

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2007-03**

---

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-2007-ACT-003>

---

### Gestion du document

Référence	CERTA-2007-ACT-003
Titre	Bulletin d'actualité 2007-03
Date de la première version	19 janvier 2007
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-2007-ACT-003.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-2007-ACT-003/>

## 1 Activité en cours

### 1.1 Les inclusions de pages PHP

Cette semaine, le CERTA a, une nouvelle fois, traité des incidents de défigurations de sites Web vulnérables à des attaques dites de PHP `Include`.

Dans certains cas, ces compromissions sont allées jusqu'à la mise en ligne de sites de filoutage (*phishing*). Le CERTA recommande de contrôler l'intégrité de toutes les variables (passées en paramètre dans l'adresse réticulaire ou non) avant de les utiliser et dans la mesure du possible de ne pas se servir de la fonctionnalité `Include` dans les pages web PHP. L'utilisation de cette fonctionnalité du langage PHP peut, en effet, s'avérer dangereuse.

Les exemples ci-dessous indiquent de bonnes pratiques en matière de vérifications de données. Ces exemples ne doivent en aucun cas être appliqués tels quels mais peuvent faire partie d'une réflexion globale en matière de contrôle des variables et des entrées :

- La plupart des intrusions utilisent des failles PHP `Include` se servant de scripts téléchargés depuis un site Internet. Une bonne pratique consiste à limiter la directive `Include` aux variables ne contenant pas les mots clef HTTP et FTP et WWW :

```
<? if (
```

```

$page && !strncmp($page,"http",4) &&
!strncmp($page,"ftp",3) &&
!strncmp($page,"www",3) && stat($page)
)
INCLUDE($page); else ... ?>

```

Cette technique ne protège pas des scripts malveillants déjà présents sur le serveur.

- Il est beaucoup plus sûr de limiter les pages pouvant être passées en paramètre à celles autorisées et présentes sur le serveur Web (liste blanche) :

```

<? $tab_pages=Array( "mapage1.php" , "mapage2.php" , "mapage3.php" );
    if (in_array($page,$tab_pages)) { include $page; } ?>

```

Les exemples de code fournis, le sont à titre d'information uniquement et ne peuvent en aucun cas remplacer un audit de sécurité. Le CERTA recommande également d'interdire, au niveau du pare-feu, les téléchargements à partir du serveur lui-même.

## Documentation

- Alerte du CERTA du 09 septembre 2003 sur l'exploitation massive de la vulnérabilité « PHP Include » : <http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-003>
- Note d'information du CERTA du 19 décembre 2005 sur les bonnes pratiques concernant l'hébergement mutualisé : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005>
- 'Secure Programming for Linux and Unix HOWTO – Creating Secure Software', D. Wheeler : <http://www.dwheeler.com/secure-programs/>

## 1.2 Rejetés par Google

L'utilisation régulière des grands moteurs de recherche, en l'occurrence Google, peut parfois présenter quelques effets de bord. Cela est dû à la mise en place de quelques mécanismes de protection par Google contre des codes considérés comme malveillants (virus, spyware, etc.).

Sur des critères définis par lui-même, le moteur de recherche Google peut limiter l'accès aux formulaires de recherche en imposant à l'utilisateur de recopier un cryptogramme visuel. Ce dernier est inclus dans une page prévenant l'utilisateur d'une éventuelle compromission de son système par un virus ou un *spyware*. Cela permet à Google de s'assurer que la recherche provient bien d'un humain, et non d'un outil automatique malveillant.

Cette mesure du moteur de recherche Google présente des conséquences indésirables dans le cas d'une connexion Internet partagée avec une seule adresse IP publique. Une utilisation non standard du moteur de recherche Google depuis l'un des postes du réseau conduit tous les autres postes du réseau partageant la même adresse IP publique à la même sanction, à savoir un accès avec cryptogramme au formulaire de recherche.

