



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 septembre 2006
N° CERTA-2006-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-36

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-036>

Gestion du document

Référence	CERTA-2006-ACT-036
Titre	Bulletin d'actualité 2006-36
Date de la première version	08 septembre 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-036.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-036/>

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 31 août 2006 et le 07 septembre 2006.

1.2 Vulnérabilité dans Microsoft Office - Word

Une vulnérabilité non corrigée existe dans Microsoft Office. Elle a fait l'objet d'un avis Microsoft 925059 et le CERTA a publié l'alerte ALE-2006-ALE-0011 à ce sujet.

Cette vulnérabilité semble affecter Word 2000, et des codes malveillants exploitant celle-ci se propagent actuellement sur l'Internet. Ceux-ci se nomment, en fonction des antivirus :

- W32/Mofei.worm.de (McAfee)
- Trojan.Mdropper.Q (Symantec)
- Trojan-Dropper.MSWord.1Table.bv (Kaspersky)
- TROJ_MDROPPER.BR (TrendMicro).

Dans l'attente d'un correctif, le CERTA recommande :

1. de n'ouvrir que les documents bureautiques de confiance ;
2. d'utiliser une suite bureautique alternative à jour ;
3. de vérifier la mise à jour des antivirus

2 Listes blanches *anti-spam*

Certains sites web, au nom de la lutte contre les messages électroniques non désirés, proposent d'entretenir des listes blanches d'adresses de messagerie. Le principe est le suivant : lorsque vous envoyez un message électronique, vous êtes invités à vous inscrire auprès d'un site web, qui se pose comme tiers de confiance. Ce dernier validera pour tous vos échanges futurs le fait que vous n'êtes pas un robot de *spam*.

Ces listes blanches soulèvent toutefois de nombreuses questions :

- avez-vous accès à l'information stockée dans ces bases de données ?
- pouvez-vous modifier ces informations ?
- quelle confiance accordez-vous dans ce tiers que vous ne connaissez pas ?
- le transit de vos messages électroniques par ces tiers de confiance est-il conforme à votre politique de sécurité ?
- est-il souhaitable de communiquer une adresse électronique réellement utilisée ?
- une adresse de messagerie ainsi stockée chez un tiers de confiance peut-elle être utilisée par un robot de *spam* ?

Le CERTA vous recommande de bien réfléchir à ces questions avant d'imposer l'utilisation d'une quelconque liste blanche d'adresses de messagerie à vos correspondants.

Des questions similaires se posent pour toute solution utilisant des listes noires, c'est à dire des listes à *éviter*. Ce procédé est employé dans des outils proposant de combattre le spam, ou le filoutage.

3 Vulnérabilités de BIND

Le CERTA a publié le 07 septembre 2006 un avis sur le service ISC BIND (*Berkeley Internet Name Domain*). Ce dernier met en œuvre le protocole DNS servant à la résolution de noms de domaine (association entre une adresse IP et un nom).

Le CERTA annonce dans cet avis (CERTA-2006-AVI-384) deux vulnérabilités pouvant conduire une personne malveillante à provoquer un mauvais fonctionnement (arrêt de service) d'un serveur DNS vulnérable.

DNS est un élément important dans le bon fonctionnement d'un système d'information connecté à l'Internet. Il est utilisé par de nombreuses applications, comme les navigateurs, mais parfois de manière discrète, comme par exemple les messageries. Un mauvais fonctionnement des serveurs DNS peut ainsi entraîner des dysfonctionnements en chaîne.

Le CERTA recommande donc vivement d'appliquer les mises à jour signalées dans l'avis.

4 Analyse de journaux Microsoft

Microsoft utilise dans un ensemble d'applications une numérotation particulière pour identifier les événements. Par exemple, sous Windows XP, une liste d'événements observés se trouve à l'emplacement suivant :

- démarrer
- Panneau de configuration
- Performances et maintenance
- Outils d'administration
- Observateur d'événements.

Les événements sont classés en trois grandes catégories, celles ayant trait aux applications installées, celles liées au système d'exploitation et celles de sécurité.

