

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2008-45

---

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-2008-ACT-045>

---

### Gestion du document

|                             |                              |
|-----------------------------|------------------------------|
| Référence                   | CERTA-2008-ACT-045           |
| Titre                       | Bulletin d'actualité 2008-45 |
| Date de la première version | 07 novembre 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-045.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-045/>

## 1 Vulnérabilités Adobe

Le CERTA a publié cette semaine plusieurs avis de sécurité concernant des produits Adobe.

- CERTA-2008-AVI-541 : Multiples vulnérabilités dans Adobe Acrobat et Adobe Reader
- CERTA-2008-AVI-544 : Vulnérabilité dans Adobe ColdFusion
- CERTA-2008-AVI-546 : Multiples vulnérabilités dans Adobe Flash Player

Certaines des vulnérabilités citées dans ces publications concernent l'interprétation de fichiers PDF par Adobe Reader et Adobe Acrobat. D'autres concernent l'interprétation de codes Flash.

Dans les deux cas, il s'agit de formats fréquemment utilisés. De mauvaises configurations du poste de travail peuvent faciliter l'exploitation de ces dernières.

A titre d'exemple, la vulnérabilité Adobe JavaScript touchant la fonction `util.printf()` est très semblable à celles publiées en janvier 2008. Adobe a mis plusieurs mois à corriger celle-ci. Les précédentes sont encore massivement exploitées par différentes « boîtes à outil de compromission ». Plusieurs articles de bulletins d'actualité y font référence cette année. Il est donc important de vérifier, comme le CERTA l'avait signalé en janvier, la désactivation de l'interprétation Adobe JavaScript par les lecteurs Adobe Reader et Acrobat. Cette fonctionnalité n'est que très rarement utile. Elle peut être activée ponctuellement pour des fichiers de confiance y ayant recours.

Flash est une application très souvent présente sur les postes des utilisateurs. Cette application présente de multiples vulnérabilités ayant fait l'objet par Adobe des bulletins APSB08-18 et APSB08-20.

De manière générale, il est important d'appliquer les correctifs et de désactiver par défaut toute fonctionnalité qui n'est pas couramment demandée. Cette règle s'applique pour toute application, dont celles d'Adobe. Chacune de ces fonctionnalités peut être vue comme une surface d'attaque supplémentaire pour le système. Cette pratique est indispensable et il faut éviter que de telles applications puissent être activées ou lancées spontanément au cours d'une navigation Web (l'ouverture automatique d'un document PDF dans le navigateur est à proscrire par exemple).

## 2 Vulnérabilité MS08-067

Cette semaine, de nouveaux codes exploitant la vulnérabilité décrite dans le bulletin Microsoft MS08-067 et l'avis CERTA-2008-AVI-523 ont été signalés par des éditeurs d'antivirus et Microsoft. Ceux-ci font suite à l'apparition de preuves de faisabilité publiques ciblant des systèmes anglais de Windows XP et Windows 2003.

Pour le moment, l'exploitation de la vulnérabilité semble relativement limitée. Il n'est toutefois pas impossible de voir apparaître des codes plus virulents ou sophistiqués prochainement. La mise à jour reste une impérative nécessité.

### 2.1 Documentation

- Bulletin d'actualité CERTA-2008-ACT-043, « Bulletin Microsoft MS08-067 », 24 octobre 2008 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-043.pdf>
- Entrée du bloc-notes du MSRC :  
<http://blogs.technet.com/msrc/archive/2008/11/05/latest-on-ms08-067.aspx>
- Entrée du bloc-notes de F-Secure :  
<http://www.f-secure.com/weblog/archives/00001526.html>

## 3 Vulnérabilités dans certaines mises en oeuvre de WPA

### 3.1 Présentation des faits

La presse s'est fait l'écho ces derniers jours de problèmes de sécurité associés à une mesure de sécurité Wi-Fi, WPA. Des chercheurs annonceront lors d'une prochaine conférence de sécurité des vulnérabilités concernant WPA associé au protocole de gestion de clés TKIP (*Temporal Key Integrity Protocol*).

