Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 avril 2009
N° CERTA-2009-ACT-016

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-16

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-2009-ACT-016`

Gestion du document

Référence	CERTA-2009-ACT-016
Titre	Bulletin d'actualité 2009-16
Date de la première version	17 avril 2009
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-2009-ACT-016.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-2009-ACT-016/

1 Incidents de la semaine

Le CERTA a traité cette semaine un nouveau cas de compromission de site Web, dont le scénario est très proche de celui décrit dans le dernier bulletin (« Intrusion FTP », CERTA-2009-ACT-015). L'ordinateur de l'un des rédacteurs (contributeurs) du site Web a été compromis. Les données de connexion (adresse du site, identifiant et mot de passe) ont été dérobées puis utilisées depuis plusieurs adresses IP afin de changer régulièrement le code source des pages du site Web.

Dans le cadre du traitement d'incident, le CERTA a cherché à identifier quel contributeur a eu sa machine compromise. Cette tâche s'avère être impossible dans la mesure où :

1. il y a une douzaine de personnes se connectant fréquemment pour des besoins de rédaction au serveur ;
2. elles partagent toutes le même compte pour l'accès (identifiant, mot de passe).

Lorsque plusieurs personnes contribuent de cette manière à un site Web, il est important d'appliquer quelques pratiques de sécurité afin de limiter les intrusions mais aussi de pouvoir conserver une trace utile des accès :

- mettre en place une politique de filtrage stricte en limitant l'accès FTP à certaines adresses IP identifiées des contributeurs ;
- fournir à chacune des personnes un compte distinct.

2 Correctifs Microsoft du mois d'avril

Cette semaine, Microsoft a émis huit mises à jour de sécurité. Trois de ces mises à jour sont particulièrement importantes car elles corrigent des failles ayant fait l'objet d'alertes du CERTA et dont le code d'exploitation est disponible sur l'Internet :

- le bulletin de sécurité MS09-010 qui corrige plusieurs vulnérabilités dans les convertisseurs de texte WordPad et Office permettant l'exécution de code arbitraire à distance ;
- le bulletin de sécurité MS09-012 qui corrige plusieurs élévations de privilèges (vols de jetons) dans Microsoft Windows ;
- le bulletin de sécurité MS09-009 qui corrige deux vulnérabilités permettant l'exécution de code arbitraire à distance via l'ouverture d'un document `Excel` spécialement conçu.

Les cinq autres bulletins sont les suivants :

- le bulletin MS09-011 concerne une vulnérabilité dans DirectX permettant l'exécution de code arbitraire à distance ;
- le bulletin MS09-013 décrit plusieurs vulnérabilités dans les services HTTP Windows permettant l'exécution de code arbitraire à distance ;
- le bulletin MS09-014 concerne plusieurs vulnérabilités touchant toutes les versions de Microsoft Internet Explorer permettant l'exécution de code arbitraire à distance ;
- le bulletin MS09-015 corrige une autre élévation de privilèges dans Microsoft Windows ;
- enfin, le bulletin MS09-016 qui concerne des vulnérabilités dans Microsoft ISA Server permettant à des personnes malintentionnées d'effectuer des dénis de service à distance et des injections de code indirectes.

Il est évidemment recommandé d'appliquer ces mises à jour dès que possible. Microsoft a également mis à jour son bloc-notes « Security Research and Defense » avec plusieurs articles commentant certaines des vulnérabilités.

Le CERTA rappelle également que les versions 2000 SP3, 2002 SP3 (XP SP3), et 2003 SP3 de Microsoft PowerPoint sur Windows et 2004 de Microsoft PowerPoint sur Mac sont toujours concernées par une vulnérabilité non corrigée et actuellement exploitée. Celle-ci fait l'objet de l'alerte CERTA-2009-ALE-005.

2.1 Documentation

- Bloc-notes « Security Research and Defense » :
  http://blogs.technet.com/srd/

3 De l'aspect bénin d'un balayage

3.1 Généralités

Il est fréquent d'entendre qu'un balayage réseau est une opération bénigne, qu'il s'agisse de *scanner* des ports ou des plages d'adresses IP.

