Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 septembre 2009
N° CERTA-2009-ACT-037

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-37

Gestion du document

Référence	CERTA-2009-ACT-037
Titre	Bulletin d'actualité 2009-37
Date de la première version	11 septembre 2009
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-2009-ACT-037.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-2009-ACT-037/

1 Vulnérabilités dans TCP/IP

En 2008, plusieurs failles de la pile TCP/IP trouvées par des chercheurs finlandais ont été largement médiatisées. Ces vulnérabilités ont été communiquées à divers éditeurs, parmi lesquels certains ont arrêté une date (mardi 08 septembre 2009) pour publier des correctifs. Cette date correspond à la publication mensuelle des mises à jour de Microsoft.

Ainsi, cette semaine, les éditeurs Microsoft, Cisco, et Check Point ont publié des correctifs concernant ces vulnérabilités de TCP. D'autres éditeurs ont annoncé que leurs produits ne sont pas affectés, et d'autres qu'ils ne publieraient pas de correctif (Red Hat) mais des contournements permettant d'atténuer les effets d'une potentielle attaque. En ce qui concerne Microsoft, si l'éditeur a émis des correctifs pour certains systèmes d'exploitation, il a également annoncé ne pas être en mesure de le faire pour Windows 2000 et Windows XP. L'éditeur Sun, en revanche, a déclaré que ses produits sont affectés mais seraient corrigés à une date ultérieure.

Dans cette optique, le CERTA a décidé de publier l'alerte CERTA-2009-ALE-017 concernant les produits non corrigés. Il est important de noter que même si un seul CVE a été attribué (CVE-2008-4609), il s'agit toutefois de plusieurs vulnérabilités. Le principe est généralement le même et consiste à saturer les systèmes au moyen de certains paramètres TCP tel que le *window size*. Les impacts peuvent également largement varier selon les systèmes.

S'agissant de failles dans l'implémentation du protocole TCP, il n'existe pas de contournement adapté notamment pour les serveurs. Les postes clients peuvent utiliser un pare-feu à état (*stateful*) pour bloquer les connexions entrantes non sollicitées. Les administrateurs de serveurs vulnérables peuvent éventuellement limiter le nombre de sessions TCP autorisées par adresse IP.

1.1 Documentation

– Vulnérabilités dans TCP/IP, alerte CERTA-2009-ALE-017 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-017/index.html

2 Actualité Microsoft

2.1 Vulnérabilité de SMBv2 dans Microsoft Windows Vista et Server 2008

L'alerte CERTA-2009-ALE-016 publiée cette semaine concerne une faille du pilote `srv2.sys`. Une personne malintentionnée peut provoquer un déni de service ou potentiellement exécuter du code arbitraire, au moyen d'un paquet `SMBv2` spécialement conçu.

En attendant un correctif de sécurité la part de Microsoft, il est recommandé de désactiver `SMBv2` sur les systèmes vulnérables. Cela peut évidemment avoir des effets secondaires. Le filtrage des ports tcp/139 et tcp/445 permettant de bloquer les paquets `SMB`, il convient également d'appliquer un tel filtrage sur le périmètre du système d'information. Seuls Windows Server 2008 et Windows Vista sont concernés par cette faille. Les versions finales de Windows 7 et Windows Server 2008 R2 ont, d'ores et déjà, été corrigées et `SMBv2` n'est pas inclus dans les versions antérieures de Windows.

2.2 Les bulletins mensuels de Microsoft

Cette semaine, *Microsoft* a publié ses bulletins mensuels de sécurité. Le CERTA revient sur ces différents bulletins :

