

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-08

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-008>

Gestion du document

Référence	CERTA-2007-ACT-008
Titre	Bulletin d'actualité 2007-08
Date de la première version	23 février 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-008.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-008/>

1 Activités en cours

1.1 Problème lié à l'hébergement mutualisé

Le CERTA a traité deux incidents concernant des cas de défigurations. Dans la première d'entre elles, il s'agissait d'un simple fichier `index.html` modifié ou écrasé qui empêchait une redirection vers le bon site. Après lecture des journaux du système affecté, il a été impossible de déterminer la nature de l'attaque. Dans la seconde compromission, l'auteur de la défiguration a utilisé une vulnérabilité de type « inclusion php » présente dans un gestionnaire de contenu Joomla! vulnérable. Dans ce cas, il a été possible d'identifier le type d'attaque en exploitant les journaux du système. Or, après analyse, ces deux incidents n'en faisaient qu'un. En effet, les deux sites se trouvaient sur la même machine en hébergement mutualisé. Le CERTA a donc pu déterminer que le point d'entrée sur la machine fut le site Joomla! vulnérable, depuis lequel le pirate s'attaqua aux autres sites présents sur la machine. On parle dans ce cas d'une défiguration en masse.

Recommandations:

Le CERTA vous recommande de vous reporter à la note d'information CERTA-2005-INF-005 concernant l'hébergement mutualisé et les risques inhérents à ce type de solutions.

1.2 Règle de filtrage pour les serveurs

Il est d'usage que les pare-feux laissent passer les connexions HTTP (port 80) sortantes sans restriction et qu'un proxy soit chargé de limiter ces connexions à certaines adresses réticulaires (URL). Ce filtrage est souvent appliqué aux connexions issues des postes de travail. Il doit l'être également aux serveurs, même en zone publique (DMZ). Lors du traitement récent d'un incident, le CERTA a constaté qu'un serveur en zone publique s'est trouvé compromis. Le manque de filtrage des connexions vers l'Internet initiées par ce serveur a permis l'utilisation frauduleuse du serveur pour participer à un déni de service.

Recommandations:

Le CERTA recommande la mise en oeuvre d'un politique contrôlant les « rebonds ». Dans ce cadre, il convient :

- d'appliquer un filtrage pour les connexions des serveurs vers l'Internet, même sur les protocoles classiquement autorisés (HTTP, FTP, SMTP) ;
- de mettre en place un filtrage adapté à ces serveurs.

1.3 La configuration des services de messagerie

Cette semaine le CERTA a reçu des appels concernant des incidents de messagerie. En effet durant les périodes de congés il est fréquent de constater que des utilisateurs mettent en place des réponses automatiques voir des redirections de courrier de leur messagerie professionnelle vers leur messagerie personnelle. Mal configurées, ces fonctionnalités peuvent devenir la source d'importante nuisances, comme par exemple des courriels qui transitent en boucle infinie entre la messagerie de l'utilisateur et une liste de diffusion, des réponses automatiques qui remplissent une boîte aux lettres électronique ou encore la sortie d'information confidentielle relayée vers une boîte aux lettres externe.

Recommandations:

Il est préférable d'éviter de paramétrer un message d'absence ou une réponse automatique pour les courriels venant de l'extérieur et d'interdire la redirection de messages vers des boîtes aux lettres externes ou personnelles.

1.4 Vulnérabilités dans Firefox

Ces derniers jours, plusieurs vulnérabilités ont été publiées sur l'Internet ou dans des listes de diffusion touchant principalement le navigateur Firefox. Internet Explorer 7 pourrait être concerné également par certaines d'entre elles. Pour le moment, le CERTA n'a pas publié sur le sujet autrement que par le biais de ce bulletin, car l'exploitation de ces vulnérabilités ne peut conduire à une compromission sérieuse de l'intégrité d'un système. Tout au plus, l'exploitation de ces vulnérabilités pourrait être intégrée dans un processus d'attaque (comme du *phishing*, par exemple), ce qui reste néanmoins hypothétique. Certaines de ces vulnérabilités sont examinées en ce moment par les éditeurs afin de les qualifier, dans un premier temps, puis d'apporter d'éventuels correctifs.

Recommandations:

Le CERTA recommande de naviguer sur l'Internet avec la plus grande prudence, en ne consultant dans la mesure du possible que des sites de confiance, et en n'autorisant l'activation du contenu dynamique (ActiveX, Javascript, Java) qu'en cas d'extrême nécessité.

