



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 novembre 2008
N° CERTA-2008-ACT-046

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-46

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-2008-ACT-046>

Gestion du document

Référence	CERTA-2008-ACT-046
Titre	Bulletin d'actualité 2008-46
Date de la première version	14 novembre 2008
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-2008-ACT-046.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-2008-ACT-046/>

1 Logiciels obsolètes : danger

1.1 Cas général

Le CERTA recommande vivement à ses lecteurs de mettre à jour les logiciels qu'ils utilisent de manière à diminuer les possibilités d'attaques contre leurs systèmes d'information.

Au cours du temps, des logiciels ou des branches de développement de logiciel ne sont plus maintenus. La réponse à des vulnérabilités ou à des attaques ne sera plus fournie par l'éditeur ou la communauté en charge de la maintenance. Sauf à maîtriser parfaitement un tel logiciel et à être capable d'en assurer lui-même la maintenance, un utilisateur de logiciel non maintenu doit migrer vers des logiciels maintenus pour conserver un système qui bénéficie de réponse aux vulnérabilités publiées et aux attaques.

Le CERTA tient une liste (non exhaustive) de logiciels avec les versions maintenues et non maintenues dans la note CERTA-2005-INF-003 (voir documentation). Le plus sûr moyen de connaître l'état de maintenance d'un logiciel est de consulter le site de l'éditeur ou du projet (logiciels libres).

1.2 Actualité

Le logiciel de gestion de contenus (*CMS*) SPIP-Agora entre dans la catégorie des logiciels dont la maintenance n'est plus assurée. La fin de la maintenance du *CMS* SPIP-Agora est officielle depuis mai 2008, comme indiqué sur le site du projet (voir documentation).

À l'approche de la fin de vie du projet, les développeurs de SPIP-Agora ont encouragé la migration des sites des utilisateurs vers d'autres gestionnaires de contenus, SPIP en particulier. Un script PHP d'aide à la migration vers SPIP 1.9.2 est même fourni (voir documentation).

Malgré cet effort, des sites en exploitation restent contruits autour de ce logiciel.

D'un autre côté, des vulnérabilités du logiciel SPIP-Agora continuent à être publiées. La publication de vulnérabilité de la fin octobre 2008 affecte la dernière version stable du logiciel SPIP-Agora. Elle est de type *PHP include*. Il n'y aura pas de correctif. Les sites qui sont restés en SPIP-Agora sont vulnérables.

Il est donc important, dès lors que le logiciel est utilisé sur un système d'information relié à l'Internet :

- à très court terme, de prendre les précautions usuelles contre ce type de vulnérabilité (filtrage entrant et sortant, configuration de PHP...), voire de déconnecter le site ;
- pour les utilisateurs en ayant la capacité, de corriger le logiciel ;
- à moyen terme, de migrer le site vers un autre gestionnaire de contenus.

Ces actions doivent, bien entendu, s'inscrire dans la politique de sécurité du système d'information.

Il ne faut pas oublier, dans l'évaluation des risques qui sous-tend cette politique, qu'un site qui ne comporte aucune donnée qualifiée de sensible reste une cible pour un cyber attaquant. Il pourra vouloir utiliser les ressources matérielles du serveur pour mener d'autres attaques en faisant porter le chapeau au possesseur légitime de la machine vulnérable ainsi détournée.

1.3 Documentation

- Note d'information CERTA-2005-INF-003, « Les systèmes et logiciels obsolètes » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Site du projet Agora :
<http://www.agora.gouv.fr/>
- Script de migration d'Agora vers SPIP :
<http://www.agora2spip.agora.gouv.fr/Le-migrateur-Agora-Spip-un-outil.html>
- Alerte CERTA-2003-ALE-003, « Exploitation massive de la vulnérabilité « *include PHP* » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-003/>
- Note d'information CERTA-2007-INF-002, « Du bon usage du PHP » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

