Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 janvier 2010
N° CERTA-2010-ACT-001

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-01

Gestion du document

Référence	CERTA-2010-ACT-001
Titre	Bulletin d'actualité 2010-01
Date de la première version	08 janvier 2010
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-2010-ACT-001.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-2010-ACT-001/

1 Vulnérabilités des routeurs Juniper

La presse a relayé l'envoi d'un bulletin de sécurité par Juniper à ses clients pour les mettre en garde contre plusieurs vulnérabilités affectant ses produits. Ce bulletin, référencé PSN-2010-01-63 et non public, porte sur sept vulnérabilités corrigées. L'une d'entre elles permet à un utilisateur malveillant de faire s'arrêter puis redémarrer un routeur vulnérable. Elle a immédiatement attiré l'attention des spécialistes. En effet, pouvoir interrompre à distance le fonctionnement d'un routeur est considéré comme un problème critique, en particulier par les opérateurs de réseaux.

L'éditeur informe que les versions de son logiciel JunOS construites après le 28 janvier 2009 ne sont plus vulnérables.

L'application de correctifs sur des routeurs est toujours une opération délicate, nécessitant méthode et planification. Elle est rarement immédiate dans les environnements en production. Cependant, près d'un an après la publication d'une version corrigée des différentes versions maintenues par l'éditeur, ce bulletin de sécurité peut être lu comme un rappel en direction des clients.

Le maintien à jour des logiciels sur tous les composants reste un principe de base.

Documentation

- Article de Praetorian Perfect du 06 janvier 2010 :
  http://praetorianprefect.com/archives/2010/01/junos-juniper-flaw-exposes-core-routers-to-kernel-crash/
- Bulletins de sécurité de Juniper (non publics) :
  http://www.juniper.net/support/security/security_notices.html
- Cycle de vie des produits Juniper :
  http://www.juniper.net/support/eol/junos.html

2 L'avancée des attaques par PDF

Trop d'utilisateurs considèrent encore le `PDF` (`Portable Document Format`) comme un format statique et inoffensif, ce qui est loin d'être le cas, c'est même l'un des vecteurs d'attaque les plus prisés à l'heure actuelle.

La plupart des gens utilisent `Adobe Reader`, ce logiciel est donc la cible privilégiée des attaques par fichiers `PDF`. Cette tendance est renforcée par les délais de correction de la part d'`Adobe`. À titre d'exemple, l'alerte CERTA-2009-ALE-023 (`http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-023/`) publiée le 15 décembre 2009 ne sera pas corrigée avant le 12 janvier 2010, malgré la criticité élevée de cette faille de sécurité.

Il n'est donc pas surprenant que cette faille soit actuellement activement exploitée, avec en plus une sophistication généralisée des attaques par `PDF` qui commencent à se rapprocher du niveau de celles utilisées dans les documents de type `Compound File` (format `Microsoft Office` notamment). Pour preuve, un document `PDF` apparu il y a quelques jours, exploite cette faille non corrigée de façon relativement évoluée.

Ce `PDF` exécute un code `JavaScript` construisant et injectant le *payload* de l'exploitation, constitué classiquement d'une zone *NOP* améliorée et d'un *shellcode*. Ce *shellcode* est en fait le premier étage d'un `egg-hunt shellcode` (*shellcode* à étages) et est obscurci, il est donc de taille très réduite : 38 octets. Là où l'attaque est plus évoluée, c'est dans la forme du deuxième étage du *shellcode*, qui est stocké comme un objet de type couleur dans le `PDF` et est marqué comme compressé avec `FlateDecode` (format de compression `zlib`). Ce `PDF` contient également deux fichiers binaires obscurcis, l'un est une porte dérobée bien connue des spécialistes : `PoisonIvy`, l'autre exécute `Adobe Reader` pour ouvrir un document `PDF` sain embarqué dans ce même binaire.

Lorsque ce fichier `PDF` est ouvert dans `Adobe Reader` avec le support `JavaScript` activé, une porte dérobée est installée sur le système et un document `PDF` sain est ouvert pour faire croire à l'utilisateur que tout s'est passé normalement. Pourtant l'exploitation de la vulnérabilité a bel et bien corrompu le système à la première exécution d'`Adobe Reader`. Ce comportement n'est pas sans rappeler celui des documents *Office* malveillants générés par des *binders* (outils automatisant la génération de documents malveillants).

Le `CERTA` recommande fortement l'application des solutions de contournement présentées dans l'alerte de sécurité CERTA-2009-ALE-023 (`http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-023/`).

