Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 octobre 2005
N° CERTA-2005-ACT-042

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-42

Gestion du document

Référence	CERTA-2005-ACT-042
Titre	Bulletin d'actualité n° 2005-42
Date de la première version	21 octobre 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 13 octobre et le 21 octobre 2005.

2 Recommandations suite au spam à caractère pédophile

Le CERTA a reçu cette semaine de nombreux appels et messages à propos de messages non sollicités à caractère pédophile. A cette occasion, il a été rappelé dans deux notes de communication, les actions à engager, en particulier la nécessité de déposer une plainte auprès des services de police (OCLCTIC). Une déclaration peut aussi être faite auprès du site : http://www.internet-mineur.gouv.fr. Le CERTA conseille également la lecture d'une note d'information sur les mails non sollicités en ligne sur son site internet. Il est enfin rappelé qu'au delà du caractère choquant des photos ainsi diffusées, ces messages peuvent véhiculer des codes malveillants (note d'information n4 du CERTA du 03/10/05 : CERTA-2005-INF-004). A ce propos, le CERTA poursuit son analyse et a demandé à ses abonnés de contrôler leur journaux afin de vérifier si des machines de leurs réseaux n'étaient pas à l'origine de l'envoi de ce spam. Si ce cas se présentait il serait sans doute dû, à une machine compromise par un cheval de Troie et sur laquelle un Bot IRC pourrait avoir été installé, cette machine devenant ainsi, entre autre, un relais de spam. Le CERTA demande a être tenu informé si une machine était à l'origine de l'envoi de spam. Le CERTA reste à votre disposition pour vous aider.

3 Vulnérabilité sur Snort du 19 octobre :

Suite à la publication de CERTA-2005-AVI-408 sur une vulnérabilité dans le préprocesseur `Back Orifice` du logiciel libre de détection d'intrusion `Snort`, sont apparus plusieurs outils exploitant cette faille. Un simple paquet `UDP` malicieusement construit suffit pour compromettre une machine. Il convient donc d'être très vigilant sur la mise à jour rapide de cette application. Il est à noter que `Snort` est parfois inclus dans des produits *clefs-en-mains* de sécurité intégrant pare-feu, détecteur d'intrusion, antivirus...

Remarque :

Compte tenu de la diversité des plateformes sur lesquelles `Snort` peut être déployé , l'efficience d'une exploitation à grande échelle et de façon automatique pourrait être limitée par la difficulté à développer un outil fonctionnant dans de nombreux environnements différents. Cependant la relative facilité d'utilisation de la faille vient contrebalancer cet écueil.

Recommandation :

Il convient donc de vérifier que vous ne disposez pas dans vos équipements de surveillance de réseau, un détecteur d'intrusion `Snort` sous quelque forme que ce soit. Le cas échéant, une mise à jour de `Snort`, du microgiciel ou du système d'exploitation s'impose dans les plus brefs délais. Si toutefois vous constatiez des tentatives d'exploitations réussies ou pas d'utilisation de cette faille veuillez en avertir le CERTA.

4 Rappel des avis et mises à jour émis

Durant la période du 10 au 14 octobre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-386 : Vulnérabilité dans sysreport ;
- CERTA-2005-AVI-387 : Vulnérabilité dans Dia ;
- CERTA-2005-AVI-388 : Vulnérabilité de la bibliothèque multimedia xine-lib ;
- CERTA-2005-AVI-389 : Vulnérabilité de SUN Java System Directory Server ;
- CERTA-2005-AVI-390 : Vulnérabilités de libwww ;
- CERTA-2005-AVI-391 : Vulnérabilité des antivirus Kaspersky et F-Secure ;
- CERTA-2005-AVI-392 : Vulnérabilité de xli ;
- CERTA-2005-AVI-393 : Multiples vulnérabilités de WinRAR ;
- CERTA-2005-AVI-394 : Vulnérabilité dans Microsoft DirectX ;
- CERTA-2005-AVI-395 : Vulnérabilité dans le client FTP Microsoft ;
- CERTA-2005-AVI-396 : Vulnérabilité de Microsoft Internet Explorer ;
- CERTA-2005-AVI-397 : Vulnérabilité dans le service client pour Netware de Microsoft ;
- CERTA-2005-AVI-398 : Vulnérabilité dans le module Plug and Play (PnP) de Microsoft Windows ;
- CERTA-2005-AVI-399 : Vulnérabilité d'un composant Microsoft Windows et Exchange Server ;
- CERTA-2005-AVI-401 : Multiples vulnérabilités dans Microsoft Windows Shell et Web View ;
- CERTA-2005-AVI-402 : Vulnérabilité dans SGI IRIX ;
- CERTA-2005-AVI-403 : Multiples vulnérabilités dans Microsoft Windows ;
- CERTA-2005-AVI-400 : Faiblesse dans OpenSSL 0.9.x ;
- CERTA-2005-AVI-404 : Vulnérabilité dans VERITAS NetBackup ;
- CERTA-2005-AVI-405 : Multiples vulnérabilités dans Sun Solaris ;
- CERTA-2005-AVI-406 : Vulnérabilité de Microsoft Network Connection Manager ;
- CERTA-2005-AVI-407 : Vulnérabilité dans la bibliothèque libcURL.