Cet article n'a pas pour but de déterminer s'il s'agit d'un effet d'annonce, ni de faire de suppositions sur une future présentation. Il tient cependant à clarifier certains termes et à rappeler quelques bonnes pratiques.

WPA, pour *Wi-Fi Protected Access*, est une solution mise en place pour combler les lacunes de sécurité de la solution optionnelle WEP initiale. WPA est une solution mettant partiellement en oeuvre les recommandations du standard de sécurité Wi-Fi IEEE 802.11i (datant de juin 2004). L'implémentation complète du standard IEEE 802.11i conduit à la certification « WPA2 ».

Le standard IEEE 802.11i présente trois algorithmes de chiffrement possibles : WEP, TKIP et CCMP. Les deux premiers sont basés sur l'algorithme RC4 tandis que CCMP s'appuie sur AES (*Advanced Encryption Standard*). RC4 est un algorithme de chiffrement à flot, à la différence d'AES qui considère des blocs, plus adaptés à des paquets. Les mises en oeuvre dites « WPA » n'utilisent pas l'option de chiffrement CCMP (AES), qui reste bien optionnel pour les équipements. Il faut donc bien comprendre le chiffrement et la méthode de gestion de clés qui sont déployés. Les termes WPA et WPA2 ne sont pas toujours explicitement distingués. Il est également indispensable de connaître les « capacités » des équipements et la réalité de la mise en oeuvre et du déploiement.

Certains points d'accès sont par exemple configurés pour ne pas avoir une politique trop rigide. Ainsi, afin de permettre à des équipements de génération antérieure de pouvoir communiquer, ils peuvent automatiquement choisir un chiffrement TKIP plutôt que CCMP/AES. Cette modification peut être faite pour le seul équipement ou l'ensemble des équipements associés, baissant ainsi le niveau de sécurité global.

Il est donc important de vérifier la configuration de son point d'accès, y compris les options avancées de sécurité. Cette bonne pratique est valable quelle que soit l'annonce qui pourra être faite dans les prochains jours.

## 3.2 Recommandations

Sans faire aucune présomption sur les annonces qui pourraient être faites au cours de la semaine prochaine, les bons principes ci-dessous restent applicables :

- vérifier les configurations des points d'accès afin de s'assurer que leur configuration est conforme à la politique de sécurité ;
- dans le cas d'un déploiement sans-fil, préférer CCMP (AES) à TKIP ;
- éviter au niveau du point d'accès d'autoriser de multiples algorithmes de chiffrement ;
- utiliser des solutions de chiffrement complémentaires (VPN, IPSec, SSH, etc.) ;
- pour TKIP, si son utilisation est inévitable, configurer une renégociation de clés très fréquente.

Les technologies sans-fil présentent des risques intrinsèques qu'il n'est pas possible de supprimer, quel que soit le mécanisme de sécurité mis en place. Il faut donc déconnecter physiquement toute interface sans-fil qui n'est pas nécessaire ou qui n'est pas utilisée.

## 3.3 Documentation associée

- Liste des produits certifiés par la Wi-Fi Alliance :  
[http://certifications.wi-fi.org/wbcs\\_certified\\_products.php?lang=en](http://certifications.wi-fi.org/wbcs_certified_products.php?lang=en)
- FAQ, Wi-Fi Alliance, "Security (Wi-Fi Protected Access)" :  
[http://wi-fi.org/knowledge\\_center\\_overview.php?type=2](http://wi-fi.org/knowledge_center_overview.php?type=2)
- Standard IEEE 802.11i :  
<http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>
- Fonctionnement de TKIP, document Intel :  
[http://cache-www.intel.com/cd/00/00/01/77/17769\\_80211\\_part2.pdf](http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf)

