

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2009-51

---

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-051>

---

### Gestion du document

Référence	CERTA-2009-ACT-051
Titre	Bulletin d'actualité 2009-51
Date de la première version	18 décembre 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-051.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-051/>

## 1 Vulnérabilité dans Adobe Reader et Adobe Acrobat

L'éditeur Adobe a publié le 15 décembre 2009 un bulletin de sécurité portant sur l'existence d'une vulnérabilité dans les produits *Adobe Reader* et *Adobe Acrobat*. Cette vulnérabilité a fait l'objet d'un bulletin d'alerte du CERTA (cf. CERTA-2009-ALE-023) dans lequel le risque associé à son exploitation est l'exécution de code arbitraire. En effet, cette vulnérabilité peut être exploitée lors de l'ouverture d'un fichier au format PDF spécialement construit. Le savoir-faire destiné à exploiter cette vulnérabilité est d'ores et déjà disponible sur l'Internet. De plus, des codes exploitant cette vulnérabilité ont également été découverts.

L'éditeur *Adobe* a annoncé qu'un correctif de sécurité serait normalement publié le 12 janvier 2010. En l'attente de celui-ci, il est recommandé d'appliquer les contournements provisoires afin de limiter les risques d'exploitation de cette vulnérabilité. L'utilisation de logiciels alternatifs reste un contournement provisoire de même que la désactivation de l'interprétation du `Javascript`. Ce dernier point reste globalement une bonne pratique. L'activation du DEP (*Data Execution Prevention*) sous *Windows* peut également s'appliquer.

## 2 Vulnérabilités dans Cisco WebEx WRF Player

Cette semaine, le CERTA a publié un avis (CERTA-2009-AVI-550) à propos de multiples vulnérabilités affectant *Cisco WebEx WRF Player*. Cette application est utilisée pour lire les fichiers au format WRF. Une particularité de ce lecteur réside dans son installation :

- soit un utilisateur va télécharger « manuellement » ce programme sur le site <http://www.webex.com> ;
- soit le lecteur est installé automatiquement lors de la première connexion à un serveur WebEx pour lire un fichier WRF.

En cas d'installation manuelle, la mise à jour du logiciel doit également être effectuée manuellement. Par contre, si l'installation du programme a été faite automatiquement, alors la mise à jour du lecteur est effectuée automatiquement lors d'une connexion sur un serveur WebEx, à condition que ce serveur possède une version du client à jour.

Le principe de téléchargement automatique du lecteur est très pratique pour l'utilisateur. Le mécanisme de mise à jour qui en découle semble efficace. Pour autant, ce système présente les risques suivants :

- si un utilisateur va consulter un fichier au format WRF malveillant hébergé sur un serveur qui ne contient pas la version du lecteur à jour, alors une des vulnérabilités pourra être exploitée ;
- si un utilisateur va se connecter à un serveur WebEx maîtrisé par des personnes malintentionnées, alors il téléchargera automatiquement une version vulnérable du lecteur avant de consulter le fichier malveillant.

Il est difficile d'émettre des recommandations pour se protéger de ces vulnérabilités. L'installation manuelle du lecteur semble préférable dans la mesure où le mécanisme de mise à jour est davantage maîtrisé. Néanmoins, le problème reste entier pour ceux qui n'ont jamais installé ce logiciel. Le plus sûr peut être de télécharger le lecteur sur le site officiel si l'on a l'intention d'aller consulter un fichier au format WRF.

## 3 Compte utilisateur sous Windows et mises à jour

Il est généralement admis qu'une bonne pratique de sécurité est d'utiliser un compte avec des droits limités pour naviguer sur l'Internet ou encore faire de la bureautique. Ainsi, l'impact d'un incident de sécurité sera moindre, certains codes malveillants héritant des privilèges de l'utilisateur. Néanmoins, cette pratique pose un problème lorsqu'il faut appliquer des mises à jour. En effet, l'installation des correctifs de sécurité de certains logiciels tiers nécessite généralement de basculer sur un compte administrateur.

La recherche des mises à jour est une opération qui tend à s'automatiser, mais cette automatisation n'est pas toujours adaptée aux comptes ayant des droits limités. Si certains logiciels font apparaître un message pour signaler clairement l'existence d'une nouvelle version, ce n'est pas le cas pour toutes les applications. Par exemple, *Mozilla Firefox*, sous certaines versions de *Windows*, n'informe pas les utilisateurs de la possibilité d'installer une mise à jour (l'option de recherche de mises à jour est même « grisée » lorsque l'on utilise le navigateur avec un compte utilisateur). D'autres programmes posent des problèmes encore plus subtils. Par exemple, la mise à jour manuelle d'*Adobe Flash Player* provoque le téléchargement d'un greffon (*plug-in*) pour le navigateur. C'est ce greffon qui est chargé ensuite de récupérer les mises à jour. Lorsque l'opération est effectuée depuis un compte utilisateur, en apparence, les mises à jour sont recherchées mais dans les faits, rien ne se passe.