2 Retour sur le correctif MS08-068

2.1 Présentation

le CERTA a publié l'avis CERTA-2008-AVI-549 suite au bulletin de sécurité Microsoft MS08-068. Celui-ci corrige une attaque nommée SMB Relay qui profite d'une erreur dans la mise en oeuvre de l'authentification par SMB/NTLM (NT LAN Manager). Le principe est le suivant :

- le client SMB est amené à se connecter à un service SMB distant contrôlé par une personne malveillante. Cet accès peut être forcé en incitant la victime à accéder à une ressource distante par exemple. Il est possible d'imaginer une page Web lue par Internet Explorer ou un message électronique au format HTML visualisé dans Outlook avec une ligne du type suivant dans le code :

```

```

- le serveur SMB distant accepte les sessions authentifiées. Il peut forcer le client à le faire en rejetant sa session anonyme (NULL). Dans ce cas, le client transmet son nom d'utilisateur, le domaine et le mot de passe de l'utilisateur connecté via les procédures NTLM ;
- durant la phase d'authentification, le serveur envoie une valeur aléatoire, un « challenge ». Le mot de passe qui est transmis par le client sous forme de condensat (*hash*) au serveur est donc en principe unique pour un mot de passe et une valeur de « challenge » donnée. Le client envoie en revanche son nom et le domaine en clair ;

- le serveur malveillant qui utilise le même « challenge » systématiquement peut effectuer une attaque par recherche exhaustive ou par table précalculée sur le condensat du mot de passe ;
- le serveur malveillant peut également utiliser ces mêmes informations d'authentification pour essayer de se connecter sur le poste client : le « challenge » que va demander le poste client peut également être celui que le serveur propose au client qui cherche involontairement à se connecter. En d'autres termes, le serveur demande au client ce que le client exige pour se connecter à lui. Il obtient cette information et peut alors se connecter et exécuter du code.

Cette forme d'attaque est aussi dite *réflexive*.

Le correctif de Microsoft mentionné dans MS08-068 protège du dernier point en vérifiant que le « challenge » reçu par un serveur SMB ne correspond pas à l'un de ceux que la machine vient de fournir.

Le correctif n'apporte cependant pas de mesure pour limiter les risques d'un relais SMB illégitime qui redirige correctement le trafic vers un serveur fonctionnel. Il reste donc envisageable de dérouter une phase d'authentification vers une autre machine locale et d'abuser d'un service autorisant NTLM comme authentification. Ce scénario reste possible quand des services s'appuient sur la suite *Integrated Windows Authentication* dans une zone de confiance.

Plusieurs mesures s'appliquent pour éviter ce genre de problèmes :

- mettre à jour les postes Windows avec le correctif décrit dans MS08-068 ;
- désactiver le partage de fichiers et d'imprimantes s'il n'est pas utile ;
- filtrer les ports 139 et 445 par une politique rigoureuse ;
- ne pas utiliser de comptes administrateur par défaut (bloquer les droits d'écriture dans ADMIN\$ et les permissions pour manipuler les services Windows) ;
- avoir des mots de passe de comptes utilisateur robustes ;
- mettre en place des solutions de sécurité complémentaires (IPsec, signature SMB, etc.).

2.2 Documentation

- Avis CERTA-2008-AVI-549 du mercredi 12 novembre 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-549/>
- Bloc-Notes Microsoft SWI du 11 novembre 2008 :
<http://blogs.technet.com/swi/archive/2008/11/11/smb-credential-reflection.aspx>
- Bloc-Notes Microsoft MSRC du 11 novembre 2008 :
<http://blogs.technet.com/msrc/archive/2008/11/11/ms08-068-and-smbrelay.aspx>
- Description de "*SMB Relay*" à @tlantacon 2001 :
<http://www.xfocus.net/articles/200305/smbrelay.html>

3 L'actualité de Mozilla Firefox

3.1 Présentation

Cette semaine, le CERTA a publié un avis faisant état de nombreuses vulnérabilités dans Mozilla Firefox. Parmi celles-ci, il est noté que des exécutions de code arbitraire à distance sont possibles :

