Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 décembre 2005
N° CERTA-2005-ACT-048

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-48

Gestion du document

Référence	CERTA-2005-ACT-047
Titre	Bulletin d'actualité n° 2005-48
Date de la première version	02 décembre 2005
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.

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 novembre 2005.

1.2 Vulnérabilité sur de multiples navigateurs

Le 21 novembre le CERTA a publié une alerte (CERTA-2005-ALE-017) concernant une vulnérabilité non corrigée dans le navigateur Microsoft Internet Explorer. Cette vulnérabilité permet l'exécution de code arbitraire sur la machine vulnérable, sans interaction de la part de l'utilisateur. Une démonstration pratique d'exploitation est disponible sur l'Internet mettant en lumière les dangers d'une telle faille. Microsoft a publié un bulletin de sécurité (911302) donnant des détails sur la vulnérabilité, notamment les méthodes de contournement provisoire.
A ce jour, la vulnérabilité n'est toujours pas corrigée. Un correctif devrait être mis à disposition par Microsoft le mardi 13 décembre 2005, à l'occasion des prochaines mises à jour de sécurité Microsoft de décembre 2005. Selon quelques messages dans plusieurs listes de diffusion, il est possible qu'un correctif soit disponible avant cette date, à savoir dans la semaine qui vient.
Mozilla Firefox et Mozilla Suite sont également affectés par cette vulnérabilité, qui permet un déni de service. L'exécution de code arbitraire sous Mozilla Firefox et Mozilla Suite n'est pas avérée.
En attendant un correctif pour Microsoft Internet Explorer, le CERTA précise dans son alerte un certain nombre de

contournements provisoires, au choix : désactiver l'Active Scripting, ne naviguer que sur des sites de confiance ou utiliser un navigateur alternatif autre que Internet Explorer et Mozilla Firefox / Mozilla Suite.

1.3 Incidents traités

1.3.1 Les messages non sollicités

Le CERTA a traité un incident cette semaine concernant un message non sollicité qui n'était pas véritablement du SPAM. Le message en question était envoyé depuis une société spécialisée dans le « e-mailing » qui agit pour le compte de clients. La liste d'adresses électroniques utilisée provenait d'un autre site gérant une liste de membres.

Tous les messages à caractère publicitaire, si ce n'est pas du SPAM, sont normalement issus d'une liste où se trouve votre adresse électronique et pour laquelle vous avez validé la possibilité de recevoir des messages, suite à quoi un message de confirmation doit vous êtes envoyé. Dans les autres cas, l'utilisation de votre adresse n'est pas réglementaire. Si vous souhaitez recevoir de la publicité par message éléctronique, le CERTA vous conseille d'utiliser de multiples adresses électroniques afin d'empêcher que votre adresse électronique professionelle ne soit récupérée pour une utilisation malveillante.

1.3.2 Présence de mots de passe dans le fichier .bash_history

Le CERTA a pu constater, lors de l'analyse de machines compromises, qu'il était possible, pour un intrus ayant obtenu les droits de l'administrateur, de récupérer des mots de passe en clair dans les divers fichiers de l'historique (notamment le fichier `.bash_history`). En effet, certains utilisateurs tapent directement les mots de passe en clair en ligne de commande pour effectuer certaines connexions (c'est souvent le cas pour MySQL ou encore ftp). Cette mauvaise pratique permet aux intrus de récupérer facilement des mots de passe, et ensuite de compromettre d'autres machines, parfois en dehors du périmètre du réseau.

Recommandation :

Il est conseillé aux administrateurs de sensibiliser les utilisateurs sur la divulgation des mots de passe au travers des fichiers de l'historique. Si de telles pratiques étaient en usage sur vos réseaux, il serait préférable de procéder à un changement de ces mots de passe.

2 Liens utiles

- Note d'information pour limiter l'impact du SPAM ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-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

3 Rappel des avis et mises à jour émis

Durant la période du 18 novembre au 1 décembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-463 : Vulnérabilité dans phpMyAdmin
- CERTA-2005-AVI-464 : Vulnérabilité de Lynx
- CERTA-2005-AVI-465 : Vulnérabilité de Mambo
- CERTA-2005-AVI-466 : Vulnérabilité de Netpbm
- CERTA-2005-AVI-467 : Vulnérabilité dans le navigateur Opéra
- CERTA-2005-AVI-468 : Vulnérabilité dans phpSysInfo
- CERTA-2005-AVI-469 : Vulnérabilité de gestionnaire de contenu Zope
- CERTA-2005-AVI-470 : Vulnérabilité du pare-feu PIX de CISCO
- CERTA-2005-AVI-471 : Multiples vulnérabilités du logiciel Joomla!
- CERTA-2005-AVI-472 : Vulnérabilité dans le logiciel FUSE
- CERTA-2005-AVI-473 : Vulnérabilité sur CISCO CSA
- CERTA-2005-AVI-474 : Multiples vulnérabilités dans la machine virtuelle

