Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 février 2010
N° CERTA-2010-ACT-006

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-06

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-006`

Gestion du document

Référence	CERTA-2010-ACT-006
Titre	Bulletin d'actualité 2010-06
Date de la première version	12 février 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-006.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-006/

1 Incidents de la semaine

Cette semaine, le CERTA a traité un cas de courriel piégé avec une pièce jointe malveillante. Celle-ci, au format *PDF*, tentait d'exploiter plusieurs vulnérabilités selon la version du lecteur `Adobe Reader` utilisé. Cela est possible grâce à l'interprétation du *JavaScript* par le logiciel. En effet, l'exécution de scripts permet de cibler la version d'`Adobe Reader` utilisée et de faciliter l'exploitation des différentes vulnérabilités.

Si le *PDF* malveillant visait plusieurs versions d'`Adobe Reader`, fort heureusement le *shellcode* ensuite exécuté était plus capricieux. En effet, celui-ci tente de copier la charge malveillante dans un répertoire spécifique du système avant de l'exécuter. L'écriture dans ce répertoire nécessitait toutefois des droits administrateur, ce que le code ne vérifie pas. La victime ayant ouvert la pièce jointe utilisant un compte aux droits limités, son poste n'a finalement pas été compromis.

Si de nombreux codes malveillants fonctionnent quel que soit le type de compte utilisé, le CERTA rappelle que, selon le principe de défense en profondeur, outre la mise à jour des applications qui reste un principe fondamental, l'utilisation d'un poste pour des tâches bureautiques doit se faire avec un compte qui n'a pas de droits d'administration. De même, les utilisateurs d'`Adobe Reader` doivent désactiver l'interprétation du *JavaScript* qui est très rarement indispensable à la lecture d'un document.

2 Actualité Microsoft

2.1 Les correctifs du mois de février

Mardi, Microsoft a publié son lot mensuel de correctifs. Ils sont au nombre de 13 et corrigent 26 vulnérabilités. Voici un rappel des bulletins émis :

- une vulnérabilité dans Microsoft Office permet d'exécuter du code arbitraire, avec les droits de l'utilisateur sur l'ordinateur vulnérable lors de l'ouverture d'un fichier spécialement conçu ;
- six vulnérabilités dans Microsoft Powerpoint, permettant d'effectuer une exécution de code arbitraire, ont été corrigées ;
- une vulnérabilité dans Microsoft Paint permet à une personne malintentionnée distante de provoquer l'exécution de code arbitraire via un fichier *JPEG* spécialement conçu ;
- deux vulnérabilités dans le client *SMB* de Microsoft Windows ont été corrigées ;
- une vulnérabilité est exploitable par le biais d'un navigateur Web envoyant des données spécialement conçues à la fonction *ShellExecute* via le gestionnaire de *Shell Windows* ;
- une vulnérabilité permet l'exécution de code arbitraire à distance par le biais d'une page Web spécialement conçue appelant un contrôle *ActiveX* vulnérable ;
- des erreurs dans l'implémentation du protocole *IPv6* dans Microsoft Windows contient plusieurs vulnérabilités qui permettent, entre autre, à un utilisateur distant malintentionné d'exécuter du code arbitraire avec les privilèges « Système » ;
- une vulnérabilité permet à une personne malintentionnée de créer un déni de service en bloquant l'exécution d'*Hyper-V* (le système d'hypervision de Microsoft) et de toutes les machines virtuelles en service. L'exploitation de cette vulnérabilité nécessite d'être authentifié dans l'une des machines virtuelles et de pouvoir y exécuter du code localement ;
- une vulnérabilité dans le processus *CSRSS* (*Client-Server Run-time Subsystem*) permet à une personne malintentionnée d'élever ses privilèges sur le système ;
- plusieurs vulnérabilités dans Microsoft Windows SMB permettent d'exécuter du code arbitraire à distance, de provoquer un déni de service ou d'élever ses privilèges ;
- une vulnérabilité dans Microsoft DirectShow affecte le filtre *AVI* et permet à une personne malveillante d'exécuter du code arbitraire au moyen d'un fichier au format *AVI* spécialement construit ;
- une vulnérabilité dans *Kerberos* due à un traitement incorrect de certaines requêtes permet à une personne malintentionnée de provoquer un déni de service sur un contrôleur de domaine Windows ;
- une vulnérabilité dans le sous-système MS-DOS (*ntvdm.exe*) et affectant potentiellement toutes les versions 32 bits de Microsoft Windows, permet à un utilisateur local d'élever ses privilèges au moyen d'un exécutable spécialement construit. Ce correctif comble la vulnérabilité décrite dans l'alerte CERTA-2010-ALE-002.