Les incidents de ce type, déjà traités par le CERTA, ont permis de mettre en évidence deux éléments importants :

- ne pas paniquer à l'affichage d'un tel message de la part du moteur de recherche Google et avertir sans délai son service informatique ;
- analyser le trafic réseau dès que possible afin de faciliter l'identification d'un éventuel système compromis.

D'une manière générale, le moteur de recherche Google ne constitue pas la seule solution en matière de recherche sur l'Internet.

## 2 Les logiciels gratuits pseudo-miracles

### 2.1 Cas général

Certains logiciels, gratuits ou non, apparaissent subitement dans les médias, car offrant une fonctionnalité peu courante, voire inexistante jusqu'alors. Il peut s'agir par exemple de navigateurs.

Parmi les cas les plus récents, les « avantages » mis en avant sont les suivants :

- anonymat de la navigation ;
- nettoyage des traces laissées par la navigation sur la machine ;

- remplissage « magique » des formulaires ;
- suppression de publicités envahissantes ;
- personnalisation poussée de l'apparence du navigateur ;
- etc.

Ces outils s'appuient souvent sur un produit existant, comme par exemple Internet Explorer ou Firefox. Ils sont donc non seulement vulnérables aux mêmes classes d'attaques, mais ils ouvrent aussi d'autres opportunités d'attaques, à la mesure des fonctionnalités offertes si généreusement.

## 2.2 Que faire ?

Les outils mentionnés ci-dessus ont tous un point en commun : ils offrent de manière alléchante une ou plusieurs fonctionnalités. Il est donc prudent de :

- s'enquérir sur la bonne facture de l'outil auprès de spécialistes en sécurité ;
- tester que les fonctionnalités annoncées sont bien celles installées, et elles seules, qu'il n'y a ni cheval de Troie ni publiciel ;
- valider que les outils restent conformes à la politique de sécurité.

## 3 « *Month of Apple Bug* » (troisième semaine)

Voici pour cette semaine les vulnérabilités sur les produits Apple publiées par le projet « *Month of Apple Bug* », et non corrigées à la date de parution de ce bulletin. Depuis vendredi dernier, on notera les publications suivantes :

- Une vulnérabilité dans la mise en œuvre du protocole AppleTalk dans MacOS X permettant de provoquer un déni de service ou d'exécuter du code arbitraire à distance ;
- une vulnérabilité dans le positionnement des droits d'accès à certains fichiers du répertoire /Applications avec le bit `suid` positionné permettant une élévation de privilèges ;
- une vulnérabilité dans le service `slpd` (Service Location Protocol Daemon) permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Problème GIF et Java

Le CERTA a publié cette semaine l'avis CERTA-2007-AVI-033, concernant une vulnérabilité dans la machine virtuelle Java de Sun. Elle ne manipulerait pas correctement certaines images au format GIF (pour *Graphics Interchange Format*). Ce format est très répandu, et une attaque peut se produire via une page Web contenant du code Java mettant en œuvre l'affichage d'un GIF spécialement construit.

Il est donc recommandé de :

- vérifier que le support de Java est désactivé par défaut au niveau du navigateur, tout comme cela doit être fait pour Javascript ;
- vérifier que vous disposez bien de la dernière version de la machine virtuelle Java.

## 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 11 et le 18 janvier 2007.

## 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 12 au 18 janvier 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-026 : Multiples vulnérabilités dans VMware
- CERTA-2007-AVI-027 : Vulnérabilité dans Cisco IOS
- CERTA-2007-AVI-028 : Vulnérabilité dans Cisco Unified Contact Center
- CERTA-2007-AVI-029 : Vulnérabilités dans Computer Associates BrightStor ARCserve Backup
- CERTA-2007-AVI-030 : Vulnérabilité d'ordinateurs portables Acer
- CERTA-2007-AVI-031 : Vulnérabilités dans HP OpenView Network Node Manager
- CERTA-2007-AVI-032 : Multiples vulnérabilités dans les produits Oracle
- CERTA-2007-AVI-033 : Vulnérabilité dans la machine virtuelle Java de Sun
- CERTA-2007-AVI-034 : Vulnérabilité de Wordpress
- CERTA-2007-AVI-035 : Vulnérabilités de Squid 26
- CERTA-2007-AVI-036 : Vulnérabilité de HP JetDirect
- CERTA-2007-AVI-037 : Vulnérabilité de Xpdf et ses dérivés