– CERTA-2005-AVI-475 : Vulnérabilité dans pcAnywhere
– CERTA-2005-AVI-476 : Multiples vulnérabiltés dans Mac OS X

Pendant cette même période, la mise à jour suivante a été publiée :

– CERTA-2005-AVI-180-002 : Vulnérabilités dans Qpopper (ajout référence au bulletin de sécurité FreeBSD)

– CERTA-2005-AVI-393-001 : Multiples vulnérabilités de WinRAR (ajout de la référence au bulletin de sécurité Gentoo)

– CERTA-2005-AVI-407-002 : Vulnérabilité dans la bibliothèque libcURL (ajout des références aux bulletins de sécuritiés Gentoo et RedHat)

– CERTA-2005-AVI-428-001 : Multiples vulnérabilités dans PHP (ajout des références CVE et des références aux bulletins de sécurité RedHat, Gentoo et Mandriva)

– CERTA-2005-AVI-438-001 : Vulnérabilité du logiciel Macromedia Flash (ajout de la référence au bulletin de sécurité Eeye et des mises à jour de sécurité FreeBSD)

– CERTA-2005-AVI-452-001 : Vulnérabilité des clients de messagerie Sylpheed et Sylpheed-Claws (ajout de la référence au bulletin de sécurité Gentoo)

– CERTA-2005-AVI-461-001 : Vulnérabilité des blibliothèques graphiques GTK+2 (ajout des références aux bulletins de sécurité Mandriva et Gentoo)

– CERTA-2005-AVI-434-001 : Vulnérabilité dans l'utilitaire unzip (ajout des références aux bulletins de sécurité Debian et Ubuntu)

– CERTA-2005-AVI-452-002 : Vulnérabilité des clients de messagerie Sylpheed et Sylpheed-Claws (ajout des références aux bulletins de sécurité Debian DSA-906 et DSA-908)

– CERTA-2005-AVI-105-005 : Vulnérabilité de libexif (ajout référence au bulletin de sécurité Sun #102041)

– CERTA-2005-AVI-190-002 : Vulnérabilité de divers outils gérant le format ELF (ajout de la référence au bulletin de sécurité Mandriva)

– CERTA-2004-AVI-351-001 : Vulnérabilité dans Ghostscript (ajout des références aux bulletins de sécurité FreeBSD)

– CERTA-2005-AVI-438-002 : Vulnérabilité du logiciel Macromedia Flash Player (ajout de la référence au bulletin de sécurité Gentoo GLSA 200511-21 et de la réference CVE CAN-2005-2628)

– CERTA-2005-AVI-461-002 : Vulnérabilité des blibliothèques graphiques GTK+2 (ajout de la référence au bulletin de sécurité Debian)

– CERTA-2005-AVI-461-003 : Vulnérabilité des blibliothèques graphiques GTK+2 (ajout de la référence au bulletin de sécurité Debian DSA-913)

– CERTA-2005-AVI-465-001 : Vulnérabilité de Mambo (ajout de la référence à la mise à jour FreeBSD)

– CERTA-2005-AVI-466-001 : Vulnérabilité de Netpbm (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:217)

– CERTA-2005-AVI-467-001 : Vulnérabilité dans le navigateur Opéra (ajout des références aux mises à jour FreeBSD et à la référence CVE CAN-2005-3750)

4 Actions suggérées

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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

5 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.

