Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 novembre 2007
N° CERTA-2007-ACT-046

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-46

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-2007-ACT-046`

Gestion du document

Référence	CERTA-2007-ACT-046
Titre	Bulletin d'actualité 2007-46
Date de la première version	16 novembre 2007
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-2007-ACT-046.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-2007-ACT-046/

1 Le générateur d'aléas de Microsoft Windows

Le CERTA a publié cette semaine un avis CERTA-2007-AVI-490 relatif à une vulnérabilité dans le serveur DNS de `Microsoft Windows`. La faille conserne la génération pseudo aléatoire des identifiants de transaction DNS, son exploitation pourrait ainsi permettre à une personne malintentionnée de prédire certaines valeurs.

Par ailleurs, de nombreuses discussions font état de faiblesse dans la fonction *CryptGenRandom()* de `Microsoft Windows 2000`. Des chercheurs auraient en effet réussi à prédire certains aléas déjà générés, sous reserve d'un accès à la mémoire. Il n'est pas exclu que d'autres versions de Microsoft Windows soient affectées. `Microsoft` prévoit une mise à jour pour cette vulnérabilité.

Pour l'instant rien ne permet d'affirmer que ces deux événements sont liés. Le CERTA tient à rappeler que le gestion des aléas est un élément fondamental dans la conservation du secret, notamment dans la fonctionnalité *SSL*.

Documentation

- Avis CERTA-2007-AVI-490 du 14 novembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-490/index.html

2 Que voyez-vous ? Qu'entendez-vous ?

Le CERTA présentait dans son bulletin d'actualité CERTA-2007-ACT-044 le MoBiC, ou *Month of Bugs in Captchas*.

L'auteur de l'événement a respecté son annonce initiale, et publie donc depuis le début du mois des vulnérabilités associées à cette technique de discrimination entre utilisateurs humains et robots.

2.1 Des modules largement déployés

Plusieurs personnes tendent, pour déployer rapidement de telles méthodes de tests, à utiliser des codes existants. Plusieurs modules sont ainsi disponibles sur l'Internet pour des éditeurs de contenus (CMS) comme WordPress ou Drupal. On retrouve la problématique de codes développés par des tiers, non validés et pas nécessairement maintenus.

Le fait que le code soit téléchargé un grand nombre de fois (indicateur souvent présent sur les sites de téléchargement) n'est pas un gage de la qualité du code.

L'auteur du MoBiC montre que l'un de ces modules ne présente en réalité que dix valeurs distinctes possibles aux visiteurs, suite à une erreur de programmation. Il n'est donc pas compliqué, pour une personne connaissant les caractéristiques de ce module, de faire des tests exhaustifs sur ces dix valeurs. Un outil automatique peut également s'en charger.

Un autre composant, cette fois dans PHP-Nuke, est contournable si l'outil, qui veut se faire passer pour un humain, envoie des requêtes au site en trichant sur les valeurs des variables envoyées, et en lui transmettant dans le cas présent toujours les mêmes : une valeur de contrôle et un nombre aléatoire.

Dans certains cas, il peut suffire d'envoyer des valeurs nulles pour perturber la création de l'image.

2.2 Les informations par défaut

Plusieurs méthodes déployées pour les captchas sont donc vulnérables, comme l'auteur le démontre depuis le début du mois de novembre.

Il est aussi possible d'utiliser les moteurs de recherche pour identifier rapidement des sites déployant de telle ou telle méthode pour les captchas. En effet, dans les modules existants, les phrases sont relativement standards ("Veuillez saisir le code de sécurité ci-dessus/dessous, etc.), le nom des images et des scripts également (XXX.cgi). On peut imaginer par exemple l'utilisation de Google Image Search... Les valeurs par défaut des variables sont également un indicateur, comme la chaîne `123456` dans le cas suivant :

```
<p>Veuillez saisir le code de s&eacute;curit&eacute; dans la zone de droite :</p>

<p>
   <_img src="http://URL_de_monSite/crypto.php?imgcible=ABCD" alt="" width="80" hei
   <_input type="hidden" name="cryptocheck" value="123456">
   <_input type="hidden" name="cryptoimg" value="ABCD">
   <_input type="text" name="crypto"/>
</p>
```

Une option mentionnée par l'auteur consiste à modifier toutes ces valeurs par défaut au moment du déploiement. Il faut cependant bien comprendre qu'il ne s'agit pas là d'une mesure de sécurité, mais d'une bonne pratique. Cela ne protégera pas mieux une solution qui est vulnérable, mais peut rendre son exploitation moins automatique.

