

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-41

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-041>

Gestion du document

Référence	CERTA-2006-ACT-041
Titre	Bulletin d'actualité 2006-41
Date de la première version	13 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-041.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-041/>

1 Incidents traités

Le CERTA a traité de nombreux incidents cette semaine :

- *Cahier de Texte* est une application qui permet de gérer les devoirs d'une classe sur un site Web. Plusieurs sites ont subi des attaques sur cet applicatif. Des identifiants de connexion ont été volés, ce qui a permis à l'intrus d'effectuer des modifications dans la base de données. La vulnérabilité exploitée dans l'application *Cahier de Texte* a fait l'objet de la publication de l'avis CERTA-2006-AVI-452.
- Une défiguration datant de *février 2005* (!), qui n'avait jamais été remarquée par la victime, a été traitée. Une faille dans l'applicatif *Awstats.pl* avait permis cette attaque. Cet exemple montre l'importance du traitement des incidents : les intrus peuvent se maintenir sur un système pendant des mois, voire des années, si une détection puis une réponse adéquate ne sont pas apportées.

2 Problèmes de sécurité avec une version 1.8.0 de Claroline

2.1 Présentation des faits

Le 10 octobre 2006, une nouvelle version stable de Claroline, la version 1.8.0, était annoncée sur le site

<http://www.claroline.net> .

Très rapidement, des vulnérabilités de type `php include` ont été annoncées. Le CERTA a téléchargé les sources de la version 1.8.0 et vérifié la véracité de ces failles. Comme annoncé publiquement, la variable `includePath` du fichier `claroline/inc/lib/import.lib.php` permettait l'inclusion de fichiers externes. Par ailleurs, les recherches effectuées par le CERTA ont permis de mettre en évidence d'importants problèmes de sécurité et des oublis de programmation dans le fichier `claroline/inc/lib/export.lib.php`.

Alors qu'aucune annonce officielle n'a été faite sur le site de Claroline, les sources de la version 1.8.0 ont été modifiées, tout en conservant le même numéro de version. Les fichiers `import.lib.php`, `export.lib.php`, `export_zip.lib.php` et `import.xmlparser.lib.php` ont été complètement supprimés des sources.

Il est à noter que la version 1.8.0 de Claroline ne correspond pas à une mise à jour de sécurité, mais à une amélioration de plusieurs fonctionnalités.

2.2 Recommandations :

Si la version 1.8.0 de Claroline a été téléchargée avant le 12 octobre 2006, il est fortement recommandé de la télécharger de nouveau et de veiller à ce que les quatre fichiers (dont `claroline/inc/lib/import.lib.php` et `claroline/inc/lib/export.lib.php`) n'apparaissent plus.

3 Clés USB U3

3.1 Introduction

L'USB (pour *Universal Serial Bus*) est une interface de connexion définie dans les années 90 et destinée à remplacer les ports série et parallèle sur les ordinateurs. Elle est fréquemment utilisée de nos jours sur les équipements informatiques pour y brancher tout type de périphérique, que ce soient les imprimantes, les claviers, les souris, les scanners, les modems, ou des appareils de stockage, comme les clés USB.

Le système d'exploitation Microsoft Windows dispose d'une fonctionnalité appelée *autorun*. Elle consiste à exécuter automatiquement un logiciel lorsqu'un périphérique de stockage qui le contient est connecté. Microsoft autorise uniquement cette fonction pour les périphériques de type CDROM/DVDROM, ou les disques fixes. Cette fonctionnalité est visible, quand, par exemple, à l'insertion de certains CDs, une fenêtre de navigation Internet Explorer s'ouvre.

Un périphérique USB classique ne permet pas, lors de son insertion dans une machine fonctionnant sous Windows, d'exécuter automatiquement des programmes ou des commandes. Microsoft autorise cette fonction de manière restreinte aux CDROM/DVDROM, et aux disques fixes. Cette fonctionnalité, nommée *autorun*, est visible, quand, par exemple, à l'insertion de certains CDs, une fenêtre de navigation Internet Explorer s'ouvre.