Plusieurs outils permettent ainsi d'auditer son réseau afin de vérifier la topologie et le comportement des différents équipements. Ils peuvent aussi servir à contrôler la politique de filtrage. Peut-on plus librement les utiliser sur des machines tiers de l'Internet ?

La question peut être posée d'une autre manière : est-il si facile de maîtriser et savoir l'impact que peut avoir cette opération de balayage sur les systèmes cibles ou intermédiaires ? La réponse est malheureusement non. Même si l'envoi de quelques trames peut sembler anodin, ces dernières peuvent perturber le bon fonctionnement d'un système d'information.

Un exemple concret est présenté au paragraphe ci-dessous.

3.2 Vulnérabilité de *Packet Filter*

Le CERTA a publié cette semaine l'avis CERTA-2009-AVI-136 concernant une vulnérabilité du pare-feu Packet Filter d'OpenBSD.

Les opérations de NAT ou de redirection (`nat`, `binat`, `rdr`) peuvent provoquer sous certaines conditions une panique du noyau et ainsi perturber le service de filtrage. Elles ne manipulent pas correctement les datagrammes IP qui indiquent un en-tête protocolaire suivant de type ICMPv6 (*proto_id*=58).

Les différentes valeurs possibles du champ Protocole de l'en-tête IP ont été d'abord précisées dans les standards RFC 1340 et 1700 mais elles sont actuellement mises à jour directement via le site Web de l'IANA (RFC 3232).

Les RFC 1340 (juillet 1992) et 1700 (octobre 1994) sont obsolètes et ne font pas mention d'ICMPv6. La liste actualisée se trouve à l'adresse réticulaire :

– IANA, "Assigned Internet Protocol Numbers" :
  http://www.iana.org/assignments/protocol-numbers/

OpenBSD a publié un correctif. Un contournement consiste aussi à renforcer les règles de traduction/redirection en leur précisant à quels protocoles elles s'appliquent, comme :

```
nat on xxx proto { tcp udp icmp } from...
```

En conclusion, une simple trame peut perturber le bon fonctionnement d'un pare-feu. Utiliser un outil de balayage qui, involontairement ou non, émet cette trame, peut avoir une conséquence relativement importante.

3.3 Recommandations

– Pour les utilisateurs de *Packet Filter* : il faut penser à appliquer le correctif OpenBSD qui corrige le problème. L'exploitation de cette vulnérabilité est triviale et peut avoir de lourdes conséquences sur le fonctionnement d'un système ou d'un réseau ;
– Pour les utilisateurs d'outils de balayage : comme tout outil de sécurité, leur usage doit être maîtrisé et utilisé dans un contexte professionnel, uniquement afin de garantir la sécurité de son propre réseau.

4 Vulnérabilité CIFS du noyau Linux

Cette semaine, une vulnérabilité dans le noyau Linux a été rendue publique et a fait l'objet de la publication d'un correctif. La version stable courante est donc passée de 2.6.29 à 2.6.29.1. Le risque associé à cette faille, détaillé dans l'avis CERTA-2009-AVI-153, est le déni de service ou potentiellement de l'exécution de code arbitraire.

En l'espèce, il s'agit d'un mauvais calcul de taille de tampon mémoire. L'allocation de celui-ci pourrait donc être sous-dimensionnée par rapport à la taille réelle des données qui y sont écrites. Le correctif proposé pour la version 2.6.29.1 consiste d'ailleurs en une modification de ce calcul pour obtenir une taille plus importante. Mais, d'après certains développeurs, le nouveau calcul reste encore insuffisant. Il resterait, donc, une faille résiduelle. D'autres proposent d'ailleurs une réécriture complète de cette portion de code car elle consiste en une approximation de taille de tampon plus ou moins grossière. Ce qui ne constitue pas une gage de fiabilité *in-fine*.

Il faudra donc être vigilant sur la suite donnée à ce correctif dans le noyau Linux, car, visiblement, les choses pourront encore évoluer en la matière. De manière plus générale, lors de l'application de correctif, outre les effets de bords évidents que cela peut entraîner, il faudra toujours prendre garde à de possibles « correctifs de correctifs » ultérieurs.

