Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 août 2006
N° CERTA-2006-ACT-034

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-34

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-034`

Gestion du document

Référence	CERTA-2006-ACT-034
Titre	Bulletin d'actualité 2006-34
Date de la première version	25 août 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-034.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-034/

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 17 et le 24 août 2006.

2 Alerte CERTA-2006-ALE-010 concernant Internet Explorer

Le CERTA a publié mercredi 23 août 2006 une alerte concernant Internet Explorer, correspondant au bulletin de sécurité Microsoft numéro 923762 (CERTA-2006-ALE-010). En voici brièvement l'historique :

Des vulnérabilités ont été identifiées dans le navigateur Internet Explorer, puis corrigées par le bulletin Microsoft MS06-042 en date du 08 août 2006 (CERTA-2006-AVI-340). Cependant, il est apparu au cours des semaines suivantes que l'application du correctif introduit une nouvelle vulnérabilité et peut être la cause d'un déni de service lors de la visite de pages Web sous Internet Explorer. Plus exactement, la visite de pages par le biais du protocole HTTP1.1 et mettant en œuvre de la compression de données pouvait perturber le fonctionnement du

système, si le navigateur était en version SP1. Cette version est fournie par défaut avec les systèmes d'exploitation Windows 2000 SP4 et Windows XP SP1.

Une mise à jour du correctif MS06-042 était attendue pour mardi 22 août 2006. Microsoft a annoncé ce jour-là que la diffusion sur l'Internet d'un code d'exploitation visant à profiter de la vulnérabilité nouvellement introduite repousse cette date à une autre non précisée.

Le CERTA, conformément à sa définition d'une alerte (situation critique pour laquelle il n'existe pas de solution idéale, par exemple un avertissement correspondant à une vulnérabilité non corrigée mais dont le code d'exploitation est connu) a publié celle de référence CERTA-2006-ALE-010 liée à ce problème.

A la date de rédaction de ce document, Microsoft a rendu public la mise à jour du correctif. Le CERTA vient donc d'actualiser son alerte, et conseille vivement d'appliquer celui-ci sur les systèmes employant Internet Explorer 6 SP1.

3 Sur l'usage de composants et modules PHP

Certaines applications populaires, comme le forum phpBB ou encore les gestionnaires de contenu Mambo et Joomla!, sont modulaires. Il est possible d'ajouter des composants optionnels. Ces modules sont souvent mis à disposition en téléchargement sur le site de l'éditeur de l'application (par exemple, pour phpBB, sur la page `http://www.phpbb.com/mods/`).

Depuis plusieurs semaines, des vulnérabilités affectant de tels composants sont régulièrement rendues publiques. D'une manière générale, nous constatons qu'il s'agit d'une même vulnérabilité de type `php include` commune à beaucoup de modules d'une même application. Ces vulnérabilités ne sont pas toutes corrigées.

Le CERTA ne publie aucun avis concernant ces vulnérabilités.

Recommandations :

Le CERTA recommande de désinstaller ces composants s'ils ne sont pas d'une réelle utilité. Il existe souvent un contournement provisoire pour les failles de type `php include`. Celui-ci consiste à positionner, dans la mesure du possible, la variable `register_globals` à `off` dans le fichier de configuration de PHP. Il est possible également de positionner la variable `magic_quotes_gpc` à `on` (l'effet de cette manipulation est expliquée sur la page `http://fr2.php.net/magic_quotes`). Attention toutefois, malgré ces mesures de contournement, la vulnérabilité reste présente tant qu'un correctif n'est pas appliqué.

L'exploitation de vulnérabilités de type `php include` repose sur le fait que le serveur vulnérable puisse télécharger du code. Le CERTA recommande donc de configurer les règles de filtrage du réseau pour empêcher le serveur Web de se connecter sur d'autres sites Web, hormis ceux légitimes.

4 Migration vers des systèmes maintenus

Des vulnérabilités sont régulièrement identifiées, et certaines peuvent affecter des sytèmes qui ne font plus l'objet de suivi de la part des éditeurs. A valeur d'exemple, le CERTA a publié en août 2006 un avis concernant le système Microsoft et plus précisément le service `Serveur` (CERTA-2006-AVI-338). Il semblerait que le code d'exploitation actuellement en circulation dans l'Internet affecterait aussi les machines utilisant Windows NT4.0. Microsoft a arrêté de maintenir cette version fin 2004.

Un document du CERTA énumère de tels systèmes obsolètes :

http://www/certa.ssi.gouv.fr/CERTA-INF-2005-003/

Les correctifs n'existent plus pour ces systèmes, qui restent néanmoins vulnérables aux attaques, parfois récentes. Le CERTA rappelle donc qu'il ne publie pas d'avis sur les produits qui ne sont plus maintenus. Il est important de faire régulièrement l'inventaire des systèmes d'information à administrer, de procéder à une analyse de risques, et d'envisager suffisamment tôt la migration des systèmes critiques.