- l'une de ces vulnérabilités est exploitable grâce à un manque de contrôle dans les tests de déchargement dynamique du module *Flash*. Il est possible via un fichier *SWF* spécialement conçu d'accéder à une adresse mémoire qui n'est plus affectée au module *Flash* et par conséquent d'exécuter du code arbitraire à distance. Cette vulnérabilité n'affecte que la version 2 du navigateur ;
- une altération de *window.__proto__.__proto__object* peut inciter le navigateur à placer un verrou sur un objet non natif. Le fondation Mozilla précise que cette vulnérabilité pourrait aboutir à une exécution de code arbitraire ;
- plusieurs erreurs dans le moteur du navigateur ont été corrigées, dont certaines présentaient des possibilités de corruption de la mémoire entraînant une éventuelle exécution de code arbitraire ;
- une erreur dans le traitement de l'*http-index-format* de *MIME* permet via l'envoi d'une réponse (*HTTP index*) spécialement conçue d'exécuter du code arbitraire à distance ;
- une vulnérabilité dans le code de construction des *DOM (Document Object Model)* Mozilla permet, dans certaines conditions, l'accès par le navigateur à des parties de la mémoire non initialisées. Une personne malveillante pourrait exécuter du code arbitraire à distance en utilisant cette vulnérabilité.

Il est également indiqué dans l'avis du CERTA que d'autres vulnérabilités permettent d'effectuer des dénis de service à distance, de contourner la politique de sécurité, de porter atteinte à la confidentialité des données et d'élever ses privilèges sur le système victime.

Le CERTA profite de cette actualité pour rappeler à ses lecteurs que, comme précisé sur la page de téléchargement de Firefox 2, le support de cette version devrait être arrêté vers la mi-décembre. Le CERTA recommande de passer directement à la version 3.0.4 de Firefox.

3.2 Documentation

- Avis CERTA-2008-AVI-555 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-555/>

4 Applications Web enrichies

On peut aisément constater que les navigateurs Web vont bien au-delà des fonctionnalités classiques que l'on attendrait de ce type de logiciels : l'affichage de pages HTML contenant éventuellement des scripts ou des images.

Depuis assez longtemps déjà, le navigateur, à la demande de certaines directives contenues dans les pages Web consultées, peut agir sur le système d'exploitation lui-même en lui faisant exécuter certaines tâches. À l'image de Windows Update et de ses contrôles `activeX`, on peut lancer une application tierce par le biais d'un appel présent dans une page Web.

Cette imbrication du navigateur dans le système d'exploitation croît au fil des améliorations et de nouvelles fonctionnalités qui apparaissent. Il est ainsi possible via un simple navigateur d'activer `micro` et `webcam` pour faire de la visio-conférence, et ce, par simple pression d'un bouton dans une page Web.

On peut voir l'apparition d'une convergence entre `webmail`, messagerie instantanée et maintenant visio-conférence dans une seule et même interface. L'utilisateur passe ainsi allégrement, par le truchement de quelques `sockets` réseaux judicieusement choisies, de la rédaction d'un courriel à la conversation en direct avec le destinataire.

Dans ce contexte, et à défaut de pouvoir se passer de toutes ces nouvelles technologies, il est peut-être bon de rappeler un vieux principe de l'informatique : le KISS (Keep It Stupidely Simple) ou autrement dit « garder le système le plus simple possible ». Moins on a de code dans une application, moins on aura, potentiellement, de bogues et plus l'application sera, théoriquement, facile à appréhender.

L'idéal est d'avoir une application par fonction et que ces applications communiquent entre elles de façon maîtrisée. Lorsqu'un navigateur peut, presque à loisir, activer une caméra ou un microphone, c'est qu'il a acquis d'une certaine manière des privilèges élevés sur la machine. Il est alors indispensable de connaître la façon dont cette activation a lieu et de la maîtriser sous peine de voir une page malveillante réaliser la même opération à l'insu de l'utilisateur.

5 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 06 et le 13 novembre 2008.

