

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-48

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-2006-ACT-048>

Gestion du document

Référence	CERTA-2006-ACT-048
Titre	Bulletin d'actualité 2006-48
Date de la première version	01 décembre 2006
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-2006-ACT-048.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-2006-ACT-048/>

1 Activité en cours

1.1 Défiguration

Cette semaine, le CERTA a traité un cas de défiguration faisant suite à l'exploitation de droits permissifs sur la requête PUT. Les auteurs de ces défigurations recherchent souvent les extensions WebDAV en essayant quelques requêtes telles que PROPFIND sur les serveurs.

Microsoft donne une méthode pour désactiver WebDAV :

<http://support.microsoft.com/kb/241520/>

Sous IIS, il existe également un outil fourni par Microsoft permettant de gérer des droits sur les méthodes. Cet outil est disponible à l'adresse :

<http://www.microsoft.com/technet/security/tools/locktool.mspx>

1.2 Les outils de découverte topologique du réseau

Le CERTA a traité cette semaine un incident, et a trouvé sur la machine analysée un outil de découverte de réseau. De telles applications se proposent de découvrir automatiquement la topologie du réseau, en balayant les

plages adresses voisines, ainsi qu'en interrogeant certains services. Ces outils peuvent être installés aussi bien par l'administrateur que par un intrus cherchant à récupérer de l'information concernant le réseau de la machine qu'il vient de compromettre. Ils permettent d'obtenir des informations délicates, qui doivent rester confidentielles.

L'utilisation de ces outils doit susciter plusieurs questions :

- l'outil est-il de confiance ? Dans le cas traité cette semaine, il s'agissait d'un outil d'origine méconnue. Il faut envisager que ce dernier, aussi performant soit-il, puisse communiquer les informations obtenues vers un site externe ;
- l'outil conserve-t-il les informations localement ? Comme plusieurs applications, ces outils gardent souvent un historique des topologies effectuées. Si l'application n'est pas installée sur une machine dédiée, ou n'est pas proprement configurée, des informations résiduelles peuvent subsister sur le système ;
- l'outil ne perturbe-t-il pas son environnement ? Ces applications ont un comportement actif (envoi de paquets et de requêtes), voire agressif, qui peuvent produire beaucoup de bruits dans les journaux ou provoquer de fausses alertes par les outils de détection et de surveillance (et donc, *a fortiori*, de dissimuler d'autres activités moins légitimes).

De manière générale, il est toujours regrettable que des outils de sécurité augmentent les risques. Il vaut mieux éviter de tester ces derniers à un moment critique (incident). Dans le doute, prenez contact avec le CERTA qui vous conseillera en cas d'incident.

2 Interface Google Search

Le CERTA informe ses correspondants qu'une vulnérabilité de type « *cross site scripting* », est apparue sur les sites web utilisant l'interface "Google Search Appliance". Cette vulnérabilité permettrait aussi d'injecter des données sur le site vulnérable.

Le risque est limité dans la mesure où il est nécessaire de saisir une requête spéciale, encodée en UTF-7, dans le moteur de recherche du site vulnérable. Ce standard n'est pas très commun, mais peut être accepté par défaut dans certaines applications comme les serveurs Web.

Cette attaque permet, sous certaines conditions, de contourner les filtres mis en place pour valider les requêtes adressées au moteur de recherche.

Cette vulnérabilité, largement documentée sur le Web, peut être corrigée en effectuant un contrôle sémantique des requêtes, et en vérifiant que l'encodage UTF-7 ne soit pas accepté par le serveur Web.

3 Gestionnaire de mots de passe dans un navigateur

Une vulnérabilité de Firefox a été dévoilée le 21 novembre 2006. Nous l'avions déjà évoqué dans le bulletin d'actualité CERTA-2006-ACT-047. Elle repose sur une vérification insuffisante de l'adresse (URL) d'un formulaire d'authentification qui demande un identifiant et un mot de passe. Le site de destination de ces données confidentielles peut être autre que le site qui a présenté le formulaire. Si le gestionnaire de mot de passe est activé, alors le navigateur va remplir les champs et dévoiler ces données d'authentification à un destinataire qui n'est pas le site qui a présenté le formulaire.

Cette vulnérabilité ne se limite pas à Firefox. Elle concerne également les navigateurs Internet Explorer, versions 6 et 7, et Safari.

Recommandations :

Les bonnes pratiques consistent à ne pas utiliser les gestionnaires de mots de passe des navigateurs. Les utilisateurs qui ont déjà enregistré des mots de passe dans leur navigateur doivent, d'une part, désactiver le gestionnaire de mot de passe et, d'autre part, effacer les mots de passe déjà enregistrés.

