Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 juin 2010
N° CERTA-2010-ACT-023

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-23

Gestion du document

Référence	CERTA-2010-ACT-023
Titre	Bulletin d'actualité 2010-23
Date de la première version	11 juin 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-023.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-023/

1 Alertes publiées cette semaine

1.1 Vulnérabilité Shockwave Flash pour les produits Adobe

Le 05 juin 2010, le CERTA a publié une alerte concernant certains produits *Adobe* sur plusieurs systèmes d'exploitation. En effet, une vulnérabilité causée par une erreur dans le traitement des fichiers au format *Shockwave Flash* permet à un utilisateur malveillant d'exécuter du code arbitraire à distance. Cette exploitation peut être réalisée directement au moyen d'un fichier `SWF` spécialement construit ou indirectement au moyen d'un fichier au format `PDF`.

Cette vulnérabilité a fait l'objet d'une publication de l'éditeur *Adobe* qui fait mention de plusieurs cas d'exploitation découverts sur l'Internet. Le CERTA a également eu connaissance de tels cas d'exploitation.

Dans l'attente d'un correctif de sécurité, l'alerte CERTA-2010-ALE-007 propose un contournement provisoire qui consiste à limiter les accès à la bibliothèque vulnérable `authplay`. Le nom et l'emplacement de cette bibliothèque varient en fonction du système d'exploitation et sont repris en détail dans l'alerte.

Un correctif de sécurité concernant *Adobe Flash Player* a été publié le 10 juin 2010 (avis CERTA-2010-AVI-261). La vulnérabilité reste néanmoins non corrigée et exploitable pour les utilisateurs d'*Adobe Reader* et d'*Adobe Acrobat*.

De façon générale, le CERTA recommande de désactiver l'interprétation du JavaScript par les lecteurs *Adobe Reader* et *Adobe Acrobat*. De plus, la désactivation de l'interprétation des animations Flash ainsi que des animations 3D peut être appliquée.

Documentation :

- Avis de sécurité Adobe apsa10-01 du 04 juin 2010 :
  http://www.adobe.com/support/security/advisories/apsa10-01.html
- Bulletin d'alerte CERTA-2010-ALE-007 du 05 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-007/
- Avis CERTA-2010-AVI-261 du 11 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-261/

1.2 Vulnérabilité dans le Centre d'aide et de support Windows

Une vulnérabilité non-corrigée a été découverte dans le Centre d'aide et de support Windows. Elle permet à un utilisateur distant malintentionné d'exécuter du code arbitraire, notamment, via un navigateur Internet. Tous les navigateurs peuvent servir de vecteur d'exploitation, notamment si Windows Media Player 9 est installé sur la machine. D'autres vecteurs d'exploitation sont potentiellement possibles, notamment les documents Office.

Cette vulnérabilité concerne la gestion du protocole *HCP* utilisé par le Centre d'aide et de support Windows . Un lien *HCP* spécialement malformé permet ainsi l'exécution de code arbitraire à distance.

Des exemples de code d'exploitation de cette vulnérabilité sont d'ores et déjà recensés sur l'Internet.

Dans l'attente d'un correctif de l'éditeur, des contournements provisoires sont listés dans le bulletin d'alerte CERTA-2010-ALE-008.

Documentation :

- Bulletin d'alerte CERTA-2010-ALE-008 du 10 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-008/

2 Bulletins Microsoft

Plusieurs vulnérabilités dans des produits Microsoft ont été corrigées cette semaine. Ces mises à jour ont été traitées dans les bulletins de sécurité CERTA-2010-AVI-244 à CERTA-2010-AVI-253 le 09 juin 2010 et traitent des vulnérabilités suivantes :

- De multiples vulnérabilités ont été corrigées dans les pilotes noyau de Windows. Elles permettent une élévation de privilèges en tant qu'utilisateur Système (CERTA-2010-AVI-244) ;
- de multiples vulnérabilités ont été corrigées dans les composants de gestion multimédia de Windows. Elles permettent l'exécution de code arbitraire à distance, notamment via la lecture de documents de type ASF ou MJPEG (CERTA-2010-AVI-245) ;
- deux vulnérabilités ont été corrigées dans le contrôle ActiveX Microsoft Data Analyzer (CVE-2010-0252) et dans Microsoft Internet Explorer 8 Developer Tools (CVE-2010-0811). Ces vulnérabilités peuvent être exploitées par une personne malveillante afin d'exécuter du code arbitraire à distance au moyen d'un site Web ou d'un document Microsoft Office spécialement construits (CERTA-2010-AVI-246) ;
- deux vulnérabilités dans Internet Explorer ont été corrigées. Elles permettent à une personne malveillante d'exécuter du code arbitraire à distance au moyen d'une page Web spécialement construite (CERTA-2010-AVI-247) ;
- une vulnérabilité dans la validation des objets COM dans Microsoft Office permet à une personne malintentionnée d'exécuter du code arbitraire à distance via un document Microsoft Office spécialement conçu (CERTA-2010-AVI-248) ;
- une vulnérabilité due à une mauvaise validation de données dans le pilote OpenType Compact Font Format (CFF) permet à un utilisateur d'élever ses privilèges sur le système (CERTA-2010-AVI-249) ;