# 4 Campagne de filoutage visant un *registrar*

## 4.1 Présentation

Cette semaine, les clients d'un "bureau d'enregistrement" de noms de domaine (*registrar*) ont été ciblés par une attaque de type filoutage suivant un scénario classique. Un courriel les informait d'un problème ; ils devaient absolument se connecter à l'adresse indiquée pour y remédier. En l'occurrence, le prétexte était que les informations associées au nom de domaine, et accessible via une requête `whois`, étaient erronées. Le texte du lien à cliquer correspondait bien au site du *registrar* alors que la cible du lien pointait sur un domaine complètement différent. L'objectif des attaquants est inconnu mais, bien que le profit ne soit pas immédiat, on imagine l'intérêt que cela peut avoir de contrôler un maximum de noms de domaine. En effet, lorsqu'un utilisateur classe un site comme étant de confiance, seule l'URL et le nom de domaine associé sont pris en compte par le navigateur, plus rarement l'adresse IP. Si un attaquant arrive à changer l'IP correspondante à une URL au niveau du *registrar* pour faire transiter les requêtes par une machine sous son contrôle, il pourra injecter du code qui s'exécutera avec le niveau de confiance du site initial. Certains *registrars* offrent aussi la possibilité d'héberger les sites : la compromission des identifiants permet alors d'obtenir le contrôle total des sites associés au compte. Si l'attaque est, dans sa forme, des plus classiques, la cible est relativement innovante et il faut s'attendre à ce que d'autres *registrars* soient visés. Le CERTA recommande les mêmes bonnes pratiques que pour tous les cas de *phishing* déjà rencontrés, entre autres :

- ne pas lire les courriels au format `html` mais en texte brut ;
- ne pas cliquer sur les liens inclus dans un courriel ;
- être méfiant vis-à-vis des courriels car il n'y a pas de garantie par défaut sur l'émetteur.

## 4.2 Documentation

- Portail de la Sécurité Informatique :  
[http://www-securite-informatique.gouv.fr/gp\\_article44.html](http://www-securite-informatique.gouv.fr/gp_article44.html)

## 5 Contrôle d'intégrité des fichiers sous Microsoft Windows

Le CERTA recommande régulièrement d'effectuer des contrôles d'intégrité de fichiers afin de vérifier qu'ils n'ont pas été directement modifiés par certains codes malveillants. Voici quelques solutions possibles pour effectuer cette tâche lorsque ces fichiers appartiennent à un environnement Microsoft Windows.

### 5.1 L'outil *SFC* de Microsoft Windows

L'outil *SFC* (*System File Checker*), intégré au système d'exploitation de Microsoft, permet de vérifier l'intégrité des fichiers système. Il fait partie des outils de protection des fichiers système critique de Microsoft Windows. Selon la version du système d'exploitation, le contrôle d'intégrité se base sur différents critères (taille, source, emplacement, base de signature, ...) mais, dans tous les cas, l'outil permet une restauration du fichier dans sa version d'origine, généralement via le répertoire `%SystemRoot%\System32\Dllcache`. Il est également possible de réparer le contenu de ce répertoire si ce dernier est endommagé. Cet outil offre aussi la possibilité de planifier des contrôles au démarrage de la machine.

Il est nécessaire d'avoir des droits d'administration pour utiliser ce programme.

### 5.2 L'outil *FCIV* de Microsoft

Le programme *FCIV* (*File Checksum Integrity Verifier*) permet d'effectuer des contrôles d'intégrité de fichiers par rapport à une base de signatures. L'utilitaire en ligne de commandes n'est pas documenté, ni supporté par Microsoft.

*FCIV* permet des calculs de condensats via les algorithmes *MD5* et *SHA-1*. Il est, par exemple, possible d'effectuer des calculs de *hash* de manière récursive sur un répertoire jugé critique et d'enregistrer les résultats dans une base de données de fichier *XML*. Un contrôle peut ainsi être fait à partir de cette base. Il est donc important que ces données de référence soit enregistrées à partir de données saines.

