Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 juin 2008
N° CERTA-2008-ACT-025

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-25

Gestion du document

Référence	CERTA-2008-ACT-025
Titre	Bulletin d'actualité 2008-25
Date de la première version	20 juin 2008
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-2008-ACT-025.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-2008-ACT-025/

1 Firefox 3.0

La nouvelle version du navigateur Firefox est sortie depuis quelques jours.

1.1 Quoi de neuf ?

Trois axes classiques d'évolution sont remarquables, l'ergonomie, les performances et la sécurité.

1.1.1 Fonctionnalité et ergonomie

Comme toute nouvelle mouture d'un logiciel, celle-ci amène son lot de nouvelles fonctionnalités qui simplifient son utilisation et améliorent le rendu graphique. Elles ne doivent cependant pas être utilisées au détriment de la sécurité. Par exemple, il y a une fonctionnalité déjà présente, très «pratique», et qu'il faut pourtant éviter d'utiliser : la sauvegarde des mots de passe.

Parmis les nouvelles fonctionnalités, on trouve :

– la possibilité de reprendre un téléchargement interrompu ;
– la possibilité de zoomer, plus uniquement en grossissant le texte, mais toute la page ;

– la possibilité d'utiliser des lecteurs multimédia externes pour lire les *podcast* (Attention, dans ce cas les vulnérabilités des logiciels tiers sont exploitables au travers du navigateur) ;
– la barre d'adresse «intelligente» permet de saisir une URL ou un titre de page, et elle présente toutes les pages déjà connues. (Cela nécessite que l'historique de navigation soit conservé, ce qui peut être contraire à la politique de sécurité).

1.1.2 Performances

Un des axes de développement annoncé était l'optimisation de l'utilisation de la mémoire vive et l'amélioration des performances. *Mozilla* annonce une vitesse d'utilisation deux fois plus rapide avec *gmail* par exemple. A l'usage, la différence n'est pas flagrante, le temps de réponse étant surtout conditionné par le débit de la connexion, la charge l'utilisation globale de la machine ainsi que celle du serveur.

1.1.3 Sécurité

Plusieurs fonctionnalités d'assistance à l'utilisateur pour lutter contre les fraudes en ligne et la propagation de codes malveillants ont été ajoutées. Encore une fois, il faudra vérifier que ces nouvelles possibilités n'entrainent pas de nouvelles fragilités.

– auparavant il y avait le «cadenas» qui indiquait si un site était chiffré. Maintenant l'icône à côté de l'adresse (la *favicon*) change de couleur en fonction des informations disponibles sur le site, et permet d'accéder simplement, en cas de chiffrement, aux détails du certificat utilisé ;
– la détection de site de *phishing* a changé de signalisation, il ne s'agit plus d'un *pop-up* mais d'une page complète ;
– la même technique de *black list* est appliquée aux pages connues comme contenant du code malveillant ;
– la collaboration avec les antivirus et le contrôle parental de *Windows VISTA* a été amélioré.

1.2 Ce qui ne change pas

Firefox est une application et doit donc être utilisé avec les précautions d'usage. A savoir :
– ne pas déployer directement une nouvelle version sans en tester les impacts ;
– attendre «un peu» peut permettre à la communauté d'utilisateurs de relever des problèmes potentiels ;
– comme toute application, elle peut contenir des vulnérabilités et doit être maintenue à jour.

Une vulnérabilité aurait d'ailleurs été déjà signalée. Elle serait considérée comme critique, mais aucune information n'est pour l'instant disponible et elle affecterait aussi les versions précédentes de Firefox.

1.3 Documentation

– La page du détail des nouveautés :
http://www.mozilla-europe.org/fr/firefox/3.0/releasenotes
– La page permettant de tester les nouvelles fonctionnalités de détection des sites malveillants :
http://www.mozilla.com/firefox/its-an-attack.html

2 Actualités Microsoft

2.1 Problèmes concernant le déploiement de mises à jour

Le 13 juin 2008, Microsoft a annoncé sur le bloc-notes du MSRC (*Microsoft Security Response Center*) un problème concernant le déploiement des mises à jour sorties le 10 juin 2008. Un avis de sécurité (KB954474) a également été publié. Le problème concerne l'impossibilité de déploiement de ces mises à jour sur des clients *System Management Server 2003* en utilisant des serveurs *System Center Configuration Manager 2007*. Une mise à jour a été publiée par Microsoft le 17 juin 2008.