L'utilisation des comptes utilisateur rend ardue la tâche d'installation des correctifs de sécurité pour les applications. Il est nécessaire de régulièrement basculer sur le compte administrateur et de penser à tout mettre à jour, ce qui requiert une bonne connaissance de son propre système.

## 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=1937>
- 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 11 au 17 décembre 2009 , le CERTA a émis les avis suivants :

- CERTA-2009-AVI-542 : Vulnérabilité des produits Symantec Veritas VRTSweb
- CERTA-2009-AVI-543 : Vulnérabilité dans Ruby
- CERTA-2009-AVI-544 : Multiples vulnérabilités dans HP OpenView Network Node Manager
- CERTA-2009-AVI-545 : Multiples vulnérabilités dans Moodle
- CERTA-2009-AVI-546 : Vulnérabilités dans PostgreSQL
- CERTA-2009-AVI-547 : Multiples vulnérabilités dans Mozilla Firefox
- CERTA-2009-AVI-548 : Vulnérabilité dans VMware vCenter Lab Manager
- CERTA-2009-AVI-549 : Multiples vulnérabilités dans Drupal
- CERTA-2009-AVI-550 : Multiples vulnérabilités dans Cisco WebEx WRF Player
- CERTA-2009-AVI-551 : Multiples vulnérabilités dans IBM WebSphere
- CERTA-2009-AVI-552 : Vulnérabilité dans des produits Horde

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

- CERTA-2009-AVI-149-001 : Vulnérabilité dans mod\_perl pour Apache (ajout des bulletins de sécurité Sun Solaris et Mandriva )
- CERTA-2009-AVI-508-001 : Multiples vulnérabilités dans GIMP (ajout du bulletin de sécurité Sun Solaris)

## 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.

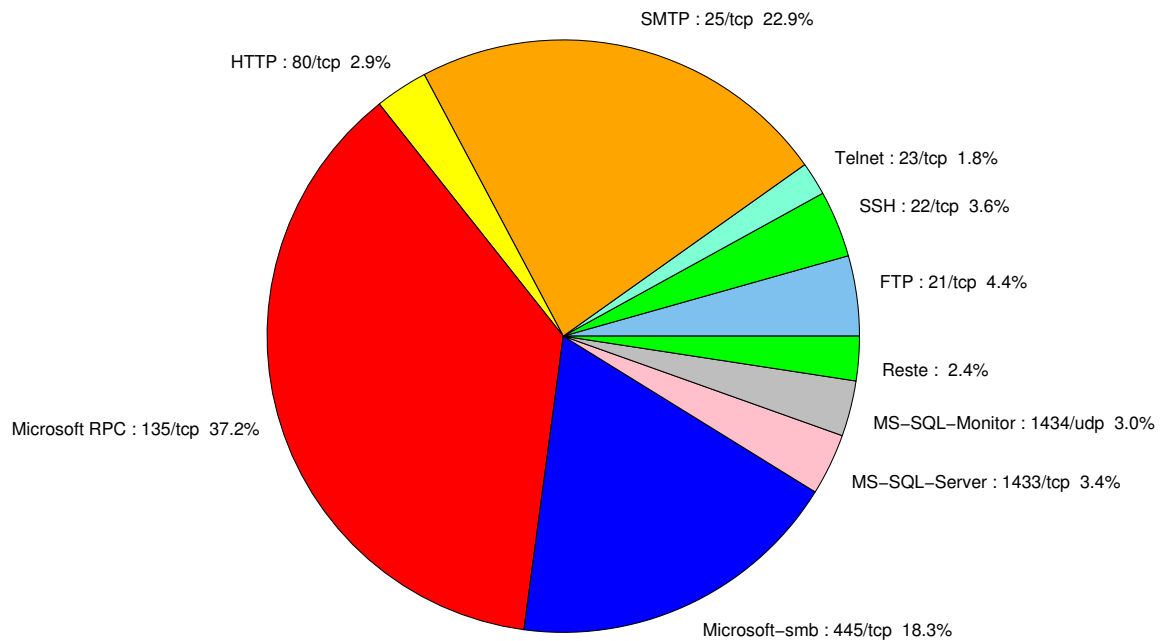


FIG. 1: Répartition relative des ports pour la semaine du 11 au 17 décembre 2009

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	37.21
25/tcp	22.94
445/tcp	18.3
21/tcp	4.37
80/tcp	3.76
22/tcp	3.63
1433/tcp	3.36
1434/udp	3.02
23/tcp	1.88
1080/tcp	0.74
2967/tcp	0.67
3128/tcp	0.53
4899/tcp	0.2
3389/tcp	0.06

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

18 décembre 2009 version initiale.