Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 octobre 2006
N° CERTA-2006-ACT-043

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-43

Gestion du document

Référence	CERTA-2006-ACT-043
Titre	Bulletin d'actualité 2006-43
Date de la première version	27 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-043.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-043/

1 Activité en cours

Le CERTA a été informé de nombreuses tentatives d'attaques en « force brute » sur des serveurs FTP. Le principe est le même que pour SSH, il s'agit de tester de nombreuses combinaisons d'identifiants et de mots de passe, jusqu'à obtention d'un compte. La récupération d'un tel compte permet d'utiliser le serveur comme zone de stockage de fichiers (*warez*). Si la machine attaquée fait également office de serveur HTTP, il est possible pour les intrus d'utiliser le compte FTP pour mettre en place des sites de filoutage (*phishing*).

Recommandations :

Il est recommandé aux administrateurs de vérifier la robustesse des mots de passe utilisés sur leurs machines et de consulter les journaux afin de s'assurer qu'aucune connexion douteuse n'a été effectuée.

2 De nouvelles versions de navigateurs

2.1 Firefox 2.0

Le projet Mozilla a publié le 24 octobre 2006 la version 2 du Navigateur Internet `Firefox version 2`. Or, la dernière pré-version de `Firefox 2` à savoir la « Release Candidate 3 » comportait probablement plusieurs vulnérabilités. 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 recommande de ne pas déployer pour le moment Firefox 2 en attendant de plus amples précisions.

2.2 Internet Explorer 7

Microsoft a sorti il y a quelques jours une version définitive d'Internet Explorer 7 (IE7). Celle-ci n'est pas encore disponible en français, mais plusieurs sites Web se sont faits écho de cette sortie.

Le CERTA recommande cependant de patienter encore, avant d'installer et d'utiliser ce logiciel. A ce jour, deux vulnérabilités non corrigées distinctes ont été identifiées dans ce dernier :

- la première vulnérabilité concerne un ActiveX particulier nommé `Msxml2.XMLHTTP` . Une personne malveillante pourrait placer un script dans une page afin de créer un objet ActiveX Msxml2.XMLHTTP. Cela lui permettrait d'accéder à des pages qui ne sont pas autorisées, ou à récupérer des informations contextuelles sur l'utilisateur. Le CERTA s'est rendu compte que le code d'exploitation fonctionne aussi, bien que les ActiveX sous IE7 soient désactivés. En effet, l'option avancée *« Enable native XMLHTTP Support »* ne prend pas en compte ce choix.
- la seconde vulnérabilité consiste à afficher une fenêtre surgissante (*pop-up*) avec une adresse dans la barre d'affichage qui n'est pas correcte. Cette vulnérabilité peut être facilement exploitée dans le cadre d'attaques par filoutage (*phishing*).

Après considération de ces deux vulnérabilités moins d'une semaine après la sortie d'IE7, il est préférable de patienter avant d'utiliser ce navigateur. De nouvelles versions (dont une en français) devraient apparaître dans les prochaines semaines.

Documentation :

- Bloc-notes du centre de sécurité Microsoft, mentionnant les deux vulnérabilités précédentes :
  http://blogs.technet.com/msrc/

3 Adobe Flash Player

Une vulnérabilité, non corrigée et confirmée par l'éditeur, est présente dans le visionneur `Flash Player` de Adobe. Cette vulnérabilité permettrait à l'attaquant de modifier à la volée l'entête des requêtes `HTTP` relative à l'objet `Flash` et ce à l'insu de l'utilisateur. En modifiant cet entête, il est possible, par exemple, d'engendrer des requêtes `HTTP` non-sollicitées. Seule la dernière version « Beta » (nommée `beta_100406`) dudit logiciel corrige le problème. En l'absence de version stable corrigée, le CERTA recommande de ne pas utiliser le visionneur `Flash Player` en l'état et d'attendre la mise à jour finale de l'éditeur.

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 19 et le 26 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 20 au 26 octobre 2006, le CERTA a émis les avis suivants :

– CERTA-2006-AVI-457 : Multiples vulnérabilités sur les produits Oracle
– CERTA-2006-AVI-458 : Vulnérabilité dans HP CIF Server
– CERTA-2006-AVI-459 : Vulnérabilité dans la bibliothèque graphique Qt
– CERTA-2006-AVI-460 : Vulnérabilité dans Kaspersky Anti-Virus
– CERTA-2006-AVI-461 : Vulnérabilité dans HP Tru64 UNIX dtmail
– CERTA-2006-AVI-462 : Multiples vulnérabilités dans Novell eDirectory
– CERTA-2006-AVI-463 : Vulnérabilité dans certains produits Symantec
– CERTA-2006-AVI-464 : Multiples vulnérabilités dans Drupal
– CERTA-2006-AVI-465 : Multiples vulnérabilités dans PostgreSQL
– CERTA-2006-AVI-466 : Vulnérabilités dans Winamp
– CERTA-2006-AVI-467 : Multiples vulnérabilités dans les produits Blue Coat
– CERTA-2006-AVI-468 : Vulnérabilité dans Cisco Security Agent