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

- CERTA-2005-AVI-164-006 : Multiples vulnérabilités dans tcpdump (ajout des références aux bulletins de sécurité Debian DSA-850 et DSA-854)
- CERTA-2005-AVI-284-003 : Multiples vulnérabilités dans le logiciel Ethereal (ajout de la référence au bulletin de sécurité Debian et aux références CVE)

- CERTA-2005-AVI-335-002 : Vulnérabilité de OpenVPN (ajout de la référence au bulletin de sécurité Debian DSA-851)
- CERTA-2005-AVI-251-003 : Vulnérabilité de cpio (ajout de la référence au bulletin de sécurité Debian DSA-846)
- CERTA-2005-AVI-268-003 : Vulnérabilité de Shorewall (ajout de la référence au bulletin de sécurité Debian DSA-849)
- CERTA-2005-AVI-350-001 : Vulnérabilité de GNU mailutils (ajout de la référence au bulletin de sécurité Debian DSA-841 et de la référence CVE CAN-2005-2878)
- CERTA-2005-AVI-353-002 : Vulnérabilité dans MySQL (ajout de la référence au Bulletin de sécurité Debian DSA-833)
- CERTA-2005-AVI-358-004 : Vulnérabilités de Mozilla Firefox et Mozilla Suite (ajout de la référence au bulletin de sécurité Debian DSA-838)
- CERTA-2005-AVI-383-001 : Vulnérabilité dans UW-imapd (ajout de la référence au bulletin de sécurité Gentoo GLSA 200510-10)
- CERTA-2005-AVI-384-001 : Multiples vulnérabilités dans cfengine (ajout des références au bulletin de sécurité Ubuntu USN-198-1 et CVE CAN-2005-3137)
- CERTA-2005-AVI-371-001 : Vulnérabilité de Squid (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:181)
- CERTA-2005-AVI-383-002 : Vulnérabilité dans UW-imapd (ajout de la référence au bulletin de sécurité Debian DSA-861)
- CERTA-2005-AVI-385-001 : Vulnérabilité de l'interpréteur de script Ruby (ajout des références aux bulletins de sécurité des éditeurs)
- CERTA-2005-AVI-388-001 : Vulnérabilité de la bibliothèque multimedia xine-lib (ajout des références aux bulletins de sécurité Debian et Mandriva)
- CERTA-2005-AVI-392-001 : Vulnérabilité de xli (ajout de la référence au bulletin de sécurité Debian DSA-858)
- CERTA-2005-AVI-385-002 : Vulnérabilité de l'interpréteur de script Ruby (ajout de la références au bulletin de sécurité Debian et référence CVE)
- CERTA-2005-AVI-384-002 : Multiples vulnérabilités dans cfengine (ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:184)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

6 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

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

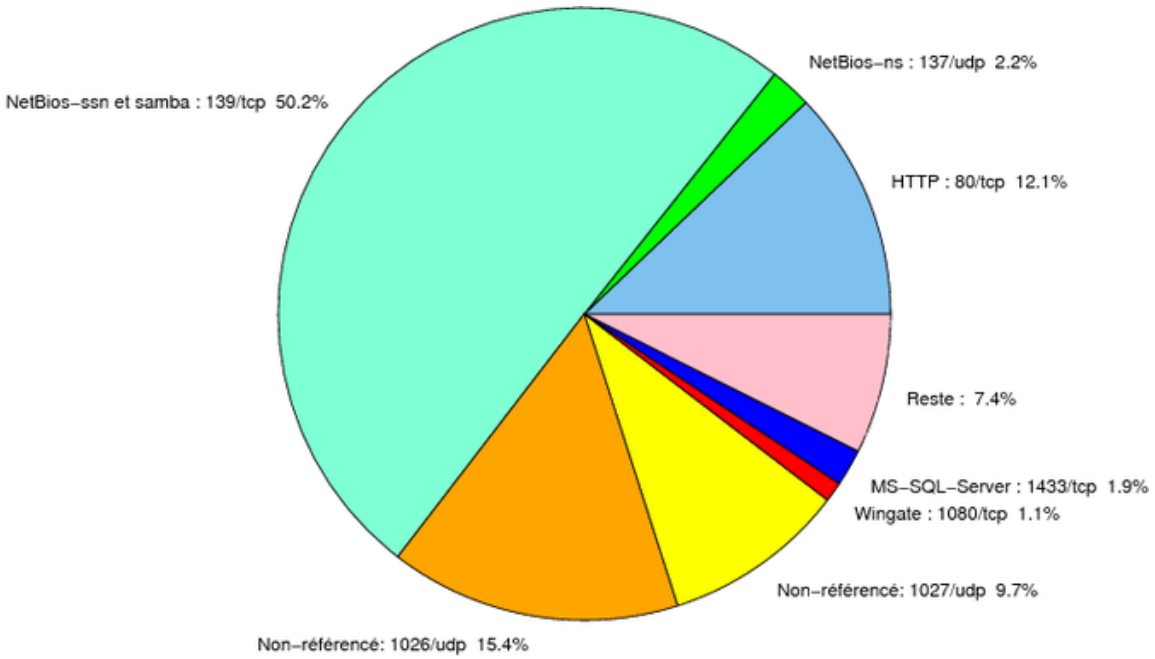

FIG. 1: Répartition relative des ports pour la semaine du 13.10.2005 au 20.10.2005

port	pourcentage
139/tcp	50.24
1026/udp	15.36
80/tcp	12.12
1027/udp	9.66
137/udp	2.19
1433/tcp	1.94
1080/tcp	1.05
3128/tcp	0.89
4899/tcp	0.86
23/tcp	0.79
10000/tcp	0.65
1434/udp	0.62
25/tcp	0.43
443/tcp	0.41
3127/tcp	0.39
15118/tcp	0.36
2745/tcp	0.32
22/tcp	0.29
5000/tcp	0.22
8866/tcp	0.21
10080/tcp	0.19
6129/tcp	0.12
9898/tcp	0.1
3306/tcp	0.09
5554/tcp	0.08
2100/tcp	0.06
1023/tcp	0.03
42/tcp	0.02
11768/tcp	0.01

TAB. 3: Paquets rejetés

Gestion détaillée du document

14 octobre 2005 version initiale.