

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-17

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-2008-ACT-017>

Gestion du document

Référence	CERTA-2008-ACT-017
Titre	Bulletin d'actualité 2008-17
Date de la première version	25 avril 2008
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-2008-ACT-017.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-2008-ACT-017/>

1 Incidents de la semaine

1.1 Des compromissions successives

Cette semaine, le CERTA a traité le cas d'un site défiguré par injection de code SQL. La compromission consistait à l'ajout de la chaîne de caractères Hacked by XXX signant la défiguration. Le gestionnaire du site victime, une fois prévenu, a contacté son prestataire qui lui-même externalisait le développement.

Deux actions ont alors été entreprises :

1. le prestataire, comprenant le problème et sensibilisé par la situation, a élargi ses recherches aux autres sites dont il est responsable. Il a découvert un autre site compromis. Il s'agit comme dans l'incident en cours de traitement d'une modification de tous les champs de type TEXT de la base. Cette fois, cela se caractérise par l'ajout discret d'un lien pointant vers un code javascript malveillant. Le prestataire en a informé le CERTA ;
2. le prestataire, une fois informé par le gestionnaire du site a parallèlement contacté le développeur pour qu'il corrige les vulnérabilités. En attendant la nouvelle version, il a nettoyé la base et a remis le site en ligne. Trois jours plus tard, le site était de nouveau compromis, mais cette fois-ci par le même ajout discret de lien vers un code javascript que celui infectant le site trouvé par ses soins. Ayant conscience de la fragilité du site, il a découvert assez rapidement cette nouvelle compromission.

Le prestataire a agi d'excellente manière en vérifiant le problème sur l'ensemble de ses sites. Le CERTA recommande par contre de ne jamais mettre en ligne un site vulnérable tant que le problème n'a pas été clairement identifié et que des mesures correctives ou palliatives n'ont pas été prises.

Il est par ailleurs conseillé de vérifier régulièrement l'intégrité des sites (arborescence des fichiers, contenu des fichiers et de la base). Les injections SQL sont actuellement un vecteur très actif de la propagation de codes maveillants (cf. bulletins d'actualités du 21 mars 2008 et du 18 avril 2008).

Documentation

- Bulletin d'actualités du CERTA du 21 mars 2008:
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-012/>
- Bulletin d'actualités du CERTA du 18 avril 2008:
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-016/>

1.2 L'autre danger de la mutualisation

Cette semaine, le CERTA a participé au traitement d'un incident relatif à la compromission d'un site web. Le site web utilisait une version vulnérable du gestionnaire de contenus, CMS (*Content Management System*), Joomla!. Lors de la compromission, les attaquants ont notamment déposé plusieurs fichiers utilisés pour lancer des attaques par injection de code (RFI ou *Remote File Inclusion*) sur des sites distants.

Lors du traitement de toute compromission, une des questions essentielles à se poser est la surface de l'attaque; autrement dit, quelles actions ont été réalisées par les attaquants et à quelles informations ont-ils eu accès ?

Dans cet incident, le serveur compromis hébergeait non-seulement un site web, mais également le service de messagerie de la société. Cet incident peut poser des problèmes comme :

- la confidentialité des données et des échanges ;
- l'intégrité des données présentes et échangées ;
- le vol d'informations et d'identifiants de connexion ;
- des problèmes d'image de marque ;
- l'ingénierie sociale.

Chaque service apportant son lot de vulnérabilités, la mutualisation des services augmente les risques pour le système et les impacts en cas de compromission. Il conviendra donc d'étudier avec attention la solution de mutualisation et de ne pas être uniquement dirigé par (l'argument de) l'optimisation des coûts.

Documentation

- Note d'information CERTA-2005-INF-005 concernant les bonnes pratiques pour l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information CERTA-2002-INF-002 concernant les bon réflexes en cas d'intrusion sur un système d'information :
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>

2 Vulnérabilités Safari

Cette semaine, Apple a publié la version 3.1.1 de son navigateur Safari. Le CERTA a eu connaissance de plusieurs vulnérabilités présentes dans cette dernière version. Deux d'entre elles permettent à un utilisateur distant de provoquer un déni de service via une page web particulière. Une autre permet d'usurper le contenu de la barre d'adresse URL tout en laissant cette dernière modifiable. Il s'agit donc d'une technique plus discrète que celle consistant à recouvrir la vraie barre par une image. Cette vulnérabilité pourrait être utilisée dans le cadre de tentatives de *phishing* ou d'ingénierie sociale.