Ce logiciel est compatible avec les versions 2000, XP et Server 2003 de Microsoft Windows.

### 5.3 Remarques

Le CERTA tient également à préciser que ces applications sont citées à titre d'exemple et que d'autres outils sont bien sûr disponibles. Il ne faut également pas oublier que les outils utilisant des commandes ou fonctions du système peuvent être biaisés en cas de compromission. Il est donc préférable, lorsque cela est possible, d'utiliser des outils externes au système pour contrôler l'intégrité de ce dernier (compilation statique de binaires sur des postes dédiés, cédérom de démarrage, ...).

## Documentation

- Manuel d'utilisation de *SFC* (en anglais) :  
<http://technet.microsoft.com/en-us/library/bb491008.aspx>
- Description de l'utilitaire *FCIV* :  
<http://support.microsoft.com/kb/841290>

## 6 Nouvelle version OpenBSD

Le CERTA informe ces correspondants qu'une nouvelle version du système d'exploitation OpenBSD a été mise à disposition pour téléchargement sous licence BSD. Il s'agit de OpenBSD 4.4. Parmi les fonctionnalités ajoutées, on peut trouver :

- l'apparition de nouveaux pilotes pour différents matériels ;
- le support matériel de nouveaux systèmes (UltraSPARC IV/T1/T2 et Fujitsu SPARC64-V/VI/VII par exemple) ;
- la prise en compte d'IPv6 pour le serveur Web Apache (httpd) ;
- une meilleure prise en compte des fichiers de configuration au cours d'une mise à jour du système par l'outil *sysmerge* ;
- la mise en oeuvre d'OpenSSH dans sa version 5.1 avec en particulier le support de *chroot* ;
- de nouveaux outils (*rpc.statd*, *tcpbench*, etc.) ;
- le support de WPA et WPA2-PSK pour plusieurs modèles de cartes sans-fil ;

- un meilleur suivi d'états TCP par pf, indépendamment des numéros de séquences ;
- etc.

La liste précédente est loin d'être exhaustive. Les informations concernant cette nouvelle version ainsi que les changements apportés sont visibles aux adresses suivantes :

- Site officiel OpenBSD :  
<http://www.openbsd.org/44.html>
- Page de changement ("*changelog*") de la version 4.4 pour OpenBSD :  
<http://www.openbsd.org/plus44.html>

## 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 30 octobre et le 06 novembre 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 01 au 07 novembre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-537 : Vulnérabilité dans phpMyAdmin
- CERTA-2008-AVI-538 : Vulnérabilité dans IBM Tivoli Storage Manager
- CERTA-2008-AVI-539 : Vulnérabilité du produit SonicWALL
- CERTA-2008-AVI-540 : Vulnérabilité dans Net-snmp
- CERTA-2008-AVI-541 : Multiples vulnérabilités dans Adobe Acrobat et Adobe Reader
- CERTA-2008-AVI-542 : Vulnérabilité des produits CISCO
- CERTA-2008-AVI-543 : Multiples vulnérabilités dans VLC

- CERTA-2008-AVI-544 : Vulnérabilité dans Adobe ColdFusion
- CERTA-2008-AVI-545 : Vulnérabilité dans Nagios
- CERTA-2008-AVI-030-001 : Multiples vulnérabilités dans XOrg (ajout de la référence au bulletin de sécurité HP-UX.)
- CERTA-2008-AVI-317-001 : Multiples vulnérabilités dans XOrg (ajout de la référence au bulletin de sécurité HP-UX.)

## **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 réglementaire, 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 inexplicables 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.

