

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2009-35

---

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-2009-ACT-035>

---

### Gestion du document

Référence	CERTA-2009-ACT-035
Titre	Bulletin d'actualité 2009-35
Date de la première version	28 août 2009
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-2009-ACT-035.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-2009-ACT-035/>

## 1 Incidents de la semaine

Cette semaine, le CERTA a traité un cas de *phishing*. Le site victime de l'intrusion avait été, quelques jours auparavant, attaqué suite à l'exploitation d'une faille du composant optionnel `com_profiler` de *Joomla!*. Le résultat de cette première attaque était une modification de page. La vulnérabilité exploitée était connue et corrigée en 2006, et ni le composant, ni le gestionnaire de contenu n'étaient à jour.

Si le scénario de défiguration, suivie quelques jours plus tard de l'installation d'un site de *phishing*, est relativement habituel, il convient de préciser que ce schéma a été rendu possible avant tout parce que le RSSI était en vacances. En effet, le tout premier incident n'a pas été correctement traité, faute de personne idoine disponible.

Le CERTA recommande donc aux RSSI de prévoir et former des personnels en vue d'assurer une continuité de service pour les périodes de congés ou de longue absence, prévue ou imprévue. Ce ou ces suppléants, et leur rôle, doivent être connus au sein de l'organisme (annuaire SSI).

## 2 Cisco Lightweight Access Point : insécurité à la mise en service

### 2.1 Vulnérabilité publiée

Dans une architecture de réseau *Cisco* comprenant une portion en WiFi, des équipements de type *Lightweight Access Point* (LAP) peuvent être installés. Ils sont alors reliés à un équipement *Wireless LAN Controller* (WLC) offrant des fonctions d'administration du réseau. Lors de sa mise en route, un LAP qui n'a pas été configuré va utiliser le protocole OTAP pour s'associer à un WLC.

En l'absence de protection native, cette association peut être détournée par un attaquant pour empêcher le LAP de s'associer avec le WLC légitime. Cette fenêtre d'opportunité est étroite pour un attaquant, mais elle existe.

Le fabricant a émis un bulletin de sécurité pour rappeler cette vulnérabilité non corrigée qui concerne les équipements *Cisco Lightweight Wireless Access Point* des séries 1100 and 1200.

### 2.2 Contournements et recommandations

L'opportunité d'attaque peut être supprimée si l'administrateur du réseau configure le LAP avant sa mise en route sur le réseau :

- en utilisant une liste de contrôleurs (WLC) ;
- en utilisant un mécanisme à clef publique d'authentification des équipements (LSC).

En complément, l'administrateur peut se tourner vers la détection de WLC non légitimes. Il lui est également recommandé de surveiller les journaux des équipements du réseau et des serveurs.

### 2.3 Documentation

- Bulletin de sécurité Cisco 18919 du 25 août 2009 :  
<http://tools.cisco.com/security/center/viewAlert.x?alertId=18919>
- Référence CVE CVE-2009-2861 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2861>
- Document Cisco d'utilisation du mécanisme LSC :  
[http://www.cisco.com/en/US/products/ps6366/products\\_configuration\\_example09186a0080a99e23.shtml](http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a0080a99e23.shtml)
- Document Cisco de détection des WLC non légitimes :  
[http://www.cisco.com/en/US/tech/tk722/tk809/technologies\\_white\\_paper09186a0080722d8c.shtml](http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a0080722d8c.shtml)

## 3 Le virus est dans le compilateur

Il y a quelques jours, des éditeurs de solutions antivirus ont découvert un nouveau code malveillant à la technique de propagation originale, baptisé par certains *Win32/Induc*. Ce virus a la particularité de compromettre les compilateurs du langage de programmation *Delphi*. Une fois installé, le code malveillant se propage en s'intégrant à tous les programmes compilés à l'aide du logiciel compromis. Dans les versions actuelles aucune charge utile n'est intégrée, le code se contente de se propager.

Afin de savoir si le compilateur est compromis, il suffit de contrôler si le fichier *sysConst.pas* est présent dans le répertoire *lib* situé à la racine du répertoire d'installation du compilateur. Si le compilateur est compromis, tous les programmes créés par le compilateur sont potentiellement infectés par ce code malveillant.

Le CERTA recommande aux développeurs de supprimer complètement le compilateur, de le réinstaller et de recompiler toutes les applications. Il est important de ne pas exécuter les applications compromises afin de ne pas infecter de nouveau le compilateur. Il est impératif ensuite de rediffuser les applications saines afin de ne pas entretenir la propagation du code malveillant.