Recommandations

Dans la mesure où ces vulnérabilités ne sont pas corrigées, il est recommandé d'utiliser un autre navigateur dans l'attente d'un éventuel correctif.

3 Lancer Internet Explorer 7 sans module complémentaire

Les systèmes d'exploitation comme Windows XP et Vista permettent à l'utilisateur de lancer le navigateur Internet Explorer 7 sans les modules complémentaires, les contrôles ActiveX et les BHO (*Browser Helper Object*).

Cette option est faisable :

Sous Windows XP en :

- cliquant sur << Démarrer >>
- sélectionnant << Programmes >>, puis << Accessoires >>, << Outils Système >>
- choisissant << Internet Explorer (sans module complémentaire) >>

Sous Windows Vista en :

- cliquant sur << Démarrer >>
- sélectionnant << Tous les programmes >>, << Accessoires >>, << Outils Système >>
- choisissant << Internet Explorer (sans modules complémentaire) >>

Les modules complémentaires ajoutent en principe des fonctionnalités au navigateur. Il peut s'agir de barres d'outils, de pointeurs de souris animés, de filtres pour les fenêtres surgissantes (*pop-ups*), etc.

Les modules actuellement utilisés sont visibles en se rendant dans le menu "Outils" puis "Gérer les modules complémentaires". La meilleure pratique consiste bien à les désactiver. Cela n'est pas toujours possible ou pratique à faire, et il peut être plus pratique de lancer cette version plus simple du navigateur. Certains codes malveillants fonctionnent par exemple sous la forme de BHO. Désactiver cette option peut ainsi dans les meilleurs cas affecter leur fonctionnement.

Cependant, l'utilisateur doit comprendre que cette option ne désactive pas toute interprétation dynamique de contenus, comme par exemple le JavaScript. Cette mesure n'est donc pas suffisante pour estimer pouvoir naviguer sur des sites n'étant pas de confiance.

4 La sécurité par la simplicité

Lorsque l'on veut rendre plus sûr un système d'information (SI), plusieurs options sont possibles. L'une d'entre elles consiste à appliquer à chaque élément du SI un équipement ou une extension supplémentaire remplissant un rôle spécifique dans la sécurisation de l'ensemble.

Ainsi, on trouvera un pare-feu pour les couches réseau basses, un mandataire dédié aux clients pour les couches applicatives ou bien encore un mandataire inverse (*reverse-proxy*) en amont d'un serveur web pour le protéger de requêtes « exotiques ». On pourra également trouver des extensions (ou modules) spécifiques à certains serveurs comme *mod_security* pour Apache permettant un filtrage fin des requêtes qui lui sont envoyées.

Le CERTA a récemment été sollicité pour juger de la pertinence de l'ajout de ce module en vue de rendre plus sûr un serveur web. Dans le cas présent, il s'agissait de limiter le nombre de requêtes possibles effectuées par un client dans un laps de temps donné.

Or, le postulat consistant à ajouter un module pour remplir cette fonction n'est pas forcément le bon... La question est plutôt de savoir si l'on peut, avec ce dont on dispose déjà, appliquer la politique de sécurité exigée. Pourquoi ajouter un applicatif, et, ce faisant, augmenter la surface d'attaque globale du serveur, alors que de façon intrinsèque le serveur possède déjà les outils suffisants.

Dans le cas présent, les serveurs Apache disposent dans leurs fichiers de configuration de directives comme *MaxClients* ou *MaxRequestsPerChild* permettant la limitation du nombre de clients concurrents et le nombre de requêtes par client. Il est aussi possible d'intervenir au niveau du pare-feu pour limiter le nombre de connexions possibles adressées au serveur en utilisant des fonctionnalités de comptage de sessions. Avec les éléments existants, il est donc envisageable d'intervenir et de mettre en oeuvre certaines limitations.

De manière générale, il n'est pas forcément nécessaire d'ajouter un nouveau composant pour rendre un SI plus sûr. Une bonne connaissance des possibilités des équipements ou logiciels en présence conduisant à une configuration efficace est bien souvent préférable à l'ajout d'un nouvel élément moins maîtrisé introduisant de nouveaux risques et contribuant à augmenter la complexité de l'architecture globale à maintenir.

