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 octobre 2008
N° CERTA-2008-ACT-043

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-43

Gestion du document

Référence	CERTA-2008-ACT-043
Titre	Bulletin d'actualité 2008-43
Date de la première version	24 octobre 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-043.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-043/

1 Bulletin Microsoft MS08-067

Cette semaine, Microsoft a publié une mise à jour hors cycle mensuel, détaillée dans le bulletin MS08-067 et l'avis CERTA-2008-AVI-523. Cette mise à jour corrige une vulnérabilité dans toutes les versions de Windows. Elle est jugée critique par Microsoft sur les systèmes Windows 2000, Windows XP et Windows 2003. L'éditeur a préféré une mise à jour hors cycle car la vulnérabilité peut être trivialement exploitée et utilisée dans le développement de vers. Des attaques sont déjà observées. Il est rappelé la nécessité d'appliquer les mises à jour.

1.1 Retour sur la vulnérabilité

La vulnérabilité concerne un débordement de mémoire dans le traitement de chemins `UNC` (*Universal Naming Convention*) par la méthode *NetPathCanonicalize* de l'interface RPC `srvsvc` (service Serveur). En exploitant cette faille, une personne malintentionnée peut exécuter du code arbitraire sur un poste vulnérable en envoyant un paquet spécialement construit lors d'une session SMB/RPC. Nous avons observé que cette vulnérabilité rappelle fortement celle du bulletin MS06-040 qui concernait le même appel RPC.

1.2 Mesures de protection et facteurs atténuants

Hormis le correctif proposé par Microsoft, il existe des facteurs atténuants pour cette vulnérabilité.

Pour pouvoir joindre l'interface concernée, un attaquant doit passer par les ports 139/TCP ou 445/TCP. Ces ports sont filtrés par défaut par le pare-feu de Windows XP SP2, Windows Vista et Windows Server 2008, sauf si le partage de fichiers et d'imprimantes est activé. Ces ports doivent évidemment toujours être filtrés par tout pare-feu de bordure de réseau.

Dans Windows Vista et Windows Server 2008, l'UAC (*User Account Control*) requiert par défaut une authentification pour accéder à l'interface vulnérable. En effet, un utilisateur non authentifié qui se connecte aura un niveau de droit *Untrusted*, inférieur au niveau « Faible » qui est requis pour l'accès. Toutefois, les personnes ayant désactivé l'option « Partage protégé par mot de passe » dans le Centre Réseau et Partage se privent de cette protection car les connexions anonymes se font alors avec le niveau « Moyen ».

L'éditeur affirme également que les systèmes Windows Vista et Windows Server 2008 sont davantage protégés de l'exécution de code grâce au mécanisme d'ASLR (*Address Space Layout Randomization*) couplé au DEP (*Data Execution Prevention*).

Un outil non garanti est également disponible sur le site de Microsoft pour retirer les autorisations d'accès aux utilisateurs anonymes dans les ACL (*Access Control List*) des canaux nommés (cf. documentation).

1.3 Filtrage possible

Les outils de filtrage réseau permettent d'isoler certaines trames particulières. Par exemple, sous Wireshark/Ethereal, il existe le filtre d'affichage `srvsvc.srvsvc_NetPathCanonicalize.path` pour visualiser des chaînes de caractères anormales de la forme :

```
\<chaîne de caractère>\..\..\<autre chaîne>
..\..\
```

1.4 Documentation

- Avis CERTA-2008-AVI-523 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-523
- Article du bloc-notes « Security vulnerability research & defense » de Microsoft :
  http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx
- Portail de la Sécurité Informatique :
  http://www.securite-informatique.gouv.fr/

2 Le protocole LLMNR

2.1 Présentation

Le protocole LLMNR (*Link-Local Multicast Name Resolution*), défini par la RFC 4795, a pour vocation de permettre à des machines de répondre à des requêtes DNS émanant du voisinage réseau, que ce soit en IPv4 ou en IPv6. Il permet ainsi de résoudre des noms de machine sur des petits réseaux dépourvus de serveur DNS.

Techniquement, le fonctionnement du protocole repose sur l'envoi de paquets à destination du port 5355/udp vers l'adresse IPv4 224.0.0.252 ou l'adresse IPv6 FF02:0:0:0:0:0:1:3 (adresses de multicast).

Le protocole LLMNR est activé par défaut sous *Windows Vista*. Il est important de comprendre qu'un poste fonctionnant sous *Windows Vista* va utiliser le protocole LLMNR, et donc engendrer du trafic réseau en conséquence, même si un serveur DNS a été correctement configuré. Ceci se traduit donc par une pollution du réseau.

