

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2006-50

---

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-2006-ACT-050>

---

### Gestion du document

Référence	CERTA-2006-ACT-050
Titre	Bulletin d'actualité 2006-50
Date de la première version	15 décembre 2006
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-2006-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-2006-ACT-050/>

## 1 Activité en cours

### 1.1 Filoutage

Cette semaine le CERTA a été informé d'un cas de filoutage (*phishing*) impliquant le serveur Web d'une collectivité territoriale. Ce serveur se trouvait physiquement chez un hébergeur privé. Suite à l'appel du CERTA indiquant la conduite à tenir en cas d'incident, les victimes ont contacté leur hébergeur. Celui-ci a immédiatement modifié la configuration de son serveur, négligeant les recommandations et faisant potentiellement disparaître des informations importantes pour une analyse.

Le CERTA rappelle qu'une bonne analyse dépend de la pertinence (et de l'existence) des informations. Quand un site Web est la victime d'une défiguration, il est préférable de tout mettre en oeuvre pour conserver des traces, et de communiquer ce besoin à l'hébergeur. La document CERTA-2004-ALE-001 intitulé « Obstacles à la résolution d'incidents » aborde ce problème. Des conseils sont dispensés par le CERTA dans la note d'information CERTA-2002-INF-002.

## 2 Avis Microsoft du mois de décembre 2006

Cette semaine sept bulletins de sécurité Microsoft ont été publiés. Ces bulletins apportent des corrections sur les produits et services suivants :

- Microsoft Windows Media ;
- Microsoft Remote Installation Service (RIS) ;
- Microsoft Outlook Express ;
- Microsoft Windows ;
- Microsoft SNMP Service ;
- Microsoft Internet Explorer ;
- Microsoft Visual Studio.

A la date de rédaction de ce bulletin d'actualité, les vulnérabilités de Microsoft Office PowerPoint et Microsoft Word ne sont pas corrigées. Microsoft a mis à disposition par erreur pendant quelques heures un correctif pour la version Mac de Word. Cette mise à jour (version 11.3.1 pour Office 2004), qui n'aurait pas été validée, a rapidement été supprimée et Microsoft demande à ceux qui ont pu l'installer de le désinstaller rapidement.

Une mise à jour d'un correctif pour Microsoft Office Excel était également disponible ce 12 décembre. Il s'agit de la référence KB924164, associée à la précédente mise à jour MS06-059 d'Excel. La version précédente du correctif ne semblait pas avoir correctement mis à jour le binaire `excel.exe`.

## 3 Concernant les réponses automatiques aux courriers électroniques

La grande majorité des clients de messagerie offre la possibilité de créer des messages de type réponses automatiques.

L'utilisation de réponses automatiques peut être sollicitée dans le cas d'absences prolongées, de congés, de départ en retraite, de mutation, etc.

Ces messages, courts, informent l'émetteur d'un courriel que le destinataire ne peut pas répondre. Les messages sont généralement standards, quelle que soit le courrier reçu.

Ces informations, bien que limitées aux réponses de courriers, peuvent très vite s'assimiler à de l'information publique. Pour s'en convaincre, il suffit d'imaginer que les courriers non sollicités (ou spam) reçoivent en retour les mêmes messages de réponses.

Il convient donc de s'interroger sur quelques points avant l'utilisation, ou l'écriture de tels messages :

- les numéros de téléphone et autres coordonnées concernant des points de contact de remplacement sont-ils publics ? Les personnes citées dans ces courriers sont-elles au courant ?
- est-il bon de diffuser comme contre-partie son adresse personnelle pour recevoir ces courriers pendant les congés ? Est-il conforme à la Politique de Sécurité PSSI de transférer des courriers professionnels vers des adresses personnelles ?
- est-il bon d'être trop bavard sur sa situation actuelle (congé maternité, retraite, formation de tel type, etc) ? Cela fournit autant d'informations permettant ensuite aux personnes d'envoyer des courriers illégitimes ou dangereux bien mieux ciblés, et trompant toujours d'avantage la vigilance de l'utilisateur.