- quatorze vulnérabilités dans Microsoft Office ont été corrigées. Certaines sont exploitables au moyen d'un fichier Microsoft Excel spécifiquement réalisé permettant ainsi à une personne malintentionnée d'exécuter du code arbitraire à distance, et cela avec les droits de l'utilisateur victime. Ce bulletin de sécurité remplace le MS10-017 pour certains systèmes affectés (CERTA-2010-AVI-250) ;
- trois vulnérabilités ont été corrigées dans Microsoft SharePoint dont une révélée publiquement. Cette dernière permet à une personne malintentionnée d'élever ses privilèges au moyen d'un lien spécifiquement écrit (CERTA-2010-AVI-251) ;
- un traitement incorrect par IIS d'informations d'authentification est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance, au moyen d'une requête HTTP particulière (CERTA-2010-AVI-252) ;
- une vulnérabilité dans Microsoft .NET concernant le traitement de la signature des documents XML permet à un utilisateur malveillant de modifier un document signé sans que cette manipulation soit detectée (CERTA-2010-AVI-253).

Compte tenu de la criticité de certaines vulnérabilités, le CERTA préconise l'application dans les plus brefs délais des correctifs.

Documentation

- Avis du CERTA CERTA-2010-AVI-244 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-244/
- Avis du CERTA CERTA-2010-AVI-245 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-245/
- Avis du CERTA CERTA-2010-AVI-246 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-246/
- Avis du CERTA CERTA-2010-AVI-247 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-247/
- Avis du CERTA CERTA-2010-AVI-248 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-248/
- Avis du CERTA CERTA-2010-AVI-249 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-249/
- Avis du CERTA CERTA-2010-AVI-250 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-250/
- Avis du CERTA CERTA-2010-AVI-251 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-251/
- Avis du CERTA CERTA-2010-AVI-252 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-252/
- Avis du CERTA CERTA-2010-AVI-253 du 09 juin 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-253/

3 Kill Bit pour Microsoft Office

Le bulletin de sécurité Office MS10-036 a introduit la notion de *Kill bit* pour les applications Office. Comme les *Kill bit* pour Internet Explorer, elle permet d'empêcher le chargement de contrôles *ActiveX* ou objets *OLE* dans les applications Office.

L'administrateur peut configurer via une entrée de registre les *CLSID* qu'il souhaite ne pas voir charger dans Office.

Cette nouvelle fonctionnalité est disponible pour Office 2003 et Office 2007.

Le bulletin d'actualité CERTA-2009-ACT-012 proposait un contournement basé sur le blocage des fichiers *XML*. Il est rendu caduc par cette nouvelle fonctionnalité de *Kill bit*.

3.1 Documentation

- Article technique Microsoft kb983632 :
  http://support.microsoft.com/kb/983632
- Bulletin d'actualité du CERTA du 20 mars 2009, CERTA-2009-ACT-012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-012/

4 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/

5 Rappel des avis émis

Dans la période du 04 au 10 juin 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-236 : Vulnérabilité dans HP StorageWorks Storage Mirroring
- CERTA-2010-AVI-237 : Vulnérabilités dans OpenSSL
- CERTA-2010-AVI-238 : Multiples vulnérabilités dans MySQL Enterprise Monitor
- CERTA-2010-AVI-239 : Vulnérabilités dans IBM DB2
- CERTA-2010-AVI-240 : Vulnérabilité dans CA ARCserve Backup
- CERTA-2010-AVI-242 : Multiples vulnérabilités dans Novell eDirectory
- CERTA-2010-AVI-243 : Multiples vulnérabilités dans Apple Safari
- CERTA-2010-AVI-244 : Multiples vulnérabilités dans les pilotes noyaux de Windows
- CERTA-2010-AVI-245 : Multiples vulnérabilités dans la décompression de fichiers multimédia sous Windows
- CERTA-2010-AVI-246 : Vulnérabilité dans certains contrôles ActiveX
- CERTA-2010-AVI-247 : Vulnérabilité dans Internet Explorer
- CERTA-2010-AVI-248 : Vulnérabilité dans Microsoft Office
- CERTA-2010-AVI-249 : Vulnérabilité dans le pilote CFF de Windows
- CERTA-2010-AVI-250 : Multiples vulnérabilités dans Microsoft Office Excel
- CERTA-2010-AVI-251 : Vulnérabilités dans Microsoft SharePoint
- CERTA-2010-AVI-252 : Vulnérabilité dans Microsoft IIS
- CERTA-2010-AVI-253 : Vulnérabilité dans Microsoft NET
- CERTA-2010-AVI-254 : Vulnérabilité dans IBM WebSphere
- CERTA-2010-AVI-255 : Vulnérabilité dans McAfee UTM Firewall
- CERTA-2010-AVI-256 : Vulnérabilités dans Cisco Unified Contact Center Express
- CERTA-2010-AVI-257 : Vulnérabilité dans Cisco Application Extension Platform