2.3 Conclusions

Dans tous les cas, l'utilisation de captchas doit être bien comprise par l'administrateur du site. Ils apportent une fonctionnalité de filtrage, afin de limiter trop d'actions malveillantes par des robots. Ce ne sont **pas des méthodes d'authentification**, et encore moins des techniques qui se suffisent à elles-même. Les problématiques des modules développés par des tiers sont également présentes.

3 Rétrogradation de version chez Apple

Un article disponible sur le site d'`Apple`, prône la rétrogradation de version pour le logiciel QuickTime Player pour Windows XP. Afin de résoudre une erreur due à des fichiers manquants, Apple conseille de désinstaller la version 7.3 de QuickTime Player et d'installer la version 7.2.

Le CERTA tient à rappeler que le passage à une version antérieure d'un logiciel n'est pas sans risque. Il est possible que des vulnérabilités, corrigées dans la version la plus récente du logiciel, réapparraissent.

Dans ce cas précis, la version 7.3 du logiciel QuickTime Player permet de combler les failles suivantes :

- des exécutions de code arbitraire (CVE-2007-2395, CVE-2007-3750, CVE-2007-4672, CVE-2007-4674, CVE-2007-4675, CVE-2007-4676, CVE-2007-4677) ;
- et une élévation de privilèges (CVE-2007-3751).

L'ensemble des vulnérabilités ci-dessus ne sont pas corrigés dans la version 7.2 du logiciel QuickTime Player d'Apple. Le CERTA tient à mettre en garde les utilisateurs des dangers potentiels que représentent cette rétrogradation logicielle et leur conseille d'utiliser en attendant un lecteur alternatif.

4 Correction de la vulnérabilité URI

Cette semaine, Microsoft a publié un correctif pour la vulnérabilité des URI (*Universal Resource Identifier*) sur Windows XP ou Windows Server 2003 avec Internet Explorer 7. Elle permettait à une personne malintentionnée d'exécuter des commandes arbitraires à distance. Elle concernait un filtrage insuffisant, par les applications et Windows, sur les URIs passés en argument à la fonction *ShellExecute()*.

Rappel, cette faille a fait l'objet de deux alertes par le CERTA :

- l'alerte CERTA-2007-ALE-013 du 27 juillet 2007 portant sur l'appel par Mozilla Firefox de la fonction *ShellExecute()* ;
- l'alerte CERTA-2007-ALE-015 du 10 octobre 2007 portant sur la faille de façon plus générale.

Au moins un code d'exploitation de cette vulnérabilité s'est diffusé sur l'Internet (Cf. le bulletin d'actualité CERTA-2007-ACT-043), sous la forme de courriers électroniques ayant une pièce jointe au format pdf. Ces fichiers exploitaient l'appel à une URI effectué par l'application Adobe Reader, ce que l'éditeur a rapidement corrigé par la suite. Mozilla avait également publié des correctifs pour ses applications touchées cet été.

Cette mise à jour de Microsoft devrait corriger le problème définitivement, puisqu'elle résout le problème à sa source.

Documentation

- Avis CERTA-2007-AVI-489 du 14 novembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-489/index.html
- Bulletin d'actualité CERTA-2007-ACT-043 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-0i43.pdf
- Bulletin Microsoft MS07-061 - KB943460
  http://support.microsoft.com/kb/943460
- Alerte CERTA-2007-ALE-013 corrigée le 14 novembre 2007
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-013/index.html

5 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 08 et le 15 novembre 2007.

6 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/

7 Rappel des avis émis

Dans la période du 09 au 15 novembre 2007, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-487 : Vulnérabilité de Cisco Unified MeetingPlace
– CERTA-2007-AVI-488 : Vulnérabilité dans gforge
– CERTA-2007-AVI-489 : Vulnérabilité dans le traitement des URI sous Windows
– CERTA-2007-AVI-490 : Vulnérabilité du serveur DNS de Microsoft Windows
– CERTA-2007-AVI-491 : Vulnérabilité dans les pilotes sans-fil MadWifi
– CERTA-2007-AVI-492 : Vulnérabilités dans PHP
– CERTA-2007-AVI-493 : Vulnérabilité dans WinPcap
– CERTA-2007-AVI-494 : Multiples vulnérabilités dans phpMyAdmin
– CERTA-2007-AVI-495 : Vulnérabilité du client Novell Netware pour Windows
– CERTA-2007-AVI-496 : Vulnérabilité dans HP-UX Aries PA-RISC Emulator
– CERTA-2007-AVI-497 : Vulnérabilité dans OpenSSH
– CERTA-2007-AVI-498 : Vulnérabilité du produit Adobe ColdFusion
– CERTA-2007-AVI-499 : Multiples vulnérabilités du système Mac OS X

