

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-10

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-2007-ACT-010>

Gestion du document

Référence	CERTA-2007-ACT-010
Titre	Bulletin d'actualité 2007-10
Date de la première version	09 mars 2007
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-2007-ACT-010.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-2007-ACT-010/>

1 Activités en cours

1.1 Les courriels non sollicités

Les auteurs de courriers non sollicités (spam ou pourriels) imaginent continuellement de nouvelles méthodes leurs permettant de contourner les règles de filtrage des passerelles anti-spam, et de tromper la vigilance des destinataires.

Dernièrement, le CERTA a reçu un cas de pourriel qui utilise une méthode basée sur de l'ingénierie sociale. Cette technique consiste à émettre un pourriel dont le sujet et une partie du corps du message ressemblent, à s'y méprendre, à un message d'erreur (Sujet du courrier : *Mail Delivery (Failure toto certa.ssi.gouv.fr)*).

Le corps du message, en HTML, contient un lien réticulaire (URL) pointant vers une vidéo.

Le CERTA recommande que les serveurs de messagerie ne soient pas configurés de façon à envoyer les pièces jointes ou l'intégralité du corps du message ayant créé l'erreur.

Les standards RFCs 3461 et 3462 spécifient le comportement attendu d'un serveur de messagerie. En d'autres termes, le contenu d'un message d'erreur doit obligatoirement :

- contenir un message lisible explicitant l'erreur à l'utilisateur ;
- contenir une section décrivant l'erreur et interprétable par un client de messagerie ou un administrateur.

Le message peut inclure, de manière optionnelle, tout ou partie du message émis et n'ayant pas pu être acheminé à sa destination. Il est déconseillé de retransmettre l'intégralité du message envoyé, mais cela dépend de la configuration du serveur. Il est par contre intéressant de retourner l'identifiant du courrier et l'adresse du destinataire afin de comprendre à quel message l'erreur correspond.

Le RFC 3463 précise les différents codes d'erreurs possibles.

Une autre bonne pratique consiste à lire les courriers électroniques au format texte, depuis son client de messagerie.

- Sous Mozilla Thunderbird, choisir dans le menu "Affichage", sélectionner "Corps du message", puis "texte brut" ;
- Sous Microsoft Outlook, cocher dans le menu "Outils", "Options", puis "Options de la messagerie..." la case "Lire tous les messages standards au format texte brut".

Documentations

- RFC 3461, "SMTP Service Extension for Delivery Status Notifications (DSNs)" :
<http://www.ietf.org/rfc/rfc3461.txt>
- RFC 3462, "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages" :
<http://www.ietf.org/rfc/rfc3462.txt>
- RFC 3463, "Enhanced Mail System Status Codes" :
<http://www.ietf.org/rfc/rfc3463.txt>

1.2 La gestion des mots de passe

Le CERTA a traité cette semaine un incident sur une machine dont les mots de passe des comptes étaient trop faibles. Il a préconisé de changer ceux-ci pour tous les comptes de la machine compromise. Les machines du réseau, dont celle analysée, sont infogérées par une société, mais certains comptes disposent de droits administratifs.

La gestion des comptes était également infogérée par la société. Celle-ci disposait du compte global Administrateur du domaine, et pouvait donc imposer aux autres comptes, administratifs ou pas, de ne pas modifier leur mot de passe.

La gestion des mots de passe par un tiers n'est pas nécessairement la meilleure idée. Si jamais cela devait se produire, il est impératif d'imposer à la société une gestion rigoureuse, avec l'utilisation de mots de passe forts (cela reste valable pour leur compte Administrateur), et un renouvellement régulier de ces derniers. Les mêmes recommandations et contraintes pour les utilisateurs doivent aussi leur être imposées. La faiblesse d'un seul compte peut compromettre l'intégralité de la machine, voire du réseau.

La note d'information CERTA-2005-INF-001 détaille les bonnes pratiques en matière de choix et de gestion de mots de passe.

Documentation associée

- Note du CERTA, « Les mots de passe » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>

2 Wordpress, ou les risques du téléchargement sur l'Internet

Cette semaine, le CERTA a publié un avis de sécurité concernant la compromission d'une des sources d'installation du logiciel de gestion de contenu (CMS) WordPress. Une personne malintentionnée s'est introduite sur l'un des serveurs de téléchargement de WordPress afin d'y modifier les sources de la version 2.1.1 de ce logiciel. La modification faite permettait de réaliser des attaques de type *PHP include* sur les sites où la version compromise était utilisée.

L'éditeur, une fois informé, a rapidement pris les mesures de sécurité adaptées mettant à disposition une nouvelle version de WordPress.