En conclusion, les réponses automatiques sont un problème délicat, dans la mesure où l'information qu'elles véhiculent est rendue publique. Certaines précautions doivent par voie de conséquence être considérées.

## 4 Concernant les vulnérabilités de cartes Wi-Fi

Le CERTA a émis la semaine dernière l'avis CERTA-2006-AVI-539 concernant les pilotes de cartes Wi-Fi Madwifi. Ceux-ci sont utilisés par diverses distributions Linux, pour les cartes possédant une puce de type Atheros. Des vulnérabilités impliquant d'autres pilotes avaient également été abordées dans le bulletin d'actualité CERTA-2006-ACT-046. Le CERTA rappelle à cet égard que les mises à jour concernant les pilotes ne sont pas toujours simples et évidentes, mais elles sont souvent suffisamment critiques pour justifier des tests et des vérifications.

Dans le cas présent, la vulnérabilité peut être exploitée par un paquet malveillant, afin de prendre le contrôle complet de la machine, qui n'aurait pas installé la version 0.9.2.1 du pilote. Les solutions de sécurité appliquées au monde Wi-Fi (WEP, WPA, 802.11i, IPsec, 802.1X, etc) aussi criticables soient-elles, ne peuvent de toutes les façons pas protéger contre une attaque de plus bas niveau (pilote).

Il faut garder à l'esprit que tout appareil (PDA, ordinateur portable), possédant un des pilotes vulnérable, présente un risque pour le réseau, si la carte est activée. Il est donc important de rappeler, à tout utilisateur de carte

Wi-Fi, que celle-ci doit rester désactivée si elle n'est pas utilisée. L'administrateur peut vérifier, au moyen d'outils simples, les cartes activées, en récupérant les adresses sources des trames circulant dans les locaux de son réseau.

De manière plus générale, il ne faut pas utiliser de technologies sans-fil qui offriraient une porte d'entrée béante à des réseaux filaires lourdement sécurisés (pare-feux, VPN, etc), sous peine de remettre en cause les considérations de contrôles d'accès au sein du réseau.

## 5 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 07 et le 14 décembre 2006.

## 6 Liens utiles

- Mémento sur les virus :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information sur l'acquisition de correctifs :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html>
- Note d'information sur les systèmes obsolètes :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html>
- Note d'information sur les mots de passe :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>
- Note d'information sur la terminologie d'usage au CERTA :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html>
- 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 CERTA-2006-INF-006, Risques associés aux clés USB :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-008/>

## 7 Rappel des avis émis

Durant la période du 07 au 14 décembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-539 : Vulnérabilité dans Madwifi
- CERTA-2006-AVI-540 : Vulnérabilité dans Computer Associates BrightStor ARCserve Backup
- CERTA-2006-AVI-541 : Vulnérabilités de Sophos Anti-Virus
- CERTA-2006-AVI-542 : Vulnérabilité dans Clam AntiVirus
- CERTA-2006-AVI-543 : Vulnérabilités dans Cahier de Texte
- CERTA-2006-AVI-544 : Vulnérabilité dans Microsoft Visual Studio 2005
- CERTA-2006-AVI-545 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2006-AVI-546 : Vulnérabilité dans le service SNMP de Microsoft Windows
- CERTA-2006-AVI-547 : Vulnérabilité dans Microsoft Windows
- CERTA-2006-AVI-548 : Vulnérabilité dans Microsoft Outlook Express
- CERTA-2006-AVI-549 : Vulnérabilité dans Remote Installation Service de Microsoft
- CERTA-2006-AVI-550 : Vulnérabilités dans le lecteur Windows Media
- CERTA-2006-AVI-551 : Vulnérabilité dans HP ILO
- CERTA-2006-AVI-552 : Vulnérabilité dans le client Novell
- CERTA-2006-AVI-553 : Vulnérabilité de ClamAV
- CERTA-2006-AVI-554 : Vulnérabilité de l'antivirus Sophos

## **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 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.

### **8.2 Concevoir une architecture robuste**

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

### **8.3 Appliquer les correctifs de sécurité**

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

### **8.4 Utiliser un pare-feu**

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

### **8.5 Analyser le réseau**

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

### **8.6 Réagir aux incidents de sécurité**

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements 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.