– MS09-045 : un défaut du moteur *JScript* permet à un utilisateur malveillant d'exécuter du code arbitraire avec les droits de l'utilisateur connecté ;
– MS09-046 : le composant d'édition DHTML sur les systèmes *Microsoft Windows* 2000, *XP* et *Microsoft Windows Server* 2003 présente une vulnérabilité exploitable par un utilisateur malveillant afin d'exécuter du code arbitraire avec les droits de l'utilisateur connecté ;
– MS09-047 : la lecture des fichiers ASF et MP3 malformés par *Microsoft Windows Media Player* n'est pas suffisamment robuste. Un utilisateur malveillant peut, par le biais de fichiers MP3 ou ASF spécialement conçus, exécuter du code arbitraire avec les droits de l'utilisateur connecté ;
– MS09-048 : des vulnérabilités dans la gestion du protocole TCP/IP, dont l'exploitation permet de réaliser un déni de service avec peu de ressources, sont corrigées pour les systèmes *Microsoft Windows Server* 2003 et 2008 et *Microsoft Windows Vista*. Aucun correctif ne sera développé pour *Microsoft Windows* 2000 dont la fin du support est en juillet 2010, et pour *Microsoft Windows XP* qui n'est vulnérable que si des exceptions sont autorisées dans la configuration du pare-feu. De nombreuses applications créent des exceptions lorsqu'elles s'installent. Il est donc fortement recommandé de vérifier les configurations et de fermer en entrée les ports inutiles ou devenus inutiles ;
– MS09-049 : l'utilitaire de configuration automatique des réseaux locaux sans fil est vulnérable. Avec des trames spécialement conçues, un utilisateur malveillant peut exécuter du code arbitraire à distance avec des droits complets sur l'ordinateur.

Le CERTA rappelle l'impérative nécessité d'appliquer au plus vite ces correctifs afin de protéger son système d'information. De plus l'utilisation de l'ordinateur avec un compte sans privilège inutile permet de réduire l'impact de l'exploitation des vulnérabilités mentionnées dans les trois premiers bulletins.

2.3 Documentation

– Vulnérabilités dans TCP/IP, alerte CERTA-2009-ALE-017 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-017/index.html
– Vulnérabilité dans SMBv2, alerte CERTA-2009-ALE-016 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-016/index.html

– Synthèse des bulletins de sécurité Microsoft de septembre 2009 :
http://www.microsoft.com/france/technet/security/bulletin/ms09-sep.mspx

3 Un ver pour WordPress

Un ver ciblant des installations de *WordPress* non mises à jour se propage depuis quelques jours. Sa méthode d'attaque est la suivante :

– un utilisateur est enregistré ;
– une vulnérabilité permettant l'élévation des privilèges est exploitée. Cette vulnérabilité est corrigée dans la version 2.8.3 de *WordPress* (voir avis CERTA-2009-AVI-315) ;
– du code exécutable `PHP` est inséré dans un *permalink* ;
– un compte avec des droits d'administrateur est alors créé via une requête `HTTP` spécifique qui exploite le code inséré dans le *permalink* .

Le ver est susceptible de modifier des fichiers tels que `.htaccess` et de désactiver l'enregistrement des nouveaux comptes. Le compte avec les droits d'administrateur n'apparaît pas dans la liste des utilisateurs du *WordPress*. Le ver peut entraîner quelques dysfonctionnements pour le site attaqué, notamment au niveau des liens. Il est censé ajouter des publicités pour des produits pharmaceutiques ou des codes malveillants sur certaines pages. Les versions 2.8.3 et 2.8.4 de *WordPress* sont réputées insensibles à ce ver.

Les administrateurs de *WordPress* sont fortement incités à mettre à jour leur gestionnaire de contenu en version 2.8.4. Il est également conseillé de vérifier les *permalinks* et de regarder dans les journaux si des utilisateurs ont été ajoutés récemment. Enfin, une lecture du document « *Hardening WordPress* » (voir documentation) est encouragée.

Documentation

– Référence au ver *WordPress* :
http://wordpress.org/development/2009/09/keep-wordpress-secure/
– Document « *Hardening WordPress* » :
http://codex.wordpress.org/Hardening_WordPress
– Avis CERTA-2009-AVI-315 :
http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-315/

4 XSS inter-protocolaire

4.1 Le XSS

Les attaques par XSS sont désormais des attaques bien connues. Pour rappel, le principe consiste à injecter du code dans une page de manière volatile ou non afin d'exécuter un script externe sur une page Internet légitime. Les vecteurs permettant ces attaques sont tout aussi connus : formulaires mal construits, pages d'erreurs verbeuses, etc. Le concept est systématiquement le même : dès l'instant qu'une page émet un *écho* contrôlable par l'attaquant et non filtré par le serveur, l'injection permettant un XSS est possible.