2.2 Mise à jour de MS08-030

Le 19 juin 2008, *Microsoft* a annoncé la mise à jour du correctif MS08-030. Pour rappel, ce bulletin concerne une vulnérabilité dans la mise en œuvre de la pile `Bluetooth` par *Windows* permettant l'exécution de code arbitraire à distance par une personne malintentionnée. Selon *Microsoft*, le correctif publié pour les systèmes *Windows XP SP2* et *Windows XP SP3* ne corrigeait pas le problème dans son intégralité. De nouvelles mises à jour ont donc été publiées. Les systèmes *Windows XP* en 64 bits ne sont pas concernés.

2.3 Documentation

- Bloc-notes MSRC :
  http://blogs.technet.com/msrc/default.aspx
- Avis de sécurité Microsoft KB #954474 du 13 juin 2008 :
  http://www.microsoft.com/france/technet/security/advisory/954474.mspx
- Bulletin de sécurité MS08-030 du 10 juin 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-030.mspx

3 Utilisation détournée des formulaires HTTP

Les formulaires sont la méthode la plus courante dont dispose un utilisateur et son navigateur pour envoyer des informations à un serveur HTTP. Or, dans la norme définissant le protocole `HTTP`, il n'est pas obligatoire que les données renvoyées suite à l'utilisation d'un formulaire aient pour destination le même serveur qui proposait le-dit formulaire.

Mieux encore, il n'est pas obligatoire que le serveur qui reçoit les données soit un serveur `HTTP`. On peut très bien les envoyer vers un port quelconque en écoute sur un serveur quelconque.

Si ces données de réponse à un formulaire sont envoyées vers un autre serveur que celui d'origine avec des réponses judicieusement construites, il est possible de réaliser sur ce serveur cible des attaques de type injection de code indirecte (*cross-site scripting*). Il conviendra, bien entendu, que l'attaquant maîtrise le serveur d'origine et qu'il incite un utilisateur à le visiter comme dans un cas de *cross-site scripting* classique.

La bonne nouvelle est que la plupart des serveurs récents ne se laissent pas abuser et demandent à ce que la réponse de formulaire soit précédée d'une requête sur la page contenant le formulaire concerné.

Cependant, dans la mesure où un port alternatif (autre que 80/tcp) peut être utilisé, il est possible avec cette méthode d'envoyer des informations vers un serveur comme un serveur `SMTP` ou `POP` qui ne fait pas ce genre de vérification. Il conviendra, là encore, pour l'attaquant de prévoir un formulaire capable de produire une réponse compréhensible par un autre serveur dans un autre protocole.

4 Sortie de la version 2.4.1 d'OpenOffice.org en français

Une vulnérabilité critique affectant les versions 2.0 à 2.4 d'*OpenOffice.org* a récemment été rendue publique. Cette faille a fait l'objet de l'avis CERTA-2008-AVI-300 le 10 juin 2008 et a été corrigée dans la version 2.4.1. Cependant, cette version n'a pas immédiatement été publiée dans toutes les langues, en particulier en français. C'est désormais chose faite, la version française d'*OpenOffice.org* 2.4.1 est disponible en téléchargement.

Documentation :

- Avis CERTA-2008-AVI-300 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-300/

5 Wine en version 1.0

Après une quinzaine d'années de développement, *Wine* la célèbre réimplémentation de l'*API Windows* fonctionnant sous les systèmes *Unix* est sorti dans sa version 1.0. Cette application permet de faire fonctionner des applications à l'origine dédié au système d'exploitation de *Microsoft* sous un environnement *Linux*, *BSD*, *Mac OS X* ou *Solaris* pour leurs versions x86.

Cette première version stable de ce logiciel est disponible depuis le 17 juin 2008. Toutes les applications *Windows* ne fonctionnent pas encore parfaitement.

Le CERTA profite de cette annonce pour rappeler qu'il est important de maintenir à jour l'ensemble des applicatifs. Même si cette nouvelle version ne fait pas état de correctif de sécurité, elle corrige un certain nombre d'erreurs qui provoquaient des dysfonctionnements de l'application.

De plus, le fait de croiser différentes plates-formes permet de rendre inopérant certains codes malveillants et certaines attaques. Enfin l'hétérogénéité d'un système d'information permet, lors de l'apparition de codes malveillants particulièrement virulents ou de vulnérabilités critiques de limiter l'impact de ces derniers. Néanmoins, le CERTA tient à insister sur le fait que *Wine* n'est pas un émulateur (`Wine Is Not an Emulator`) ni une machine virtuelle, mais un réimplémentation de l'*API Win32*. Par conséquent, les appels systèmes sont bel et bien transmis au système lors de l'exécution d'un code.

6 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 12 et le 19 juin 2008.