3.2 Risques

Dans l'objectif de faire exécuter automatiquement du code au cours de l'insertion d'un périphérique USB, certains fabricants de matériels USB ont développé une astuce, qui consiste à faire passer celui-ci auprès de Windows pour un CD ou/et un DVD. Cette technique existe, et se commercialise sous le nom de USB U3. Le principe général est que le périphérique, au moment de l'insertion, présente sa mémoire flash comme un lecteur de CDROM USB, permettant a fortiori l'exécution d'un *autorun*. De nombreux produits disposant de cette technologie sont actuellement commercialisés. A l'insertion, un « lanceur » permet d'exécuter un ensemble d'applications préalablement configurées, comme Firefox, Skype, Avast Antivirus, etc, l'éventail des applications pré-installées étant le domaine de concurrence de ces produits. Ils fonctionnent sur la version Windows 2000 ainsi que celles plus récentes.

Une clé de ce type peut présenter des avantages pour l'utilisateur mobile. Cependant, la question des mises à jour des applications fournies par les vendeurs reste très obscure.

Profitant de cet avantage, il existe également d'autres lanceurs beaucoup plus malveillants et discrets, permettant d'effectuer tout type d'opération dangereuse, avec les droits du compte actif sur Windows :

- Vol d'information
- Installation de logiciels *rootkits*
- Récupération de la base hachée des mots de passe
- etc

Ces outils sont en libre service sur l'Internet et relativement bien documentés. Par ailleurs, les clés USB U3 sont maintenant disponibles dans la plupart des boutiques de vente de matériels informatiques, à des prix abordables, et ne sont pas facilement distinguables des clés USB plus traditionnelles.

3.3 Recommandations :

Le CERTA recommande donc les actions suivantes pour limiter les impacts sus-mentionnés :

- se connecter sur une machine Windows avec un compte aux droits limités ;
- désactiver l'option *autorun* dans la base de registre (voir lien Microsoft) ;
- ne pas accepter de connexions par des clés issues de sources non fiables ;
- verrouiller l'écran de son ordinateur en cas d'absence, l'*autorun* ne fonctionnant pas sous ces conditions.

3.4 Documentation associée

- Caractéristiques de l'USB U3 :
<http://www.u3.com>
- Comment désactiver la fonction *autorun* sur une machine Windows :
<http://support.microsoft.com/kb/q155217>

4 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 05 et le 12 octobre 2006.

5 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>

6 Rappel des avis et mises à jour émis

Durant la période du 06 au 12 octobre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-430 : Vulnérabilités dans CA BrightStor Arcserve Backup
- CERTA-2006-AVI-431 : Vulnérabilité dans les produits Symantec
- CERTA-2006-AVI-432 : Vulnérabilité dans Invision Power Board
- CERTA-2006-AVI-433 : Vulnérabilité dans PHP
- CERTA-2006-AVI-434 : Vulnérabilité du serveur FTP Serv-U
- CERTA-2006-AVI-435 : Vulnérabilité dans Python
- CERTA-2006-AVI-436 : Vulnérabilité dans Microsoft ASPNET Framework

- CERTA-2006-AVI-437 : Vulnérabilité dans la gestion ActiveX par l'Explorateur Windows
- CERTA-2006-AVI-438 : Multiples vulnérabilités dans Microsoft PowerPoint
- CERTA-2006-AVI-439 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2006-AVI-440 : Multiples vulnérabilités dans Microsoft Word
- CERTA-2006-AVI-441 : Vulnérabilités dans Microsoft XML Core Services
- CERTA-2006-AVI-442 : Multiples vulnérabilités dans Microsoft Office
- CERTA-2006-AVI-443 : Vulnérabilité Microsoft (service Serveur)
- CERTA-2006-AVI-444 : Vulnérabilités dans la gestion d'IPv6 sous Windows
- CERTA-2006-AVI-445 : Vulnérabilité dans Microsoft Windows Object Packager
- CERTA-2006-AVI-446 : Vulnérabilité dans les copieurs Xerox
- CERTA-2006-AVI-447 : Vulnérabilité de httpd sous OpenBSD
- CERTA-2006-AVI-448 : Multiples vulnérabilités d'OpenSSL sous OpenBSD
- CERTA-2006-AVI-449 : Vulnérabilité de systrace sous OpenBSD
- CERTA-2006-AVI-450 : Vulnérabilité dans le noyau Linux 24.x
- CERTA-2006-AVI-451 : Multiples vulnérabilités dans IBM WebSphere
- CERTA-2006-AVI-452 : Vulnérabilité dans Cahier de Texte

