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 décembre 2008
N° CERTA-2008-ACT-050

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-50

Gestion du document

Référence	CERTA-2008-ACT-050
Titre	Bulletin d'actualité 2008-50
Date de la première version	12 décembre 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-050.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-050/

1 Actualité Microsoft

1.1 Publication de trois alertes cette semaine

Le CERTA a publié trois alertes cette semaine :

- la première (CERTA-2008-ALE-015) concerne le convertisseur de texte de `Wordpad` et permet à un utilisateur distant d'exécuter du code arbitraire par le biais d'un fichier particulier. Il est à noter que selon `Microsoft`, cette vulnérabilité est exploitée sur l'Internet ;
- la deuxième (CERTA-2008-ALE-016) est relative au navigateur `Microsoft Internet Explorer` et permet à un utilisateur malintentionné distant d'exécuter du code arbitraire par le biais d'une page web particulière. De la même façon, il existe du code d'exploiation de cette vulnérabilité sur l'Internet.
- la troisième (CERTA-2008-ALE-017) concerne Microsoft SQL Server. Elle permet à une personne distante d'exécuter du code arbitraire dans la mesure où le site souffre d'une vulnérabilité de type « injection SQL ».

Compte tenu de la nature des produits vulnérables et des risques associés, le CERTA recommande l'application des contournements provisoires détaillés dans chaque alerte et ce sans délais.

1.2 Les correctifs du mois

1.2.1 Présentation

Cette semaine a eu lieu le *Patch Tuesday* de Microsoft. Cet ensemble de correctifs est réparti en 8 bulletins de sécurité (MS08-070 à MS08-077) qui comblent pas moins de 28 vulnérabilités. Voici un rapide retour sur les bulletins publiés :

- plusieurs vulnérabilités affectent le contrôle *ActiveX Visual Basic 6.0* et permettent l'exécution de code arbitraire à distance. Les systèmes affectés sont Microsoft Visual Studio .NET 2002 et 2003, Microsoft Visual FoxPro 8.0 et 9.0 et Microsoft Visual FoxPro 8.0 ;
- plusieurs vulnérabilités dans la bibliothèque *GDI* de Microsoft Windows permettent à une personne distante d'exécuter du code arbitraire via une erreur liée au mode de traitement des calculs d'entiers ou une erreur dans le traitement des paramètres de taille de fichier grâce à un fichier *WMF* spécialement conçu ;
- huit vulnérabilités affectent la suite Microsoft Office. Ces vulnérabilités peuvent être exploitées par l'intermédiaire d'un fichier *Word* ou *RTF* spécialement construit ;
- plusieurs vulnérabilités dans Microsoft Internet Explorer, version 5 à 7, permettent à une personne malintentionnée distante d'exécuter du code arbitraire via une page web spécialement conçue ;
- trois vulnérabilités permetent d'exécuter du code arbitraire à distance via des corruptions de pointeur, pile ou mémoire via un fichier Microsoft Excel spécialement conçu ;
- deux erreurs sont présentes dans la fonction de recherche Windows Search de Microsoft Vista et Microsoft Server 2008 peuvent être exploitées par le biais d'un fichier spécialement construit de recherche sauvegardée ou *Saved Search* ou par le biais d'une URL pointant sur ce fichier. Elles permettent à un utilisateur distant malintentionné d'exécuter du code arbitraire.
- deux vulnérabilités ont été corrigées dans les composants Windows Media. La première vulnérabilité concerne l'implémentation du *Service Principal Name* et permet la réflexion des informations d'identification *NTLM*. La seconde concerne l'implémentation du protocole *ISATAP* (*Intra-Site Automatic Tunnel Addressing Protocol*) par des composants Windows Media permettant à une personne malintentionnée de récupérer les informations d'identification *NTLM* d'un utilisateur en l'incitant à visiter une page spécialement conçue ;
- une vulnérabilité dans le contrôle d'accès aux adresses réticulaires (*URL*) Microsoft Sharepoint Server 2007 permet à un utilisateur malveillant non authentifié d'exécuter des commandes d'administration.

Au vu des nombreuses vulnérabilités permettant d'effectuer des exécutions de code arbitriaire à distance, le CERTA rappelle l'impérative nécessité d'appliquer les correctifs, le savoir nécessaire à l'exploitation de certaines de ces vulnérabilités étant déjà disponible sur l'Internet. Il est également recommandé de naviguer avec un compte utilisateur aux droits limités, de désactiver par défaut l'exécution de code dynamique (JavaScript, ActiveX), et de ne jamais ouvrir de pièce jointe ni cliquer sur un lien contenu dans un courriel dont la provenance n'est pas vérifiée.

