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 février 2005
N° CERTA-2005-ACT-008

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N2005-08

Gestion du document

Référence	CERTA-2005-ACT-008
Titre	Bulletin d'actualité N2005-08
Date de la première version	25 février 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

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 10 et le 17 février 2005.

2 Le « Google Hacking »

Les moteurs de recherche indexent des pages Internet, mises à disposition par l'intermédiaire de serveurs web, en vue d'une recherche ultérieure par des utilisateurs à l'aide d'un navigateur Internet et de certains mots clefs.

Ces moteurs de recherche sont de plus en plus précis et exhaustifs.

Les techniques d'indexation de pages Internet comprennent entre autre le parcours exhaustif des sites Internet en suivant les différents liens se trouvant dans le code source des pages renvoyées par le serveur web.

Google est actuellement le moteur de recherche reconnu comme le plus efficace et le plus populaire.

A ce jour, si l'on s'en tient à ce qui est mentionné sur la page d'accueil du moteur de recherche Google, plus de 8 milliards de pages Internet sont indexées.

Depuis plusieurs mois, nous assistons à un détournement de certaines des fonctionnalités des moteurs de recherche à des fins malveillantes.

Il est en effet possible, via des requêtes judicieusement construites, d'accéder rapidement à des contenus sensibles ou à des applications vulnérables (webcam en accès non protégé, documents confidentiels, failles de sécurité connues d'un applicatif ...).

Les moteurs de recherche sont ainsi utilisés afin de rechercher des informations sur des serveurs vulnérables.

Des outils graphiques automatiques, couplés à des bases de connaissance mises à jour quotidiennement, sont également disponibles sur l'Internet.

Ceci permet à un utilisateur mal intentionné, à l'aide d'un simple outil ou d'un simple navigateur, d'accéder à des informations sensibles, potentiellement exploitables en vue d'une attaque informatique.

Depuis peu, Google semble avoir réagi contre ce phénomène en masquant certains résultats relatives à certaines requêtes ou en affichant une page d'erreur ("We are sorry...but we can't process your request right now."). Comme toujours dans le monde de la sécurité, il s'agit du jeu du chat et de la souris. A toute parade, une contre-parade. Et ainsi de suite.

Le phénomène va donc probablement se poursuivre, indépendamment de la volonté des moteurs de recherche (Google en première ligne) d'endiguer le phénomène.

Ces techniques de recherche ne laissent aucune trace dans les journaux des applications vulnérables dans la mesure où seul le cache des moteurs de recherche est interrogé. En revanche, l'exploitation d'une vulnérabilité ainsi identifiée va laisser des traces dans les journaux des serveurs concernés. Il est, comme toujours, très important d'analyser périodiquement ces journaux afin de détecter les attaques sur son système d'information.

Il est en outre important de noter que dans la plupart des cas, les flux sont en direction des serveurs web.

Dans ce cas, le pare-feu n'est donc généralement que de peu d'utilité dans la mesure où le flux autorisé (dans la mesure où l'on dispose d'un serveur web) est assimilé à une requête standard (même si malveillante a priori).

Ainsi, il est important de configurer correctement ses serveurs web afin de ne mettre à disposition uniquement l'information voulue et de n'activer uniquement les services désirés.

Ensuite, il est important de mettre à jour tout son système d'information au rythme des découvertes et des publications des vulnérabilités ; ceci de manière d'autant plus rapide que le système est accessible par tout le monde depuis l'Internet.

Il est enfin important de surveiller les informations concernant son système d'information disponibles par le biais des moteurs de recherche, Google en particulier.

