Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 avril 2006
N° CERTA-2006-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-15

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-015

Gestion du document

Référence	CERTA-2006-ACT-015
Titre	Bulletin d'actualité 2006-15
Date de la première version	14 avril 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-015.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-015/

1 Activité en cours

1.1 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 30 mars et le 06 avril 2006.

2 Attaques sur Horde Application Framework 3

Le CERTA a été informé d'attaques visant une vulnérabilité du service *Help Viewer* de *Horde Application Framework 3*. Ces attaques ont commencé au début du mois d'avril et ont augmenté depuis la publication sur l'Internet d'outils permettant l'exploitation automatique de la vulnérabilité. *Horde Application Framework* est utilisé par de nombreuses applications, notamment par le webmail *IMP*.

La vulnérabilité ne concerne que les versions 3 de *Horde Application Framework*. Elle permet d'exécuter des commandes directement sur le serveur par le biais d'adresses réticulaires *URL* habilement constituées. La tentative d'exploitation de cette vulnérabilité laisse des traces flagrantes dans les journaux de connexions.

Recommandations :

Le CERTA suggère d'appliquer le correctif pour *Horde Application Framework 3* conformément à la politique de sécurité. La mise en place d'un filtrage en sortie permet, dans certains cas, de réduire la portée des attaques, notamment pour empêcher les intrus de télécharger leurs propres outils sur les serveurs compromis. Si vous constatez des tentatives d'attaque sur cet applicatif, veuillez le signaler auprès du CERTA.

3 Mise à jour d'Internet Explorer et ActiveX

Microsoft a publié le 11 avril 2006 un ensemble de mises à jour, dont le bulletin MS06-013 qui concerne le navigateur Internet Explorer. Ce dernier corrige plusieurs vulnérabilités décrites dans l'avis CERTA-2006-AVI-150. Hormis ces corrections, il s'avère que l'installation de la mise à jour modifie le comportement d'Internet Explorer lors de la visite de pages Web utilisant des contrôles ActiveX.

Un contrôle ActiveX fournit un ensemble de méthodes, ou fonctions, pour manipuler les composants COM (pour *Component Object Model*) utilisés par plusieurs applications de Microsoft Windows.

La mise à jour MS06-013 empêche l'exécution de deux contrôles ActiveX dans Internet Explorer, par défaut activés dans les versions courantes du logiciel. Ceci est possible en définissant leur bit d'arrêt (ou *kill bit*) respectif dans le registre de Microsoft Windows. Dans le détail, il s'agit des contrôles référencés :

- IDXTRedirect : 42B07B28-2280-4937-B035-0293FB812781
- IDA3Statics : 542FB453-5003-11CF-92A2-00AA00B8A733

Cette initiative de Microsoft est transitoire, avant une mise à jour plus en profondeur d'Internet Explorer prévue en juin 2006.

Il est important de noter ici que ce changement peut engendrer des problèmes pour toute application ou page Web recourant d'une certaine manière à ces contrôles ActiveX. Certains de ces problèmes sont mentionnés par Microsoft, tels :

- dans les systèmes 64 bits, les paramètres par défaut des favoris et les paramètres avancés d'Internet Explorer sont réinitialisés ;
- il existe certaines incompatibilités avec la barre d'outils Google ;
- les administrateurs ne peuvent plus utiliser le commutateur `/integrate` pour mettre à jour les fichiers d'origine de l'installation de Windows ;
- la mise à jour est incompatible avec le logiciel de gestion *Siebel* dans sa version 7 actuelle.

Des techniques pour corriger les pages Web (afin qu'elles fonctionnent correctement dans les navigateurs mis à jour) sont détaillées sur le site Web de MSDN.

Enfin, il est important de noter que Microsoft fournit un correctif rétroactif, dans le cas où cette dernière engendrerait trop de problèmes. Ce correctif rétroactif est à appliquer une fois que la mise à jour est installée et que la machine a redémarrée.

Références :

- Avis CERTA-2006-AVI-150 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-150/
- Bulletin de sécurité MS06-013 de Microsoft du 11 avril 2006 :
  http://www.microsoft.com/technet/security/Bulletin/ms06-013.mspx
- Mise à jour de Microsoft Internet Explorer et conséquences sur les contrôles ActiveX :
  http://support.microsoft.com/kb/912945
- Comment faire pour empêcher l'exécution d'un contrôle ActiveX dans Internet Explorer :
  http://support.microsoft.com/kb/240797
- Site de MSDN en français :
  http://msdn1.microsoft.com/fr-fr/

4 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 pour 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
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
  http://www.auscert.org.au/render.html?it=1935

