



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 mars 2008  
N° CERTA-2008-ACT-011

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2008-11**

---

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-011>

---

### Gestion du document

Référence	CERTA-2008-ACT-011
Titre	Bulletin d'actualité 2008-11
Date de la première version	14 mars 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-011.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-011/>

## 1 L'actualité Microsoft de la semaine

### 1.1 Rappel

Cette semaine a eu lieu la publication des mises à jour mensuelles de Microsoft. Quatre bulletins de sécurité ont été émis et mentionnés dans les avis CERTA-2008-AVI-124, CERTA-2008-AVI-125, CERTA-2008-AVI-126 et CERTA-2008-AVI-127 :

- le bulletin MS08-014 concerne des vulnérabilités dans Microsoft Excel, dont l'une a fait l'objet de l'alerte CERTA-2008-ALE-003 le 16 janvier 2008. Le CERTA attire l'attention de ses lecteurs sur le fait que du code d'exploitation circule actuellement sur Internet, sous la forme de courriers électroniques contenant une pièce jointe au format xls.
- le bulletin MS08-015 fait état d'une vulnérabilité dans Microsoft Outlook. Cette vulnérabilité est liée au traitement des URI *mailto*. Toutes les applications pouvant invoquer ce protocole sont susceptibles d'être un vecteur d'exploitation de cette vulnérabilité. Une exploitation fructueuse permet à un individu malveillant d'exécuter du code arbitraire à distance.

- le bulletin MS08-016 informe de la découverte de deux vulnérabilités dans les produits de la suite Microsoft Office. Ces vulnérabilités permettent d'exécuter du code arbitraire à distance par une personne malintentionnée via un fichier spécialement conçu.
- le bulletin MS08-017 concerne une vulnérabilité Microsoft Office Web Component permettant via une page web spécialement conçue d'exécuter du code arbitraire à distance.

Le CERTA rappelle donc l'importance de mettre à jour, dans la mesure du possible, son système d'information afin de limiter les risques de compromission.

Par ailleurs, Microsoft peut diffuser des détails sur les vulnérabilités affectant ses produits qui n'apparaissent pas dans le bulletin officiel. A valeur d'exemple, le bloc-notes en ligne de l'équipe *Security Vulnerability Research and Defense* donne de plus amples informations sur certains des bulletins parus cette semaine. Ainsi, concernant les publications du mois de mars 2008, ce site détaille plus particulièrement la vulnérabilité affectant Microsoft Outlook et donne des méthodes afin de désactiver la fonctionnalité *mailto* ou bien informe sur la manière de changer le client de messagerie associé à cette dernière grâce aux clés de registre.

## 1.2 Documentation associée

- Avis CERTA-2008-AVI-124 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-124>
- Avis CERTA-2008-AVI-125 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-125>
- Avis CERTA-2008-AVI-126 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-126>
- Avis CERTA-2008-AVI-127 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-127>
- Le bloc-notes de l'équipe *Security Vulnerability Research and Defense* de Microsoft :  
<http://blogs.technet.com/swi/default.aspx>

## 2 Changement de politique de publication des correctifs Cisco

La société Cisco annonce que la publication des correctifs de sécurité concernant *Cisco Internetwork Operating System* (IOS) suivra désormais un calendrier très strict, à l'instar de ce que fait déjà *Microsoft*.

À partir du 26 mars 2008, Cisco publiera des collections de correctifs pour IOS le quatrième mercredi (aux États-Unis, donc sans doute le jeudi en France) des mois de mars et de septembre.

Cisco dérogera éventuellement à cette règle pour émettre des bulletins de sécurité concernant des vulnérabilités critiques déjà annoncées par des tiers ou exploitées activement.

Cisco espère ainsi satisfaire aux demandes de certains clients qui souhaitent pouvoir se préparer à des mises à jour majeures.

Les administrateurs doivent donc s'attendre à un gros déploiement de correctifs Cisco pour le 26 ou 27 mars 2008.

