

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-42

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-042>

Gestion du document

Référence	CERTA-2006-ACT-042
Titre	Bulletin d'actualité 2006-42
Date de la première version	20 octobre 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-042.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-042/>

1 Incidents traités

1.1 Considérations sur l'origine de l'intrusion

Le CERTA a traité cette semaine un incident lié à une défiguration. Après analyse, il s'avère que la page a été défigurée, mais le site Web lui-même n'en est pas la cause. L'intrusion est survenue sur un autre site Web, co-hébergé sur la même machine physique. Cet incident est un exemple concret des risques que peut engendrer un co-hébergement. En particulier, certains sites offrent des accès à des zones protégées par des mots de passe. La compromission d'un site co-hébergé permet éventuellement d'accéder de façon frauduleuse à ce type de zones, et ce quelque soit la sécurité de votre site web.

Une note d'information du CERTA peut vous aider à mieux apprécier les risques liés à l'hébergement mutualisé :

<http://www.certa.ssi.gouv.fr/CERTA-2005-INF-005/>

1.2 Sur l'importance des mots de passe

Un de nos correspondants a constaté avoir subi une attaque en « force brute » sur son proxy web (port 8080/tcp). De nombreux noms de compte différents ont été testés, sans succès. Ces attaques sont similaires à celles affectant

SSH. D'une manière générale, il est possible que tous les services s'appuyant sur une authentification (SSH, FTP, proxy web, mais aussi POP3 et quelques accès HTTP) fassent l'objet de ce type d'attaques faciles à automatiser. Il est fortement recommandé de veiller à l'utilisation de mots de passe forts. La note d'information suivante aborde ce problème :

<http://www.certa.ssi.gouv.fr/CERTA-2005-INF-001/>

2 Les défigurations de site

Les défigurations peuvent servir de tribune pour des revendications à caractère politique ou social. Dans un contexte politique bien précis, ces attaques peuvent cibler n'importe quel site web. Récemment, on a pu ainsi voir des serveurs web français défigurés avec un message en référence à la loi relative à la répression de la négation du génocide arménien.

Les auteurs de ces attaques utilisent généralement des failles bien connues afin de compromettre les sites web et d'y déposer leur message. Ces failles sont toujours du même type : soit un problème de droits en écriture qui ont été laissés, soit un applicatif web mal programmé qui permet l'importation et l'exécution de fichiers externes au serveur. On remarque par ailleurs que les applicatifs web attaqués sont souvent déployés par les webmasters alors qu'ils ne sont pas utilisés.

Il est donc important de bien mettre à jour ses applications et de réfléchir au déploiement des modules optionnels.

3 Problèmes liés aux pilotes Bluetooth

Bluetooth est une technologie sans-fil, définie par les standards IEEE 802.15.X. Elle est employée dans le cadre de communications à petite distance (de l'ordre de quelques mètres). Cela inclut les synchronisations avec des assistants personnels électroniques (PDA), les périphériques de type souris, clavier, voire même les enceintes.

Plusieurs vulnérabilités ont été identifiées ces derniers mois dans certains pilotes Bluetooth fonctionnant sous Microsoft Windows. Une personne malveillante peut construire des paquets particuliers. Cela est facilité par l'existence de documents très détaillés et disponibles sur l'Internet. En émettant de tels paquets exploitant cette vulnérabilité, il lui serait possible d'exécuter des commandes arbitraires sur la machine possédant ces pilotes vulnérables. Une limitation de ces attaques repose sur le fait que le Bluetooth a une petite portée. Ceci est vrai pour des périphériques standards. Il existe cependant dans le commerce des moyens pour augmenter la distance d'interaction à une centaine de mètres (clés USB bluetooth particulières, antennes directionnelles, etc).

Le bluetooth doit donc être considéré comme une porte d'entrée potentielle et dangereuse sur une machine ou un réseau, de la même façon qu'il faut prendre de grandes précautions avec la technologie Wi-Fi.

Recommandations :

Dans ces conditions, le CERTA recommande :

- de limiter les appareils Bluetooth, surtout si ceux-ci interagissent avec des machines sensibles ou intégrées à un réseau. C'est une porte d'entrée bien plus facile que celle qui consisterait à tromper le pare-feu du réseau ;
- de vérifier que le matériel Bluetooth des périphériques et des ordinateurs mobiles reste désactivé s'il n'est pas utilisé. Une désactivation physique est toujours préférable.