1.2.2 Documentation

- Avis CERTA-2008-AVI-584 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-584
- Avis CERTA-2008-AVI-585 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-585
- Avis CERTA-2008-AVI-586 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-586
- Avis CERTA-2008-AVI-587 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-587
- Avis CERTA-2008-AVI-588 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-588
- Avis CERTA-2008-AVI-589 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-589
- Avis CERTA-2008-AVI-590 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-590
- Avis CERTA-2008-AVI-591 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-591

2 Inclusion PHP

2.1 Présentation

Dans son bulletin d'actualité du 19 janvier 2007, le CERTA abordait les attaques par inclusions PHP et les moyens de s'en protéger. Le premier des deux exemples de code PHP proposés suggérait de rechercher dans les journaux les mots clef *http*, *ftp* et *www*. Cette méthode peut être efficace lorsque l'attaquant souhaite utiliser un code malveillant distant mais elle est totalement inefficace lors d'inclusion locale.

Cette semaine le CERTA a participé au traitement d'un incident relatif à une compromission d'un site Internet par le biais d'une inclusion PHP de code malveillant. Les pages du site en question utilisaient une méthode de protection contre les attaques par inclusion PHP, ressemblant à celles indiquées par le bulletin d'actualité du CERTA de janvier 2007. Malgré cela, l'attaquant a réussi à déposer un fichier malveillant sur le serveur. L'attaquant a exploité une vulnérabilité consistant à modifier le *UserAgent* de sa requête et forcer la page vulnérable à interpréter le contenu de ce dernier. Pour ce faire, il a inclus un fichier local capable d'afficher un certain nombre de variables d'environnement. Cette inclusion n'était pas filtrée par le contrôle mis en place. En effet, la variable incluse ne contenait qu'un certain nombre d'occurrences de "../../".

Pour lutter efficacement contre ces attaques, il existe deux pistes de réflexion :

- sécuriser l'accès à des ressources locales au serveur capables d'afficher des informations dévoilant la configuration du serveur ;
- contrôler avec précision le contenu et l'intégrité de toutes les variables avant de les utiliser et dans la mesure du possible proscrire (ou limiter) l'utilisation de la méthode PHP `include`. Comme indiqué dans de précédents bulletins d'actualité, le CERTA recommande de limiter l'inclusion PHP aux pages connues. L'exemple de code ci-dessous indique comment réaliser ce contrôle :

```
<? $tab_pages=Array("mapage1.php","mapage2.php","mapage3.php");
    if (in_array($page,$tab_pages)) { include $page;} ?>
```

Cette exemple de code est fourni par le CERTA à titre indicatif et ne saurait remplacer un véritable audit de sécurité d'un site Internet. En plus des précautions traditionnelles à mettre en œuvre, le CERTA recommande de bloquer les connexions extérieures établies depuis le serveur. Cette mesure empêche à un attaquant de télécharger un code malveillant sur le serveur.

2.2 Documentation

- Bulletin d'actualité du CERTA du 19 janvier 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-003.pdf
- Note d'information du CERTA sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

3 L'ambiguité de la configuration Thunderbird vis-à-vis du chiffrement

3.1 Présentation

Le client de messagerie Thunderbird offre plusieurs options de configuration pour sécuriser une connexion en émission (`SMTP`) ou en réception (POP3, IMAP, etc.) :

- `Jamais`
- `TLS si disponible`
- `TLS`
- `SSL`

Dans le cas des options « `TLS si disponible` » et « `TLS` », on parlera de chiffrement explicite, c'est-à-dire que l'on utilisera toujours le protocole « en clair » mais enrichi d'extensions permettant de faire du chiffrement une fois la connexion établie.

On peut prendre en exemple le protocole `SMTP` : si le serveur présente en réponse au `EHLO` initial du client la directive `STARTTLS`, c'est qu'il sera capable de négocier une session `TLS` avec le client pour le reste de la session.

Si toutefois le serveur ne dispose pas de cette fonctionnalité, deux cas peuvent se présenter :

- si le client exige `TLS` (option `TLS` dans `Thunderbird`) alors la connexion est fermée.
- si le client fait « au mieux » (option `TLS si disponible`) alors le reste de la session se fera avec le protocole standard « en clair ».

```
$telnet mail.monDomaine.tld 25
220  "Serveur de messagerie de test"
EHLO test@monDomaine.tld
250-mail.monDomaine.tld
250-PIPELINING
250-ENHANCEDSTATUSCODES
250-STARTTLS
(...)
STARTTLS
220 2.0.0 Ready to start TLS
```

Dans cette configuration, il est possible à l'initiation de la connexion de collecter quelques informations notamment le contenu du `EHLO` ainsi que la version du serveur et les options qu'il supporte. Pour améliorer cela, `Thunderbird` met à disposition une méthode de chiffrement implicite qui utilisera cette fois-ci non-plus les protocoles standard mettant en œuvre `TLS` mais leurs versions chiffrées : POP3s, IMAPs, SMTPs, etc. On parlera alors de chiffrement implicite. C'est à dire que le client et le serveur ont connaissance du chiffrement et s'attendent à communiquer sur des ports différents de ceux des protocoles standards « en clair ».