7 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information du CERTA sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/
- Note d'information du CERTA sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
- Note d'information du CERTA sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
  http://www.auscert.org.au/render.html?it=1935
- Note d'information du CERTA sur les risques associés aux clés USB :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/
- Note d'information du CERTA sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA sur la gestion des noms de domaine :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information du CERTA sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

8 Rappel des avis émis

Dans la période du 13 au 19 juin 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-311 : Vulnérabilités dans TYPO3
- CERTA-2008-AVI-312 : Vulnérabilité dans les produits Citect
- CERTA-2008-AVI-313 : Vulnérabilité dans les produits Xerox Copier/Printer
- CERTA-2008-AVI-314 : Multiples vulnérabilités dans FreeType
- CERTA-2008-AVI-315 : Vulnérabilité dans Sun StarOffice et StarSuite
- CERTA-2008-AVI-316 : Vulnérabilité dans Sun Solaris
- CERTA-2008-AVI-317 : Multiples vulnérabilités dans XOrg

– CERTA-2008-AVI-318 : Vulnérabilité du noyau Sun Solaris
– CERTA-2008-AVI-319 : Vulnérabilité de Xerox Work Centre web server
– CERTA-2008-AVI-320 : Vulnérabilités dans le navigateur Opera
– CERTA-2008-AVI-321 : Vulnérabilité de Xerox Work Centre web services
– CERTA-2008-AVI-322 : Vulnérabilité dans rdesktop
– CERTA-2008-AVI-323 : Vulnérabilités dans Horde
– CERTA-2008-AVI-324 : Vulnérabilité dans Sun Solaris
– CERTA-2008-AVI-325 : Vulnérabilité dans CA ARCserve Backup

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

10 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.

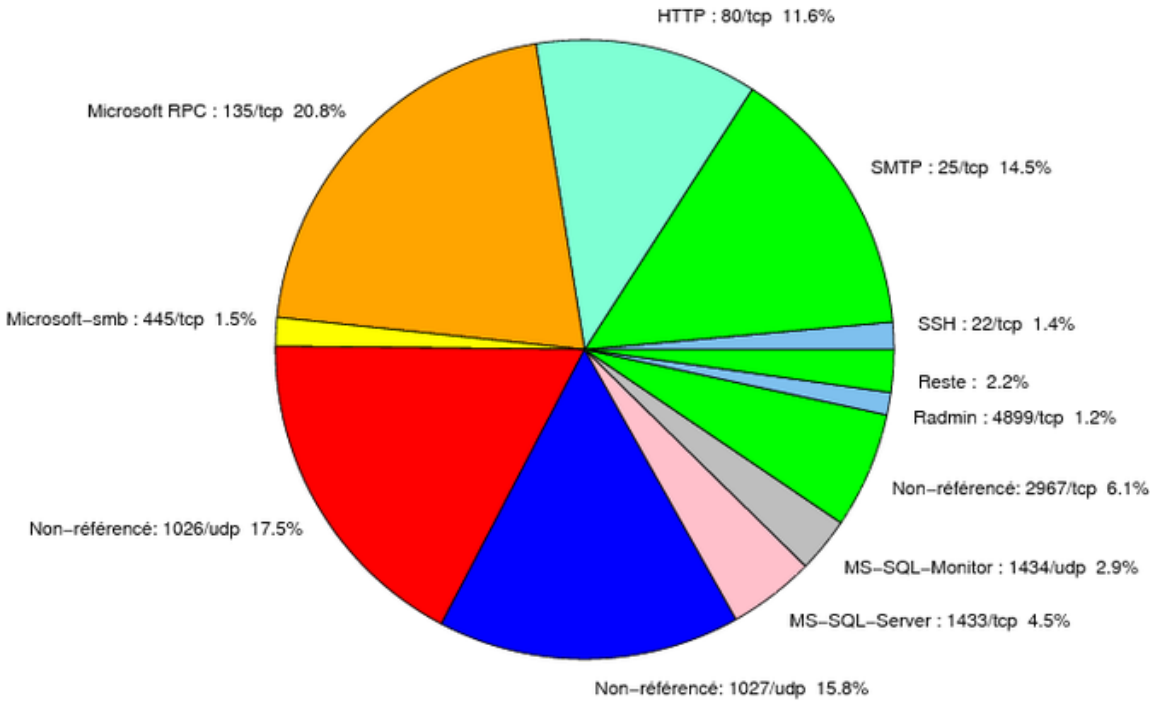

FIG. 1: Répartition relative des ports pour la semaine du 12.06.2008 au 19.06.2008

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	20.81
1026/udp	17.5
1027/udp	15.8
25/tcp	14.47
80/tcp	11.64
2967/tcp	6.06
1433/tcp	4.52
1434/udp	2.86
445/tcp	1.49
22/tcp	1.41
4899/tcp	1.17
3306/tcp	0.64
139/tcp	0.4
21/tcp	0.36
3128/tcp	0.2
2100/tcp	0.16
143/tcp	0.08
3389/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

20 juin 2008 version initiale.