



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 octobre 2005
N° CERTA-2005-ACT-041

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-41

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-2005-ACT-041>

Gestion du document

Référence	CERTA-2005-ACT-041
Titre	Bulletin d'actualité n° 2005-41
Date de la première version	14 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 06 octobre et le 13 octobre 2005.

2 Bulletins de sécurité Microsoft du 11 octobre 2005 :

Suite à la publication des bulletins de sécurité de Microsoft du 11 octobre 2005, le CERTA a émis des avis de sécurité. Nous attirons tout particulièrement votre attention sur les failles décrites dans les bulletins CERTA-2005-AVI-395 et CERTA-2005-AVI-399.

Le premier avis concerne une vulnérabilité du client ftp (File Transfert Protocol) de Windows (MS05-44) et fait déjà l'objet de codes malveillants l'exploitant. Le second avis, quant à lui, concerne une vulnérabilité d'un composant de Microsoft Exchange (MS05-048) et fait l'objet d'une preuve de faisabilité d'exploitation (*Proof of Concept*).

La nature de la seconde vulnérabilité nous laisse à penser que du code malveillant l'exploitant pourrait apparaître dans un avenir plus ou moins proche. Compte tenu de la nature du protocole utilisé (smtp: Simple Mail Transfert Protocol) ainsi que du nombre de produit Exchange déployés, **l'impact de tels codes pourrait être important.**

Recommandation :

De manière plus générale, les failles décrites dans les bulletins de sécurité Microsoft pour le mois d'octobre sont **qualifiées par l'éditeur comme critiques ou importantes** pour la plupart d'entre elles. Il est donc **impératif d'appliquer les correctifs dans les plus brefs délais**. Il convient également de surveiller l'activité sur les ports concernés (Exchange : 25/tcp, ftp : 21/tcp, ...). Si toutefois vous constatiez une activité anormale sur les ports ou les composants concernés par ces différentes vulnérabilités, il convient d'en informer le CERTA.

3 Rappel des avis et mises à jour émis

Durant la période du 03 au 07 octobre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-370 : Vulnérabilité de l'utilitaire AIX getconf ;
- CERTA-2005-AVI-371 : Vulnérabilité de Squid ;
- CERTA-2005-AVI-372 : Vulnérabilité dans Bugzilla ;
- CERTA-2005-AVI-373 : Vulnérabilité de ZoneAlarm ;
- CERTA-2005-AVI-375 : Vulnérabilité dans Sun Java Desktop System ;
- CERTA-2005-AVI-376 : Vulnérabilités dans Apachetop ;
- CERTA-2005-AVI-377 : Vulnérabilités dans MailEnable ;
- CERTA-2005-AVI-378 : Vulnérabilité de l'antivirus Kaspersky ;
- CERTA-2005-AVI-374 : Vulnérabilité de CVS ;
- CERTA-2005-AVI-379 : Vulnérabilités dans HP OpenView ;
- CERTA-2005-AVI-380 : Vulnérabilité de l'antivirus Symantec ;
- CERTA-2005-AVI-381 : Vulnérabilité de l'antivirus BitDefender ;
- CERTA-2005-AVI-382 : Vulnérabilité de IBM Tivoli Monitoring ;
- CERTA-2005-AVI-383 : Vulnérabilité dans UW-imapd ;
- CERTA-2005-AVI-384 : Multiples vulnérabilités dans cfengine ;
- CERTA-2005-AVI-385 : Vulnérabilité de l'interpréteur de script Ruby.