3 Rappel des avis et des mises à jour émis

Durant la période du 07 au 11 février 2005, le CERTA a émis l'avis suivant :

- CERTA-2005-AVI-069 : Vulnérabilité de cpio
- CERTA-2005-AVI-070 : Vulnérabilité de GNU enscript
- CERTA-2005-AVI-071 : Vulnérabilité dans les produits ZoneAlarm & Check Point Integrity
- CERTA-2005-AVI-072 : Vulnérabilité du module Apache mod_python
- CERTA-2005-AVI-073 : Vulnérabilité de ht://Dig
- CERTA-2005-AVI-074 : Vulnérabilité de PowerDNS
- CERTA-2005-AVI-075 : Multiples vulnérabilités des systèmes AIX de IBM
- CERTA-2005-AVI-076 : Vulnérabilité de IBM Websphere Application Server
- CERTA-2005-AVI-077 : Multiples vulnérabilités dans IBM DB2
- CERTA-2005-AVI-078 : Vulnérabilité de l'application sympa
- CERTA-2005-AVI-079 : Vulnérabilité de MySQL
- CERTA-2005-AVI-080 : Multiples vulnérabilités de Solaris
- CERTA-2005-AVI-081 : Vulnérabilité de Midnight Commander
- CERTA-2005-AVI-082 : Vulnérabilité de gFTP

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

- CERTA-2004-AVI-370-003 : Vulnérabilités du serveur HTTP Apache
  (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-046-003 : Vulnérabilité de Perl
  (ajout de la référence au bulletin de sécurité Gentoo GLSA 200502-13)
- CERTA-2005-AVI-065-001 : Vulnérabilité dans les produits F-Secure
  (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-066-001 : Vulnérabilité de Mailman
  (ajout de la référence au bulletin de sécurité FreeBSD)

- CERTA-2005-AVI-067-001 : Vulnérabilité de Emacs et XEmacs
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-019-006 : Vulnérabilité dans Xpdf
  (ajout des références aux bulletins de sécurité SGI 20050201-01-U et 20050202-01-U)
- CERTA-2005-AVI-022-004 : Vulnérabilité de Ethereal
  (ajout de la référence au bulletin de sécurité SGI)
- CERTA-2005-AVI-027-002 : Vulnérabilité de Konversation
  (ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:004)
- CERTA-2005-AVI-046-004 : Vulnérabilité de Perl
  (ajout des références aux bulletins de sécurité Gentoo GLSA 200502-13, SUSE SUSE-SR:2005:004 et SGI 20050202-01-U)
- CERTA-2005-AVI-070-001 : Vulnérabilité de GNU enscript
  (ajout de la référence au bulletin de sécurité SGI 20050202-01-U)
- CERTA-2005-AVI-049-001 : Vulnérabilité de PostgreSQL
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:141 et des références CVE CAN-2005-244, CAN-2005-245, CAN-2005-246 et CAN-2005-247)
- CERTA-2005-AVI-063-002 : Vulnérabilité de Python
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:109)
- CERTA-2005-AVI-035-001 : Vulnérabilité de AWStats
  (ajout de la référence au bulletin de sécurité Debian DSA-682 et des références CVE CAN-2005-0116 et CAN-2005-0363)
- CERTA-2005-AVI-042-003 : Multiples vulnérabilités dans Squid
  (ajout des références CVE CAN-2005-0211 et CAN-2005-0241 (nouvelle vulnérabilité), des notes de vulnérabilité de l'US-CERT afférantes, des bulletins de sécurité RedHat et SUSE et de seconds bulletins pour Debian et FreeBSD)
- CERTA-2005-AVI-049-002 : Vulnérabilité de PostgreSQL
  (ajout de la référence au bulletin de sécurité Gentoo GLSA 200502-19)
- CERTA-2005-AVI-066-002 : Vulnérabilité de Mailman
  (ajout des références aux bulletins de sécurité Mandrake MDKSA-2005:037 et SUSE SUSE-SA:2005:007)
- CERTA-2005-AVI-035-002 : Vulnérabilité de AWStats
  (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-066-003 : Vulnérabilité de Mailman
  (ajout de la référence au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-049-003 : Vulnérabilité de PostgreSQL
  (ajout de la référence au bulletin de sécurité Debian DSA-683)
- CERTA-2005-AVI-067-002 : Vulnérabilité de Emacs et XEmacs
  (ajout de la référence aux bulletins de sécurité Gentoo et Mandrake)
- CERTA-2004-AVI-357-003 : Vulnérabilités du lecteur PDF xpdf et de ses dérivés et du service d'impression CUPS
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:066)
- CERTA-2004-AVI-405-004 : Multiples vulnérabilités de PHP
  (ajout référence au bulletin de sécurité Red Hat RHSA-2005-032)
- CERTA-2004-AVI-411-004 : Vulnérabilité de MIT Kerberos 5
  (ajout référence au bulletin de sécurité RedHat RedHat RHSA-2005-045)
- CERTA-2004-AVI-418-005 : Vulnérabilité de Xpdf
  (ajout des références aux bulletins de sécurité RedHat)
- CERTA-2005-AVI-001-001 : Vulnérabilité sur CUPS
  (ajout des références aux bulletins de sécurité RedHat)
- CERTA-2005-AVI-003-005 : Multiples vulnérabilités de libtiff
  (ajout référence au bulletin de sécurité RedHat RHSA-2005:035)
- CERTA-2005-AVI-006-002 : Vulnérabilité de KDE
  (ajout de la référence au bulletin de sécurité RHSA-2005:065 de RedHat)
- CERTA-2005-AVI-014-003 : Multiples vulnérabilités dans Exim
  (ajout référence au bulletin de sécurité RedHat RHSA-2005-025)

