Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 mai 2009
N° CERTA-2009-ACT-021

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-21

Gestion du document

Référence	CERTA-2009-ACT-021
Titre	Bulletin d'actualité 2009-21
Date de la première version	22 mai 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-021.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-021/

1 Retour sur l'alerte concernant IIS - WebDAV

1.1 Introduction

Le CERTA a publié cette semaine l'alerte CERTA-2009-ALE-007 concernant une vulnérabilité du serveur Web Microsoft Internet Information Server (IIS) configuré avec WebDAV. Elle consiste en une élévation de privilèges, dans la mesure où une requête HTTP anonyme peut obtenir accès à un endroit exigeant une authentification préalable.

WebDAV ne manipule pas correctement l'adresse réticulaire (URL) demandée.

Cette vulnérabilité ne fonctionne cependant que sous certaines conditions, rappelées sur le site de Microsoft :

– WebDAV doit être activé. Ce n'est pas le cas par défaut avec IIS 6.0 ;
– l'accès au système de fichiers est autorisé pour le compte anonyme IUSR_XXX, y compris pour les contenus restreints ;
– un répertoire parent au sous-répertoire privé est possible par accès anonyme.

L'utilisateur anonyme doit avoir des droits limités. Le système de fichiers NTFS permet d'appliquer cette politique de sécurité sur les répertoires et les fichiers du serveur.

Les conditions d'exploitation de la vulnérabilité ne sont malheureusement pas si rares. Des premiers cas d'incidents (défigurations de site) ont ainsi été traités cette semaine au CERTA. Le CERTA invite donc ses correspondants à vérifier la configuration de leurs serveurs et à se reporter à la section 5 de l'alerte CERTA-2009-ALE-007 pour de possibles contournements provisoires.

http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-007/

1.2 WebDAV

WebDAV (*Web-based Distributed Authoring and Versioning*, ou DAV, est un protocole utilisé avec HTTP pour aider à gérer et administrer les fichiers sur des serveurs Web distants. Il permet ainsi plusieurs opérations, comme la récupération, le dépôt, la publication, l'accès concurrentiel, le suivi des modifications ou la synchronisation de documents.

Le standard RFC 4918 précise les champs d'en-tête et les méthodes pour que ces opérations soient correctement effectuées entre un client et le serveur. Il précise en particulier plusieurs méthodes HTTP, comme par exemple `PROPFIND` et `PROPPATCH` pour récupérer les « propriétés » définies dans la ressource précisée par l'URL, voire les modifier si nécessaire. Une autre méthode, `MKCOL` (resp. `DELETE`) peut être employée pour créer (resp. supprimer) des ressources à l'adresse précisée par l'URL. Les méthodes `COPY` et `MOVE` sont aussi apparues avec WebDAV tandis que certaines ont été mises à jour (`OPTIONS`, `PUT`, etc.).

Des documentations très complètes concernant WebDAV sont disponibles à l'adresse suivante :
http://www.webdav.org/specs/

La désactivation de WebDAV sous IIS 6.0 se fait de la manière suivante :

1. lancer l'interface IIS Manager MMC ;
2. cliquer sur le nom de la machine dans le menu de gauche ;
3. choisir « Extensions du Service Web » ;
4. cliquer dans le menu de droite sur `WebDAV` puis le bouton *Interdire*.

1.3 La surveillance

Il existe plusieurs points de surveillance possibles. L'un d'eux consiste à vérifier les journaux IIS et rechercher l'apparition de caractères particuliers de la forme `%xx`. Les codes d'exploitation actuels connus utilisent actuellement la chaîne "`%c0%af`".

L'exploitation de la vulnérabilité se fait également via une requête HTTP particulière dont l'en-tête présente l'information suivante :

```
GET .....Mon_URL_malveillante HTTP/1.1
Translate: f
```

L'information `Translate` précisée dans l'en-tête demande au serveur Web de retourner l'information en l'état, sans autre interprétation particulière. Ce choix est proposé par le client WebDAV. Si l'option est `'t'` (*true* par défaut), le serveur peut interpréter et manipuler le contenu avant de le retourner au client. Par contre, si les valeurs sont `'f'` ou `'F'` (*false*), alors le contenu doit être transmis en l'état.

1.4 Documentation

– Microsoft MSDN, "2.2.2 Translate Header", 2009 :
http://msdn.microsoft.com/en-us/library/cc250063(PROT.10).aspx
– Site du projet WebDAV :
http://www.webdav.org/
– Site du projet WebDAV, RFC 4918, "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)", juin 2007 :
http://www.webdav.org/specs/rfc2518.html
– Bloc-notes Microsoft SRD, "More information about the IIS authentication bypass", 18 mai 2009 :
http://blogs.technet.com/srd/archive/2009/05/18/more-information-about-the-iis-authentication-bypass.aspx

2 Verbosité de l'historique Bash

L'historique des commandes est un point de surveillance intéressant de son système. Il peut également être fort utile dans le cas d'une analyse suite à un incident. L'objet n'est pas ici de présenter la qualité de cette information et les possibilités de contournement utilisés par certains codes. Cet article tient seulement à rappeler qu'il est possible et fort utile d'augmenter un peu la verbosité de ce journal en prévision d'un traitement d'incident.