Généralement, l'appréhension générale d'un XSS reste assez mauvaise. L'impact de telles attaques est souvent minimisé. Nous ne reviendrons pas dessus, mais différents articles du bulletin d'actualité du CERTA traitent de ce problème.

4.2 Les échos protocolaires

Le concept même d'un XSS reste parfois bien flou. Pour beaucoup de personnes, le XSS ne se cantonne qu'au seul protocole `HTTP`. Et qui dit protocole `HTTP` dit vulnérabilité web. C'est malheureusement faux. Il est tout à fait possible de réaliser un XSS en utilisant des faiblesses de différents protocoles d'échanges (DNS, FTP, POP3, SMTP, etc.). Le principe de l'attaque reste le même : il suffit de trouver un *écho* dont le contenu est peu ou pas contrôlé par le serveur. Prenons par exemple, la commande `HELO` (ou `EHLO`). Cette commande sert de *poignée de main* avec un serveur SMTP. Les standards définissent le principe même de cette *poignée de main*, mais le type

de réponse (hors code retour) et son implémentation sont laissés libre. Ainsi chaque serveur pourra répondre à sa manière. Par exemple :

```
envoi client :              HELO mail@exemple.tld
réponse du serveur :  250 hello mail@exemple.tld
```

Dans ce cas, on remarque la réponse en *écho* du serveur. Une personne malveillante peut alors utiliser cette faille pour obliger le serveur de mail à répondre par un script. Il faut alors trouver une méthode pour provoquer l'interrogation du serveur de messagerie via un navigateur. Certaines études récentes démontrent la faisabilité de ce type d'attaque.

4.3 Comment s'en protéger ?

Du côté serveur, on peut limiter l'exploitation de ces faiblesses en apportant une attention toute particulière aux produits utilisés et aux interactions entre le client et ce produit. Parfois, un audit pourra s'avérer utile.

Du côté client, le meilleur moyen de se protéger de manière générique des attaques de type XSS reste de désactiver l'interprétation de toute forme de script par le navigateur (vbscript, JavaScript, etc.) et de ne réactiver la fonctionnalité qu'en cas d'impérieuse nécessité vis à vis d'un site de confiance. Cette mesure draconienne semble pour beaucoup impossible à tenir et pourtant, il apparaît que la navigation sans script reste encore possible, même si la perte en ergonomie est grande.

5 Firefox : une mise à jour bienveillante

Cette semaine, une nouvelle version du navigateur `Mozilla Firefox` a été publiée. Cette nouvelle mouture corrige plusieurs vulnérabilités détaillées dans l'avis CERTA CERTA-2009-AVI-379, mais ajoute également une fonctionnalité intéressante.

En effet, après l'installation de la mise à jour, un message apparaît si le module `Adobe Flash` installé n'est dans sa dernière version. Un lien vers la page officielle du site d'`Adobe` est également présenté afin d'obtenir la dernière version du module. Cette initiative ne peut être que saluée surtout lorsque des mises à jour du système d'exploitation `Apple Mac OS X` provoquent une régression de ce module (cf. le bulletin d'actualité CERTA-2009-ACT-036). La fondation `Mozilla` projette d'intégrer ce contrôle de version pour d'autres modules dans une prochaine évolution de son navigateur.

Documentation

- Avis CERTA-2009-AVI-379 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-379/
- Bulletin d'actualité CERTA-2009-ACT-036 du 04 septembre 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-036/

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 04 août au 10 septembre 2009, le CERTA a émis les avis suivants :

