



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 mai 2010
N° CERTA-2010-ACT-019

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-19

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-2010-ACT-019>

Gestion du document

Référence	CERTA-2010-ACT-019
Titre	Bulletin d'actualité 2010-19
Date de la première version	14 mai 2010
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-2010-ACT-019.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-2010-ACT-019/>

1 Vulnérabilité dans Safari

Cette semaine, une vulnérabilité relative au navigateur Safari de Apple a été publiée sur l'Internet. Cette faille non-correctée a fait l'objet de l'alerte CERTA-2010-ALE-006. Elle est relative à un problème dans la gestion des fermetures de fenêtres intempestives (*pop-ups*) et permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire via un site web construit de façon particulière.

Documentation

- Alerte CERTA-2010-ALE-006 du 14 mai 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-006/>

2 Actualité Microsoft

Les bulletins correctifs mensuels de Microsoft ont été publiés cette semaine. Les vulnérabilités découvertes sont les suivantes :

- une vulnérabilité affectant Microsoft Outlook Express, Windows Mail et Windows Live

Mail permet, à une personne malintentionnée d'exécuter du code arbitraire à distance. L'exploitation de cette vulnérabilité ne nécessite aucune authentification préalable, mais demande que l'utilisateur ciblé se connecte à un serveur de messagerie malveillant. Du code permettant d'exploiter cette vulnérabilité est déjà disponible sur l'Internet ;

- la seconde permet, par le biais d'un fichier prenant en charge *Visual Basic pour Applications (VBA)*, comme un document Office, d'exécuter du code arbitraire à distance.

Le CERTA rappelle qu'il est recommandé d'appliquer ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de mai 2010 :
<http://www.microsoft.com/france/technet/security/bulletin/ms10-may.msp>
- Avis CERTA-2010-AVI-205 (Vulnérabilité dans Microsoft Outlook Express, Windows Mail et Windows Live Mail) du 12 mai 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-205/>
- Avis CERTA-2010-AVI-206 (Vulnérabilité dans Microsoft Visual Basic pour Applications) du 12 mai 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-206/>

3 Month of PHP bugs, bilan à mi-parcours

Le mois de mai 2010 voit se dérouler un *Month of PHP bugs*, comme en mars 2007. Le principe consiste à publier chaque jour une vulnérabilité de PHP ou d'une application écrite avec ce langage. Des articles sur la sécurité de PHP sont également insérés.

À ce jour, 26 vulnérabilités ont été publiées, dont la plupart ont été découvertes antérieurement. Globalement :

- 8 vulnérabilités concernent des applications développées en PHP ;
- 9 vulnérabilités portent sur l'interpréteur de code PHP lui-même ;
- 9 vulnérabilités se situent dans l'interaction entre PHP et le moteur de scripts Zend.

Six applications présentent des possibilités d'injections SQL. Deux seulement ont émis des correctifs en réponse aux informations publiées. Deux applications offrent des possibilités d'injection de fichiers.

Les vulnérabilités liées à l'interface avec Zend appartiennent à une classe de vulnérabilités présentée à Black-Hat USA en 2009.

Le site du mois des bogues PHP donnant des preuves de faisabilité, il est à redouter que des individus malintentionnés utilisent ces informations à des fins malveillantes. Les administrateurs sont donc invités à :

- surveiller les évolutions de leurs logiciels et à appliquer les correctifs dans les plus brefs délais ;
- restreindre les accès au strict nécessaire ;
- analyser les journaux de connexions à la recherche de requêtes suspectes.

4 Gestion des comptes de services sous Windows et les secrets LSA

Aujourd'hui nous allons nous intéresser à la gestion des mots de passe des comptes de services sous Windows.

De nombreuses applications métiers sont implémentées sous forme d'un service, et souvent ces services sont paramétrés pour utiliser un compte spécifique (compte local ou du domaine).

Le gestionnaire de services (CM) utilise les secrets LSA pour stocker les mots de passe des comptes de services. Nous parlons bien de mots de passe et non de condensés...