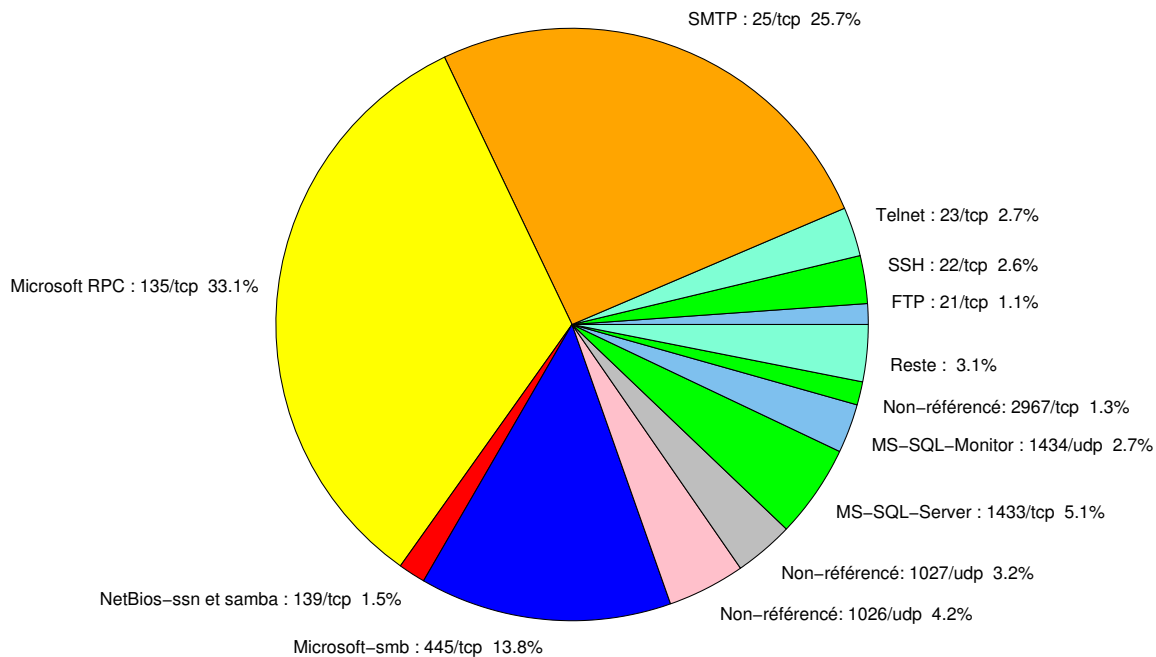


FIG. 1: Répartition relative des ports pour la semaine du 30.10.2008 au 07.11.2008