– CERTA-2009-AVI-366 : Vulnérabilité Java de Mac OS X
– CERTA-2009-AVI-367 : Vulnérabilité dans IBM Tivoli Identity Manager
– CERTA-2009-AVI-368 : Vulnérabilité dans IBM Lotus Domino Web Acess
– CERTA-2009-AVI-369 : Vulnérabilité de Microsoft JScript
– CERTA-2009-AVI-370 : Vulnérabilité dans le composant d'édition DHTML de Microsoft Windows
– CERTA-2009-AVI-371 : Vulnérabilités dans Windows Media Format
– CERTA-2009-AVI-372 : Multiples vulnérabilités dans TCP/IP sous Windows
– CERTA-2009-AVI-373 : Vulnérabilité dans Microsoft Wireless LAN AutoConfig Service
– CERTA-2009-AVI-374 : Vulnérabilité dans Asterisk
– CERTA-2009-AVI-375 : Vulnérabilité de Ruby on Rails
– CERTA-2009-AVI-376 : Vulnérabilité dans les produits Check Point
– CERTA-2009-AVI-377 : Vulnérabilités des produits Cisco
– CERTA-2009-AVI-378 : Multiples vulnérabilités dans Apple QuickTime
– CERTA-2009-AVI-379 : Vulnérabilités dans Mozilla Firefox

Pendant la même période, les avis suivants ont été mis à jour :

– CERTA-2009-AVI-335-001 : Multiples vulnérabilités dans libxml2 (ajout des références Sun et Ubuntu)
– CERTA-2009-AVI-362-001 : Vulnérabilités dans OpenOfficeorg (ajout des références aux bulletins Debian, Fedora et RedHat.)

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 règlementaire, 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

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.

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 inexpliqués 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_rubrique63.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.

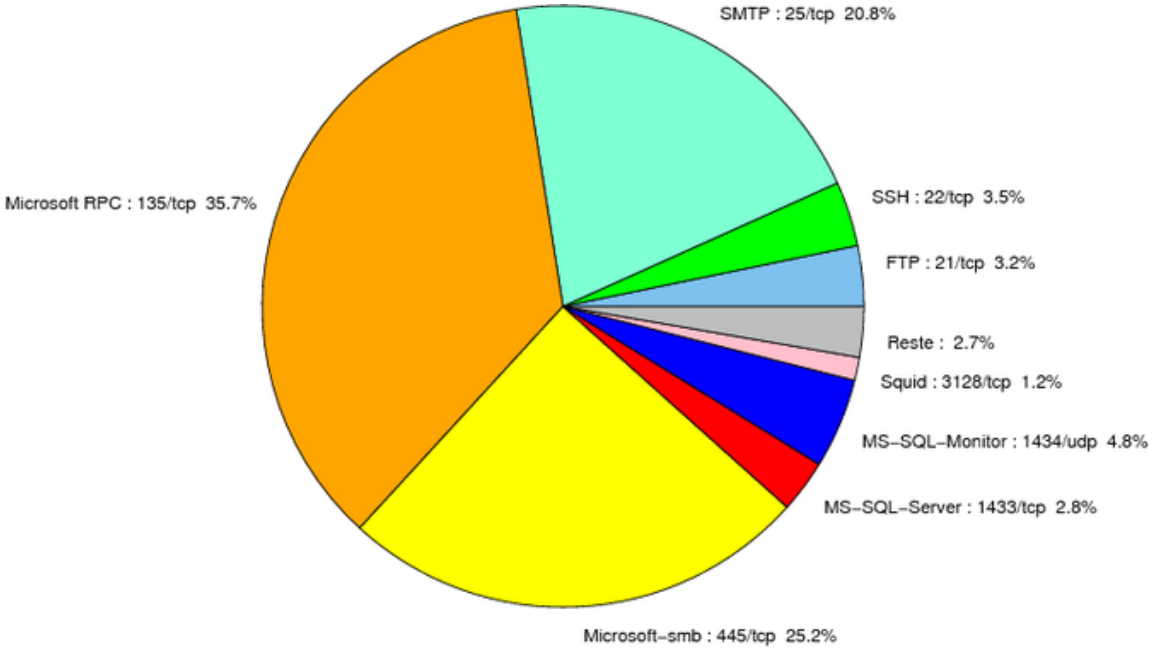

FIG. 1: Répartition relative des ports pour la semaine du 05 au 10 septembre 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
135/tcp	35.69
445/tcp	25.19
25/tcp	20.76
1434/udp	4.83
22/tcp	3.48
21/tcp	3.24
1433/tcp	2.83
3128/tcp	1.23
2967/tcp	0.76
1080/tcp	0.58
80/tcp	0.47
4899/tcp	0.35
3389/tcp	0.23
3306/tcp	0.11

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

11 septembre 2009 version initiale.