3 Alertes, correction d'alertes et avis

Cette semaine le CERTA a publié l'avis de sécurité CERTA-2010-AVI-007 qui corrige l'alerte CERTA-2009-ALE-021 concernant `Adobe Illustrator`. Des codes permettant l'exploitation de cette vulnérabilité étant disponibles sur l'Internet, le CERTA rappelle l'impérieuse nécessité de mettre à jour les logiciels concernés dans les plus brefs délais.

Documentation

- Alerte CERTA-2009-ALE-021 du 10 décembre 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-021/
- Avis CERTA-2010-AVI-007 du 08 janvier 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-007/

4 Bogue de l'année 2010

Certaines applications ont été victimes d'un bogue tout-à-fait inattendu, le bogue de l'année 2010. En effet, certains programmes ne gèrent pas correctement les dates au-delà du 31 décembre 2009. C'est le cas notamment pour certaines versions des jeux de règles de *SpamAssassin* qui considèrent comme *spam* tout message électronique

daté de 2010. Le problème est en fait lié à une règle vérifiant que la date du message électronique reçu n'est pas ultérieure à 2010. Ce bogue était théoriquement corrigé depuis juin 2009, mais cette correction n'a pas été répercutée par toutes les distributions.

Le produit *Symantec Endpoint Protection* a également rencontré des problèmes. En effet, les mises à jour des signatures de virus postérieures au 31 décembre 2009 étaient considérées comme antérieures à cette date. Ce bogue n'est pas complètement corrigé pour le moment.

D'autres applications peuvent rencontrer des problèmes. Il est difficile de tenir une liste exhaustive ou d'associer un dysfonctionnement de logiciel avec un problème de date. Un article du SANS évoque quelques incidents liés au passage en 2010.

Documentation

- Bogue #6269 de SpamAssassin :
  https://issues.apache.org/SpamAssassin/show_bug.cgi?id=6269
- Article de Symantec concernant des problèmes de date dans Symantec Endpoint Protection :
  http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2010010308571348
- Article du SANS à propos de dysfonctionnements liés au passage en 2010 :
  http://isc.sans.org/diary.html?storyid=7873

5 GNU/Linux et les modèles de sécurité

Traditionnellement, les systèmes d'exploitation de type GNU/Linux utilisent le concept de DAC (Discretionary Access Control) pour définir la politique de sécurité encadrant les droits et accès aux ressources du système.

Ainsi on définit pour chaque fichier un propriétaire, un groupe et des droits qui y sont associés : lecture, écriture, exécution. On peut de cette façon écrire des règles du type, l'utilisateur 'u' peut exécuter le binaire 'b' ou encore le groupe 'g' peut lire et écrire dans le fichier 'f'.

Ce mécanisme est relativement ancien et peut dans certains cas être insuffisant au regard du niveau de sécurité requis. Par exemple, un utilisateur peut très bien changer les droits des fichiers ou programmes dont il est le propriétaire. La sécurité repose alors en partie sur celle définie par les utilisateurs du système eux-mêmes. Un administrateur de système pourrait vouloir, plutôt, définir une liste explicite des autorisations par utilisateur sur les ressources du système (fichiers, périphériques, zones de la mémoire, etc.).

Pour compléter le système de DAC, il existe d'autres mécanismes comme le RBAC (Role Base Access Control) basés sur des définitions de rôles donnés aux utilisateurs. Ces rôles sont construits en fonction du système d'information par une autorité. Cette dernière donnera les accès selon les rôles aux différents éléments du système. Ainsi le *patch* noyau Grsecurity permet, par exemple, de définir diverses permissions sur les ressources réseau (*sockets*) en fonction de l'appartenance à des groupes du système : client, serveur, client/serveur.

Enfin une dernière catégorie existe : le MAC (Mandatory Access Control). Il part du principe qu'aucun accès aux ressources du système ne peut être définit par son propriétaire lui-même. Poussé à l'extrême, ce principe impose que le compte administrateur ne pourra pas tout faire sur un système en fonctionnement et sera contraint par une politique que même lui ne pourra défaire ou contourner. Sous GNU/Linux, Il existe essentiellement deux systèmes de ce type s'appuyant tout deux sur les extensions de sécurité du noyau (LSM: Linux Security Modules): SELinux et AppArmor.

Le premier est intégré au noyau et initié par la NSA pour ses systèmes sensibles. On le trouve essentiellement dans les distributions comme Debian ou RedHat mais pas forcement de façon active.