En tout état de cause, il est important de vérifier quelle est la méthode de chiffrement la plus robuste supportée par le serveur de messagerie et de consolider la configuration du poste client en conséquence.

3.2 Documentation

- MozillaZine, "Secure Connections - Thunderbird", 29 septembre 2008 : http://kb.mozillazine.org/Secure_connections_-_Thunderbird
- S. Bortzmeyer, "Thunderbird et la cryptographie, des options pas toujours évidentes", 06 décembre 2008 : http://www.bortzmeyer.org/thunderbird-et-crypto.html
- RFC 2487, "SMTP Service Extension for Secure SMTP over TLS", janvier 1999 : http://www.ietf.org/rfc/rfc2487.txt

4 Un Referer pas si innocent

Lors de la consultation d'une page HTML, outre le chemin d'accès à la page demandé, plusieurs informations sont envoyées au serveur distant par le navigateur. Parmi celle-ci, on retrouve le *Referer*, champ de données souvent considéré comme anodin. Est-ce bien le cas ?

4.1 Qu'est-ce que le Referer ?

Le Referer est un champ défini dans les standards HTTP (RFC 1945 pour le HTTP/1.0 et RFC 2616 pour le HTTP/1.1). Ce champ contient l'adresse de la page dont la consultation a provoqué la requête. Par exemple, lorsqu'on fait une recherche via un moteur de recherche quelconque, puis que l'on clique sur un des liens fournis, la requête HTTP sera de la forme :

```
GET /index.html HTTP/1.0
[d'autres champs HTTP]
Referer: http://www.moteurderecherche.tld/recherche?recherche=
                                                    "ce\%20que\%je\%recherche"
```

4.2 Dangers

A priori, ce champ ne représente aucun réel danger en terme de sécurité informatique pour la personne qui navigue. Et pourtant le Referer peut être bien indiscret. En effet, tant qu'il contient une URL correspondant à une navigation classique, l'information transmise n'est pas très sensible. En revanche, si la visite d'une page se fait par l'intermédiaire d'un autre site, cela peut devenir plus problématique. Voici quelques exemples :

- l'URL fournie dans le Referer correspond à un site interne à une administration ou une entreprise. Dans ce cas, l'analyse du Referer permet d'obtenir des informations sensibles (existence du site, adresse IP, etc.) ;
- l'URL fournie correspond à la partie "administration" d'un site Internet. L'analyse du Referer permet alors de prendre connaissance de l'accès au "backoffice". Il en est de même pour toute partie d'un site accessible uniquement après authentification (accès aux statistiques, forum, etc.) ;

– pour certains sites, l'URL fournie peut contenir des identifiants de session qui pourraient être rejoués ;
– l'URL est celle d'un *webmail* présentant l'identifiant de l'utilisateur (souvent lié à son nom).

4.3 Que faire ?

Le filtrage du champ Referer, même si cela va à l'encontre de la RFC, peut être envisagé. Pour cela, il est possible d'agir au niveau poste ou, idéalement, d'agir au niveau d'un serveur mandataire, placé en coupure sur l'accès des postes à l'Internet.

Fort heureusement, les adresse du type *file://* ou *https://* sont déjà filtrées par les navigateurs classiques tels que `Internet Explorer` ou `Firefox`.

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 04 et le 11 décembre 2008.

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 05 au 12 décembre 2008, le CERTA a émis les trois alertes et les avis suivants :

– CERTA-2008-ALE-015 : Vulnérabilité dans le convertisseur de texte WordPad
– CERTA-2008-ALE-016 : Vulnérabilité dans Microsoft Internet Explorer
– CERTA-2008-ALE-017 : Vulnérabilité dans Microsoft SQL Server
– CERTA-2008-AVI-580 : Vulnérabilité dans Nagios
– CERTA-2008-AVI-581 : Vulnérabilité dans PowerDNS
– CERTA-2008-AVI-582 : Vulnérabilité dans Apache pour Novell Netware