Un tel événement montre que la sécurité absolue n'existe pas. Il est préférable de télécharger les logiciels sur le site principal de l'éditeur plutôt que sur un site miroir non connu, et de ne pas installer de mises à jour à la hâte pour un site jugé critique.

Documentation

- Avis CERTA-2007-AVI-107 du 05 mars 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-107>

3 Fuite d'informations

L'ingénierie sociale est une pratique consistant à manipuler pour obtenir un bien ou une information, en exploitant par exemple la confiance, l'ignorance ou la crédulité.

Historiquement, la motivation de l'ingénierie sociale est de recueillir des informations sur l'organisme qui est ciblé. Cela peut-être : noms et numéros de téléphone, jargon utilisé, projets en cours, congés, stratégie de l'entreprise, etc. Il s'agit de collecter, progressivement, par différentes étapes, des informations. En principe, la première étape se fait sans interaction avec la victime, par le biais d'autres sources. La deuxième étape peut exploiter les premières données collectées auprès, cette fois-ci, de la victime, afin d'en obtenir davantage. Les informations peuvent donc être réutilisées pour différents objectifs :

- s'introduire physiquement au sein de l'organisme avec les informations nécessaires pour s'y orienter ;
- échanger des appels téléphoniques ;
- envoyer de courriers électroniques redirigeant vers des pages malveillantes, comme le filoutage ;
- etc.

Il est très difficile de quantifier les informations qui fuient, mises à disposition accidentellement sur la place publique. Mais ceci est un problème bien visible et réel. Par exemple :

- Le forum de discussions sur lequel se rend le salarié chez lui, indiquant qu'il ne peut se connecter tôt le lendemain à cause d'une réunion importante à (Paris) ;
- des listes de diffusion sur lesquelles un administrateur demande des conseils techniques, indiquant par la même occasion la configuration matérielle et logicielle de son réseau ;
- les bloc-notes (*blogs*) personnels relatant les faits de la journée ;
- les réponses automatiques aux courriels signalant le départ de la société, la prise de congés maternités, etc ;

Les exemples sont multiples et variés.

Le CERTA recommande aux administrateurs de vérifier sur l'Internet la disponibilité de telles informations pour leur(s) service(s). S'il est impossible techniquement d'empêcher de telles informations de fuir, il est cependant important de sensibiliser les utilisateurs à cette problématique.

4 Les vulnérabilités PHP du mois de mars 2007

4.1 Retour sur le *The Month of PHP Bugs*

Depuis le début du mois de mars, et à l'image du «Month of Apple Bugs», a commencé un projet similaire concernant PHP : le MOPB, ou «Month Of PHP Bugs». D'après les responsables du projet, ils s'attachent à trouver des vulnérabilités dans le moteur de rendu PHP et non dans les applications développées avec ce langage (gestionnaires de contenus, forums).

Depuis qu'il a commencé, le projet a publié quotidiennement des failles dans l'interpréteur PHP. La plupart d'entre elles ont déjà fait l'objet d'un correctif dans la dernière version de PHP soit la 5.2.1 (ou la 4.4.6 pour ceux restés sur cette branche de développement). Il conviendra cependant de rester vigilant sur l'éventuelle publication d'une faille non corrigée permettant une possible exécution de code arbitraire à distance.

4.2 Remarques concernant *phpinfo()*

L'une des vulnérabilités publiées concerne la fonction PHP `phpinfo()`. Celle-ci permet de collecter un ensemble d'informations liées à l'environnement PHP. Cela inclut :

- la version détaillée du système d'exploitation et de PHP ;
- sa date d'installation ;
- les modules exigés au moment de la configuration de PHP ;
- le serveur Web associé ;
- le chemin vers le fichier de configuration `php.ini` ;

- les formats supportés ;
- etc.

Cela représente de riches informations, largement suffisantes pour aider une personne malveillante à cibler son attaque contre le serveur. Cette information est souvent accessible par le biais d'une page php dédiée : `phpinfo.php`.

La page `phpinfo.php` peut être insérée sur le site, soit par l'administrateur effectuant des modifications dessus, soit par l'application elle-même, qui la dépose par défaut (phpBB par exemple). Dans tous les cas, l'accès public à cette page présente un danger.

- révéler la version d'une application n'est pas une vulnérabilité à proprement parlé. Cependant, le lecteur aura compris, après un regard sur le paragraphe précédent, qu'un grand nombre de vulnérabilités PHP peuvent être identifiées et exploitées selon la version utilisée.
- la version de la fonction actuelle présente une vulnérabilité, qui affecterait les versions les plus récentes de PHP. Elle permettrait de lancer des attaques de type "injection de code indirecte", ou *cross-site scripting*.