## 4 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/>

## 5 Rappel des avis émis

Dans la période du 21 au 27 août 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-344 : Vulnérabilités de Cisco IOS XR
- CERTA-2009-AVI-345 : Vulnérabilité dans Cisco Firewall Services Module
- CERTA-2009-AVI-346 : Vulnérabilité dans le client IBM AFS pour Linux
- CERTA-2009-AVI-347 : Vulnérabilités dans la bibliothèque neon
- CERTA-2009-AVI-348 : Vulnérabilité dans les produits VMware
- CERTA-2009-AVI-349 : Vulnérabilité dans Radix Antirookit
- CERTA-2009-AVI-350 : Vulnérabilité du client de messagerie Mozilla Thunderbird
- CERTA-2009-AVI-351 : Vulnérabilité dans les produits Symantec
- CERTA-2009-AVI-352 : Vulnérabilité dans Xerox WorkCentre
- CERTA-2009-AVI-353 : Vulnérabilité dans Lotus Notes
- CERTA-2009-AVI-354 : Vulnérabilité dans Sun Solaris Print Service
- CERTA-2009-AVI-355 : Multiples vulnérabilités du navigateur Google Chrome
- CERTA-2009-AVI-356 : Multiples vulnérabilités dans Symantec Altiris Deployment Solution
- CERTA-2009-AVI-357 : Vulnérabilités de Cisco Unified Communications Manager
- CERTA-2009-AVI-358 : Vulnérabilité dans Sun Solaris

Pendant la même période, les avis suivants ont été mis à jour :

- CERTA-2009-AVI-336-001 : Vulnérabilité dans GnuTLS (ajout de la référence au bulletin de sécurité Ubuntu)
- CERTA-2009-AVI-337-003 : Vulnérabilité du noyau Linux (ajout de la référence au bulletin de sécurité Suse)
- CERTA-2009-AVI-338-002 : Vulnérabilité de cURL et libcurl (ajout des références aux bulletins Mandriva et Debian)

## **6 Actions suggérées**

### **6.1 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.

### **6.2 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.

### **6.3 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.

### **6.4 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.

### **6.5 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.

### **6.6 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.

## 6.7 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, l'ANSSI dispose d'un centre de formation :

[http://www.ssi.gouv.fr/site\\_rubrique63.html](http://www.ssi.gouv.fr/site_rubrique63.html)

## 7 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.

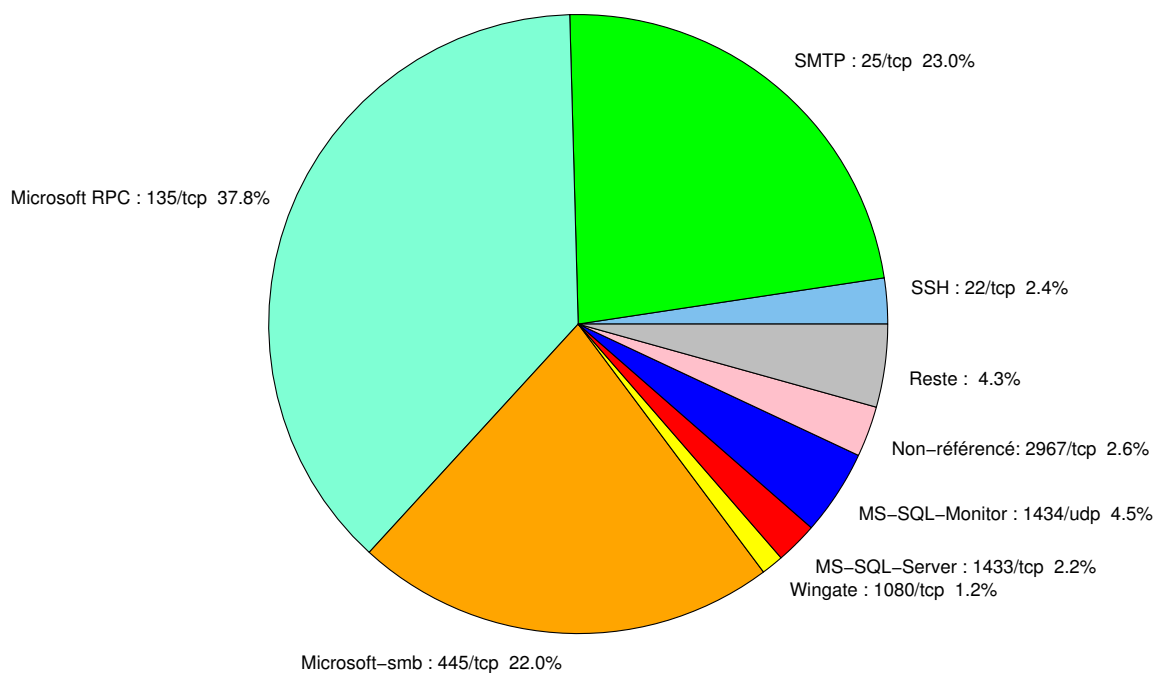


FIG. 1: Répartition relative des ports pour la semaine du 20 au 27 août 2009

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 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 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 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	–	– 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 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 CERTA-2007-AVI-321
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 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
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 CERTA-2007-AVI-321 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 CERTA-2004-AVI-186 CERTA-2004-AVI-316 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 CERTA-2006-AVI-212 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 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 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 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	37.76
25/tcp	23.04
445/tcp	22.01
1434/udp	4.45
2967/tcp	2.64
22/tcp	2.38
1433/tcp	2.19
80/tcp	1.67
1080/tcp	1.16
3128/tcp	0.9
4899/tcp	0.64
21/tcp	0.38
3389/tcp	0.25

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

28 août 2009 version initiale.