Le protocole LLMNR peut être désactivé sous *Vista* :

- soit par une stratégie de groupe :

```
Computer Configuration\Administrative Templates\Network\DNS Client\
                        Turn off Multicast Name Resolution = Enabled
```

- soit par le registre :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\
                                        EnableMulticast = 0x0
```

2.2 Documentation

- RFC 4795 :
  http://www.ietf.org/rfc/rfc4795.txt
- Site TechNet de Microsoft :
  http://technet.microsoft.com/en-us/library/bb878128.aspx

3 Migration de version et sécurité

3.1 Présentation

Des tâches essentielles lorsque l'on administre des serveurs sont de les maintenir à jour (applications et système d'exploitation) et de consulter régulièrement les journaux d'événements. Récemment, à la suite d'une récente mise à jour de sécurité d'un serveur, le CERTA a pu constater un effet de bord assez inattendu en examinant les journaux d'un des services installés. Les journaux, ayant auparavant une taille respectable sur le disque, étaient vides depuis le dernier changement de version du logiciel. La première hypothèse orienta l'analyse vers un changement dans le fichier de configuration suite à la mise à jour. Après quelques tests, le CERTA a constaté qu'une des directives qui, d'ordinaire, indiquait au service de filtrer les données envoyées vers les fichiers d'événements, n'avait plus aucun effet. La conséquence est que tous les événements se trouvaient non plus journalisé suite à ce dysfonctionnement mais bien l'inverse : plus aucun événement dans les journaux !

La mise-à-jour de l'application avait donc entraîné l'ajout d'une coquille dans la fonction de filtrage la rendant inopérante. Un contournement au problème fut rapidement trouvé mais les effets n'étaient en aucun cas bénins (perte de traces).

3.2 Recommandations

Lors de l'application de correctifs impliquant un changement de version d'un produit, il convient toujours de passer en revue les nouvelles directives ou les variations de comportement par défaut induites par ce changement. Il faudra également s'assurer, comme c'est le cas ici, qu'aucune fonctionnalité n'a été altérée ou tout simplement supprimée. Enfin, seule l'analyse des journaux a permis de mettre rapidement en évidence le problème, il est donc indipensable de consacrer du temps à cette tâche lorsque l'on a à mettre en œuvre un SI quel qu'il soit.

4 Ouverture spontanée de documents par Microsoft Office

En règle générale, le système d'exploitation Windows s'appuie sur l'extension d'un fichier pour y associer une application à l'ouverture. Ces correspondances sont précisées dans la base de registre Windows. Il est également possible de les vérifier en tapant dans un terminal les commandes `assoc` ou `ftype`. Par exemple :

```
C:\Documents and Settings\USER>assoc .doc
.doc=Word.Document.8

C:\Documents and Settings\USER>ftype Word.Document.8
Word.Document.8="C:\Program Files\Microsoft Office\Office10\WINWORD.EXE" /n /dde"