Pour mémoire, la liste des avis publiés par le CERTA pendant la semaine (du jeudi au jeudi) précédent ce document est disponible dans la section « Rappel des avis émis » du bulletin d'actualité.

2.2 Vulnérabilités Microsoft liées à la gestion du SMB

2.2.1 Détails

Parmi les bulletins de sécurité Microsoft publiés cette semaine, deux concernent la gestion du protocole *SMB*.

Le bulletin MS10-006 concerne la partie cliente de la gestion du protocole *SMB*. Dans ce bulletin nous nous intéresserons plus spécifiquement à la vulnérabilité CVE-2010-0016. Pour cette vulnérabilité, le scénario d'attaque typique suppose qu'un serveur ait été compromis. Dans ce cas, chaque client se connectant à ce serveur sera à son tour compromis (via une exécution de code) lors de la réception d'une requête *SMB* spécialement malformée qui lui sera envoyée par le serveur.

On peut aussi envisager qu'une machine cliente infectée se transforme en serveur infectant via, par exemple, l'usurpation de paquets *NBNS* (*NetBIOS Name Service*).

Il est à noter que le chercheur à l'origine de la découverte de la vulnérabilité a publié un document détaillé expliquant le savoir faire nécessaire à l'exploitation de cette vulnérabilité.

L'autre bulletin, MS10-012, concerne la partie serveur de la gestion du protocole *SMB*. L'une des vulnérabilités (CVE-2010-0020) couverte par ce bulletin permet l'exécution de code arbitraire à distance en envoyant une requête *SMB* malformée à toute machine dont le service serveur est démarré.

Pour les deux vulnérabilités dont nous venons de parler, l'exécution de code s'effectue avec les privilèges « Système » permettant un contrôle total de la machine.

Le fait que l'exploitation de ces deux vulnérabilités nécessite une authentification n'est qu'un facteur atténuant partiel car c'est le cas dans la plupart des réseaux d'entreprises utilisant un annuaire.

2.2.2 Recommandation

L'exploitation de ces vulnérabilités pouvant potentiellement servir à la propagation d'un ver, le CERTA recommande l'installation au plus tôt de ces deux correctifs.

2.2.3 Documentation

- Bulletin de sécurité Microsoft MS10-006 du 09 février 2010 :
  http://www.microsoft.com/france/technet/security/bulletin/ms10-006.mspx
- Bulletin de sécurité Microsoft MS10-012 du 09 février 2010 :
  http://www.microsoft.com/france/technet/security/bulletin/ms10-012.mspx

2.3 Problème de stabilité lié à la mise a jour du bulletin Microsoft MS10-015

2.3.1 Détails

Il a été remonté par plusieurs utilisateurs que suite à l'application du correctif MS10-015 un redémarrage inopiné de la machine pouvait survenir (redémarrage en boucle). Comme spécifié dans le blog `MSRC`, ce problème est en cours d'étude chez `Microsoft`.

La diffusion par *Windows Update* de cette mise à jour est pour le moment suspendue.

2.3.2 Recommandations

Le CERTA recommande de tester exhaustivement ce correctif avant toute mise en production ou d'appliquer temporairement les contournements proposés par l'éditeur.

2.3.3 Documentation

- Bulletin de sécurité Microsoft MS10-015 du 09 février 2010 :
  http://www.microsoft.com/france/technet/security/bulletin/ms10-015.mspx
- Blog MSRC du 11 février 2010 :
  http://blogs.technet.com/msrc/archive/2010/02/11/restart-issues-after-installing-ms10-015.aspx

3 Annonce d'une mise à jour pour Adobe Reader et Adobe Acrobat

L'éditeur *Adobe* annonce la publication de correctifs pour le mardi 16 février 2010, donc hors du cycle trimestriel annoncé l'été dernier.