Les secrets LSA sont stockés dans la clé :

```
HKLM\Security/Policy/Secret
```

Cette clé n'est accessible qu'à l'utilisateur "Système" par défaut (bien entendu, un administrateur peut s'élever en tant qu'utilisateur "système" très facilement). De plus les mots de passe ne sont pas stockés en clair mais sont chiffrés.

Le mot de passe (chiffré) pour un service donné se trouve dans :

```
HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets\_SC_<Nom du Service>\CurrVal
```

Ensuite pour retrouver le compte associé à ce mot de passe il faut aller voir la valeur :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<Nom du Service>\ObjectName
```

Le problème est que ce chiffrement est facilement réversible et qu'il existe de nombreux outils disponibles sur internet pour afficher en clair la liste des mots de passe stockés dans les secrets LSA, et donc ceux des comptes de services...

Maintenant prenons le scénario suivant, un service lié à une application X a été déployé sur tous les serveurs (voire toutes les machines), avec le même couple "compte de service" / "mot de passe". Ajoutons que généralement ce type de compte de service a des droits importants, souvent de type administrateur.

Nous avons donc une situation où, si une des machines est compromise, toutes les autres machines le sont, car l'attaquant est maintenant en possession d'un compte utilisateur privilégié avec son mot de passe.

Évidemment le scénario est encore pire si le compte de service utilisé n'est pas un compte local mais un compte du domaine, et pourquoi pas de type administrateur du domaine...

Une des solutions à ce problème est de ne pas utiliser de comptes spécifiques mais plutôt d'utiliser les comptes de services par défaut (Local system, Network Service etc...). On peut aussi utiliser des comptes locaux, mais avec des mots de passe unique pour chaque machine.

L'effort en terme d'administration est important mais nécessaire vu la nature du risque ...

5 Avertissement concernant le site de PHP-Nuke

Le site officiel de *PHP-Nuke* (<http://phpnuke.org>) a fait l'objet d'une compromission aux alentours du 7 mai 2010. Celle-ci s'est caractérisée par l'injection d'un *iframe* resté actif pendant plusieurs jours. Les internautes navigant sur ce site avec l'exécution de JavaScript activée étaient redirigés vers un site malveillant exploitant plusieurs vulnérabilités (notamment une concernant *Acrobat Reader*, voir avis CERTA-2010-AVI-012).

Cette information a été diffusée par de nombreux sites d'antivirus, mais elle n'a pas été relayée sur le site officiel de *PHP-Nuke*. Il est donc assez difficile d'en évaluer la portée et de savoir si les sources du produit disponibles en téléchargement ont été modifiées.

Le CERTA recommande aux administrateurs de vérifier les postes ayant navigué sur ce site en mai 2010 ainsi que l'intégrité des sources (voir avec l'éditeur) téléchargées au cours de cette période.

6 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1937>
- Note d'information du CERTA sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

7 Rappel des avis émis

Dans la période du 07 au 13 mai 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-201 : Vulnérabilité dans les imprimantes laser Lexmark
- CERTA-2010-AVI-202 : Vulnérabilité de PCRE