C:\Documents and Settings\USER>
```

DDE est le protocole d'échange dynamique de données. L'objet de cet article n'est cependant pas de discuter cette option, mais de considérer les extensions qui n'apparaissent pas via les commandes ci-dessus ou dans les clés de registre. Un fichier nommé `test.aabbcc` ne sera pas pris en compte, et en cliquant dessus, Windows fait apparaître une fenêtre demandant quelle application choisir pour l'ouvrir.

Est-ce toujours le cas ?

Démonstration par l'exemple. Prenons un document Office nommé `test.doc`, changeons l'extension par `test.aabbcc` et cliquons dessus. La fenêtre précédente n'apparaît pas et l'application Word s'ouvre avec le contenu du document.

Cette propriété fonctionne pour les applications Word, Excel ou PowerPoint. Access ne semble pas en disposer. Un module propre à l'explorateur Windows examine ainsi le contenu du fichier lorsque l'extension n'est pas connue.

Il apparaît clairement de cette courte démonstration que vérifier l'extension n'est pas une opération suffisante pour identifier un document Office. En l'occurence, il est tout à fait envisageable d'imaginer des courriers malveillants qui exploitent cette astuce en renommant le fichier de façon à tromper ce contrôle. Par exemple, un fichier nommé « `test.txt ;` » peut entraîner en cliquant dessus l'ouverture d'Office.

Il est donc important de ne pas avoir un excès de confiance dans les extensions. Le cas présenté ici n'est qu'une illustration des manipulations et des exceptions aux règles classiques. Les solutions de sécurité proposent également différents filtres et signatures adaptées aux formats de fichiers. Il faut se renseigner sur leurs méthodes d'identification d'un format. Toute solution de sécurité doit être maîtrisée : cela commence par connaître son fonctionnement et ses limites.

5 Des bibliothèques discrètes mais bien présentes

Le CERTA a publié l'avis de sécurité CERTA-2008-AVI-526 concernant la bibliothèque *libspf2*. Une vulnérabilité de type débordement de mémoire affecte cette bibliothèque et permet à un utilisateur distant malintentionné de provoquer un déni de service et/ou d'exécuter du code arbitraire.

Cette bibliothèque de fonctions est largement répandue dans la mise en oeuvre des passerelles de messagerie pour permettre le filtrage des messages.

Cette vulnérabilité peut être exploitée à distance au moyen d'une réponse DNS (Domain Name System) spécialement contruite (enregistrement TXT de longueur excessive). A l'heure actuelle, seul l'éditeur Debian a publié un correctif pour cette vulnérabilité et il n'est pas exclu que d'autre éditeurs soient également affectés.

Le CERTA recommande de conduire les actions suivantes :

- maintenir à jour les serveurs en interaction avec Internet ;
- vérifier si cette bibliothèque en particulier est déployée sur les serveurs ;
- contrôler le trafic DNS et ne pas directement exposer les serveurs. Un serveur de nom local peut filtrer ce genre de réponses.

6 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 16 et le 23 octobre 2008.

7 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/

8 Rappel des avis émis

Dans la période du 17 au 24 octobre 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-512 : Multiples vulnérabilités dans Adobe Flash Player
– CERTA-2008-AVI-513 : Vulnérabilités dans Veritas File System
– CERTA-2008-AVI-514 : Multiples vulnérabilités dans Wireshark
– CERTA-2008-AVI-515 : Vulnérabilités dans IBM WebSphere
– CERTA-2008-AVI-516 : Vulnérabilités dans TikiWiki CMS/Groupware
– CERTA-2008-AVI-517 : Vulnérabilité dans les produits F-Secure
– CERTA-2008-AVI-518 : Vulnérabilité dans Mantis
– CERTA-2008-AVI-519 : Vulnérabilité dans Trend Micro OfficeScan
– CERTA-2008-AVI-520 : Vulnérabilités dans IBM DB2
– CERTA-2008-AVI-521 : Vulnérabilités dans Symantec Altiris Deployment Solution
– CERTA-2008-AVI-522 : Vulnérabilités dans Cisco PIX et ASA
– CERTA-2008-ACT-523 : Vulnérabilité dans Windows Service Server

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

– CERTA-2008-AVI-465-001 : Vulnérabilité dans libxml2
(ajout de la référence au bulletin Debian)
– CERTA-2008-AVI-466-001 : Vulnérabilité de OpenSSH pour Debian
(ajout des bulletins de sécurité Ubuntu et SuSE)
– CERTA-2008-AVI-493-002 : Multiples vulnérabilités dans CUPS
(ajout de la référence au bulletin Debian pour cupsys)

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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

10 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.

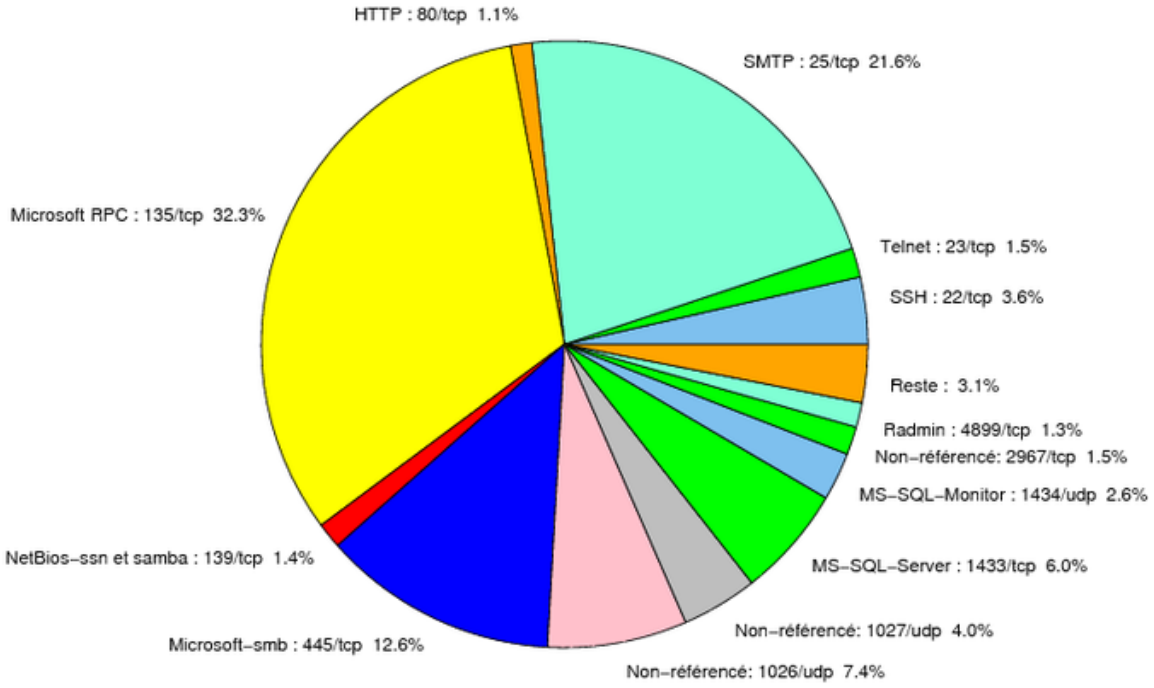

FIG. 1: Répartition relative des ports pour la semaine du 16.09.2008 au 23.09.2008

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	32.32
25/tcp	21.6
445/tcp	12.55
1026/udp	7.44
1433/tcp	5.95
1027/udp	4.04
22/tcp	3.57
1434/udp	2.55
23/tcp	1.6
2967/tcp	1.48
4899/tcp	1.42
139/tcp	1.36
80/tcp	1.13
21/tcp	0.77
3389/tcp	0.65
1080/tcp	0.23
3306/tcp	0.17
143/tcp	0.11
9898/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

24 octobre 2008 version initiale.