5 Élévation de privilèges sous Linux

Le logiciel `udev`, qui permet de gérer les noeuds de périphériques sur un système Linux, présentait une vulnérabilité importante. En effet, udev est à l'écoute de message en provenance du noyau sur une socket de type netlink, qui lui permet d'avoir des informations sur les événements liés principalement à l'apparition et la disparition de périphériques. La vulnérabilité provient du fait que udevd ne vérifie pas la provenance des messages qu'il reçoit sur cette socket ; or n'importe quel utilisateur peut y envoyer des messages, qui seront traités directement.

Il est ainsi possible de créer des noeuds de périphériques avec des droits permettant aux utilisateurs normaux d'y accéder. On pourra par exemple penser à /dev/mem, pour accéder à la mémoire physique et y charger un rootkit, ou à /dev/sda afin d'accéder directement au système de fichier sans vérification des droits.

L'exploitation de la vulnérabilité est d'autant plus aisée que, depuis les dernières versions, les règles fournies par défaut avec udev comprennent la possibilité d'exécuter une commande arbitraire spécifiée dans le message envoyé via netlink. Celle-ci sera exécutée avec les droits root, ce qui permet à un utilisateur non privilégier d'élever simplement ses privilèges.

En conséquent, sur les systèmes vulnérables, l'exploitation de la faille pour un attaquant est extrêmement simple et parfaitement fiable.

Pour se prémunir du problème, il faut mettre à jour udev. Le CERTA a publié à ce sujet l'avis de sécurité CERTA-2009-AVI-155.

6 Vulnérabilité JBIG2... les autres aussi !

Le CERTA publie à la date de rédaction de ce bulletin une mise à jour de l'avis CERTA-2009-AVI-094. Pour mémoire, cet avis faisait suite à la mise à jour d'une faille `JBIG2` (mauvaise interprétation de cet encodage) par les lecteurs `PDF` d'`Adobe` (dans un premier temps, cette vulnérabilité avait fait l'objet de l'alerte du CERTA CERTA-2009-ALE-001). Il s'avère que d'autre lecteurs `PDF` sont vulnérables, même si l'exploitation dans ces cas là n'était pas connue.

Plus globalement, les vulnérabilités portant sur des fonctions de manipulation de formats produisent souvent cet effet. Les éditeurs, afin d'éviter de réinventer la roue, intègrent en général la même mise en oeuvre des mêmes algorithmes. C'est le cas, par exemple, pour l'interprétation des formats de compression par les antivirus.

Dans ces cas spécifiques, l'utilisation de produits alternatifs peut s'avérer bien souvent insuffisante. Il vaut mieux alors mettre en oeuvre d'autres contournements provisoires, tels que la mise en quarantaine des fichiers incriminés provenant de sources extérieures, et ce, jusqu'à ce qu'un correctif soit publié. Cette décision, comme toute autre, ne doit pas se prendre à la légère et doit résulter d'une étude de risques permettant de choisir la bonne posture et par conséquent le bon contournement provisoire.

7 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 09 et le 16 avril 2009.

8 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/

9 Rappel des avis émis

Dans la période du 10 au 17 avril 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-134 : Vulnérabilités des produits Cisco
- CERTA-2009-AVI-135 : Vulnérabilité dans HP OpenView

– CERTA-2009-AVI-136 : Vulnérabilité du pare-feu Packet Filter d'OpenBSD
– CERTA-2009-AVI-137 : Multiples vulnérabilités des produits VMWare
– CERTA-2009-AVI-138 : Multiples vulnérabilités dans SPIP
– CERTA-2009-AVI-139 : Vulnérabilités dans Wireshark
– CERTA-2009-AVI-140 : Vulnérabilités dans les convertisseurs de texte WordPad et Office
– CERTA-2009-AVI-141 : Vulnérabilité dans Microsoft DirectX
– CERTA-2009-AVI-142 : Vulnérabilités dans Microsoft Windows
– CERTA-2009-AVI-143 : Vulnérabilités dans les services HTTP Windows
– CERTA-2009-AVI-144 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTA-2009-AVI-145 : Vulnérabilité dans Microsoft Windows
– CERTA-2009-AVI-146 : Vulnérabilité dans Microsoft ISA Server
– CERTA-2009-AVI-147 : Vulnérabilité dans Microsoft Excel