Les vulnérabilités corrigées lors de cette mise à jour sont considérées critiques par l'éditeur. Cette qualification laisse supposer la possibilité pour l'attaquant d'exécuter du code arbitraire à l'insu de l'utilisateur.

Les logiciels concernés sont :

- Adobe Acrobat 9.3 et 8.2 sur Windows et MacOS ;
- Adobe Reader 9.3 sur Windows, Unix et MacOS ;
- Adobe Reader 8.2 sur Windows et MacOS.

3.1 Documentation

- Bulletin de sécurité Adobe APSB17-07 du 11 février 2010 :
  http://www.adobe.com/support/security/bulletins/apsb10-07.html

4 Home Network Administration Protocol

4.1 De quoi s'agit-il

Il s'agit d'un protocole basé sur `HTTP-SOAP` (*Simple Object Access Protocol*) qui peut servir à administrer des équipements (routeurs, caméras, *NAS* ...). Plus simplement, il s'agit d'envoyer un message en `XML`, respectant un certain format, en utilisant le protocole `HTTP`. Ce message peut par exemple contenir une demande d'informations (*GetDeviceSetting*) ou des consignes de configurations (*SetDeviceSetting*). Il est censé faciliter la réalisation d'une topologie précise du réseau, chaque appareil se décrivant à la demande (type, model, version de logiciel, ...). Pour savoir si un équipement supporte le protocole `HNAP`, il suffit de lui demander à l'aide d'un simple *GET* sur *http://[IPdevice]/HNAP1/*.

4.2 Le danger

Il est décrit comme « *simple, rapide et facile à mettre en œuvre* ». Avec une telle approche, sans parler des risques hypothétiques du protocole ou des problématiques d'avoir un serveur Web embarqué et potentiellement vulnérable, il est fort à parier que le développement et l'intégration d'un tel protocole suive l'idée du « *rapide* » et « *simple* », trop peut être.

4.3 Les conséquences

Il y a quelques semaines, une présentation a montré que certains matériels ont une implémentation vulnérable du protocole `HNAP`. Si ceux-ci demandent bien un identifiant et un mot de passe pour accéder aux informations sensibles, la demande d'informations est elle librement accessibles. Le problème est qu'elle permet de contourner la demande d'authentification en encapsulant des commandes de configurations, dans un message de type demande d'informations.

Le CERTA recommande, dans la mesure du possible la désactivation de ce type de service, ou de ne les laisser accessible qu'a des réseaux dédiés ou tout du moins contrôlés.

4.4 Documentation

- Le site du protocole HNAP :
  http://hnap.org
- Simple Object Access Protocol :
  http://www.w3.org/TR/soap/

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 05 au 11 février 2010, le CERTA a émis les avis suivants :

– CERTA-2010-AVI-056 : Vulnérabilité dans HP Enterprise Cluser Master Toolkit
– CERTA-2010-AVI-057 : Vulnérabilités de DokuWiki
– CERTA-2010-AVI-058 : Vulnérabilité dans Oracle WebLogic Server
– CERTA-2010-AVI-059 : Vulnérabilité dans OTRS
– CERTA-2010-AVI-060 : Vulnérabilité dans Novell eDirectory
– CERTA-2010-AVI-061 : Vulnérabilité dans Microsoft Office
– CERTA-2010-AVI-062 : Vulnérabilités de Microsoft PowerPoint
– CERTA-2010-AVI-063 : Vulnérabilité dans Microsoft Paint
– CERTA-2010-AVI-064 : Vulnérabilités dans le client SMB de Microsoft Windows
– CERTA-2010-AVI-065 : Vulnérabilité dans le gestionnaire de Shell Windows
– CERTA-2010-AVI-066 : Vulnérabilité dans certains contrôles ActiveX
– CERTA-2010-AVI-067 : Multiples vulnérabilités dans Microsoft Windows TCP/IP
– CERTA-2010-AVI-068 : Vulnérabilité dans Microsoft Hyper-V
– CERTA-2010-AVI-069 : Vulnérabilité dans Microsoft Windows CSRSS
– CERTA-2010-AVI-070 : Multiples vulnérabilités dans Microsoft Windows SMB
– CERTA-2010-AVI-071 : Vulnérabilité dans Microsoft DirectShow
– CERTA-2010-AVI-072 : Vulnérabilité dans Kerberos sous Microsoft Windows
– CERTA-2010-AVI-073 : Vulnérabilité dans le sous-système MS-DOS de Microsoft Windows
– CERTA-2010-AVI-074 : Vulnérabilité dans Oracle WebLogic Server
– CERTA-2010-AVI-075 : Vulnérabilité dans HP Network Node Manager
– CERTA-2010-AVI-076 : Multiples vulnérabilités dans Cisco IronPort
– CERTA-2010-AVI-077 : Multiples vulnérabilités dans Google Chrome