6 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/>

7 Rappel des avis émis

Dans la période du 07 au 14 novembre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-546 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2008-AVI-547 : Vulnérabilité dans les produits VMware
- CERTA-2008-AVI-548 : Vulnérabilité dans HP Tru64 UNIX
- CERTA-2008-AVI-549 : Vulnérabilité de SMB dans Microsoft Windows
- CERTA-2008-AVI-550 : Vulnérabilités dans Microsoft XML Core Services
- CERTA-2008-AVI-551 : Vulnérabilités dans Joomla!
- CERTA-2008-AVI-552 : Multiples vulnérabilités du serveur DHCP de Sun Solaris
- CERTA-2008-AVI-553 : Vulnérabilité dans ClamAV
- CERTA-2008-AVI-554 : Vulnérabilités dans TYPO3
- CERTA-2008-AVI-555 : Multiples vulnérabilités dans Mozilla Firefox

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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>

9 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.

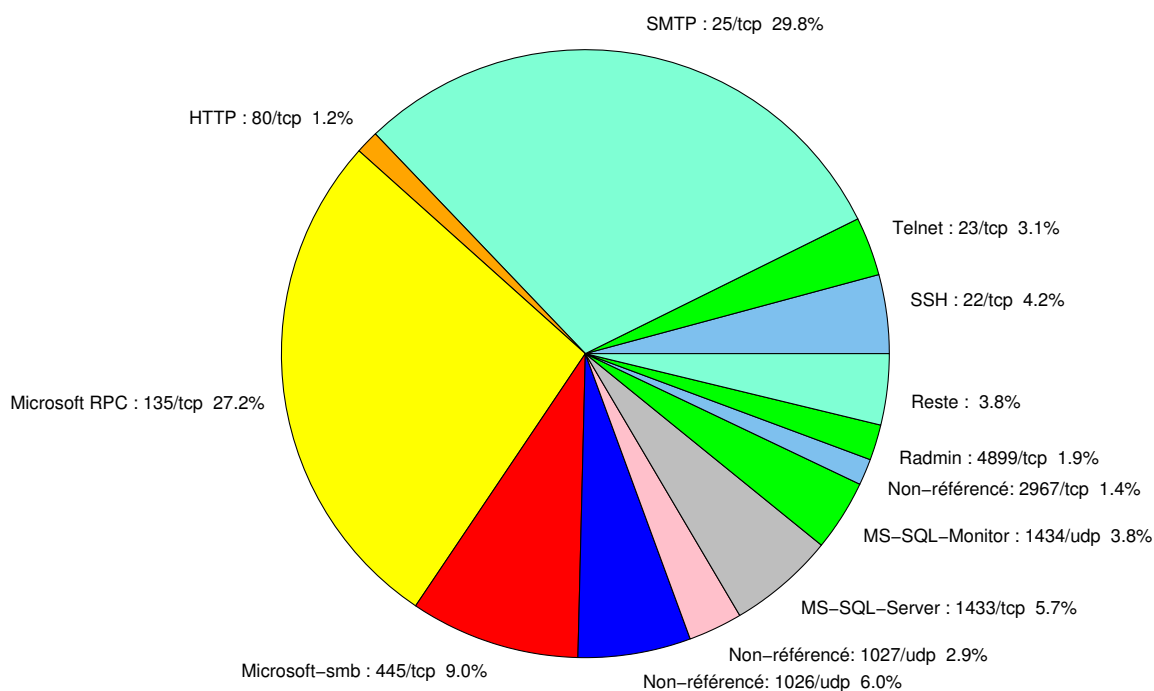


FIG. 1: Répartition relative des ports pour la semaine du 06.11.2008 au 13.11.2008

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
25/tcp	29.82
135/tcp	27.19
445/tcp	9.03
1026/udp	5.99
1433/tcp	5.66
22/tcp	4.19
1434/udp	3.77
23/tcp	3.2
1027/udp	2.87
4899/tcp	1.88
2967/tcp	1.39
80/tcp	1.23
139/tcp	0.82
137/udp	0.73
3389/tcp	0.41
3306/tcp	0.32
1080/tcp	0.24
42/tcp	0.08

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

14 novembre 2008 version initiale.