En cliquant sur un événement particulier, il peut arriver que le champ `description` soit manquant, car des droits empêchent de récupérer cette information ou la bibliothèque installée ne le fournit pas. Plusieurs sites se

proposent de lister et expliciter les messages associés à chaque événement, en fonction d'un numéro d'identifiant et des sources (ou bibliothèques). Il est intéressant de se reporter à ceux-ci pour éclaircir des événements donnés :

- le site de Microsoft concernant les événements et les erreurs :
http://www.microsoft.com/technet/support/ee/ee_advanced.aspx
- le site *EventID* :
<http://www.eventid.net/search.asp>

Ces deux sites fournissent par ailleurs d'autres informations utiles :

- des détails sur les bibliothèques Microsoft dll :
<http://support.microsoft.com/dllhelp/>
- une liste de services installés sur les différentes distributions Windows :
<http://www.microsoft.com/technet/prodtechnol/serveros.msp>
- une liste associant des applications avec leurs ports TCP/UDP usuels :
<http://www.eventid.net/searchprot.asp>

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 de la mise à jour émis

Durant la période du 01 au 07 septembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-382 : Vulnérabilité dans Webmin et Usermin
- CERTA-2006-AVI-383 : Vulnérabilités dans OpenLDAP
- CERTA-2006-AVI-384 : Vulnérabilité dans OpenSSL
- CERTA-2006-AVI-385 : Vulnérabilités de BIND

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

- CERTA-2006-INF-003-003 : Les systèmes et logiciels obsolètes
(mises à jour des versions pour les systèmes BSD et ajout de la référence pour le système AIX)

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'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.

7.2 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.

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 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.

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.

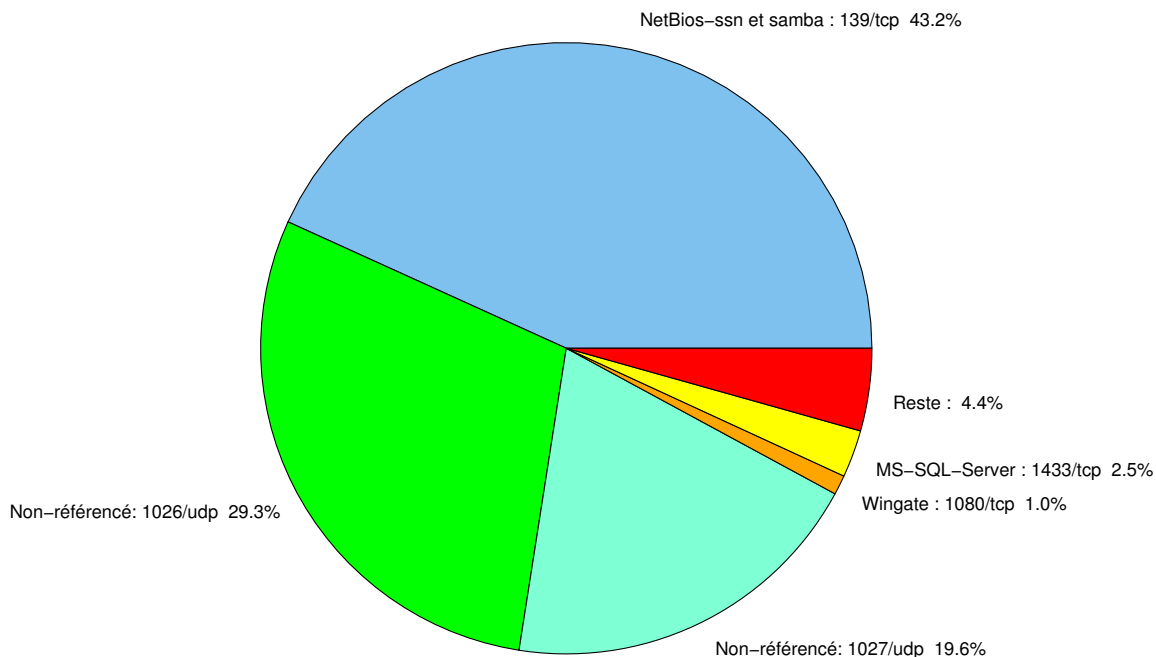


FIG. 1: Répartition relative des ports pour la semaine du 31.08.2006 au 07.09.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	-	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	-	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
80	TCP	HTTP	-	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	-	-
111	TCP	Sunrpc-portmapper	-	CERTA-2003-AVI-052
119	TCP	NNTP	-	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	-	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	-	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	-	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338
143	TCP	IMAP	-	CERTA-2005-AVI-185
389	TCP	LDAP	-	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126
443	TCP	HTTPS	-	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	-	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338
1023	TCP	-	Serveur ftp de Sasser.E	-
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	-	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	-	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	-	CERTA-2005-ALE-002

2381	TCP	–	HP System Management	CERTA-2006-AVI-248
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
139/tcp	43.21
1026/udp	29.31
1027/udp	19.57
1433/tcp	2.5
1080/tcp	1.03
4899/tcp	0.94
1434/udp	0.9
137/udp	0.72
80/tcp	0.54
22/tcp	0.43
3128/tcp	0.32
25/tcp	0.23
15118/tcp	0.16
443/tcp	0.04
11768/tcp	0.02
21/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	7
3	Paquets rejetés	8

Gestion détaillée du document

08 septembre 2006 version initiale.