



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 10 novembre 2006
N° CERTA-2006-ACT-045

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-45

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-045>

Gestion du document

Référence	CERTA-2006-ACT-045
Titre	Bulletin d'actualité 2006-45
Date de la première version	10 novembre 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-045.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-045/>

1 Activité en cours

1.1 Défiguration

Le CERTA a traité cette semaine un cas de défiguration dans lequel les attaquants ont une nouvelle fois utilisé une faille par injection de code. Le ou les intrus ont trouvé le site par le biais d'une recherche ciblée sur un moteur de recherche. Ils ont ensuite testé le contrôle, par le site, du contenu des variables passées en paramètre. L'une, au moins, de ces variables n'était pas protégée. Ce paramètre ne devrait contenir être qu'un entier, hors dans les journaux du serveur web nous avons constaté que derrière l'entier les attaquants ont pu ajouter du code SQL qui a été interprété par le serveur. Plus concrètement, la valeur du paramètre attendue était "ID=1", mais a été remplacée par "ID=1 update TABLE set CHAMPS=***MESSAGE***";.

Ils ont pu, alors, insérer leur message dans la base de données du site web.

Afin d'éviter cette attaques il aurait suffi de contrôler que la valeur passée au paramètre ID était un entier compris dans des bornes raisonnables.

Recommandations :

Cette compromission rappelle une nouvelle fois l'importance de vérifier la valeur, le contenu et la cohérence des paramètres avant leur traitement.

1.2 Des responsabilités

Le CERTA rappelle, suite à un incident ayant été traité cette semaine, que des responsabilités particulières s'imposent quand un site Internet offre des services en ligne. De manière générale, il est important de garder à l'esprit certains articles de loi, afin d'administrer le site en conséquence. Parmi eux :

– Art. 226-17 du Code Pénal :

"Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende."

– Art 34 de la loi n°78-17 du 6 janvier 1978 (informatique et libertés), modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004 :

"Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis à vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés."

2 Bulletins de sécurité et Firefox 2.0

Le projet Mozilla a annoncé publiquement le 24 octobre 2006 la version 2 du Navigateur Internet Firefox version 2.

En l'absence d'information sur les corrections apportées dans la version 2 définitive et dans la mesure où la branche 1.5 de Firefox est encore maintenue, le CERTA avait recommandé d'attendre un peu avant de déployer la version 2.

Cette semaine, Mozilla a publié trois avis de sécurité qui ont conduit à l'apparition de la version 1.5.0.8. Les avis font également mention de la version 2.0, et des corrections qui y ont été apportées.

La version 2.0 de Firefox est donc maintenue, et peut *a fortiori* être utilisée, en remplacement de la version 1.5.0.8. Cette dernière reste cependant toujours valable et actualisée.

Documentation :

– Avis du CERTA CERTA-2006-AVI-482 du 09 novembre 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-482/>

3 Vulnérabilités de Windows

Le CERTA a fait mention dans le bulletin d'actualité CERTA-2006-ACT-043 de l'existence d'une vulnérabilité qui serait exploitable via le navigateur Internet Explorer 7.

Il est apparu que cette vulnérabilité n'est pas directement liée à cette nouvelle version du navigateur de Microsoft, mais réside dans la gestion des redirections `mhtml`. Celles-ci sont effectuées au moyen de la librairie `inetcomm.dll`, un composant du client de messagerie Outlook.

La vulnérabilité devrait être corrigée prochainement. Dans l'attente du correctif, le CERTA rappelle quelques bonnes pratiques à appliquer :

- le client de messagerie doit être configuré pour ne recevoir que des courriels au format texte ;
- le client de messagerie doit être configuré pour envoyer par défaut des courriels au format texte ;
- Les activeX et le Javascript doivent être désactivés par défaut au cours de l'utilisation d'Internet Explorer. Leur activation doit être ponctuelle et maîtrisée.

Documentation :

- Note d'information du CERTA CERTA-2006-INF-002, « Mesures de prévention relatives à la messagerie » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/>

4 Recommandations concernant les supports de stockage USB

Les périphériques USB (pour Universal Serial Bus) occupent actuellement une place prépondérante dans l'univers de l'appareillage informatique. Ils peuvent être de tout type, comme par exemple un support de données amovible (clé USB, lecteur de musique au format MP3, etc).

De part leur facilité d'installation, ces périphériques s'échangent très facilement d'une machine à une autre. Cependant, cette opération présente des risques, aussi bien pour le périphérique que pour l'ordinateur d'accueil.

Du fait de la simplicité et de la furtivité des attaques basées sur ces échanges, il est important de prendre des mesures préventives. Il n'est bien sûr pas question de remettre en cause l'utilité de l'USB, notamment les différents périphériques de stockage, mais certaines considérations doivent être prises avant leur utilisation, que ce soit pour l'utilisateur ou l'administrateur.

Le CERTA a publié cette semaine la note d'information CERTA-2006-INF-006, présentant les risques et des recommandations à ce sujet.