Les gestionnaires de sites web, en particulier les sites sur lesquels les internautes peuvent déposer des contributions, doivent vérifier qu'aucun attaquant ne va utiliser cette fonction de dépôt pour inclure du code HTML piégeant le site et permettant d'exploiter la vulnérabilité des navigateurs.

4 Joomla!

Suite au bulletin d'actualité CERTA-2006-ACT-047, le CERTA a eu plusieurs remontées d'informations concernant des intrusions dans des serveurs Joomla! par l'exploitation d'une faille de `ext_calendar`. Ces

remontées nous ont permis d'établir que les serveurs ainsi compromis étaient intensivement utilisés (au point d'être indisponibles) pour réaliser des dénis de service. Ces intrusions se sont manifestées par des connexions aux serveurs suivants :

- blog156448.123-reg-blogs.co.uk
- Bucharest.RO.EU.Ultra-Chat.Org
- seks.irctr.net
- linux.Ircd.net
- 194.145.200.200

Il est conseillé de vérifier que tout trafic à destination de ces serveurs est légitime et d'en informer le CERTA.

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 23 et le 30 novembre 2006.

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/>

7 Rappel des avis et mises à jour émis

Durant la période du 24 au 30 novembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-514 : Vulnérabilité de GNU Radius
- CERTA-2006-AVI-515 : Vulnérabilité dans Symantec NetBackup PureDisk
- CERTA-2006-AVI-516 : Vulnérabilité de GNU tar
- CERTA-2006-AVI-517 : Multiples vulnérabilités dans Apple Mac OS X

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

À 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.

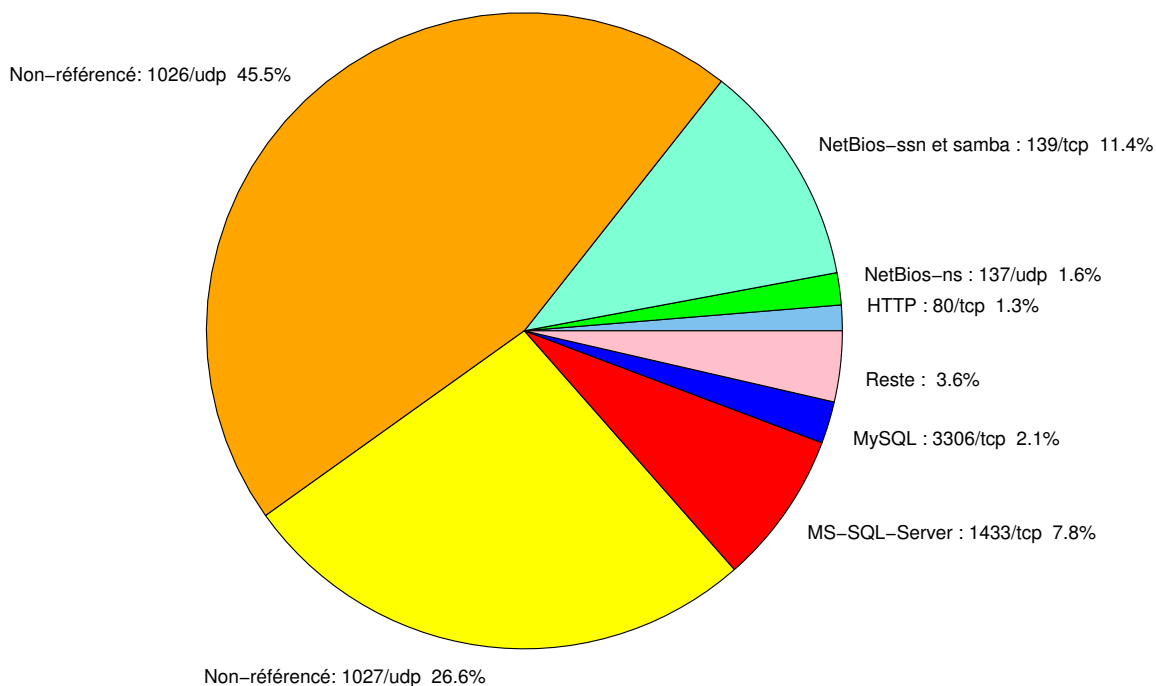


FIG. 1: Répartition relative des ports pour la semaine du 23.11.2006 au 30.11.2006

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	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	45.5
1027/udp	26.61
139/tcp	11.43
1433/tcp	7.78
3306/tcp	2.13
137/udp	1.63
80/tcp	1.29
1434/udp	0.9
4899/tcp	0.86
1080/tcp	0.33
22/tcp	0.31
25/tcp	0.28
3128/tcp	0.15
15118/tcp	0.14
135/tcp	0.12
143/tcp	0.08
3127/tcp	0.04
3389/tcp	0.03
6101/tcp	0.01

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

01 décembre 2006 version initiale.