Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 janvier 2010
N° CERTA-2010-ACT-002

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-02

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-2010-ACT-002

Gestion du document

Référence	CERTA-2010-ACT-002
Titre	Bulletin d'actualité 2010-02
Date de la première version	15 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-002.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-002/

1 Vulnérabilité non corrigée dans Microsoft Internet Explorer

Le 14 janvier 2010, `Microsoft` a publié un bulletin de sécurité concernant une vulnérabilité non corrigée dans son navigateur `Internet Explorer`. Le CERTA a donc publié l'alerte CERTA-2010-ALE-001 afin de prévenir sa communauté des risques associés à cette vulnérabilité.

La faille est due à une référence à un pointeur non valide et permet à une personne malintentionnée d'exécuter du code arbitraire à distance. Les versions 6, 7 et 8 d'`Internet Explorer` sont concernées. Des exploitations limitées de cette vulnérabilité ont déjà été constatées. Dans l'attente d'un correctif, il est préférable d'utiliser un navigateur alternatif.

Sinon, afin de limiter l'impact de cette vulnérabilité, le CERTA recommande les actions suivantes :

- désactiver l'interprétation de code dynamique (ex: *JavaScript*) ;
- naviguer sur l'Internet avec un compte utilisateur aux droits limités ;
- activer le *DEP Data Execution Prevention*.

Documentation

- Alerte CERTA-2010-ALE-001 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-2010/
- Bulletin de sécurité Microsoft #979352 du 14 janvier 2010 :
  http://www.microsoft.com/technet/security/advisory/979352.mspx

2 Trois avis critiques

Le CERTA a publié, le 13 janvier 2010, 3 avis critiques qu'il est impératif de prendre en compte dès que possible :

Multiples vulnérabilités dans des produits Oracle

De nombreuses vulnérabilités, dont certaines permettant l'exploitation de code arbitraire à distance, ont été corrigées dans les produits `Oracle` suivants :

- Oracle Database ;
- Oracle Application Server ;
- Oracle Access Manager ;
- Oracle E-Business Suite ;
- PeopleSoft Enterprise HCM (TAM) ;
- Oracle WebLogic Server ;
- Oracle JRockit ;
- Primavera P6 Enterprise Project Portfolio Management ;
- Primavera P6 Web Services.

Vulnérabilité dans Microsoft Windows

Une vulnérabilité concernant la mise en œuvre de la technologie `EOT` (*Embedded OpenType*) permet à un utilisateur mal intentionné d'exécuter du code arbitraire.

Multiples vulnérabilités dans Adobe Reader et Acrobat

De multiples vulnérabilités présentes dans `Adobe Reader` et `Acrobat` peuvent être exploitées, au moyen d'un fichier au format `PDF` spécialement construit, par une personne malveillante afin de provoquer l'arrêt inopiné de l'application ou d'exécuter du code arbitraire à distance. Cet avis corrige l'alerte CERTA-2009-ALE-023.

Documentation

- Avis de sécurité CERTA-2010-AVI-010 (Multiples vulnérabilités dans des produits Oracle) :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-010/
- Avis de sécurité CERTA-2010-AVI-011 (Vulnérabilité dans Microsoft Windows) :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-011/
- Avis de sécurité CERTA-2010-AVI-012 (Multiples vulnérabilités dans Adobe Reader et Acrobat) :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-012/
- Alerte de sécurité CERTA-2009-AVI-023 (Vulnérabilités dans Adobe Reader et Adobe Acrobat) :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-023/

3 La version d'Adobe Flash Player installée par défaut avec Windows XP est vulnérable

Cette semaine Microsoft a publié un avis de sécurité rappelant que la version 6 d'`Adobe Flash Player` installée par défaut avec `Windows XP` est vulnérable et permet l'exécution de code arbitraire au moyen d'un document spécifiquement construit. Ce défaut de sécurité a déjà été signalé par Microsoft dans son bulletin du 13 novembre 2006, MS06-069.

Microsoft recommande de mettre à jour `Adobe Flash Player` avec la dernière version proposée par `Adobe`. Attention, la mise à jour nécessite des droits administrateur. Si un utilisateur aux droits restreints tente de la faire, il n'aura pas obligatoirement de message d'erreur l'informant de l'échec de celle ci et il pourra croire que son `player` est à jour.

Documentation

- Avis de sécurité Microsoft #979267 du 12 janvier 2010 :
  http://www.microsoft.com/technet/security/advisory/979267.mspx
- Bulletin de sécurité Microsoft MS06-069 du 14 novembre 2006 :
  http://www.microsoft/france/technet/security/bulletin/ms06-069.mspx

4 Vulnérabilité dans différents modèles de clés USB chiffrées

La société `Syss` a révélé en décembre 2009 une vulnérabilité dans l'implémentation logicielle du mécanisme de chiffrement de certains modèles de clés USB chiffrées (`http://www.syss.de/index.php?id=108&L=1&tx_ttnews[tt_news]=528&tx_ttnews[backPid]=59&cHash=d0a8db6e51`).

Les modèles affectés utilisent un mécanisme de chiffrement logiciel qui s'exécute sur la machine et non un mécanisme matériel s'exécutant sur la clé elle-même.

Il est à noter que certains de ces modèles avaient obtenu la certification *FIPS 104-2 Level 2*.