Documentation :

- Note d'information du CERTA CERTA-2006-INF-006, « Risques associés aux clés USB » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>

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 02 et le 09 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>

7 Rappel des avis et mises à jour émis

Durant la période du 03 au 09 novembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-470 : Vulnérabilité sur le produit CSA de CISCO
- CERTA-2006-AVI-471 : Vulnérabilité OpenSSL sur les produits Nortel

- CERTA-2006-AVI-472 : Plusieurs vulnérabilités dans les produits Sophos
- CERTA-2006-AVI-473 : Vulnérabilité dans IBM Informix Dynamic Server (IDS)
- CERTA-2006-AVI-474 : Vulnérabilité dans Novell eDirectory
- CERTA-2006-AVI-475 : Multiples vulnérabilités dans HP System Management Homepage
- CERTA-2006-AVI-476 : Multiples vulnérabilités dans HP-UX VirtualVault et HP-UX Webproxy
- CERTA-2006-AVI-477 : Vulnérabilités dans SAP
- CERTA-2006-AVI-478 : Vulnérabilité du noyau Linux avec IPv6
- CERTA-2006-AVI-479 : Vulnérabilité dans Microsoft Visual Studio
- CERTA-2006-AVI-480 : Vulnérabilité des drivers NVidia
- CERTA-2006-AVI-481 : Vulnérabilité dans PHP
- CERTA-2006-AVI-482 : Vulnérabilités des produits Mozilla
- CERTA-2006-AVI-483 : Vulnérabilité dans FreeBSD
- CERTA-2006-AVI-484 : Multiples vulnérabilités de Cisco Secure Desktop
- CERTA-2006-AVI-485 : Vulnérabilité dans le module pam_ldap
- CERTA-2006-AVI-486 : Vulnérabilité sur OpenSSH
- CERTA-2006-AVI-487 : Multiples vulnérabilités dans Lotus Domino pour Linux
- CERTA-2006-AVI-488 : Vulnérabilités dans la bibliothèque imlib2

Pendant cette période, les avis suivants ont été mis à jour :

- CERTA-2006-AVI-454-002 : Vulnérabilités dans Clam Antivirus (ajout des bulletins de sécurité Gentoo, Debian, Suse et Mandriva)
- CERTA-2006-AVI-465-001 : Multiples vulnérabilités dans PostgreSQL (ajout du bulletin de sécurité de Mandriva)

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.

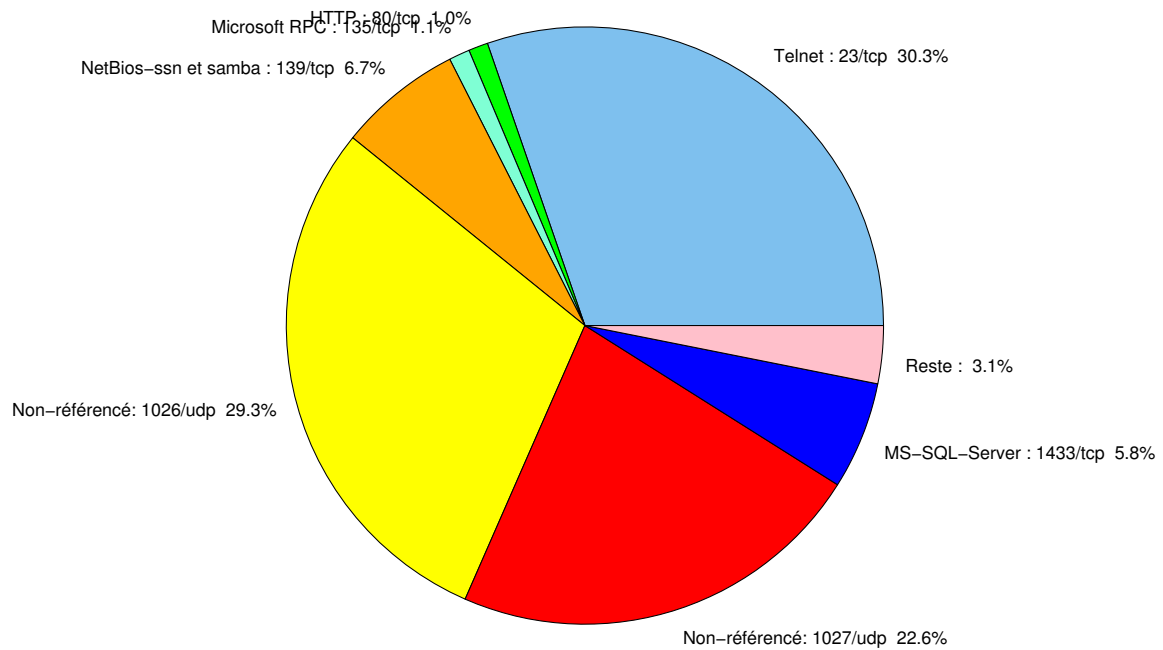


FIG. 1: Répartition relative des ports pour la semaine du 02.11.2006 au 09.11.2006

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
23/tcp	30.29
1026/udp	29.25
1027/udp	22.62
139/tcp	6.7
1433/tcp	5.81
135/tcp	1.12
80/tcp	1.04
137/udp	0.74
1434/udp	0.5
1080/tcp	0.47
4899/tcp	0.34
22/tcp	0.27
3306/tcp	0.18
3128/tcp	0.17
25/tcp	0.1
15118/tcp	0.06
5554/tcp	0.05
9898/tcp	0.02
143/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

10 novembre 2006 version initiale.