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

– CERTA-2010-AVI-241-001 : Vulnérabilités dans OpenOffice.org (précision sur les versions touchées.)

Enfin, deux vulnérabilités non corrigées ont chacune fait l'objet d'une alerte :

– CERTA-2010-ALE-007 : Vulnérabilité Shockwave Flash pour les produits Adobe
– CERTA-2010-ALE-008 : Vulnérabilité dans le Centre d'aide et de support Windows

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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_rubrique67.html

7 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.

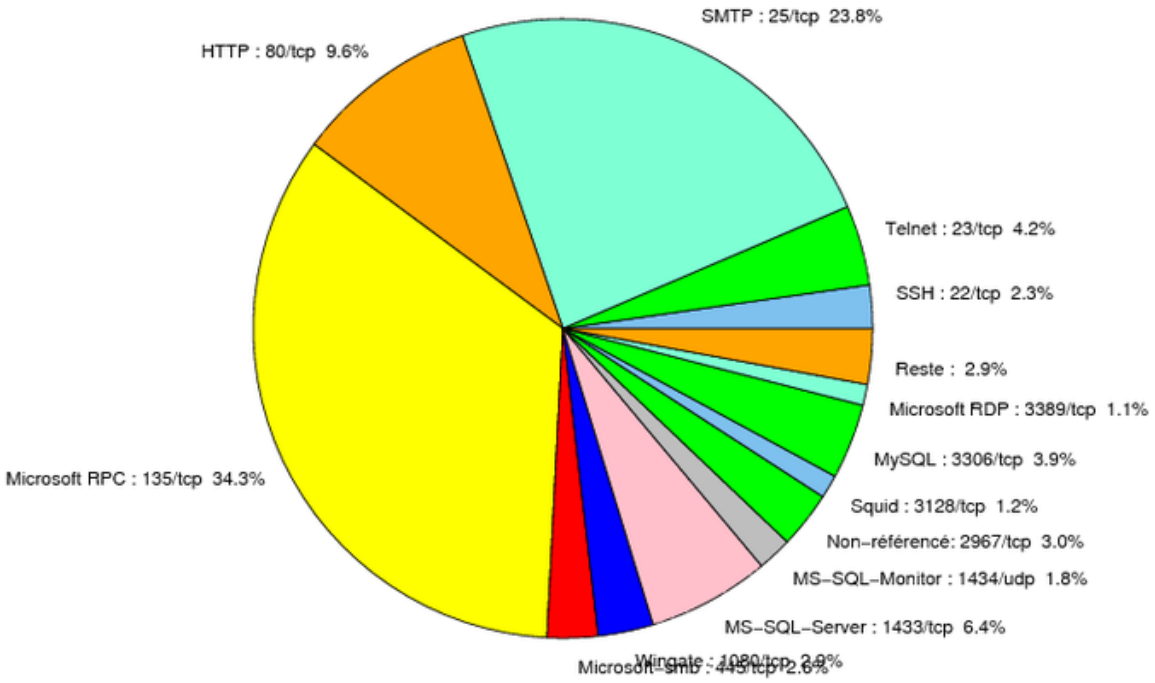

FIG. 1: Répartition relative des ports pour la semaine du 04 au 10 juin 2010

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
80/tcp	44.55
135/tcp	34.32
25/tcp	23.82
1433/tcp	6.37
22/tcp	5.02
23/tcp	4.18
3306/tcp	3.92
2967/tcp	2.96
1080/tcp	2.89
445/tcp	2.64
143/tcp	2.06
1434/udp	1.8
3128/tcp	1.22
3389/tcp	1.15
4899/tcp	0.96
3127/tcp	0.45
139/tcp	0.38
137/udp	0.32
15118/tcp	0.25
1027/udp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

11 juin 2010 version initiale.