### Documentation :

- Annonce de changement de politique de publication des correctifs par Cisco :  
[http://www.cisco.com/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html)

## 3 Arrêt du support de GNU/Debian 3.1

### 3.1 Description

Comme annoncé précédemment par le projet Debian, le support de l'ancienne version stable de leur système d'exploitation GNU/Debian 3.1 s'arrêtera fin mars. Ceci signifie en particulier que cette version de distribution GNU/Linux ne sera plus mise à jour et ne fera plus l'objet de correctifs de sécurité.

## 3.2 Recommandations

Les outils de gestion de *packages* : `apt` ou `aptitude` permettent un changement de version assez aisé. Il est donc fortement recommandé, dans la mesure du possible, de migrer vers la nouvelle version stable de Gnu/Debian, à savoir la version 4.0 aussi nommée « *etch* ».

<http://www.debian.org/News/2008/20080229>

# 4 Se protéger contre les attaques Firewire

## 4.1 Introduction

Dernièrement, les attaques via Firewire ont fait beaucoup de bruit à cause de la publication d'outils permettant de contourner l'authentification de Windows. Le principe est toutefois connu depuis plusieurs années, et un outil de preuve de concept avait déjà été publié il y a plusieurs mois. La principale fonctionnalité permettant cela est l'accès direct à la mémoire (DMA) par certains périphériques Firewire. Le problème n'est pas nouveau ni catastrophique - les accès physiques aux postes de travail ont toujours été un point faible au niveau de la sécurité.

Les moyens de se protéger sont différents selon le système d'exploitation. Cet article a pour but de présenter quelques méthodes pour différents systèmes d'exploitation.

## 4.2 Désactiver le Firewire sous Microsoft Windows

Sous Microsoft Windows, le principal moyen de se protéger de ce type d'attaque est de désactiver le périphérique permettant de gérer le Firewire. Celui-ci se trouve dans la catégorie « Contrôleurs hôte de bus IEEE 1394 » du gestionnaire de périphériques. En faisant un click droit il faut alors choisir l'option « Désactiver. »

Un autre moyen de se protéger est d'empêcher le chargement du driver `ohci1394.sys` au démarrage de Windows. La valeur *Start* de la clé de registre

```
HKLM\System\CurrentControlSet\Services\ohci1394\
```

permet de choisir cela : par défaut à 3 (démarrage manuel), la valeur 4 permet de ne plus charger ce pilote.

Pour les administrateurs souhaitant désactiver le Firewire sur un parc important de machines, il est possible de créer un modèle d'administration facilitant cette tâche. Voici un exemple de ce que l'on peut y mettre :

```
CLASS MACHINE
CATEGORY !!categorie
CATEGORY !!nomcategorie
POLICY !!nompolitique
    KEYNAME "SYSTEM\CurrentControlSet\Services\ohci1394"
    EXPLAIN !!explication
    PART !!label DROPDOWNLIST REQUIRED
        VALUENAME "Start"
        ITEMLIST
            NAME !!Desactiv  VALUE NUMERIC 3 DEFAULT
            NAME !!Activ  VALUE NUMERIC 4
        END ITEMLIST
    END PART
END POLICY
END CATEGORY
END CATEGORY
```

```
[strings]
categorie="Politiques personnalis es"
nomcategorie="Firewire"
nompolitique="D sactiver le Firewire"
explication="Ceci d sactive le Firewire en ne chargeant pas le pilote
ohci1394.sys au d marrage."

label="D sactiver le Firewire"
Active="Activ "
Desactive="D sactiv "
```

Ce fichier est à nommer en `.adm` et peut être importé dans la catégorie « Configuration ordinateur » - « Modèles d'administration » dans les stratégies de groupe. On peut ensuite visionner et choisir de désactiver le Firewall dans « Modèles d'administration classiques. » Il faut également configurer l'affichage en décochant « Afficher uniquement les paramètres de stratégie pouvant être entièrement gérés » dans l'option filtrage.

