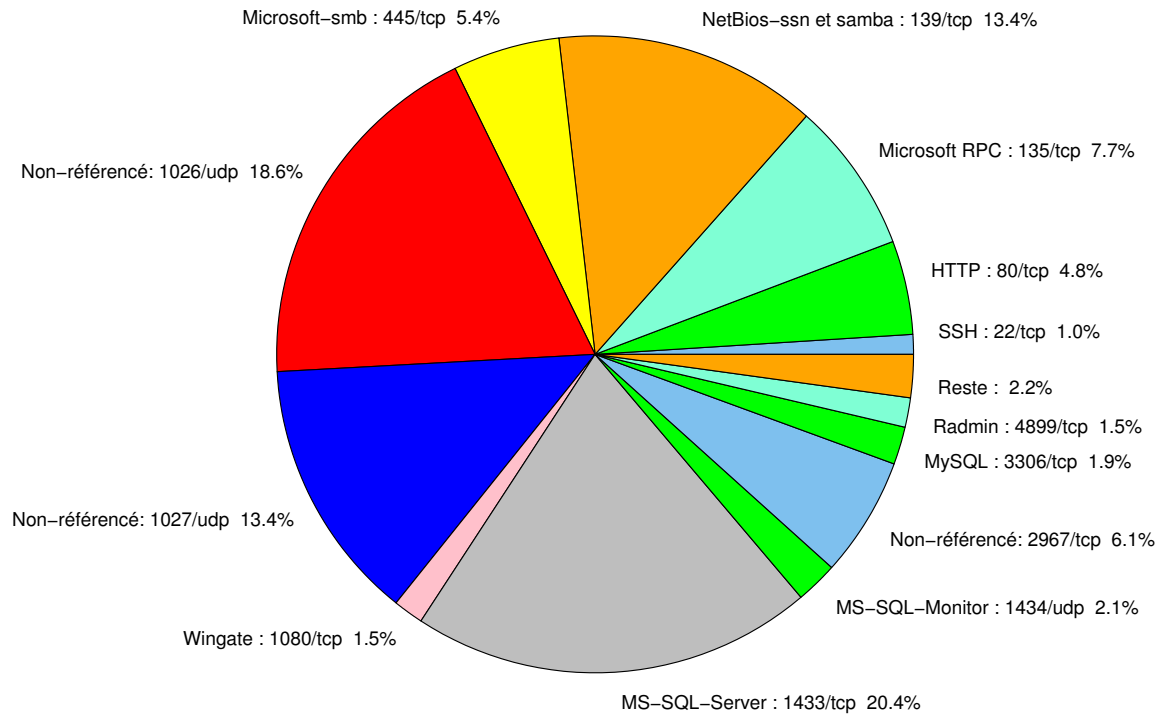


FIG. 1: Répartition relative des ports pour la semaine du 01.11.2007 au 08.11.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
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 et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283

				CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
1433/tcp	20.4
1026/udp	18.61
1027/udp	13.38
139/tcp	13.36
135/tcp	7.68
2967/tcp	6.08
445/tcp	5.43
80/tcp	4.76
1434/udp	2.13
3306/tcp	1.91
1080/tcp	1.53
4899/tcp	1.49
22/tcp	1
137/udp	0.75
3128/tcp	0.48
23/tcp	0.2
25/tcp	0.17
143/tcp	0.13
15118/tcp	0.08
11768/tcp	0.04
3389/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	9
3	Paquets rejetés	10

Gestion détaillée du document

09 novembre 2007 version initiale.