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

- CERTA-2007-AVI-025-001 : Multiples vulnérabilités de Xorg (Systèmes affectés et référence Suse.)

## 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.

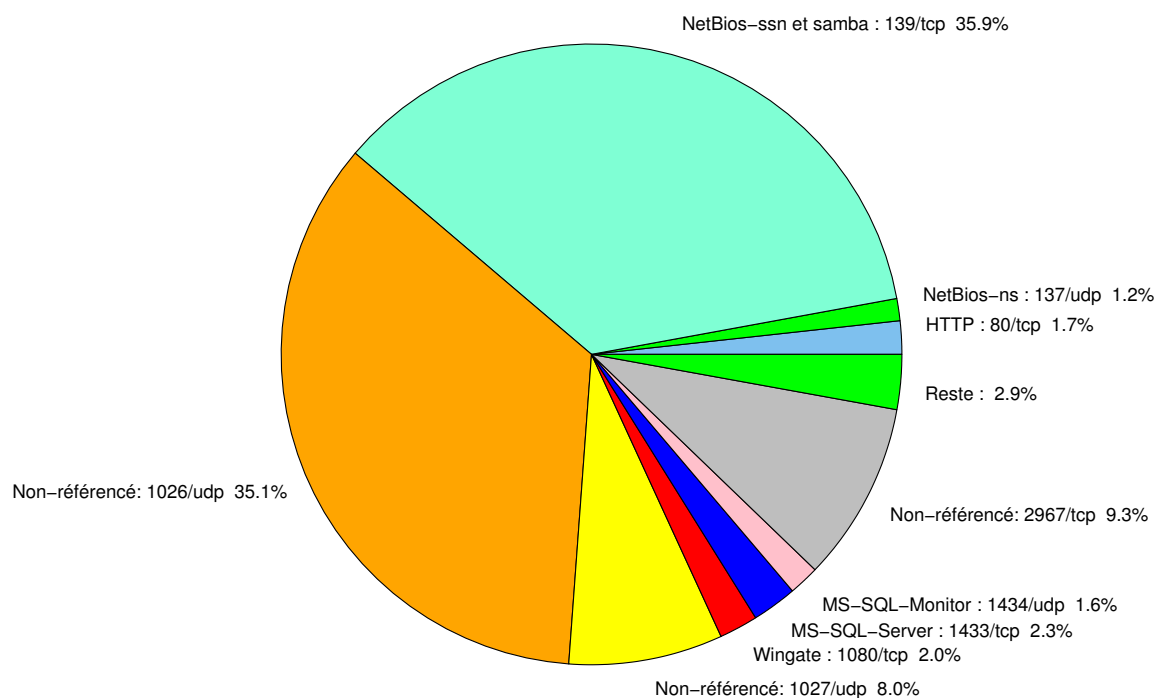


FIG. 1: Répartition relative des ports pour la semaine du 11.01.2007 au 18.01.2007

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	Yellow Worm	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
139/tcp	35.89
1026/udp	35.05
2967/tcp	9.34
1027/udp	8.02
1433/tcp	2.33
1080/tcp	2.01
80/tcp	1.73
1434/udp	1.58
137/udp	1.15
4899/tcp	0.69
3128/tcp	0.66
25/tcp	0.37
3306/tcp	0.31
22/tcp	0.25
21/tcp	0.2
443/tcp	0.17
3389/tcp	0.11
143/tcp	0.05

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

19 janvier 2007 version initiale.