5 Rappel des avis et mises à jour émis

Durant la période du 07 au 13 avril 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-140 : Multiples vulnérabilités dans ClamAV
- CERTA-2006-AVI-141 : Vulnérabilités dans Dokeos
- CERTA-2006-AVI-142 : Vulnérabilité dans phpMyAdmin
- CERTA-2006-AVI-143 : Vulnérabilités dans Claroline
- CERTA-2006-AVI-144 : Vulnérabilités dans phpBB
- CERTA-2006-AVI-145 : Vulnérabilités sur CACTI
- CERTA-2006-AVI-146 : Vulnérabilité dans Mailman
- CERTA-2006-AVI-147 : Vulnérabilité sur les commutateurs 11500 CISCO
- CERTA-2006-AVI-148 : Vulnérabilité dans l'explorateur de Microsoft Windows
- CERTA-2006-AVI-149 : Vulnérabilité dans Microsoft Outlook Express
- CERTA-2006-AVI-150 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2006-AVI-151 : Vulnérabilité sur la fonction Microsoft Data Access Components (MDAC)
- CERTA-2006-AVI-152 : Vulnérabilité dans Microsoft FrontPage
- CERTA-2006-AVI-153 : Vulnérabilité dans Horde Application Framework 3
- CERTA-2006-AVI-154 : Vulnérabilité de LDAP2 sous Sun Solaris

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2006-AVI-129-001 : Vulnérabilité dans Samba
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2006-AVI-140-001 : Multiples vulnérabilités dans ClamAV
  (ajout des références aux bulletins de sécurité Mandriva, Gentoo et FreeBSD)
- CERTA-2006-AVI-139-001 : Vulnérabilité d'OpenVPN
  (ajout de la référence au bulletin de sécurité Mandriva)
- CERTA-2006-AVI-142-001 : Vulnérabilité dans phpMyAdmin
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2006-AVI-144-001 : Vulnérabilités dans phpBB
  (mise à jour de la section Risque, modification de la section Documentation et ajout des références CVE)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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

7 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.

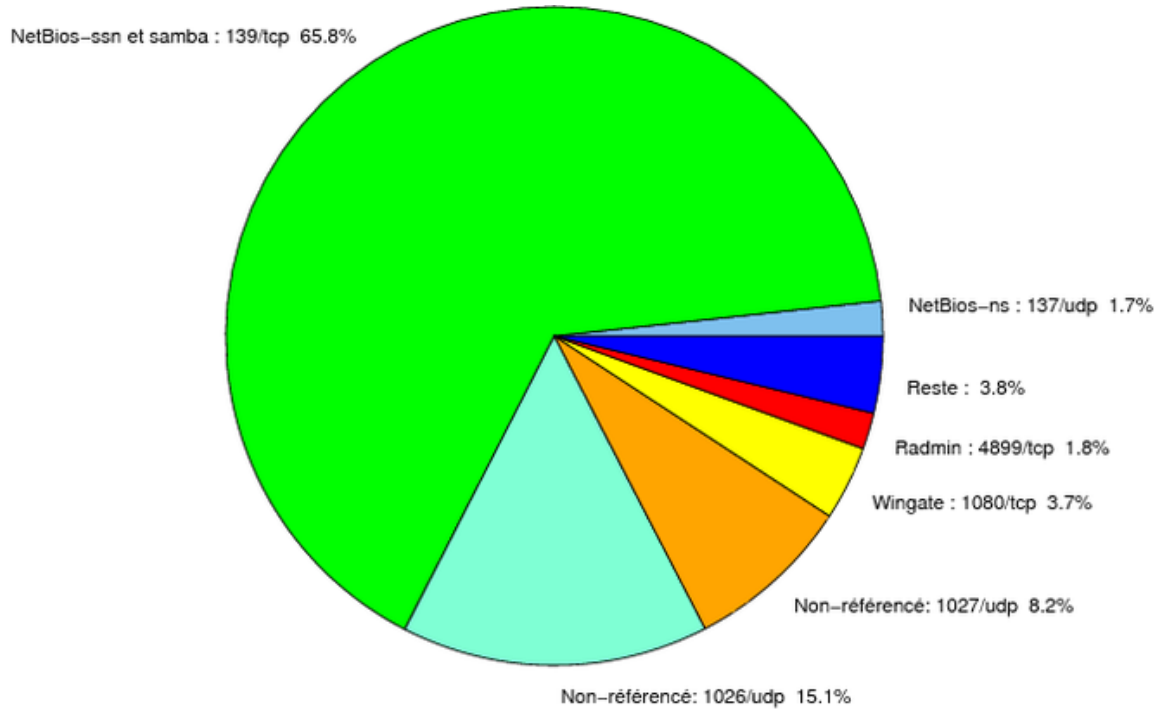

FIG. 1: Répartition relative des ports pour la semaine du 06.04.2006 au 13.04.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT

80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CER
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070 6101	TCP TCP	BrightStor ARCserve/Enterprise Backup Veritas Backup Exec	– –	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CERT
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	65.77
1026/udp	15.1
1027/udp	8.2
1080/tcp	3.65
4899/tcp	1.78
137/udp	1.7
1434/udp	0.86
22/tcp	0.64
1433/tcp	0.59
80/tcp	0.46
15118/tcp	0.4
3128/tcp	0.12
3306/tcp	0.11
143/tcp	0.08
3127/tcp	0.04
2100/tcp	0.03
389/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

14 avril 2006 version initiale.