- CERTA-2010-AVI-203 : Vulnérabilité dans VMware View
- CERTA-2010-AVI-204 : Vulnérabilité de produits 3Com
- CERTA-2010-AVI-205 : Vulnérabilité dans Microsoft Outlook Express, Windows Mail et Windows Live Mail
- CERTA-2010-AVI-206 : Vulnérabilité dans Microsoft Visual Basic pour Applications
- CERTA-2010-AVI-207 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2010-AVI-208 : Vulnérabilité dans Cisco IronPort Desktop Flag Plug-in for Outlook
- CERTA-2010-AVI-209 : Multiples vulnérabilités dans Adobe ColdFusion

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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 CERTA peut vous aider dans ce travail d'analyse.

8.6 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.

8.7 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique67.html

9 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.

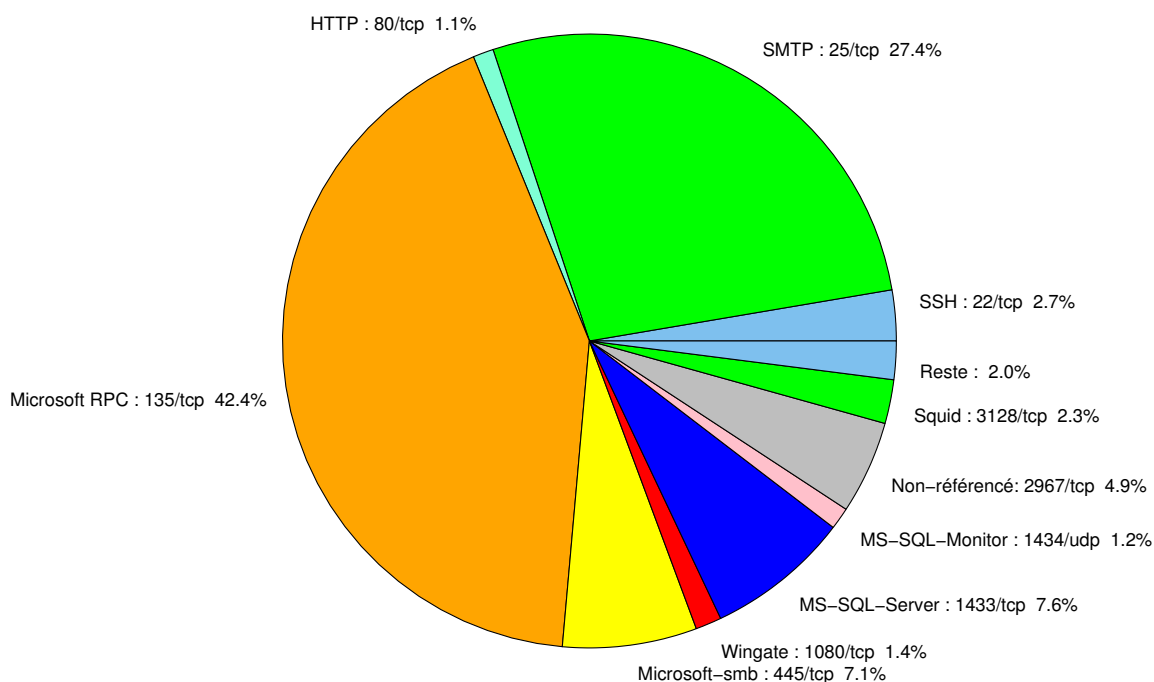


FIG. 1: Répartition relative des ports pour la semaine du 07 au 13 mai 2010

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 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
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	–	– CERTA-2007-AVI-008
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 CERTA-2007-AVI-321
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 CERTA-2007-AVI-294
427	TCP	Novell Client	-	CERTA-2006-AVI-538
443	TCP	HTTPS	-	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
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 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	-	CERTA-2007-ALE-010
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
2512	TCP	Citrix MetaFrame	-	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	-	CERTA-2006-AVI-491
2745	TCP	-	Bagle	-
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	-	CERTA-2007-AVI-331
3127	TCP	-	MyDoom	-
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	-	CERTA-2007-AVI-294
3306	TCP	MySQL	-	-
4899	TCP	Radmin	-	-
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	-	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	-	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	-
5900	TCP	VNC	-	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	-	CERTA-2007-AVI-183

6070	TCP	BrightStor ARCserve/Enterprise Backup	-	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	-	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	-	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	-	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	-	CERTA-2007-AVI-153
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	-
10110	TCP	IBM Tivoli Monitoring	-	CERTA-2007-AVI-183
10916	TCP	Ingres	-	CERTA-2007-AVI-275-001
10925	TCP	Ingres	-	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	-	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	-	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	-	CERTA-2005-AVI-310
54345	TCP	HP Mercury	-	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	-	CERTA-2007-AVI-176

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

port	pourcentage
135/tcp	42.42
25/tcp	27.41
1433/tcp	7.57
445/tcp	7.07
2967/tcp	4.9
22/tcp	2.66
3128/tcp	2.3
80/tcp	2.02
1080/tcp	1.37
1434/udp	1.15
3389/tcp	0.93
21/tcp	0.57
4899/tcp	0.43
1026/udp	0.14

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

14 mai 2010 version initiale.