| Port | Protocole | Service                         | Porte dérobée | Référence possible CERTA   |
|------|-----------|---------------------------------|---------------|--|
| 21   | TCP       | FTP                             | –             | CERTA-2003-AVI-132<br>CERTA-2004-AVI-064<br>CERTA-2004-AVI-066<br>CERTA-2006-AVI-040   |
| 22   | TCP       | SSH                             | –             | CERTA-2003-AVI-152<br>CERTA-2006-AVI-100   |
| 23   | TCP       | Telnet                          | –             | CERTA-2003-AVI-209<br>CERTA-2003-AVI-131<br>CERTA-2007-ALE-005-001   |
| 25   | TCP       | SMTP                            | –             | CERTA-2006-AVI-124<br>CERTA-2006-AVI-135   |
| 42   | TCP       | WINS                            | –             | CERTA-2004-AVI-384   |
| 69   | UDP       | IBM Tivoli Provisioning Manager | –             | CERTA-2007-AVI-320   |
| 80   | TCP       | HTTP                            | –             | CERTA-2004-AVI-195<br>CERTA-2004-AVI-239<br>CERTA-2006-AVI-055<br>CERTA-2006-AVI-069<br>CERTA-2006-AVI-156<br>CERTA-2006-AVI-315   |
| 106  | TCP       | MailSite Email Server           | –             | –<br>CERTA-2007-AVI-008  |
| 111  | TCP       | Sunrpc-portmapper               | –             | CERTA-2003-AVI-052   |
| 119  | TCP       | NNTP                            | –             | CERTA-2004-AVI-340   |
| 135  | TCP       | Microsoft RPC                   | –             | CERTA-2003-ALE-002<br>CERTA-2003-AVI-111<br>CERTA-2004-AVI-127   |
| 137  | UDP       | NetBios-ns                      | –             | CERTA-2004-AVI-031   |
| 139  | TCP       | NetBios-ssn et samba            | –             | CERTA-2004-AVI-368<br>CERTA-2003-AVI-168<br>CERTA-2004-AVI-126<br>CERTA-2005-AVI-051<br>CERTA-2005-AVI-213<br>CERTA-2005-AVI-302<br>CERTA-2005-AVI-398<br>CERTA-2006-AVI-283<br>CERTA-2006-AVI-338<br>CERTA-2007-AVI-321 |
| 143  | TCP       | IMAP                            | –             | CERTA-2005-AVI-185   |
| 389  | TCP       | LDAP                            | –             | CERTA-2003-AVI-102<br>CERTA-2003-AVI-068<br>CERTA-2003-AVI-041<br>CERTA-2003-AVI-004<br>CERTA-2004-AVI-126<br>CERTA-2007-AVI-294   |
| 427  | TCP       | Novell Client                   | –             | CERTA-2006-AVI-538   |
| 443  | TCP       | HTTPS                           | –             | CERTA-2003-AVI-156<br>CERTA-2004-AVI-126<br>CERTA-2004-AVI-247<br>CERTA-2004-AVI-343<br>CERTA-2007-AVI-153   |
| 445  | TCP       | Microsoft-smb                   | –             | CERTA-2004-AVI-053<br>CERTA-2003-AVI-105<br>CERTA-2004-AVI-126<br>CERTA-2005-AVI-051<br>CERTA-2005-AVI-302<br>CERTA-2006-AVI-283   |