2 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 16 et le 23 février 2007.

3 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/>

4 Rappel des avis émis

Durant la période du 16 au 23 février 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-087 : Vulnérabilité dans la mise en oeuvre du protocole TCP sous Sun Solaris
- CERTA-2007-AVI-088 : Vulnérabilité de HP-UX SLS
- CERTA-2007-AVI-089 : Multiples vulnérabilités du module IPS de Cisco IOS
- CERTA-2007-AVI-090 : Multiples vulnérabilités de produits Cisco
- CERTA-2007-AVI-091 : Multiples vulnérabilités dans Apple iChat
- CERTA-2007-AVI-092 : Vulnérabilité dans Apple UserNotification
- CERTA-2007-AVI-094 : Vulnérabilité dans SpamAssassin
- CERTA-2007-AVI-095 : Vulnérabilité de Snort
- CERTA-2007-AVI-096 : Vulnérabilité de TrendMicro ServerProtect
- CERTA-2007-AVI-097 : Vulnérabilités dans Cisco Secure Services Client
- CERTA-2007-AVI-098 : Multiples vulnérabilités dans les équipements CISCO Unified IP

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

- CERTA-2007-AVI-076 : Multiples vulnérabilités dans php (ajout des références CVE et Redhat)
- CERTA-2007-AVI-093 : Multiples vulnérabilités dans ClamAV (ajout de la référence Mandriva)

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 œuvre (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 COSSI/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.formation.ssi.gouv.fr>

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.

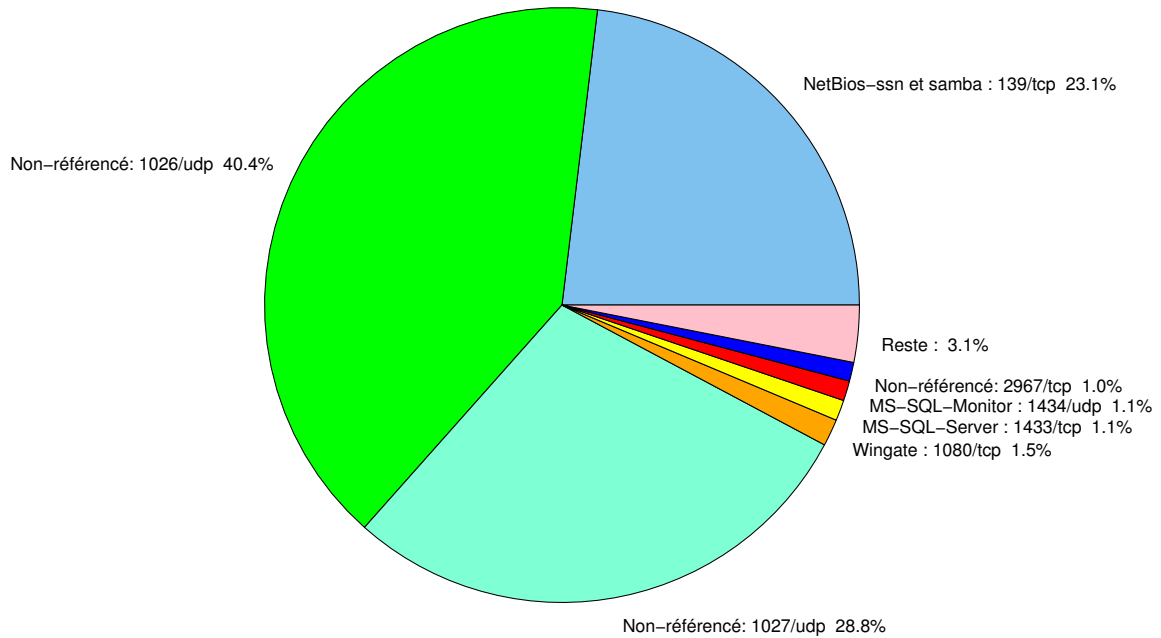


FIG. 1: Répartition relative des ports pour la semaine du 16.02.2007 au 23.02.2007

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
1026/udp	40.35
1027/udp	28.77
139/tcp	23.09
1080/tcp	1.46
1433/tcp	1.12
1434/udp	1.08
2967/tcp	1.02
4899/tcp	0.88
25/tcp	0.4
137/udp	0.34
80/tcp	0.32
22/tcp	0.25
3128/tcp	0.22
3306/tcp	0.17
21/tcp	0.13
143/tcp	0.11
2100/tcp	0.1
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

23 février 2007 version initiale.