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
– 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 18 au 24 août 2006, le CERTA a émis les avis suivants :

– CERTA-2006-AVI-363 : Multiples vulnérabilités dans HP-UX
– CERTA-2006-AVI-364 : Vulnérabilité du contrôle ActiveX IBM eGatherer
– CERTA-2006-AVI-365 : Vulnérabilité dans Symantec Enterprise Security Manager
– CERTA-2006-AVI-366 : Multiples vulnérabilités dans Horde Application Framework 3
– CERTA-2006-AVI-367 : Multiples vulnérabilités dans PHP
– CERTA-2006-AVI-368 : Multiples vulnérabilités dans Horde IMP
– CERTA-2006-AVI-369 : Vulnérabilités dans les concentrateurs Cisco VPN 3000
– CERTA-2006-AVI-370 : Vulnérabilité dans ppp
– CERTA-2006-AVI-371 : Vulnérabilité dans les produits pare-feux de Cisco

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

– CERTA-2006-AVI-216-004 : Vulnérabilités dans PostgreSQL
(ajout de la référence au bulletin de sécurité FreeBSD)
– CERTA-2006-AVI-312-003 : Multiples vulnérabilités dans les produits Mozilla
(ajout de la référence au bulletin de sécurité)
– CERTA-2006-AVI-315-002 : Vulnérabilité dans Apache httpd
(ajout des références IBM HTTP Server PK29154 et PK29156)
– CERTA-2006-AVI-329-001 : Multiples vulnérabilités dans la bibliothèque libTIFF
(ajout des références aux bulletins de sécurité Gentoo, Mandriva et Avaya)
– CERTA-2006-AVI-336-001 : Vulnérabilité dans ClamAV
(ajout de la référence au bulletin de sécurité Debian)
– CERTA-2006-AVI-350-001 : Vulnérabilités dans Mysql
(ajout de la référence au bulletin de sécurité FreeBSD)
– CERTA-2006-AVI-351-002 : Vulnérabilité de SquirrelMail
(ajout du bulletin de sécurité Debian)
– CERTA-2006-AVI-356-001 : Plusieurs vulnérabilités dans MIT Kerberos krb5
(ajout des bulletins de sécurité Ubuntu, Debian, Fedora, RedHat et Mandriva)
– CERTA-2006-AVI-367-001 : Multiples vulnérabilités dans PHP
(ajout des références aux bulletins de SUSE et Mandriva)

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.

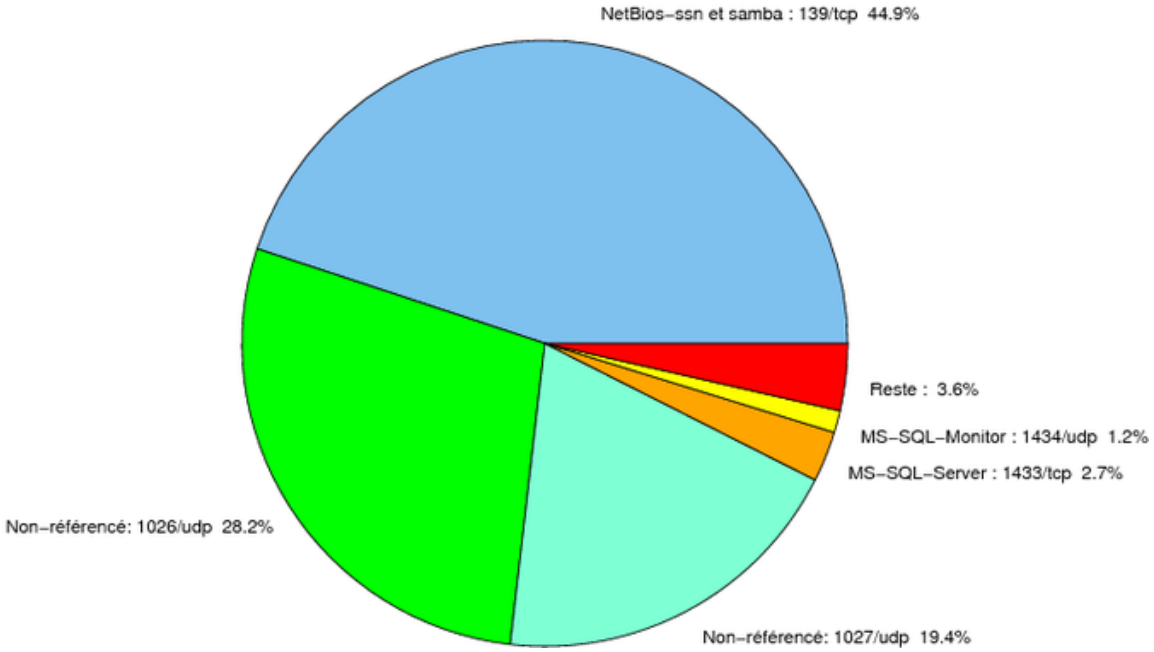

FIG. 1: Répartition relative des ports pour la semaine du 17.08.2006 au 24.08.2006

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
139/tcp	44.94
1026/udp	28.23
1027/udp	19.38
1433/tcp	2.69
1434/udp	1.17
4899/tcp	0.79
137/udp	0.73
1080/tcp	0.46
80/tcp	0.44
25/tcp	0.18
3128/tcp	0.14
15118/tcp	0.12
143/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

25 août 2006 version initiale.