5 Portée et Bluetooth

Le Bluetooth est une technologie de communication sans fil actuellement assez répandue sur différents types d'équipements (téléphones, ordinateurs portables, cadres photos numériques, voitures, etc.).

Le CERTA a publié une note d'information à ce sujet : CERTA-2007-INF-003. Cet article n'a pas la prétention de reprendre l'ensemble des points abordés dans le document, mais fournit une réponse à l'affirmation suivante :

« *Les risques du Bluetooth me concernent moins que ceux associés au Wi-Fi, car la portée est bien moindre.* »

Les équipements vendus dans le commerce se distinguent par le débit offert, ainsi que la puissance d'émission. Ils sont donc définis par une classe et une version, dont les valeurs peuvent prêter à confusion :

- classe 1 : équipements d'une puissance d'émission maximale de 100 mW, soit une portée annoncée d'une centaine de mètres ;
- classe 2 : équipements d'une puissance d'émission maximale de 2.5 mW, soit une portée annoncée d'une dizaine de mètres ;
- classe 3 : équipements d'une puissance d'émission maximale de 1 mW, soit une portée annoncée de l'ordre d'un mètre.

- version 1.2 : équipements offrant un débit théorique de 1Mb/s ;
- version 2.0 : équipements offrant un débit théorique de 3Mb/s.

D'autres versions ont existé ou sont encore à l'état de discussion entre constructeurs.

Le CERTA attire l'attention sur le fait que ces valeurs peuvent être modifiées, notamment du point de vue de la portée. Certaines cartes Bluetooth permettent de brancher une antenne externe. Dans le cas contraire, des sites Internet proposent de modifier physiquement certaines cartes en remplaçant les antennes intégrées. En d'autres termes, un équipement modifié de manière relativement simple peut avoir une portée de quelques centaines de mètres.

Bluetooth souffre des mêmes problèmes que le Wi-Fi. Certaines vulnérabilités peuvent directement affecter les pilotes. L'exploitation se fait alors via les couches protocolaires les plus basses et rend inutile les méthodes de sécurité mises en place à des niveaux plus élevés.

Comme pour toute technologie sans fil :

- les cartes sont en écoute et peuvent interpréter des signaux émis à plusieurs centaines de mètres ;
- la diffusion des signaux est difficilement contrôlable ;
- les normes et les matériels évoluent rapidement et sont bien souvent peu matures.

La politique de sécurité doit prendre en compte les risques du Bluetooth comme de toute autre technologie sans fil. Il est important de désactiver physiquement les interfaces si elles ne sont pas utiles et de sensibiliser les utilisateurs à ne l'activer que ponctuellement quand cela est indispensable.

Documentation

- Note d'information « Sécurité des réseaux sans fil Bluetooth » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/>

6 Du nouveau dans l'indexation de Google

La semaine dernière Google publiait un article sur un bloc-notes relatif à l'indexation des sites. L'indexation traditionnelle des pages dans le moteur de recherche repose sur le suivi de liens statiques contenu dans les pages. Le robot de Google semble apporter une nouveauté en indexant les résultats de requêtes obtenues en complétant des formulaires postés avec des informations prédites par le robot. Ces informations semblent générées en fonction du contenu du site. Selon l'article seuls les sites de confiance sont indexés de cette manière.

Cette approche semble liée au rachat par Google de la société Transformic en 2005.

De manière plus générale, les moteurs de recherche ne sont pas complètement objectifs et s'appuient sur différentes techniques pour présenter à l'utilisateur l'information qu'ils estiment la plus pertinente. Il est donc important de varier les modes de recherche et les moteurs utilisés afin d'avoir une vue plus complète des résultats.

Documentation

- Bloc-notes, "Google starts to index the invisible web" :
<http://googlesystem.blogspot.com/2008/04/google-starts-to-index-invisible-web.html>

7 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 17 et le 24 avril 2008.