Comment faire cela ?

Il est par exemple possible de renseigner la variable `HISTTIMEFORMAT`. Cette variable permet d'ajouter dans l'historique une information temporelle (date) associée à l'utilisation des commandes.

Un moyen de procéder est :

```
$history
(...)
  201  cd ..
  202  ls
$echo 'HISTTIMEFORMAT="[ %h/%d - %H:%M:%S ] "' >> ~/.bash_profile
$source ~/.bash_profile
$history
(...)
  201  mai/20 - 08:14:51 cd ..
  202  mai/20 - 08:14:51 ls
  203  mai/20 - 08:14:51 history
  204  mai/20 - 08:14:51 echo 'HISTTIMEFORMAT="[ %h/%d - %H:%M:%S ] "' >>
  ~/.bash_profile
  205  mai/20 - 08:13:51 source ~/.bash_profile
  206  mai/20 - 08:14:13 history
$
```

Les dates sont insérées dans le fichier `~/.bash_history` par une nouvelle ligne précédent chaque commande, sous forme d'entiers (nombre de secondes écoulées depuis le 01 janvier 1970 à minuit UTC - *epoch time*).

D'autres variables peuvent également être renseignées pour personnaliser et adapter les journaux *history* aux différents besoins :

- `HISTFILE` pour changer le fichier par défaut *~/.bash_history* ;
- `HISTSIZE` pour adapter le nombre d'entrées (commandes) à conserver (doit être cohérent avec `HISTFILESIZE` ;
- `HISTCONTROL` et `HISTIGNORE` pour préciser les commandes à ne pas insérer et la manière de gérer les lignes particulières.

3 Des listes d'appels de fonction à bannir

`Microsoft` maintient depuis plusieurs années une liste d'appels de fonctions à bannir par les développeurs. Cette liste contient un ensemble d'*API* à ne pas utiliser afin de limiter les risques de vulnérabilités dans les codes développés dans différents langages (*Visual Basic*, *C#*, *C++*, *J#*, *JScript* et *XAML*).

`Microsoft` vient récemment d'ajouter à sa liste *Security Development Lifecycle (SDL) Banned Function Calls* la fonction *memcpy()* et fournit quelques recommandations afin de remplacer cette fonction dans les différents codes d'applications sur le bloc-note de l'équipe *SDL.*

De manière plus générale, le CERTA recommande aux développeurs de prendre le temps d'appliquer les différentes bonnes pratiques de sécurisation de code et de consulter les documentations et autres listes de fonctions « sensibles » afin de limiter dès la création des applications les risques de vulnérabilités.

Documentation

- Liste SDL Banned Function Calls :
  http://msdn.microsoft.com/en-us/library/bb288454.aspx
- Bloc-note de l'équipe Security Developement Lifecycle :
  http://blogs.msdn.com/sdl/archive/2009/05/14/please-joinme-in-welcoming-memcpy-to-the-sdl-rogues-gallery.aspx

– Recommandations pour les developpeurs par le Cert.org :
https://www.securecoding.cert.org/confluence/display/seccode/CERT+Secure+Coding+Standards
– Outil Microsoft, "The Microsoft SDL Process Template for Visual Studio Team System" :
http://msdn.microsoft.com/fr-fr/security/dd670265(en-us).aspx

4 Journaux et bases de données

Le CERTA a déjà insisté sur la nécessité de mettre en œuvre dans son système d'information une politique adaptée de gestion des journaux. Ceux-ci sont indispensables à plusieurs titres. On pourra, pour s'en convaincre, consulter la note d'information CERTA-2008-INF-005 sur le sujet. Un des intérêts de disposer des journaux est de pouvoir mieux appréhender, a posteriori, un événement qui s'est produit sur la machine.

Dans ce contexte, certains journaux peuvent prendre une importance toute particulière dans la compréhension d'un incident. Par exemple, les systèmes de gestion de bases de données (SGBD) sont souvent capables de produire des fichiers de *logs* mais ceux-ci sont rarement activés, configurés ou lus. Pourtant, certains SGBD sont capables de consigner les requêtes SQL qui lui sont passées.

On peut y voir un intérêt évident dans un contexte de déverminage. Au-delà, le fait d'avoir ce type de journaux sur un serveur de type LAMP (Linux Apache Mysql Php) afin de mettre en œuvre un gestionnaire de contenu peut aider à détecter des attaques de type injection SQL. Cela peut aussi aider à retracer les actions d'un attaquant déjà introduit sur le système utilisant un utilitaire PHP pour contrôler la machine.

Lors d'une analyse *post-mortem*, il sera intéressant de s'attarder sur ce type de journaux souvent mal connus car ils peuvent offrir des informations pertinentes sur les techniques employées par l'intrus pour prendre le contrôle de la machine : contenus en base de données capturées ou modifiés, comptes utilisateur supplémentaires, modifications de droits, etc.