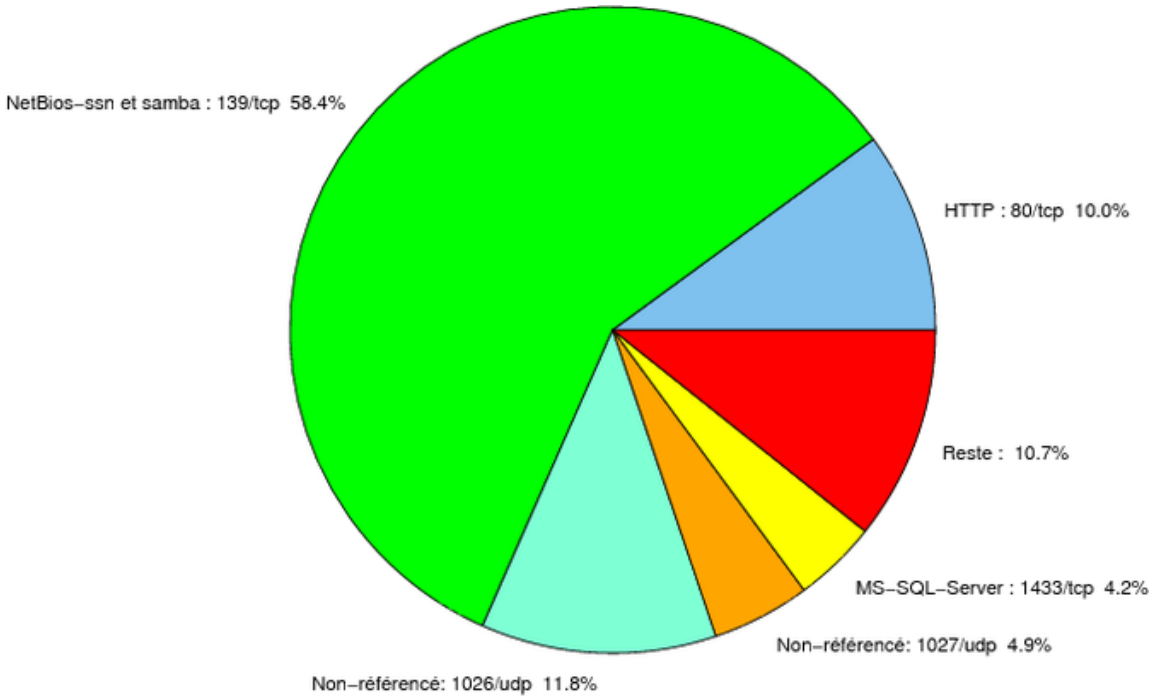

FIG. 1: Répartition relative des ports pour la semaine du 24.10.2005 au 30.11.2005

Port	Protocole	Service	Porte dérobée	Référ
21	TCP	FTP	–	–
22	TCP	SSH	–	http:/
23	TCP	Telnet	–	http:/ http:/
25	TCP	SMTP	–	http:/
42	TCP	WINS	–	http:/
53	UDP	DNS	–	http:/
80	TCP	HTTP	–	http:/ http:/

				http:/
111	TCP	Sunrpc-portmapper	–	http:/
123	TCP	NTP	–	http:/
135	TCP	Microsoft RPC	–	http:/ http:/ http:/
137	UDP	NetBios-ns	–	http:/ http:/
139	TCP	NetBios-ssn et samba	–	http:/ http:/ http:/ http:/ http:/
143	TCP	IMAP	–	http:/ http:/ http:/
389	TCP	LDAP	–	http:/ http:/
443	TCP	HTTPS	–	http:/ http:/
445	TCP	Microsoft-smb	– zotob	http:/ http:/ http:/ http:/ http:/ http:/
500	UDP	IPSEC sur UDP	–	http:/ http:/ http:/ http:/
544	TCP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-451	
1023	TCP	–	Serveur ftp de Sasser.E	–
1434	UDP	MS-SQL-Monitor	–	http:/
2100	TCP	Oracle XDB FTP	–	http:/
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-371	 http:/ http:/
3306	TCP	MySQL	–	http:/
3389	TCP	Microsoft RDP	–	http:/
4500	UDP	IPSEC sur UDP	–	http:/ http:/ http:/ http:/ http:/
4899	TCP	Radmin	–	–
5631	TCP	PC Annywhere	–	http:/
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http:/
6101	TCP	Veritas Backup Exec	–	http:/
6129	TCP	Dameware Miniremote	–	http:/ http:/
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http:/ http:/
10080	TCP	Amanda	MyDoom	–

11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	58,35
1026/udp	11,79
80/tcp	10,04
1027/udp	4,92
1433/tcp	4,18
137/udp	1,7
1080/tcp	1,62
4899/tcp	1,1
10000/tcp	1
1434/udp	0,98
3128/tcp	0,92
445/tcp	0,61
23/tcp	0,45
22/tcp	0,36
15118/tcp	0,33
6129/tcp	0,28
3306/tcp	0,24
9898/tcp	0,14
5554/tcp	0,12
143/tcp	0,09
42/tcp	0,08
21/tcp	0,06
11768/tcp	0,02
6101/tcp	0,01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

02 décembre 2005 version initiale.