4 Problème avec Internet Explorer 7

Une vulnérabilité affectant le navigateur *Internet Explorer 7* a été rendue publique. Cette faille affectait déjà la version *Internet Explorer 6*. Sur une version d'*Internet Explorer 7* installée par défaut, et avec un *Windows XP SP2* à jour, la vulnérabilité permet de récupérer des informations d'un autre site dans le contexte de l'utilisateur. Le danger provient encore d'un contrôle ActiveX (*Mxml2.XMLHTTP*). La sortie d'*Internet Explorer 7* ne change rien aux risques liés à l'usage de ces composants. Il est donc à nouveau fortement recommandé de désactiver l'utilisation de ces composants. Le CERTA publiera prochainement une note d'information à ce sujet.

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 12 et le 19 octobre 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>

7 Rappel des avis et mises à jour émis

Durant la période du 13 au 19 octobre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-453 : Vulnérabilité de OpenSSH
- CERTA-2006-AVI-454 : Vulnérabilités dans Clam Antivirus
- CERTA-2006-AVI-455 : Vulnérabilité du module mod_tcl de Apache
- CERTA-2006-AVI-456 : Vulnérabilité dans Opera

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

- CERTA-2006-AVI-454-001 : Vulnérabilités dans Clam Antivirus
(ajout du bulletin de sécurité FreeBSD)

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.

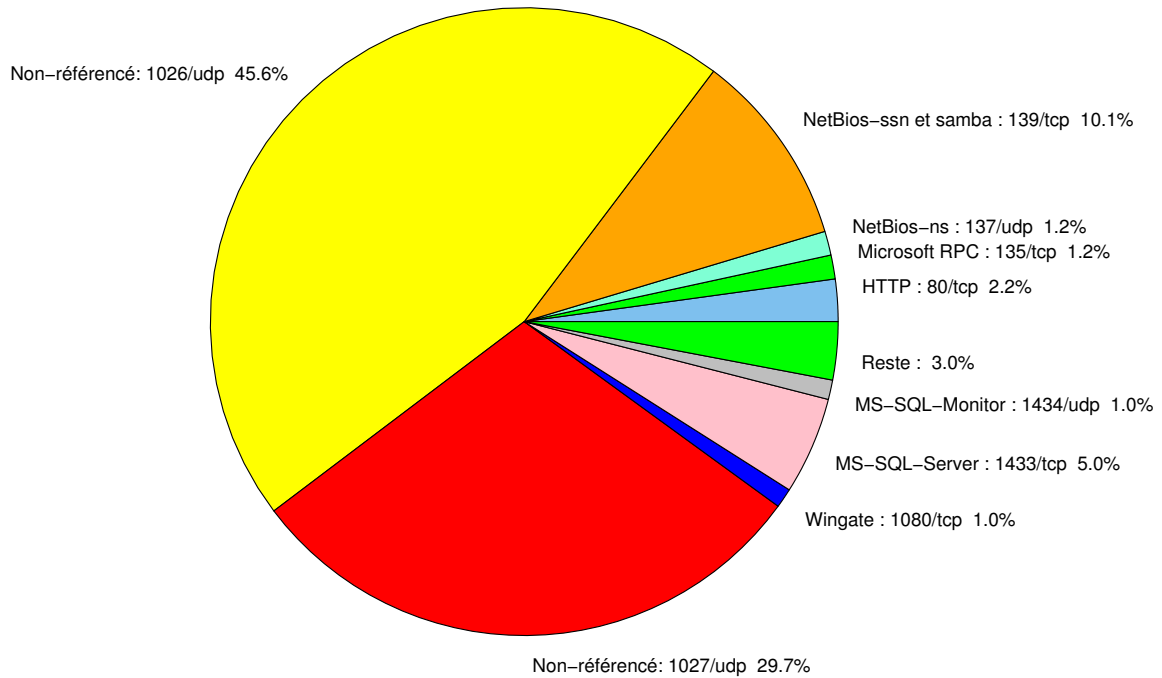


FIG. 1: Répartition relative des ports pour la semaine du 12.10.2006 au 19.10.2006

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	45.6
1027/udp	29.68
139/tcp	10.05
1433/tcp	5.01
80/tcp	2.17
137/udp	1.23
135/tcp	1.22
1434/udp	1
4899/tcp	0.81
3306/tcp	0.54
22/tcp	0.31
25/tcp	0.25
3128/tcp	0.23
15118/tcp	0.16
2100/tcp	0.14
21/tcp	0.11
443/tcp	0.08
42/tcp	0.05
9898/tcp	0.04
3127/tcp	0.03
3389/tcp	0.02
11768/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

20 octobre 2006 version initiale.