Durant la même période, les alertes suivantes ont été mises à jour :

– CERTA-2008-ALE-012-001 : Vulnérabilité dans Microsoft Windows
– CERTA-2008-ALE-015-001 : Vulnérabilité dans le convertisseur de texte WordPad
– CERTA-2009-ALE-002-001 : Vulnérabilité dans Microsoft Excel

10 Actions suggérées

10.1 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 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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 CERTA peut vous aider dans ce travail d'analyse.

10.6 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.

10.7 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.ssi.gouv.fr/fr/formation/

11 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.

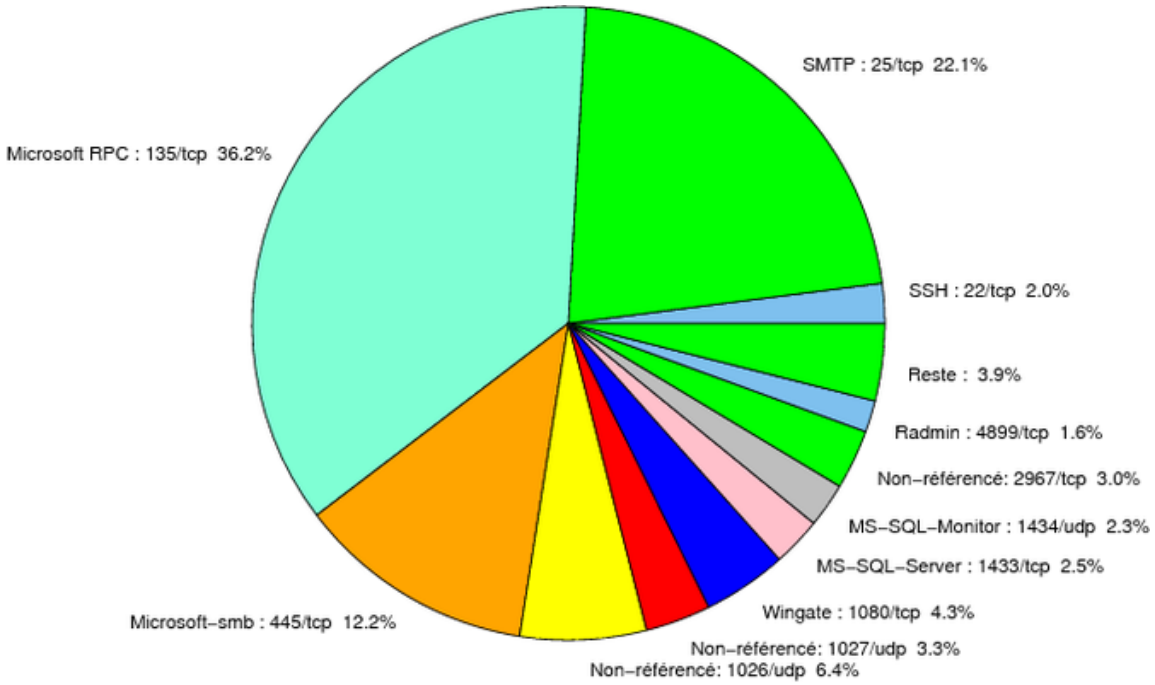

FIG. 1: Répartition relative des ports pour la semaine du 09 au 16 avril 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
135/tcp	36.23
25/tcp	22.08
445/tcp	12.17
1026/udp	6.44
1080/tcp	4.29
1027/udp	3.34
2967/tcp	3.04
1433/tcp	2.5
1434/udp	2.26
22/tcp	2.08
4899/tcp	1.61
80/tcp	1.01
23/tcp	0.95
21/tcp	0.53
3128/tcp	0.41
3389/tcp	0.29
139/tcp	0.23
3306/tcp	0.11

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

17 avril 2009 version initiale.