### 4.3 sous Linux

La désactivation du Firewall sous GNU/Linux peut passer par différents moyens :

- le déchargement du module de support du Firewall :

```
modprobe -r ohci1394
```

- interdire le chargement de ce module au démarrage du système, en rajoutant la ligne suivante dans le fichier `/etc/modprobe.d/blacklist` :

```
blacklist ohci1394
```

- dans le cas où le module `ohci1394` doit être chargé, il est possible de le faire avec une option permettant de désactiver l'accès direct à la mémoire :

```
modprobe ohci1394 phys_dma=0
```

Il est à noter, qu'il existe, sur l'Internet, des tutoriels permettant de « patcher » les sources du module "ohci1394.c" de façon à désactiver le DMA par défaut.

### 4.4 Conclusion

Pour conclure, un aspect souvent négligé par les administrateurs est simplement de protéger les accès physiques aux machines. Cela couvre un panel plus large d'attaques, dont celle présentée dans cet article. De plus, il est souvent possible de désactiver le Firewall dans le BIOS des machines.

## 5 Le choix du réglage des filtres antispam

### 5.1 Présentation

Les filtres contre les pourriels (*antispam*) peuvent utiliser des algorithmes pour noter les courriers électroniques, comme le fait SpamAssassin. Ces systèmes de notation permettent de qualifier de *spam* un courrier ayant certaines caractéristiques connues ou apprises. Si dans la majorité des cas les réglages par défaut permettent de supprimer bon nombre de ces *spam*, il ne faut pas oublier qu'il existe obligatoirement un nombre, parfois non-négligeable, de faux-positifs c'est à dire de courriers marqués comme étant indésirables bien qu'ils soient légitimes. Toute la difficulté du réglage de ces dispositifs réside donc dans la gestion des faux-positifs et le choix des seuils.

Etant donné le risque de perte de messages légitimes, le CERTA recommande de ne pas supprimer systématiquement les courriers marqués comme *spam*. En revanche, un double traitement peut être appliqué en fonction de la notation du courrier. En effet, on observe qu'au-delà d'un certain seuil (par exemple "X-Spam-Level=10" pour SpamAssassin) on observe beaucoup moins de faux-positifs, il peut donc être intéressant de marquer et délivrer les mails ayant une note inférieure à ce seuil pour permettre aux utilisateurs de trouver des courriers légitimes marqués comme *spam*. Quelle que soit la gestion des courriers indésirables adoptée, il est important d'en informer les utilisateurs et de les sensibiliser aux dangers inhérents aux *spam*. Les utilisateurs doivent également avoir la possibilité de remonter à l'administrateur de la messagerie les éventuels problèmes créés par la gestion des *spam* sur le système d'information. Les outils s'appuyant sur des paramètres empiriques doivent faire l'objet d'un contrôle et d'un suivi permanent. Ils doivent être testés avant leur mise en production.

### 5.2 Documentation

- Site officiel de SpamAssassin :  
<http://spamassassin.apache.org>

## 6 Les organisations de sites malveillants

Le CERTA avait présenté dans son bulletin d'actualité CERTA-2007-ACT-049 des architectures possibles de gestion de machines zombies. Celles-ci sont complexes, afin de rendre les activités malveillantes plus opaques et robustes aux analyses et actions réactives.

Le bulletin mentionnait donc l'importance, dans le cas d'un traitement d'incident, de fournir le maximum d'informations disponibles. Si l'information retournée concerne une adresse IP ou le nom d'une machine distante, il faut envisager :

- l'adresse IP ;
- le nom de machine associée ;
- le serveur DNS ayant permis la résolution ;
- la date précise à laquelle cette résolution s'est effectuée.

Ces architectures se trouvent dans de nombreux incidents de sécurité informatique relatés dans la presse, et inquiètent plusieurs organisations mondiales. L'ICANN (*Internet Corporation for Assigned Names and Numbers*), qui est l'organisme international en charge de la gestion globale du DNS, a publié à ce sujet un avis de sécurité. Elle y fournit plusieurs mesures, ainsi que leurs limitations. Parmi celles-ci :

