Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juillet 2008
N° CERTA-2008-ACT-030

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-30

Gestion du document

Référence	CERTA-2008-ACT-030
Titre	Bulletin d'actualité 2008-30
Date de la première version	25 juillet 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-030.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-030/

1 Retour sur les incidents traités cette semaine

Les injections SQL, ça continue !

Le CERTA a encore traité cette semaine des incidents concernant des serveurs victimes d'injection d'*iFRAME* via injection *SQL*. Le scénario de l'attaque reste inchangé. Le CERTA rappelle donc les bonnes pratiques listées dans les différents articles ci-dessous.

Documentation

- Bulletin d'actualité CERTA-2008-ACT-003, « Les rumeurs d'activités malveillantes » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-003/
- Bulletin d'actualité CERTA-2008-ACT-012, « Attaques massives de type *SQL Injection* » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-012/
- Bulletin d'actualité CERTA-2008-ACT-016, « Attaques massives de type *SQL Injection* - Suite » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-016/

– Bulletin d'actualité CERTA-2008-ACT-019, « Incidents traités cette semaine : attaque par injection SQL » :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-019/
– Bulletin d'actualité CERTA-2008-ACT-027, « Injection SQL : vérification des pages ASP » :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-027/

2 Note d'information sur le DNS

Chose promise, chose due ! Comme annoncé dans le dernier bulletin d'actualité, le CERTA publie, aujourd'hui, une note d'information sur le *DNS*. Loin d'être une note exhaustive sur ce service. Ce document n'a absolument pas la prétention de présenter en quelques pages l'ensemble du système. En revanche, il a pour objectif de présenter quelques risques qui peuvent concerner l'utilisateur ou l'administrateur d'un réseau.

Il apporte donc quelques éléments de réponses à ces risques, en s'appuyant sur des incidents déjà constatés ou pouvant se réaliser de manière relativement réaliste.

Ce document se destine avant tout aux personnes curieuses de comprendre les enjeux de *DNS*, mais possédant également quelques expériences d'informatique et du monde des réseaux.

La note d'information est disponible sur le site du CERTA à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/

3 iPhone AppStore = applications sécurisées ?

Avec la sortie de nouveau *firmware* 2.0 pour *iPhone*, de nombreuses applications sont maintenant facilement installables depuis l'*AppStore* d'*Apple*. Elles sont réalisées par des développeurs indépendants et sont mises à disposition par *Apple*. Les obligations de ce dernier quant à la validation des applications qu'il offre ne sont pas explicitement définies et il semblerait que des tests de validation ne soient pas faits avant chaque mise en ligne.

Ainsi, le jeu *Aurora Faint* a été retiré des programmes disponibles. Il envoyait systématiquement à un serveur tiers des informations sur les contacts de l'utilisateur, lorsque ce dernier voulait jouer en ligne.

Le CERTA recommande la plus grande prudence quant à l'utilisation de ces appareils mobiles contenant des informations personnelles et qui cumulent de nombreuses fonctions et applications, parfois mal contrôlées. Il convient de n'installer que les applications nécessaires, après vérification du sérieux de l'éditeur et de ne pas utiliser ces appareils pour des données sensibles.

Documentation

– Forum Apple où le sujet est abordé :
http://discussions.apple.com/thread.jspa?messageID=7709472
– Forum de l'éditeur du jeu traitant du problème :
http://aurorafeint.proboards1000.com/index.cgi?board=crach&action=display&thread=346

4 Vulnérabilité dans Apple Safari

Plusieurs sites de sécurité ont récemment fait état d'une nouvelle vulnérabilité non corrigée concernant Safari 3.1.2 (CVE-2008-3174) sur Microsoft Windows. D'autres versions sont probablement concernées. La faille permet l'injection de *cookies* de certains domaines spécifiques vers d'autres.

Cette vulnérabilité est en fait connue depuis plusieurs années et a notamment affecté les navigateurs Mozilla Firefox jusqu'à la version 3 récemment publiée (CVE-2004-0867) et Konqueror (CVE-2004-0746). « Officiellement » (RFC 2965), les *cookies* peuvent être émis pour des sous-domaines (par exemple : `google.fr`) et non pour des `TLD` ou *Top Level Domains* comme par exemple `.com`. La RFC spécifie en effet qu'un *cookie* est refusé si le domaine ne contient pas de point (littéralement, il faut un point dans le domaine et non au début ou à la fin). Toutefois, certains `ccTLD` « effectifs » sont en réalité des sous-domaines, alors que leur `ccTLD` officiel est en général interdit d'utilisation. L'exemple typique est `.co.uk`. Ainsi, Safari donne la possibilité d'émettre des *cookies* qui seront lisibles par tous les sites en `.co.uk`.