Certains fabricants des modèles concernés proposent des mises à jour logicielles pour corriger le problème :

- Kingston :
  http://www.kingston.com/driveupdate/
- Sandisk :
  http://www.sandisk.com/business-solutions/enterprise/technical-support/security-bulletin-december-2009
- Verbatim :
  http://www.verbatim.com/security/security-update.cfm
  Cette vulnérabilité rappelle l'impérieuse nécessité de mette à jour tous les éléments du poste informatique et de ne pas se limiter à la seule partie logicielle.

5 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/

6 Rappel des avis émis

Dans la période du 08 au 14 janvier 2010, le CERTA a émis les avis suivants :

– CERTA-2010-AVI-006 : Vulnérabilité dans Novell iManager eDirectory
– CERTA-2010-AVI-007 : Vulnérabilités dans Adobe Illustrator
– CERTA-2010-AVI-008 : Mulitples vulnérabilités dans VMware ESX
– CERTA-2010-AVI-009 : Multiples vulnérabilités dans IBM Lotus Domino Web Access
– CERTA-2010-AVI-010 : Multiples vulnérabilités dans des produits Oracle
– CERTA-2010-AVI-011 : Vulnérabilité dans Microsoft Windows
– CERTA-2010-AVI-012 : Multiples vulnérabilités dans Adobe Reader et Acrobat
– CERTA-2010-AVI-013 : Vulnérabilité dans MIT Kerberos
– CERTA-2010-AVI-014 : Vulnérabilité dans Zope
– CERTA-2010-AVI-015 : Vulnérabilité dans Solaris Trusted Extensions
– CERTA-2010-AVI-016 : Vulnérabilité dans Sun Identity Manager
– CERTA-2010-AVI-017 : Vulnérabilité dans Novell ZENWorks Asset Management
– CERTA-2010-AVI-018 : Multiples vulnérabilités dans Red Hat Linux

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

– CERTA-2009-AVI-482-004 : Vulnérabilité du protocole SSL/TLS (ajout du bulletin de sécurité IBM du 13 janvier 2010)
– CERTA-2009-AVI-515-002 : Vulnérabilité dans BIND avec DNSSEC (ajout du bulletin de sécurité FreeBSD)
– CERTA-2010-AVI-003-001 : Multiples vulnérabilités dans PowerDNS (Ajout de la référence au bulletin de sécurité Debian)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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

8 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.

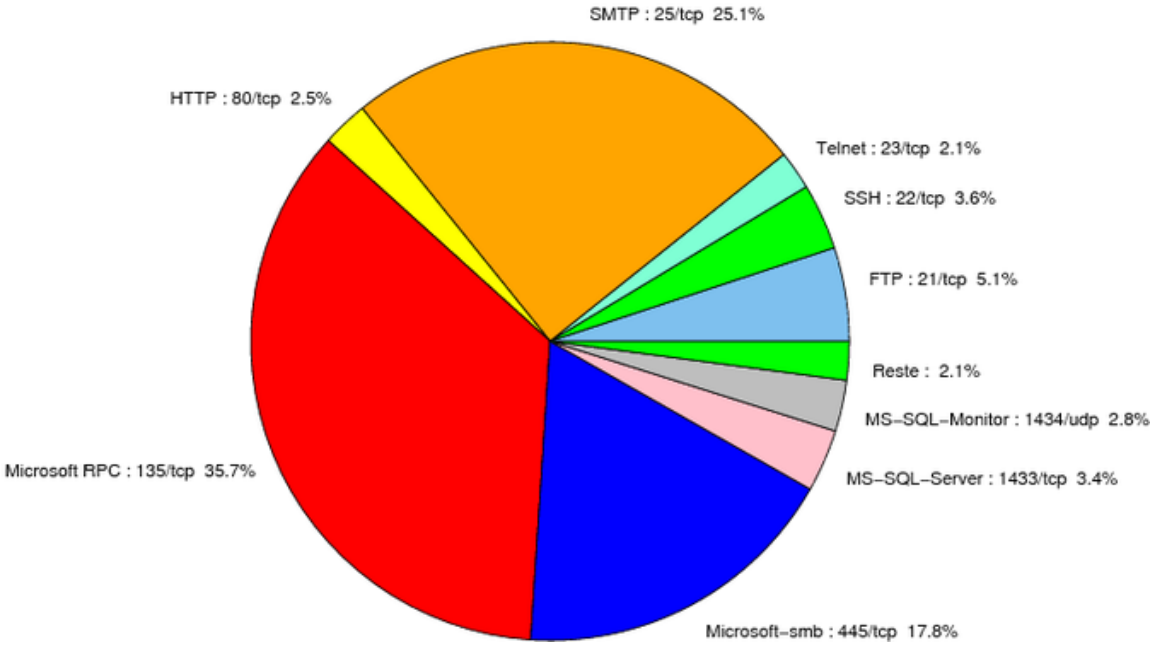

FIG. 1: Répartition relative des ports pour la semaine du 08 au 14 janvier 2010

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	35.67
25/tcp	25.08
445/tcp	17.8
21/tcp	5.12
22/tcp	3.64
1433/tcp	3.37
1434/udp	2.76
23/tcp	2.15
2967/tcp	0.8
4899/tcp	0.47
3389/tcp	0.26
3128/tcp	0.2
3306/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 8
3 Paquets rejetés 9

Gestion détaillée du document

15 janvier 2010 version initiale.