- surveiller et contrôler avec attention le trafic DNS, comme cela est rappelé dans le bulletin CERTA-2008-ACT-008 ;
- détecter les durées de vie des réponses DNS, ou (TTL) qui pourraient être anormalement courtes ou longues. Par exemple, le standard RFC 1912 préconise des valeurs minimales de l'ordre d'une journée, afin de bénéficier des propriétés de cache. Cependant, cette règle n'est pas nécessairement respectée, comme l'explique une récente présentation faite à la conférence NDSS'08. Les auteurs proposent eux de s'appuyer également sur les paramètres suivants pour identifier les utilisations malveillantes du DNS :
  - la cohérence des résolutions DNS inverses, lorsque celles-ci sont possibles ;
  - le nombre d'entrées de type "A" uniques dans la résolution DNS ;
  - le nombre d'entrées "NS" ou serveurs de noms retournés dans la résolution DNS ;
  - le nombre de blocs ASN uniques pour toutes les entrées de type "A" obtenues.

Il est important pour un administrateur de réseau de signaler tout comportement anormal d'une machine distante constaté sur les serveurs qu'il administre. Cela peut se faire auprès de son RSSI. Celui-ci peut prévenir le CERTA et/ou le gestionnaire du nom de domaine de la machine distante et/ou le fournisseur d'accès associé.

## 6.1 Documentation associée

- Bulletin d'actualité CERTA-2007-ACT-049 du 07 décembre 2007, « Les organisations des sites malveillants » :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-049.pdf>
- Bulletin d'actualité CERTA-2008-ACT-008 du 22 février 2008, « Surveiller le trafic DNS, une nécessité » :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-008.pdf>
- ICANN, "SSAC 025 Advisory on Fast Flux Hosting and DNS", janvier 2008 :  
<http://www.icann.org/committees/security/ssac-documents.htm>
- T. Holz, C. Gorecki, K. Rieck, F.C. Freiling, "Measuring and Detecting Fast-Flux Service Networks", soumis à la conférence NDSS'08, San Diego, mars 2008 :  
<https://pi1.informatik.uni-mannheim.de/filepool/research/publications/fast-flux-ndss08.pdf>
- "Know Your Enemy: Fast-Flux Service Networks", juillet 2007 :  
<http://honeynet.org/papers/ff/>
- RFC 1912, "Common DNS Operational and Configuration Errors", février 1996 :  
<http://tools.ietf.org/rfc/rfc1912.txt>

## 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 06 et le 13 mars 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 07 au 14 mars 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-117 : Vulnérabilités dans Dokeos
- CERTA-2008-AVI-118 : Vulnérabilités de Java
- CERTA-2008-AVI-119 : Vulnérabilité dans AIX
- CERTA-2008-AVI-120 : Vulnérabilité dans Check Point VPN-1 UTM Edge
- CERTA-2008-AVI-121 : Vulnérabilité dans Horde
- CERTA-2008-AVI-122 : Vulnérabilité dans Sun Java Web Console
- CERTA-2008-AVI-123 : Multiples vulnérabilités dans la bibliothèque Sun Solaris ICU
- CERTA-2008-AVI-124 : Vulnérabilité dans Microsoft Outlook
- CERTA-2008-AVI-125 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2008-AVI-126 : Vulnérabilités dans Microsoft Office
- CERTA-2008-AVI-127 : Multiples vulnérabilités dans Microsoft Office Web Component
- CERTA-2008-AVI-128 : Vulnérabilité dans le module ipsecah de Sun Solaris
- CERTA-2008-AVI-129 : Vulnérabilité dans MailEnable
- CERTA-2008-AVI-130 : Vulnérabilité dans Sun Java Server Faces
- CERTA-2008-AVI-131 : Vulnérabilité dans IBM WebSphere MQ pour HP NonStop
- CERTA-2008-AVI-132 : Multiples vulnérabilités dans IBM WebSphere Application Server
- CERTA-2008-AVI-133 : Multiples vulnérabilités dans Cisco User-Changeable Password
- CERTA-2008-AVI-134 : Vulnérabilités dans Adobe ColdFusion
- CERTA-2008-AVI-135 : Multiples vulnérabilités dans IBM AIX

Pendant la même période, l'avis suivant a été mis à jour :

- CERTA-2007-AVI-502-002 : Vulnérabilités dans Samba  
(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 COSSI/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.