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_rubrique67.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.

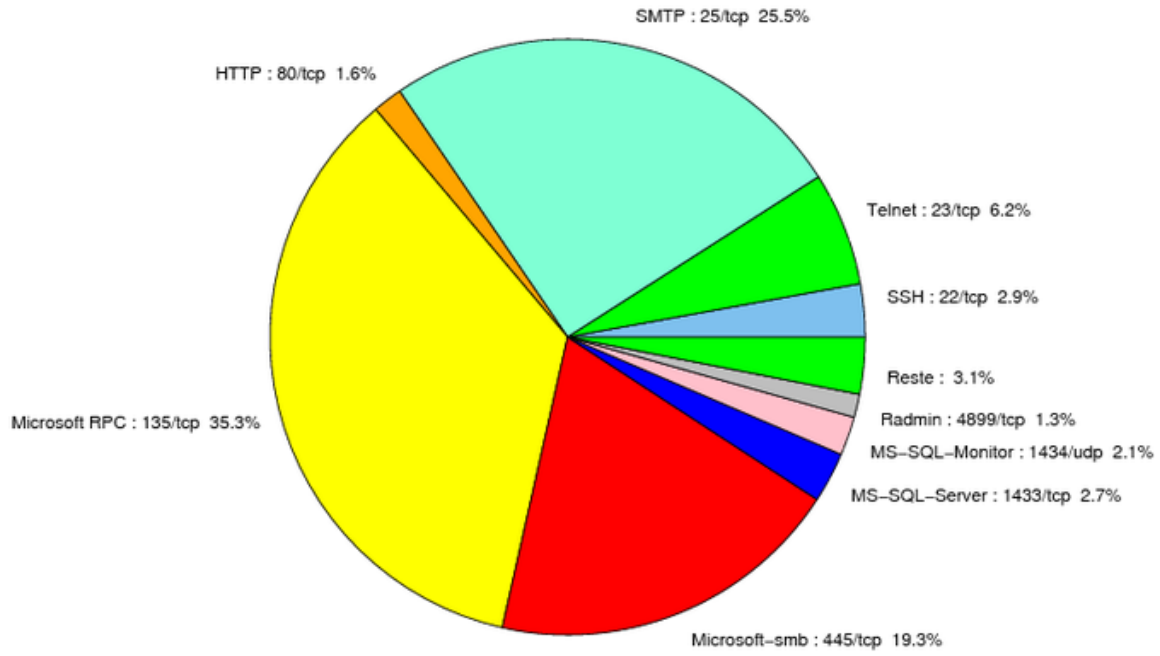

FIG. 1: Répartition relative des ports pour la semaine du 05 au 11 février 2010

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/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
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	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
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	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
445	TCP	Microsoft-smb	–	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 http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	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
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT

6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CERT
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CERT
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT
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/CERT
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CERT
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CERT
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CERT
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CERT

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	35.31
25/tcp	25.5
445/tcp	19.34
23/tcp	6.16
80/tcp	5.6
22/tcp	2.87
1433/tcp	2.73
1434/udp	2.1
4899/tcp	1.26
21/tcp	1.05
2967/tcp	0.98
1080/tcp	0.35
3306/tcp	0.28
3389/tcp	0.21

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

12 février 2010 version initiale.