Durant la même période, les avis suivants ont été mis à jour :
– CERTA-2007-AVI-484-001 : Multiples vulnérabilités dans gpdf et produits dé rivés (ajouts des produits associés)

8 Actions suggérées

8.1 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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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.

8.2 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 œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

8.3 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.

8.4 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.

8.5 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 COSSI/CERTA peut vous aider dans ce travail d'analyse.

8.6 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.

8.7 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

9 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

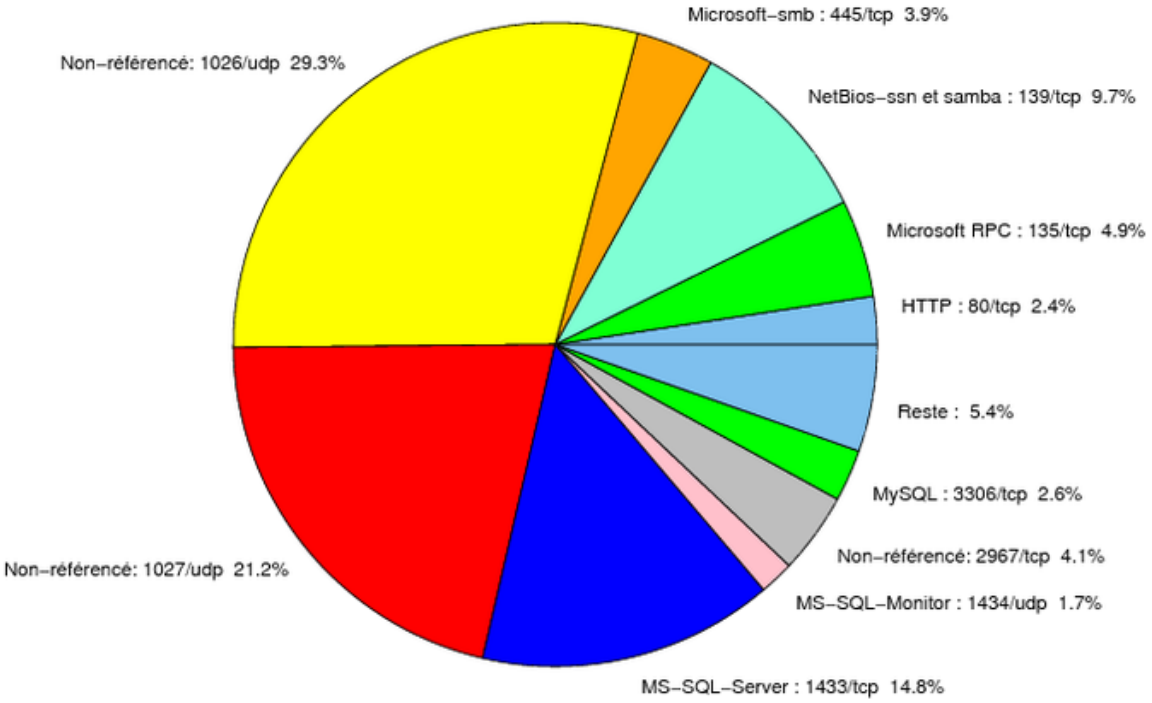

FIG. 1: Répartition relative des ports pour la semaine du 08.11.2007 au 15.11.2007

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	29.28
1027/udp	21.22
1433/tcp	14.83
139/tcp	9.67
135/tcp	4.89
2967/tcp	4.07
445/tcp	3.9
3306/tcp	2.6
80/tcp	2.4
1434/udp	1.73
1080/tcp	0.97
22/tcp	0.89
3128/tcp	0.78
4899/tcp	0.65
137/udp	0.49
25/tcp	0.46
443/tcp	0.29
3127/tcp	0.18
21/tcp	0.15
23/tcp	0.12
42/tcp	0.1
3389/tcp	0.07
143/tcp	0.06
15118/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

16 novembre 2007 version initiale.