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

– CERTA-2006-AVI-382-001 : Vulnérabilité dans Webmin et Usermin
(ajout du bulletin Debian et de la référence CVE)
– CERTA-2006-AVI-397-001 : Plusieurs vulnérabilités dans Xorg X11 et XFree86
(ajout de la référence au bulletin de sécurité Avaya.)
– CERTA-2006-AVI-430-001 : Vulnérabilités dans CA BrightStor Arcserve Backup
(ajout de la référence au nouveau bulletin CA du 19 octobre 2006)
– CERTA-2006-AVI-435-001 : Vulnérabilité dans Python
(ajout de la référence au bulletin de sécurité Debian)
– CERTA-2006-AVI-459-001 : Vulnérabilité dans la bibliothèque graphique Qt
(ajout de la référence au bulletin de sécurité Ubuntu)

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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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 règlementaire, 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 inexpliqués 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.

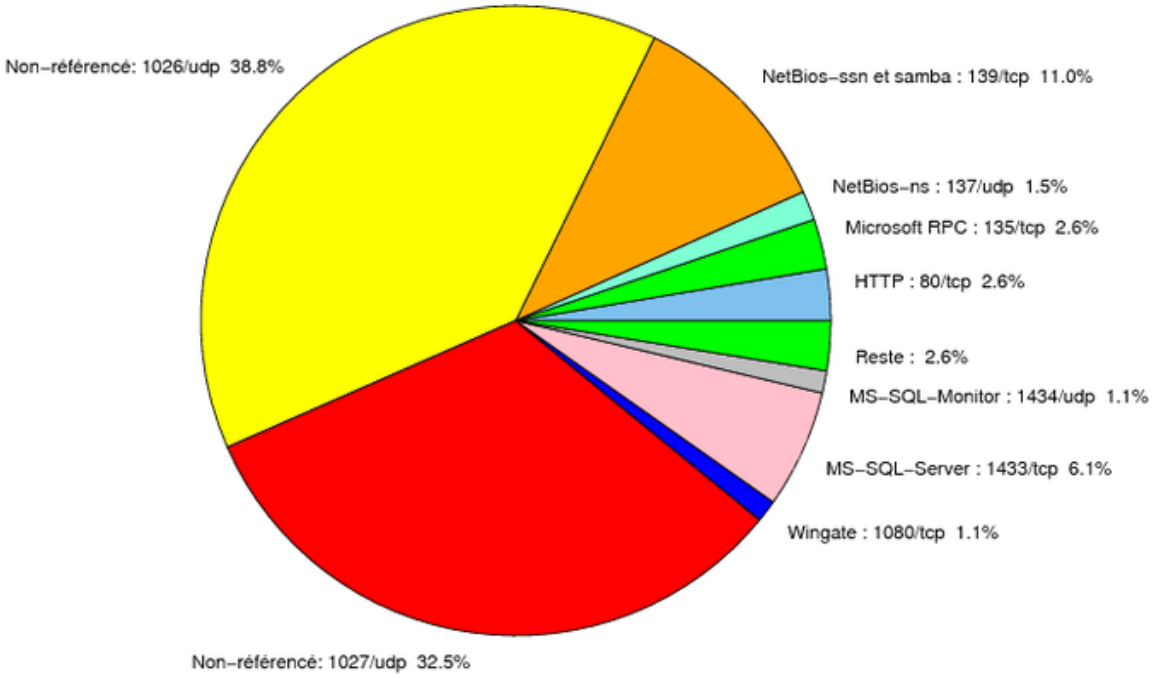

FIG. 1: Répartition relative des ports pour la semaine du 19.10.2006 au 26.10.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE

2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
1026/udp	38.83
1027/udp	32.51
139/tcp	11.03
1433/tcp	6.07
80/tcp	2.63
135/tcp	2.56
137/udp	1.5
1434/udp	1.14
1080/tcp	1.13
4899/tcp	0.84
25/tcp	0.35
22/tcp	0.32
3306/tcp	0.23
3128/tcp	0.19
21/tcp	0.1
6129/tcp	0.09
3389/tcp	0.08
143/tcp	0.06
443/tcp	0.05
5554/tcp	0.03
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

27 octobre 2006 version initiale.