La plupart des autres navigateurs ont corrigés cette vulnérabilité, au moins partiellement. On notera les différentes manières de procéder (certaines protections ont pu changer aujourd'hui) :

– pour Internet Explorer 6, les sous-domaines de deux caractères qui appartiennent à des domaines de deux caractères également, sont considérés comme des `TLD` sauf si leur domaine est dans une liste spécifiée dans

la base de registre (ce qui ne protège pas des domaines comme `ltd.uk` – CVE-2004-0866) ;
- pour Firefox 3, le `Effective TLD Service` est utilisé (utilisation d'une liste de ccTLD « effectifs ») ;
- pour Opera, les domaines en com, edu, net, org, gov, mil, et int doivent contenir deux points au minimum (`.google.fr`), alors que les autres doivent en contenir 3 (`.google.co.uk`).

Documentation

- RFC 2965 : « HTTP State Management Mechanism »
  http://www.ietf.org/rfc/rfc2965.txt
- Entrée du bogue 252342 de Mozilla Firefox :
  https://bugzilla.mozilla.org/show_bug.cgi?id=252342
- « Internet Explorer does not set a cookie for two letter domains » (KB310676)
  http://support.microsoft.com/kb/310676

5 La barre de navigation de Firefox 3

La fondation *Mozilla* a introduit dans la nouvelle mouture de son navigateur la fonctionnalité `AwesomeBar`. Cet ajout se situe dans la barre d'adresse de *Firefox* et permet la recherche automatique d'adresses correspondantes au(x) mot(s) saisi(s).

La grande différence entre les méthodes utilisées par les versions 2 et 3 pour compléter automatiquement les adresses réside dans le mode de recherche fait à partir du mot saisi.

Là où *Firefox* 2 se contente de proposer des adresses commençant par le mot saisi, la nouvelle version permet une recherche dans l'ensemble de l'*URL*. De plus, dans l'ancienne version du navigateur, la fonctionnalité exploitait l'historique de navigation. Dans la version 3, la recherche étudie aussi l'historique de navigation mais également sur les marque-pages et les titres de page. Les retours sont triés par un algorithme combinant la fréquence des visites et la date de la dernière consultation. Cette option de recherche peut néanmoins être désactivée de la façon suivante :

- dans la barre d'adresse, entrez la commande *about:config* ;
- validez la promesse de faire attention ;
- dans la barre de filtrage, saisissez la chaîne « urlbar » ;
- double-cliquez sur l'option *browser.urlbar.maxRichResults* ;
- entrez la valeur « 0 » et validez ;

Cette manipulation a pour effet de désactiver la recherche d'adresse ainsi que la complétion automatique des adresses. Le CERTA rappelle que certains codes malveillants s'appuient sur les historiques de navigations et marque-pages/favoris pour tromper l'utilisateur lors de sa navigation à des fins de filoutage par exemple.

6 OS embarqués et système d'information

On définit comme système embarqué, tout système électronique et informatique minimal dédié à une tâche précise. Ainsi, on pourra qualifier d'embarqué les systèmes d'exploitation présents dans les routeurs, les commutateurs ou les boitiers des FAI mais également dans les téléphones portables ou les imprimantes.

Ces systèmes, bien que contraints en volume et en ressources système (puissance de calcul, nombres de périphériques gérés), proposent des fonctionnalités parfois évoluées comme des piles réseau sur lesquelles s'appuient des services plus ou moins complexes : `FTP`, `HTTP`, `SNMP`, ...

Comme cela a déjà été indiqué par le CERTA, il est important de prendre en compte ces équipements pourvus d'un système d'exploitation dans la politique de gestion des mises à jours au sein du SI.

Mais, le CERTA attire l'attention sur le fait que ces systèmes particuliers peuvent être intégrés dans beaucoup de produits professionnels sans que l'administrateur ou le responsable sécurité n'en soit conscient. Ainsi, nombre de fabriquant de serveurs fournissent dans leurs machines, en plus du traditionnel `BIOS`, un système d'exploitation embarqué de gestion et de surveillance des périphériques dudit serveur. Il est ainsi possible, via une interface d'administration souvent munie d'une pile IP, d'administrer et de surveiller à distance toutes les fonctions matérielles d'un serveur allant jusqu'au contrôle de la mise sous-tension de la machine. Ceci se fait de façon totalement indépendante et, en quelque sorte, à l'insu du « vrai » système d'exploitation installé et mis en production sur la machine.

Une gestion du matériel de ce type peut même être intégrée à l'infrastructure électrique d'une salle serveur. En effet, on trouve aujourd'hui des onduleurs ou, plus remarquable, des multiprises électriques mettant en œuvre des serveurs `HTTP` ou `SNMP` offrant des fonctionnalités de mesure et d'administration.

