

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-34

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-034>

Gestion du document

Référence	CERTA-2009-ACT-034
Titre	Bulletin d'actualité 2009-34
Date de la première version	21 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-034.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-034/>

1 Incidents de la semaine

Cette semaine, le CERTA a traité un cas de compromission d'un serveur Web fonctionnant avec *SPIP*. L'objectif apparent de l'intrusion était d'ajouter des pages Web faisant la promotion de produits pharmaceutiques spécifiques. Cette attaque a été rendue possible car certains paramétrages étaient trop permissifs, notamment l'écriture dans quelques répertoires étaient autorisée.

Le scénario de l'attaque pourrait se résumer ainsi :

- l'attaquant recherche des serveurs fonctionnant avec *SPIP* ;
- il profite de droits en écriture dans un répertoire particulier pour déposer un *phpshell* (programme écrit en PHP qui a la possibilité d'exécuter un certain nombre de commandes, à l'instar d'un *shell* classique) ;
- il utilise son *phpshell* pour installer plusieurs fichiers, notamment un second *phpshell* (de secours ?) et un fichier qui, lorsqu'il est exécuté, provoque le téléchargement d'un ensemble de pages de promotion pour des produits pharmaceutiques.

La présence sur le serveur de ces pages au contenu inapproprié a été détectée à plusieurs reprises au cours des dernières semaines. Mais le traitement de l'incident n'avait pas été fait correctement. En effet, après la

première détection de cet incident, seules les pages de publicité avaient été retirées. Suite au second signalement du problème, un des *phpshell* avait été supprimé. Ce n'est qu'après la troisième alerte que le disque dur a été analysé, ce qui a conduit à la découverte de l'autre *phpshell* et du fichier responsable de l'installation des pages de promotion.

Il est important de préciser que si un filtrage en sortie avait été mis en place, le contenu publicitaire ne serait pas apparu aussi facilement et cela aurait laissé une trace flagrante dans les journaux.

2 Microsoft Office Visualization Tool (OffVis)

Microsoft a présenté à la conférence *Black Hat USA*, qui a eu lieu du 25 au 30 juillet dernier à Las Vegas, un outil gratuit d'analyse du format *Microsoft Office* (pour les versions allant de 97 à 2003). Ce logiciel, baptisé *OffVis*, permet la détection des documents malveillants au format *.doc*, *.xls*, et *.ppt*. La version bêta 1.0 est disponible gratuitement à l'adresse :

<http://go.microsoft.com/fwlink/?LinkId=158791>

Il s'agit une application *.NET* et le *framework 3.5* est recommandé.

Le format *Microsoft Office* (97 à 2003), nommé *OLE Structured Storage* (parfois également appelé *Compound File*), est en fait un système de fichiers dans un document. L'idée sous-jacente est de pouvoir stocker simplement plusieurs fichiers (images, objets OLE, etc.) dans un seul document, de pouvoir les modifier sans avoir à tout réécrire, de permettre des opérations telles que des annulations, etc.

L'analyse d'un document *Office* doit donc se faire à deux niveaux :

- le *OLE Structured Storage* ;
- son contenu, qui peut-être *Word*, *Excel* ou *PowerPoint*.

OffVis embarque quatre modules de traitement : celui pour le *OLE Structured Storage*, qui est indispensable à toute analyse de document *Office*, et un pour chacun des contenus *Word*, *Excel*, et *PowerPoint*. Ces éléments incluent également la possibilité de détecter les documents malveillants correspondant à huit vulnérabilités connues :

- CVE-2006-0009, *PowerPoint*, mars 2006 ;
- CVE-2006-0022, *PowerPoint*, juin 2006 ;
- CVE-2006-2492, *Word*, juin 2006 ;
- CVE-2006-3434, *Word*, octobre 2006 ;
- CVE-2007-0671, *Excel*, février 2007 ;
- CVE-2006-0081, *Excel*, mars 2008 ;
- CVE-2006-0238, *Excel*, avril 2009 ;
- CVE-2006-0556, *PowerPoint*, mai 2009.

L'interface de l'outil est composée de deux fenêtres, celle de gauche affiche la représentation hexadécimale du fichier analysé, et celle de droite permet la navigation dans les objets du document, sous forme arborescente.

Cependant, même si les bases sont indéniablement présentes, *OffVis* ne tient pas encore toutes ses promesses. Les modules de traitement sont encore incomplets, parfois incorrects. À titre d'exemple, l'arborescence du *OLE Structured Storage* est présentée de façon approximative, plusieurs noeuds manquent à l'appel. De plus, *OffVis* étant destiné à être un outil d'audit de document *Office*, il se doit d'embarquer une base de données de vulnérabilités connues. En effet, les huit actuellement détectées sont insuffisantes pour en faire un outil opérationnel. Enfin, l'outil étant en version bêta, il est encore instable et présente régulièrement des dysfonctionnements.