## 8.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

<http://www.formation.ssi.gouv.fr>

## 9 Les bulletins d'actualité

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

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

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

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

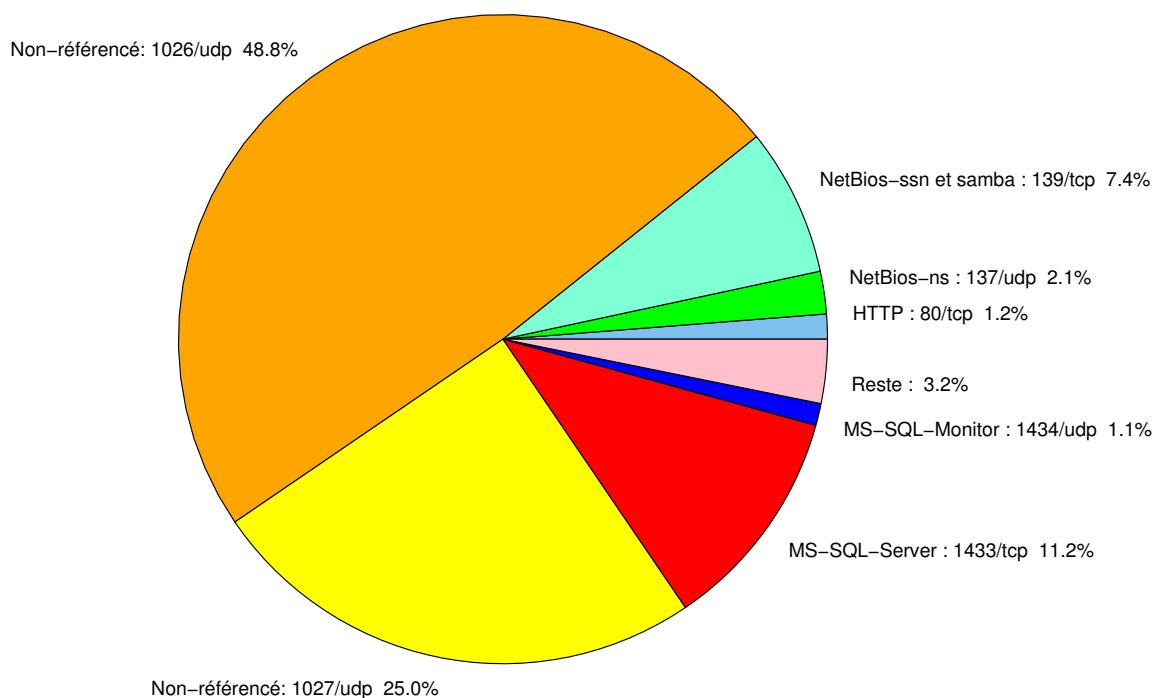


FIG. 1: Répartition relative des ports pour la semaine du 07.12.2006 au 15.12.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338
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
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
1026/udp	48.79
1027/udp	24.97
1433/tcp	11.21
139/tcp	7.36
137/udp	2.12
80/tcp	1.24
1434/udp	1.09
1080/tcp	0.83
4899/tcp	0.59
22/tcp	0.46
3306/tcp	0.24
25/tcp	0.23
3128/tcp	0.2
443/tcp	0.14
21/tcp	0.1
2100/tcp	0.08
143/tcp	0.07
42/tcp	0.04
3389/tcp	0.03
6129/tcp	0.01

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	7
3	Paquets rejetés . . . . .	8

## Gestion détaillée du document

15 décembre 2006 version initiale.