Le second, plus récent et soutenu par Novell dans sa distribution SuSE, est mis en œuvre, maintenant, par défaut dans les dernières versions d'Ubuntu. On trouve ainsi dans cette dernière deux répertoires : */etc/appamor* et /etc/apparmor.d dans lesquels sont définis des profils de sécurité par défaut relatifs à l'ensemble des ressources du système. Bien qu'assez complexe, il peut être intéressant de se pencher sur cette configuration qui apporte un gain notable du niveau de sécurité global. Ainsi, on peut y trouver des règles relatives aux navigateurs, aux lecteurs multimédia, etc.

Recommandations :

Quelque soit le choix de modèle avancé retenu pour améliorer le niveau de sécurité du système (RBAC ou MAC), il est important de bien s'attarder sur la configuration « livrée » avec la distribution. Ceci permet tout à la fois d'en connaître les limites mais également d'expliquer certains effets de bord inévitables avec ce type de fonctionnalités.

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=1937
- 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 01 au 07 janvier 2010, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-562 : Vulnérabilité dans Sendmail
- CERTA-2010-AVI-001 : Vulnérabilités dans Xoops
- CERTA-2010-AVI-002 : Vulnérabilité dans NTPD
- CERTA-2010-AVI-003 : Multiples vulnérabilités dans PowerDNS
- CERTA-2010-AVI-004 : Vulnérabilité dans MIT Kerberos 5
- CERTA-2010-AVI-005 : Vulnérabilité dans FreeBSD

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

- CERTA-2009-AVI-546-001 : Vulnérabilités dans PostgreSQL (Ajout des références aux bulletins de sécurité Ubuntu et Debian)

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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique63.html

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.

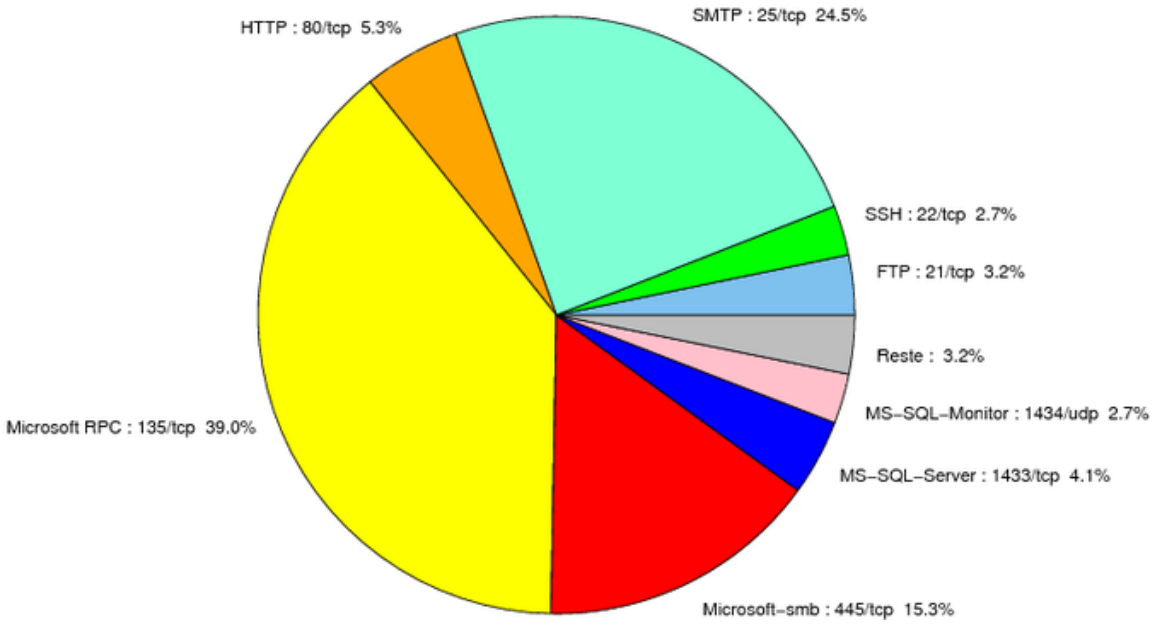

FIG. 1: Répartition relative des ports pour la semaine du 01 au 07 janvier 2010

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	38.97
25/tcp	24.54
445/tcp	15.3
80/tcp	6.13
1433/tcp	4.11
21/tcp	3.23
1434/udp	2.69
2967/tcp	0.74
1080/tcp	0.53
4899/tcp	0.4
2100/tcp	0.13
3306/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

08 janvier 2010 version initiale.