Malgré ses défauts de jeunesse, *OffVis* est très prometteur, en ce sens qu'il permet l'analyse des contenus *Word*, *Excel*, et *PowerPoint*, et soulage du développement fastidieux d'un analyseur de contenu *Office* dont les spécifications, aujourd'hui publiques, font plus de 2000 pages au total. Reste à savoir quand *OffVis* sortira dans une version finale, avec une base de données complète (et pouvant être mise à jour) de vulnérabilités.

3 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/>

4 Rappel des avis émis

Dans la période du 14 au 20 août 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-336 : Vulnérabilité dans GnuTLS
- CERTA-2009-AVI-339 : Vulnérabilités dans JRun
- CERTA-2009-AVI-340 : Multiples vulnérabilités dans Adobe ColdFusion
- CERTA-2009-AVI-341 : Vulnérabilités dans IBM WebSphere Application Server
- CERTA-2009-AVI-342 : Vulnérabilité dans CA Host-Based Intrusion Prevention System
- CERTA-2009-AVI-343 : Vulnérabilité dans CA Internet Security Suite

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

- CERTA-2009-AVI-316-001 : Vulnérabilité dans Fetchmail (ajout des références aux bulletins Debian, Mandriva et Ubuntu)
- CERTA-2009-AVI-334-001 : Vulnérabilité dans WordPress (ajout de la référence CVE)
- CERTA-2009-AVI-337-002 : Vulnérabilité du noyau Linux (correction de coquille et ajout de la référence au bulletin de sécurité Ubuntu)
- CERTA-2009-AVI-338-001 : Vulnérabilité de cURL et libcurl (ajout des références aux bulletins RedHat et Ubuntu)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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.ssi.gouv.fr/fr/formation/>

6 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.

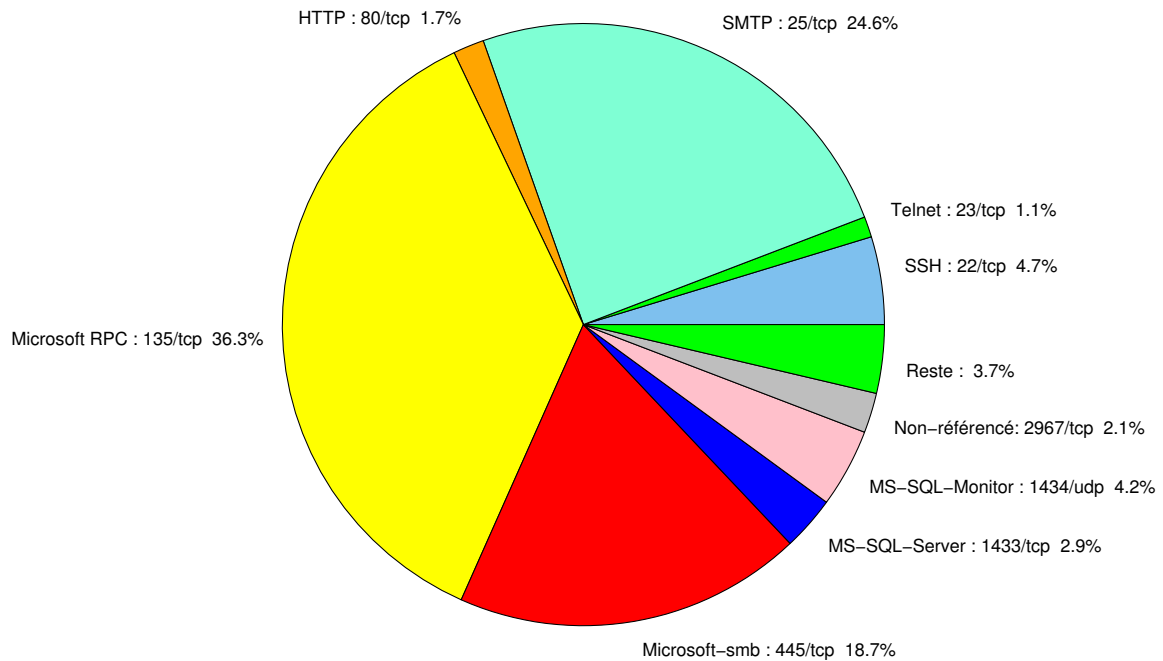


FIG. 1: Répartition relative des ports pour la semaine du 13 au 20 août 2009

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	36.28
25/tcp	24.58
445/tcp	18.76
22/tcp	4.7
1434/udp	4.22
1433/tcp	2.9
80/tcp	2.63
2967/tcp	2.14
23/tcp	1.17
1080/tcp	0.83
3128/tcp	0.62
4899/tcp	0.48
3389/tcp	0.34
42/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

21 août 2009 version initiale.