|       |     |                                       |                         |  |
|-------|-----|---------------------------------------|-------------------------|--|
|       |     |                                       |                         | CERTA-2006-AVI-338<br>CERTA-2007-AVI-321<br>CERTA-2007-ALE-010                       |
| 445   | UDP | Microsoft-smb                         | –                       | CERTA-2007-ALE-010   |
| 1023  | TCP | –                                     | Serveur ftp de Sasser.E | –  |
| 1080  | TCP | Wingate                               | MyDoom.F                | CERTA-2006-AVI-232   |
| 1433  | TCP | MS-SQL-Server                         | –                       | CERTA-2002-ALE-006   |
| 1434  | UDP | MS-SQL-Monitor                        | –                       | CERTA-2002-AVI-157   |
| 2100  | TCP | Oracle XDB FTP                        | –                       | CERTA-2005-ALE-002   |
| 2381  | TCP | HP System Management                  | –                       | CERTA-2006-AVI-248   |
| 2512  | TCP | Citrix MetaFrame                      | –                       | CERTA-2006-AVI-491   |
| 2513  | TCP | Citrix MetaFrame                      | –                       | CERTA-2006-AVI-491   |
| 2745  | TCP | –                                     | Bagle                   | –  |
| 2967  | TCP | Symantec Antivirus                    | Yellow Worm             | CERTA-2006-AVI-221   |
| 3104  | TCP | CA Message Queuing                    | –                       | CERTA-2007-AVI-331   |
| 3127  | TCP | –                                     | MyDoom                  | –  |
| 3128  | TCP | Squid                                 | MyDoom                  | CERTA-2004-AVI-062<br>CERTA-2004-AVI-186<br>CERTA-2004-AVI-316<br>CERTA-2004-AVI-348 |
| 3268  | TCP | Microsoft Active Directory            | –                       | CERTA-2007-AVI-294   |
| 3306  | TCP | MySQL                                 | –                       | –  |
| 4899  | TCP | Radmin                                | –                       | –  |
| 5000  | TCP | Universal Plug and Play               | Bobax, Kibuv            | CERTA-2001-AVI-165<br>CERTA-2006-AVI-212<br>CERTA-2006-AVI-297                       |
| 5151  | UDP | IPSwitch WS_TP                        | –                       | CERTA-2007-AVI-312   |
| 5151  | TCP | ESRI ArcSDE                           | –                       | CERTA-2007-AVI-367   |
| 5554  | TCP | SGI ESP HTTP                          | Serveur ftp de Sasser   | –  |
| 5900  | TCP | VNC                                   | –                       | CERTA-2006-AVI-198<br>CERTA-2006-AVI-299   |
| 6014  | TCP | IBM Tivoli Monitoring                 | –                       | CERTA-2007-AVI-183   |
| 6070  | TCP | BrightStor ARCserve/Enterprise Backup | –                       | CERTA-2005-AVI-293   |
| 6101  | TCP | Veritas Backup Exec                   | –                       | CERTA-2005-AVI-024   |
| 6106  | TCP | Symantec Backup Exec                  | –                       | CERTA-2007-AVI-303   |
| 6129  | TCP | Dameware Miniremote                   | –                       | CERTA-2003-AVI-214<br>CERTA-2005-AVI-326   |
| 6502  | TCP | CA BrightStor ARCserve Backup         | –                       | CERTA-2007-AVI-029   |
| 6503  | TCP | CA BrightStor ARCserve Backup         | –                       | CERTA-2007-AVI-029   |
| 6504  | TCP | CA BrightStor ARCserve Backup         | –                       | CERTA-2007-AVI-029   |
| 8080  | TCP | IBM Tivoli Provisioning Manager       | –                       | CERTA-2007-AVI-153   |
| 8866  | TCP | –                                     | Porte dérobée Bagle.B   | –  |
| 9898  | TCP | –                                     | Porte dérobée Dabber    | –  |
| 10000 | TCP | Webmin, Veritas Backup Exec           | –                       | CERTA-2005-AVI-229<br>CERTA-2005-AVI-313   |
| 10080 | TCP | Amanda                                | MyDoom                  | –  |
| 10110 | TCP | IBM Tivoli Monitoring                 | –                       | CERTA-2007-AVI-183   |
| 10916 | TCP | Ingres                                | –                       | CERTA-2007-AVI-275-001   |
| 10925 | TCP | Ingres                                | –                       | CERTA-2007-AVI-275-001   |
| 12168 | TCP | CA eTrust antivirus                   | –                       | CERTA-2007-AVI-217   |
| 13701 | TCP | Veritas NetBackup                     | –                       | CERTA-2005-AVI-447   |
| 18264 | TCP | CheckPoint interface                  | –                       | CERTA-2005-AVI-310   |
| 54345 | TCP | HP Mercury                            | –                       | CERTA-2007-AVI-075   |
| 65535 | UDP | LANDesk Management Suite              | –                       | CERTA-2007-AVI-176   |

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

| port     | pourcentage |
|----------|-------------|
| 135/tcp  | 33.07       |
| 25/tcp   | 25.66       |
| 445/tcp  | 13.75       |
| 1433/tcp | 5.07        |
| 1026/udp | 4.23        |
| 1027/udp | 3.24        |
| 23/tcp   | 2.82        |
| 1434/udp | 2.67        |
| 22/tcp   | 2.6         |
| 139/tcp  | 1.48        |
| 2967/tcp | 1.26        |
| 21/tcp   | 1.12        |
| 80/tcp   | 0.84        |
| 4899/tcp | 0.77        |
| 137/udp  | 0.49        |
| 3128/tcp | 0.28        |
| 111/tcp  | 0.21        |
| 9898/tcp | 0.07        |

TAB. 3: Paquets rejetés

## Liste des tableaux

|   |  |    |
|---|--|----|
| 1 | Gestion du document . . . . .  | 1  |
| 2 | Correctifs correspondant aux ports destination des paquets rejetés . . . . . | 9  |
| 3 | Paquets rejetés . . . . .  | 10 |

## Gestion détaillée du document

07 novembre 2008 version initiale.