8 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=1935>
- 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/>

9 Rappel des avis émis

Dans la période du 18 au 24 avril 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-210 : Vulnérabilité dans Cisco NAC Appliance
- CERTA-2008-AVI-211 : Multiples vulnérabilités dans Apple Safari
- CERTA-2008-AVI-212 : Vulnérabilité dans divers produits Computer Associates
- CERTA-2008-AVI-213 : Vulnérabilités dans IBM DB2
- CERTA-2008-AVI-214 : Multiples vulnérabilités dans HP Openview
- CERTA-2008-AVI-215 : Vulnérabilité dans Dotclear
- CERTA-2008-AVI-216 : Multiples vulnérabilités dans BEA JRockit
- CERTA-2008-AVI-217 : Vulnérabilité dans BusinessObjects XI
- CERTA-2008-AVI-218 : Multiples vulnérabilités dans OpenOffice.org
- CERTA-2008-AVI-219 : Vulnérabilité dans la bibliothèque speex
- CERTA-2008-AVI-220 : Vulnérabilité dans Xpdf
- CERTA-2008-AVI-221 : Vulnérabilité dans mplayer
- CERTA-2008-AVI-222 : Vulnérabilité dans phpMyAdmin

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

- CERTA-2008-AVI-209-001 : Vulnérabilité de Firefox (réparation du lien)

- CERTA-2007-AVI-507-001 : Vulnérabilité dans GuppY (prise en compte de la branche 46)
- CERTA-2008-AVI-208-001 : Multiples vulnérabilités dans les produits Oracle (ajout de références CVE associés à cette mise à jour)

10 Actions suggérées

10.1 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.

10.2 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 oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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>

11 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.

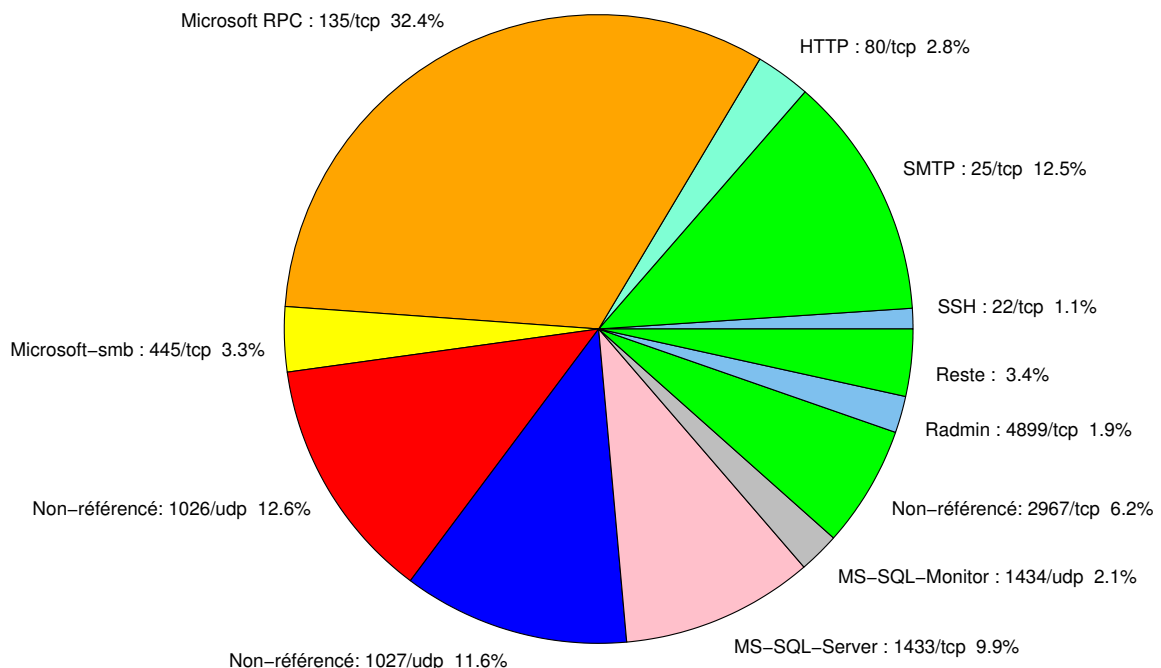


FIG. 1: Répartition relative des ports pour la semaine du 17.04.2008 au 24.04.2008

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	32.42
1026/udp	12.58
25/tcp	12.54
1027/udp	11.64
1433/tcp	9.9
2967/tcp	6.23
445/tcp	3.33
80/tcp	2.86
1434/udp	2.1
4899/tcp	1.88
22/tcp	1.05
139/tcp	0.68
143/tcp	0.65
3306/tcp	0.58
21/tcp	0.39
23/tcp	0.32
3128/tcp	0.14
1080/tcp	0.1

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	9
3	Paquets rejetés	10

Gestion détaillée du document

25 avril 2008 version initiale.