Certains SGBD sont plus riches que d'autres dans ce domaines. MySQL proposent les fonctions essentielles de journalisation avec des possibilités de rotation de fichiers pour éviter des tailles trop importantes. On pourra se référer à la page http://dev.mysql.com/doc/refman/5.0/fr/log-files.html pour se familiariser avec les journaux MySQL.

PostgreSQL offre depuis la version 8.3 des possibilités intéressantes : il est ainsi possible comme avec MySQL de trier et déposer dans des fichiers différents événements mais il est également possible d'envoyer les journaux vers d'autres destinations ou sous d'autres formes.

Ainsi, PostgreSQL peut stocker ses journaux sous forme de fichiers CSV importables dans un tableur ou bien les envoyer vers un serveur syslog en reprenant les critères propres à ce dernier. Un très bon article sur le sujet peut être trouvé à l'adresse http://www.unixgarden.com/index.php/administration-systeme/nouvelle-gestion-des-journaux-applicatifs-sous-postgresql-83.

Quel que soit le SGBD utilisé, celui-ci est souvent capable de produire des journaux. Dans un contexte comme celui d'un gestionnaire de contenu ou d'une base de comptes servant à l'authentification, il est plus que recommandé d'activer ses journaux et de les exploiter régulièrement car comme tous les autres journaux, ils peuvent être une source d'information indispensable à la détection ou à l'analyse d'un incident.

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 14 et le 21 mai 2009.

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 15 au 22 mai 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-190 : Vulnérabilités dans IPsec Tools
- CERTA-2009-AVI-191 : Vulnérabilité dans Xerox WorkCentre
- CERTA-2009-AVI-192 : Vulnérabilités dans OpenSSL
- CERTA-2009-AVI-193 : Vulnérabilités dans Claroline
- CERTA-2009-AVI-194 : Vulnérabilité dans Cyrus SASL
- CERTA-2009-AVI-195 : Vulnérabilités dans ntpd

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 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.

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.ssi.gouv.fr/fr/formation/

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.

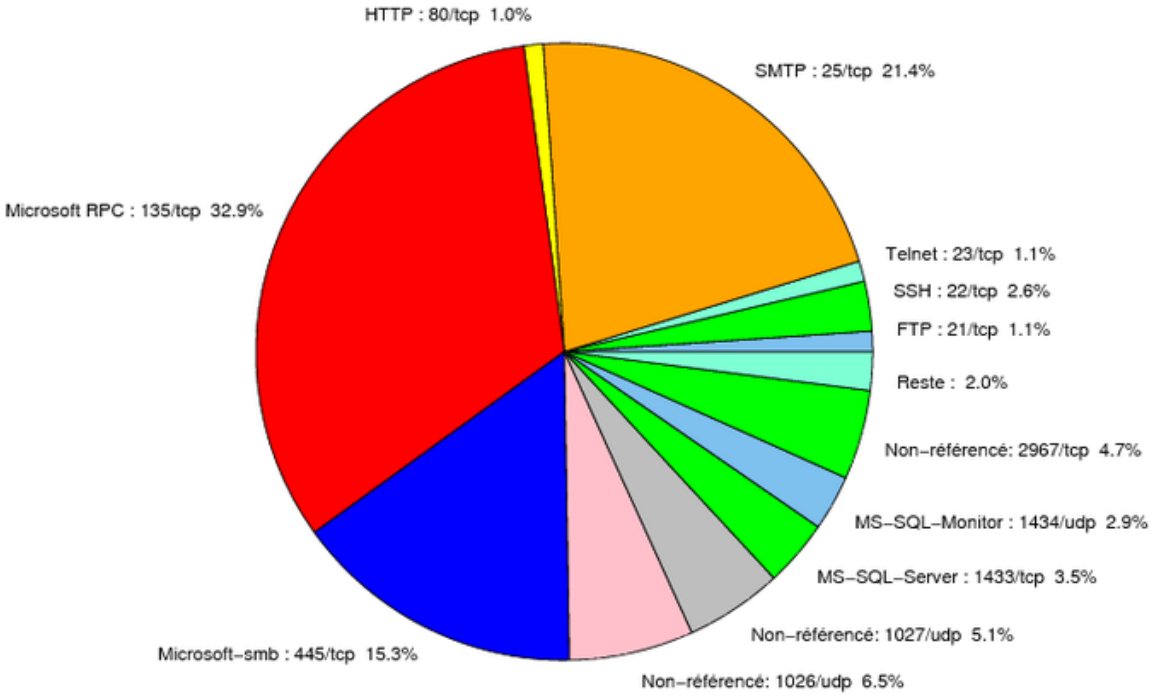

FIG. 1: Répartition relative des ports pour la semaine du 14 au 21 mai 2009

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

				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	32.85
25/tcp	21.35
445/tcp	15.36
1026/udp	6.52
1027/udp	5.1
2967/tcp	4.68
1433/tcp	3.49
1434/udp	2.9
22/tcp	2.6
80/tcp	1.12
21/tcp	1.06
4899/tcp	0.88
3389/tcp	0.47
139/tcp	0.29
3306/tcp	0.11
3128/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

22 mai 2009 version initiale.