- CERTA-2005-AVI-018-001 : Multiples vulnérabilité dans CUPS
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:053)
- CERTA-2005-AVI-019-007 : Vulnérabilité dans Xpdf
  (ajout des références aux bulletins de sécurité RedHat)
- CERTA-2005-AVI-020-003 : Vulnérabilité de ImageMagick
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-038-004 : Multiples vulnérabilités dans SquirrelMail
  (ajout de la référence à un second bulletin de sécurité RedHat, RHSA-2005:099)
- CERTA-2005-AVI-042-004 : Multiples vulnérabilités dans Squid
  (ajout d'un second bulletin de sécurité RedHat)
- CERTA-2005-AVI-046-005 : Vulnérabilité de Perl
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:103)
- CERTA-2005-AVI-049-004 : Vulnérabilité de PostgreSQL
  (ajout des références aux bulletins de sécurité RedHat)
- CERTA-2005-AVI-063-003 : Vulnérabilité de Python
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:108)
- CERTA-2005-AVI-066-004 : Vulnérabilité de Mailman
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:137)
- CERTA-2005-AVI-067-003 : Vulnérabilité de Emacs et XEmacs
  (ajout de la référence aux bulletins de sécurité RedHat RHSA-2005:110 et RHSA-2005:133)
- CERTA-2005-AVI-070-002 : Vulnérabilité de GNU enscript
  (ajout de la référence au bulletin de sécurité RedHat RHSA-2005:040)
- CERTA-2004-AVI-400-005 : Multiples vulnérabilités dans Ethereal
  (Ajout référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-022-005 : Vulnérabilité de Ethereal
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-068-001 : Vulnérabilité dans vim
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-069-001 : Vulnérabilité de cpio
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-072-001 : Vulnérabilité du module Apache mod_python
  (ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-073-001 : Vulnérabilité de ht://Dig
  (ajout de la référence au bulletin de sécurité RedHat)

4 Actions suggérées

4.1 Respecter la politique de sécurité

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.

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 immédiat. 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.

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.

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.

Liste des tableaux

Gestion détaillée du document

25 février 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-20 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-38
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-0 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-11 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-03
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-36 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-16 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-00 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-0
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-15
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-18 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-21
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-16
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-02
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-0
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-21
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

TAB. 2 – *Correctifs correspondant aux ports destination des paquets rejetés*

port	pourcentage
445/tcp	64,65
139/tcp	13,25
137/udp	5,04
1080/tcp	2,73
1433/tcp	2,57
1026/udp	2,24
1027/udp	2,14
4899/tcp	1,72
15118/tcp	1,19
6129/tcp	0,89
5554/tcp	0,60
2745/tcp	0,51
9898/tcp	0,44
80/tcp	0,38
1434/udp	0,26
135/tcp	0,20
11768/tcp	0,20
3127/tcp	0,17
3306/tcp	0,15
22/tcp	0,14
1023/tcp	0,09
5000/tcp	0,08
443/tcp	0,07
23/tcp	0,06
42/tcp	0,06
21/tcp	0,06
6101/tcp	0,04
111/tcp	0,03
3128/tcp	0,03
3389/tcp	0,01

TAB. 3 – *Paquets rejetés*