L'alerte suivante a également été mise à jour suite à la publication des bulletins de sécurité Microsoft :

- CERTA-2006-ALE-011-006 : Multiples vulnérabilités de produits Microsoft

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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>

8 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.

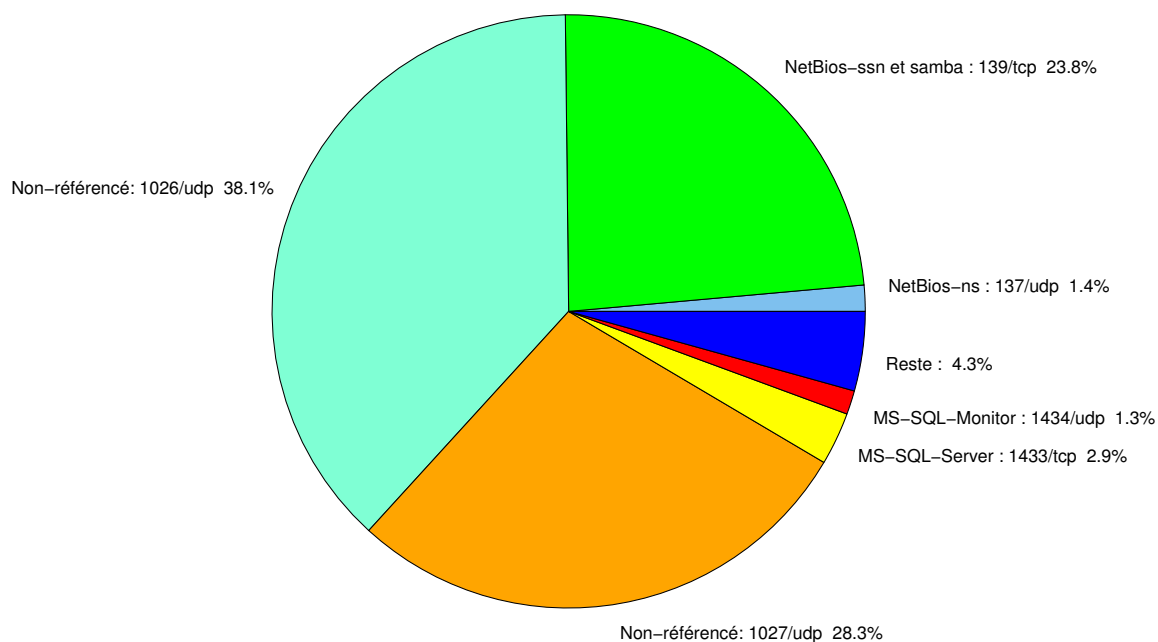


FIG. 1: Répartition relative des ports pour la semaine du 05.10.2006 au 12.10.2006

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	38.05
1027/udp	28.26
139/tcp	23.75
1433/tcp	2.88
137/udp	1.42
1434/udp	1.29
3306/tcp	0.89
80/tcp	0.84
135/tcp	0.7
4899/tcp	0.62
25/tcp	0.32
3128/tcp	0.28
22/tcp	0.15
15118/tcp	0.14
1080/tcp	0.09
143/tcp	0.03
9898/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

13 octobre 2006 version initiale.