Le CERTA recommande donc de vérifier que cette page n'est pas disponible publiquement. Vulnérabilité ou pas, une bonne pratique consiste à ôter cette page du site, et à bloquer l'exécution de la fonction associée.

5 La gestion des noms de domaines

Le CERTA a publié la note d'information CERTA-2007-INF-001 non technique sur la gestion des noms de domaines.

Elle indique les points de vigilance que sont :

- le renouvellement de la possession du nom de domaine ;
- l'abandon d'un nom de domaine.

6 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 01 et le 08 mars 2007.

7 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>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-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>
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>

8 Rappel des avis émis

Durant la période du 02 au 08 mars 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-107 : Vulnérabilité de Wordpress
- CERTA-2007-AVI-108 : Vulnérabilité dans Apache Tomcat
- CERTA-2007-AVI-109 : Vulnérabilité de Symantec SMS
- CERTA-2007-AVI-110 : Vulnérabilité de Novell Access Manager
- CERTA-2007-AVI-111 : Vulnérabilité de Webcalendar
- CERTA-2007-AVI-112 : Multiples vulnérabilités dans Apple QuickTime

Pendant la même période, l'avis suivant a été mis à jour :

- CERTA-2007-AVI-102-001 : Multiples vulnérabilités de produits Mozilla (ajout de la référence à la mise à jour de sécurité Red Hat)

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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>

10 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.

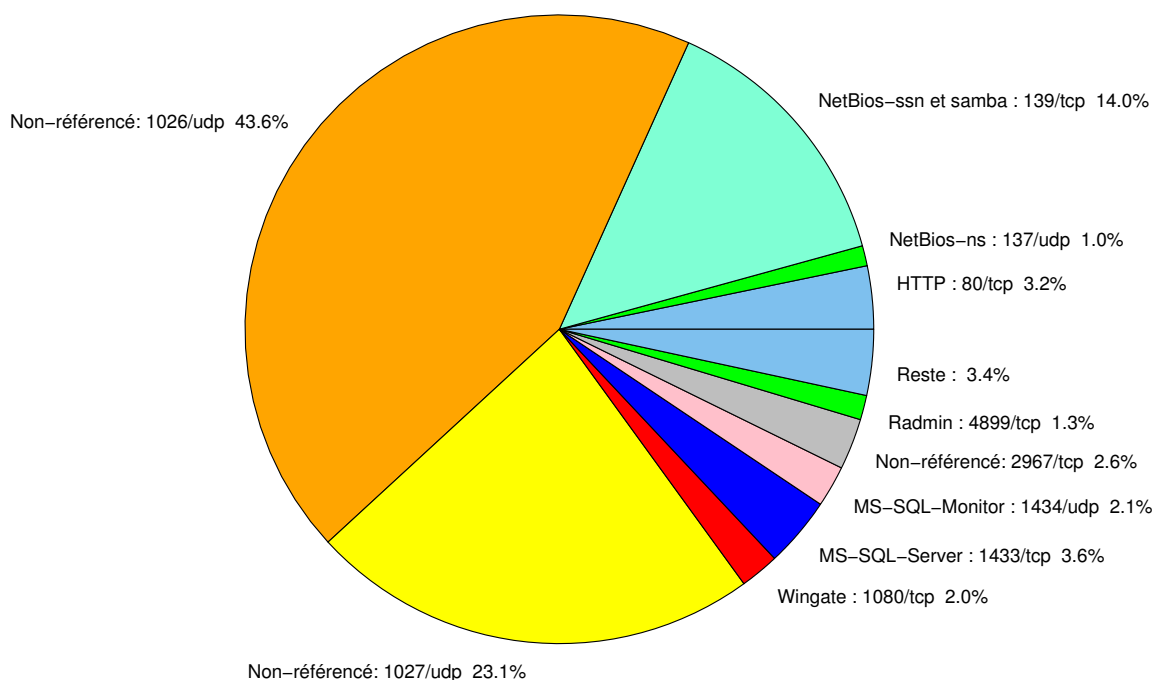


FIG. 1: Répartition relative des ports pour la semaine du 01.03.2007 au 08.03.2007

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	Yellow Worm	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
1026/udp	43.58
1027/udp	23.14
139/tcp	13.97
1433/tcp	3.6
80/tcp	3.24
2967/tcp	2.62
1434/udp	2.12
1080/tcp	2.01
4899/tcp	1.25
137/udp	1.03
21/tcp	0.78
3128/tcp	0.61
25/tcp	0.5
22/tcp	0.44
443/tcp	0.3
15118/tcp	0.19
2100/tcp	0.11
3306/tcp	0.08
143/tcp	0.05
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	8
3	Paquets rejetés	9

Gestion détaillée du document

09 mars 2007 version initiale.