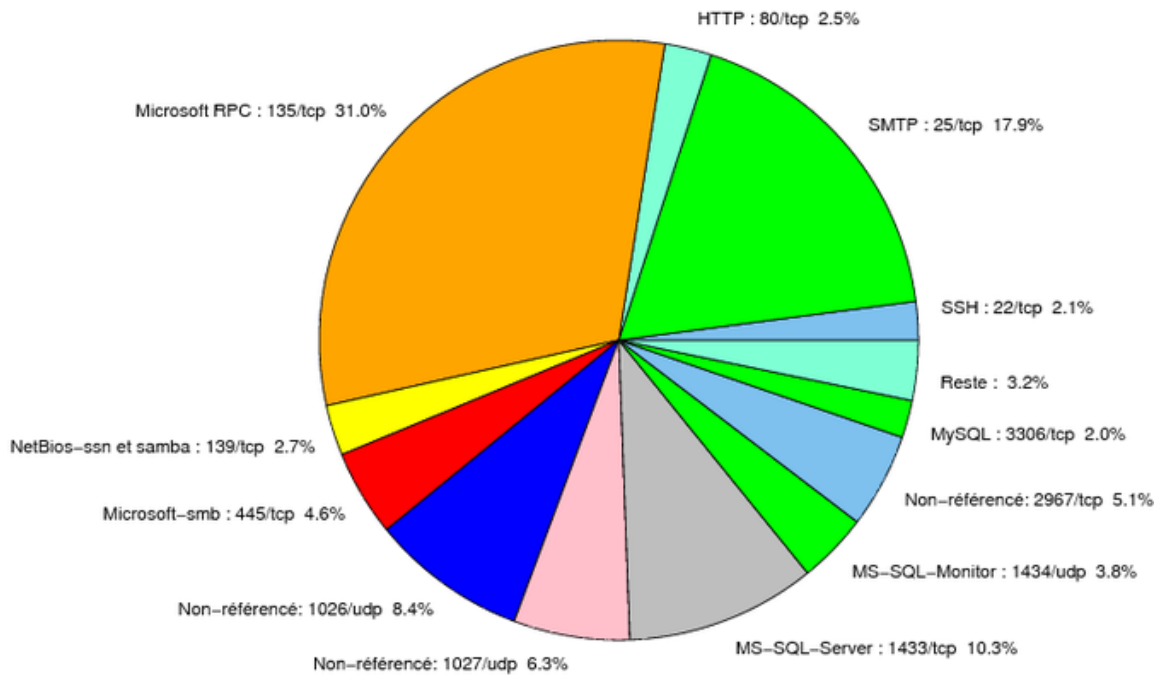


FIG. 1: Répartition relative des ports pour la semaine du 06.03.2008 au 13.03.2008



Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
22	TCP	SSH	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
23	TCP	Telnet	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> CERTA-2007-ALE-005-001
25	TCP	SMTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
42	TCP	WINS	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
69	UDP	IBM Tivoli Provisioning Manager	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
80	TCP	HTTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
106	TCP	MailSite Email Server	-	- <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
111	TCP	Sunrpc-portmapper	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
119	TCP	NNTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
135	TCP	Microsoft RPC	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
137	UDP	NetBios-ns	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
139	TCP	NetBios-ssn et samba	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
143	TCP	IMAP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
389	TCP	LDAP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
427	TCP	Novell Client	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
443	TCP	HTTPS	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
445	TCP	Microsoft-smb	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>

				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 re-  
jetés

port	pourcentage
135/tcp	31.02
25/tcp	17.93
1433/tcp	10.25
1026/udp	8.43
1027/udp	6.26
2967/tcp	5.35
445/tcp	4.64
1434/udp	3.78
139/tcp	2.72
80/tcp	2.57
22/tcp	2.07
3306/tcp	2.02
137/udp	0.96
4899/tcp	0.85
23/tcp	0.75
143/tcp	0.3
1080/tcp	0.25
42/tcp	0.05

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	10
3	Paquets rejetés . . . . .	11

## Gestion détaillée du document

14 mars 2008 version initiale.