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

- CERTA-2005-AVI-337-004 : Multiples vulnérabilités dans Squid
(ajout de la référence au bulletin de sécurité Suse.)
- CERTA-2005-AVI-346-001 : Vulnérabilité des clients web Mozilla, Firefox et Netscape
(ajout de la référence au bulletin de sécurité Debian.)
- CERTA-2005-AVI-353-001 : Vulnérabilité dans MySQL
(ajout des références aux Bulletins de sécurité Debian et Suse.)
- CERTA-2005-AVI-346-002 : Vulnérabilité des clients web Mozilla, Firefox, Thunderbird et Netscape
(ajout de Mozilla Thunderbird dans la section "Systèmes affectés".)
- CERTA-2003-AVI-180-004 : Vulnérabilité de la commande ls sous Linux
(ajout de la références au bulletin de sécurité Avaya.)
- CERTA-2005-AVI-069-004 : Vulnérabilité de cpio
(ajout de la référence au bulletin de sécurité Avaya.)
- CERTA-2005-AVI-329-002 : Vulnérabilité de OpenSSH
(Bulletin de sécurité Red Hat.)
- CERTA-2005-AVI-369-002 : Vulnérabilité dans Mozilla Thunderbird
(Ajout des références Slackware.)

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'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance

accordée par la direction générale de l'organisme 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 réglementaire, 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

À 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 inexplicables 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.

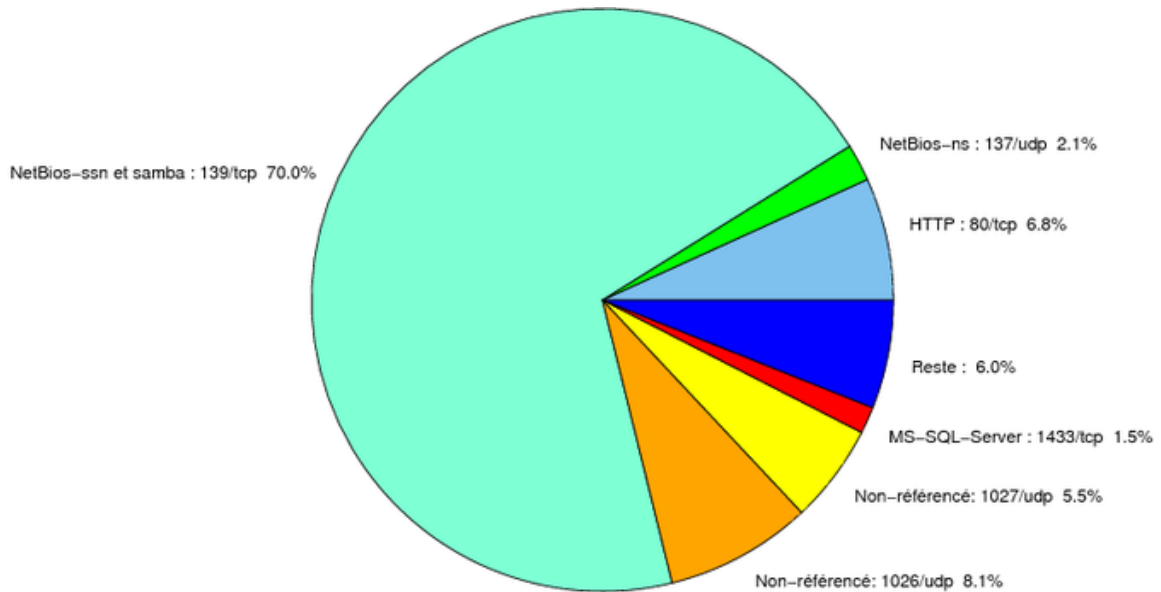


FIG. 1: Répartition relative des ports pour la semaine du 06.10.2005 au 13.10.2005

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	5
3	Paquets rejetés	6

Gestion détaillée du document

14 octobre 2005 version initiale.