Recommandations :

Ces systèmes d'exploitation embarqués peuvent offrir des fonctions avancées en terme de gestion de ressources et se retrouvent parfois dans des équipements où l'on ne les attend pas forcement. Il conviendra donc de prendre un certain nombre de précautions en la matière :

- lors de l'achat d'un produit, s'interroger sur la présence ou non de tels systèmes ;
- si système d'exploitation il y a, en appréhender toutes les possibilités et en acquérir une maîtrise complète ;
- anticiper et prévoir une politique de mise à jours adaptée à ce type de système bien spécifique ;
- limiter l'accès à ces environnements de gestion aux seules personnes habilitées car ceux-ci peuvent offrir un contrôle complet de certains éléments du SI.

7 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 17 et le 24 juillet 2008.

8 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/

9 Rappel des avis émis

Dans la période du 18 au 24 juillet 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-370 : Vulnérabilité dans des produits BlackBerry
- CERTA-2008-AVI-371 : Vulnérabilités de l'antivirus F-Prot
- CERTA-2008-AVI-372 : Vulnérabilité dans IBM WebSphere Application Server
- CERTA-2008-AVI-373 : Multiples vulnérabilités dans les produits Asterisk

10 Actions suggérées

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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

11 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.

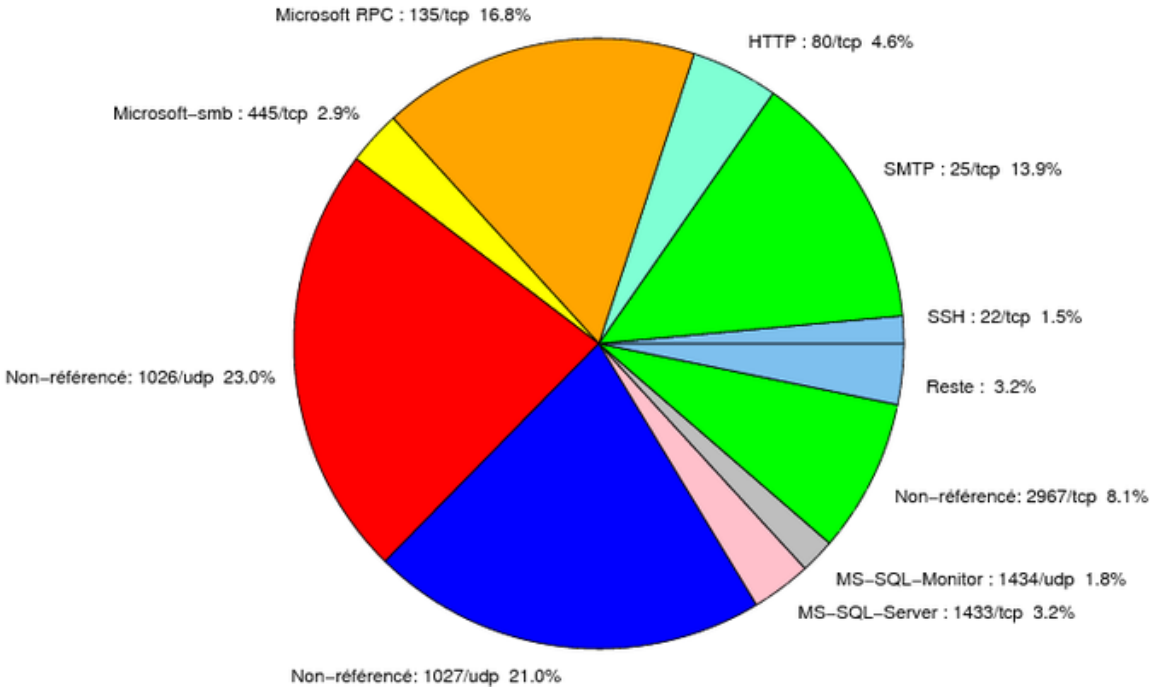

FIG. 1: Répartition relative des ports pour la semaine du 17.07.2008 au 24.07.2008

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
1026/udp	22.99
1027/udp	21
135/tcp	16.84
25/tcp	13.86
2967/tcp	8.13
80/tcp	6.56
1433/tcp	3.17
445/tcp	2.86
1434/udp	1.83
22/tcp	1.45
23/tcp	0.76
4899/tcp	0.42
3306/tcp	0.38
139/tcp	0.34
3128/tcp	0.3
21/tcp	0.15
3389/tcp	0.07
143/tcp	0.03

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

25 juillet 2008 version initiale.