– CERTA-2008-AVI-583 : Multiples vulnérabilités d'IBM WebSphere
– CERTA-2008-AVI-584 : Multiples vulnérabilités dans Visual Basic
– CERTA-2008-AVI-585 : Multiples vulnérabilités dans la bibliothèque GDI de Microsoft Windows
– CERTA-2008-AVI-586 : Multiples vulnérabilités de la suite logicielle Microsoft Office
– CERTA-2008-AVI-587 : Vulnérabilités dans Microsoft Internet Explorer
– CERTA-2008-AVI-588 : Multiples vulnérabilités dans Microsoft Excel
– CERTA-2008-AVI-589 : Multiples vulnérabilités de Windows Search
– CERTA-2008-AVI-590 : Vulnérabilités dans les composants Windows Media
– CERTA-2008-AVI-591 : Vulnérabilité de Microsoft Office Sharepoint Server
– CERTA-2008-AVI-592 : Vulnérabilité dans phpMyAdmin
– CERTA-2008-AVI-593 : Vulnérabilité dans PHP
– CERTA-2008-AVI-594 : Multiples vulnérabilités dans IBM AIX
– CERTA-2008-AVI-595 : Vulnérabilité dans HP OpenView
– CERTA-2008-AVI-596 : Multiples vulnérabilités dans Drupal
– CERTA-2008-AVI-597 : Vulnérabilité dans Sun Java System Portal Server
– CERTA-2008-AVI-598 : Vulnérabilité dans ARCserve Backup
– CERTA-2008-AVI-599 : Vulnérabilité dans Asterisk
– CERTA-2008-AVI-600 : Vulnérabilité dans OpenSSL de Sun Solaris

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'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.

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 oeuvre (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 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.ssi.gouv.fr/fr/formation/

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.

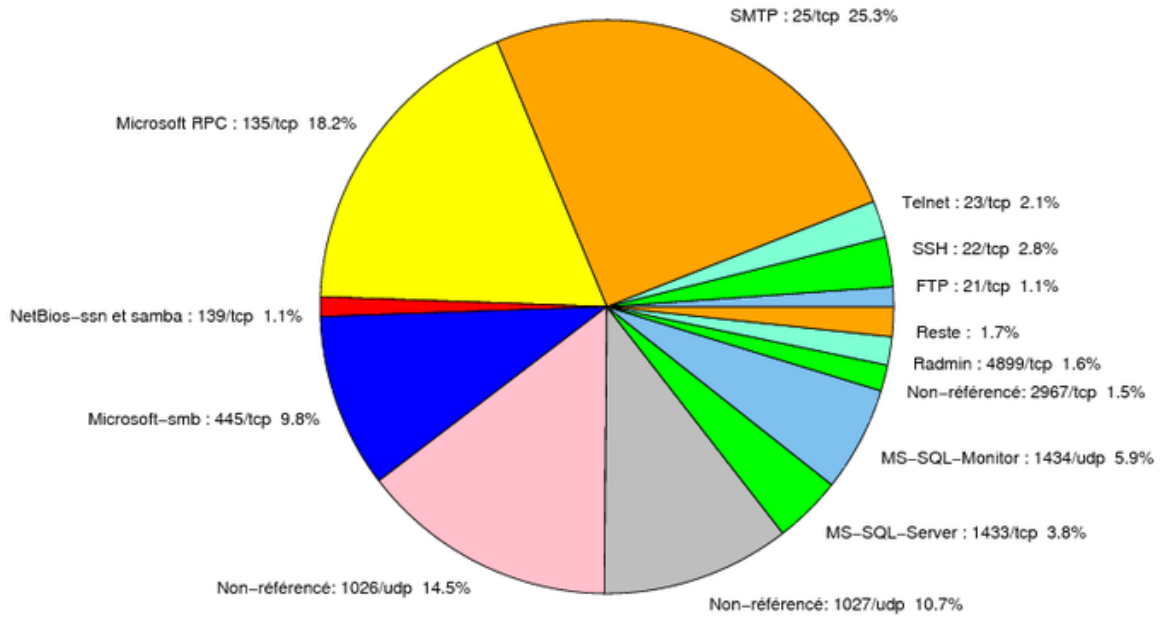

FIG. 1: Répartition relative des ports pour la semaine du 04.12.2008 au 11.12.2008

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
25/tcp	25.27
135/tcp	18.17
1026/udp	14.48
1027/udp	10.65
445/tcp	9.81
1434/udp	5.91
1433/tcp	3.83
22/tcp	2.78
23/tcp	2.22
4899/tcp	1.6
2967/tcp	1.46
139/tcp	1.11
137/udp	0.83
3128/tcp	0.27
80/tcp	0.2
3306/tcp	0.13
3389/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

12 décembre 2008 version initiale.