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-21-TCP-FTP http://www.certa.ssi.gouv.fr/site/CERTA-21-TCP-FTP http://www.certa.ssi.gouv.fr/site/CERTA-21-TCP-FTP
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-22-TCP-SSH
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-23-TCP-Telnet http://www.certa.ssi.gouv.fr/site/CERTA-23-TCP-Telnet
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-25-TCP-SMTP
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-42-TCP-WINS
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-80-TCP-HTTP http://www.certa.ssi.gouv.fr/site/CERTA-80-TCP-HTTP
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-111-TCP-Sunrpc-portmapper
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-119-TCP-NNTP
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-135-TCP-Microsoft-RPC http://www.certa.ssi.gouv.fr/site/CERTA-135-TCP-Microsoft-RPC http://www.certa.ssi.gouv.fr/site/CERTA-135-TCP-Microsoft-RPC
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-137-UDP-NetBios-ns
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-139-TCP-NetBios-ssn-et-samba http://www.certa.ssi.gouv.fr/site/CERTA-139-TCP-NetBios-ssn-et-samba http://www.certa.ssi.gouv.fr/site/CERTA-139-TCP-NetBios-ssn-et-samba http://www.certa.ssi.gouv.fr/site/CERTA-139-TCP-NetBios-ssn-et-samba http://www.certa.ssi.gouv.fr/site/CERTA-139-TCP-NetBios-ssn-et-samba
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-143-TCP-IMAP
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-389-TCP-LDAP http://www.certa.ssi.gouv.fr/site/CERTA-389-TCP-LDAP http://www.certa.ssi.gouv.fr/site/CERTA-389-TCP-LDAP http://www.certa.ssi.gouv.fr/site/CERTA-389-TCP-LDAP http://www.certa.ssi.gouv.fr/site/CERTA-389-TCP-LDAP
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-443-TCP-HTTPS http://www.certa.ssi.gouv.fr/site/CERTA-443-TCP-HTTPS http://www.certa.ssi.gouv.fr/site/CERTA-443-TCP-HTTPS http://www.certa.ssi.gouv.fr/site/CERTA-443-TCP-HTTPS
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-445-TCP-Microsoft-smb http://www.certa.ssi.gouv.fr/site/CERTA-445-TCP-Microsoft-smb http://www.certa.ssi.gouv.fr/site/CERTA-445-TCP-Microsoft-smb http://www.certa.ssi.gouv.fr/site/CERTA-445-TCP-Microsoft-smb http://www.certa.ssi.gouv.fr/site/CERTA-445-TCP-Microsoft-smb
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-1433-TCP-MS-SQL-Server
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-1434-UDP-MS-SQL-Monitor
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2100-TCP-Oracle-XDB-FTP
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-3128-TCP-Squid http://www.certa.ssi.gouv.fr/site/CERTA-3128-TCP-Squid http://www.certa.ssi.gouv.fr/site/CERTA-3128-TCP-Squid http://www.certa.ssi.gouv.fr/site/CERTA-3128-TCP-Squid
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-3389-TCP-Microsoft-RDP
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-5000-TCP-Universal-Plug-and-Play
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CERTA-6070-TCP-BrightStor-ARCserve-Enterprise-Backup
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-6101-TCP-Veritas-Backup-Exec
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-6112-TCP-Dtspcd
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-6129-TCP-Dameware-Miniremote http://www.certa.ssi.gouv.fr/site/CERTA-6129-TCP-Dameware-Miniremote
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-10000-TCP-Webmin-Veritas-Backup-Exec http://www.certa.ssi.gouv.fr/site/CERTA-10000-TCP-Webmin-Veritas-Backup-Exec
10080	TCP	Amanda	MyDoom	–

port	pourcentage
139/tcp	70
1026/udp	8.14
80/tcp	6.78
1027/udp	5.48
137/udp	2.06
1433/tcp	1.48
1080/tcp	0.87
4899/tcp	0.54
23/tcp	0.5
3128/tcp	0.42
15118/tcp	0.35
10000/tcp	0.33
25/tcp	0.31
1434/udp	0.3
2745/tcp	0.29
443/tcp	0.28
5000/tcp	0.27
10080/tcp	0.25
22/tcp	0.17
3306/tcp	0.1
2100/tcp	0.09
6129/tcp	0.07
5554/tcp	0.04
11768/tcp	0.02

TAB. 3: Paquets rejetés