Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 mars 2010
N° CERTA-2010-ACT-012

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-12

Gestion du document

Référence	CERTA-2010-ACT-012
Titre	Bulletin d'actualité 2010-12
Date de la première version	26 mars 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-012.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-012/

1 Vulnérabilité dans les cartes réseau Broadcom

Cette semaine, lors de la conférence `CanSecWest`, des ingénieurs de l'ANSSI ont fait la démonstration de l'exploitation d'une vulnérabilité dans certains contrôleurs réseau permettant d'exécuter du code arbitraire à distance. Cette vulnérabilité permet via une série de paquets spécialement construits de mettre en place une attaque de type « *Man in the middle* » (homme au milieu), de récupérer des clés cryptographiques ou d'injecter du code malveillant dans la mémoire de la machine compromise.

L'impact de cette vulnérabilité concernant les modèles `Broadcom NetXtreme` est cependant à nuancer. En effet, une configuration spécifique est nécessaire. La fonctionnalité *ASF* (*Alert Standart Format*) doit être activée et configurée, ce qui n'est pas le cas par défaut.

Le CERTA invite donc les possesseurs de ce type d'équipements à se rendre sur le site Internet de l'intégrateur de leurs machines afin de télécharger la dernière version du microcode de la carte réseau et à installer cette dernière.

Le CERTA profite également de cette actualité pour attirer l'attention sur l'utilité de mettre à jour le code embarqué dans les périphériques matériels. En effet, en faisant la démonstration que la compromission d'une machine via son contrôleur est possible, l'ANSSI rappelle que le code embarqué dans les périphériques doit lui aussi être soumis aux bonnes pratiques de développement, de test et de maintien.

1.1 Documentation

- Support de la présentation faite à la CanSecWest :
  http://www.ssi.gouv.fr/site_article186.html
- Article « Peut-on faire confiance aux cartes réseau ? » :
  http://www.ssi.gouv.fr/site_article187.html
- Avis CERTA-2010-AVI-121 concernant le correctif fourni par HP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-121

2 Durcissement de la configuration des systèmes Windows (5/8)

2.1 Désactivation du cache d'ouverture de sessions interactives

Par défaut, un système Windows conserve les empreintes des informations liées aux dix dernières connexions par des comptes membres du domaine : il s'agit des « caches de domaine ». Cette fonctionnalité est utilisée lorsque le poste de travail n'arrive plus à joindre un contrôleur de domaine. Dans ce cas, le système Windows authentifie l'utilisateur à l'aide de cette base de cache. Toutefois, un utilisateur malveillant ayant des droits d'administration ou un accès physique à la machine peut récupérer de cette manière les caches et effectuer une attaque par essais successifs sur les mots de passe.

Il est possible de configurer le nombre d'entrées de ce cache de domaine à l'aide de la GPO nommée : « Ouvertures de sessions interactives : nombre d'ouvertures de sessions précédentes réalisées en utilisant le cache ». Réduire à 1 cette valeur permettra de garder le dernier compte en cache (généralement le compte courant) et la mettre à 0 permet de désactiver cette fonctionnalité.

2.2 Augmentation du niveau de sécurité de l'authentification à distance

De manière à réduire très fortement les possibilités de cryptanalyse sur les mots de passe *via* l'écoute réseau dans un environnement Windows, il convient de ne pas permettre l'utilisation des protocoles d'authentification obsolètes que sont LM et NTLM. Seuls les mécanismes d'authentification NTLMv2 ou Kerberos doivent être acceptés.

Le paramètre intitulé « *niveau de compatibilité LM* » permet de gérer la configuration de la compatibilité LM, NTLM ou NTLMv2 en activant ou désactivant ces protocoles. Celui-ci est défini par la donnée de la valeur `LMCompatibityLevel` de la clé de registre `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\`.

Six niveaux peuvent être définis :

0	Envoyer les réponses LM et NTLM
1	Envoyer LM & NTLM - Utiliser la sécurité de session NTLMv2 si négociée
2	Envoyer uniquement les réponses NTLM
3	Envoyer uniquement les réponses NTLMv2
4	Envoyer uniquement les réponses NTLMv2\Refuser LM
5	Envoyer uniquement les réponses NTLMv2\Refuser LM et NTLM

Le niveau de compatibilité LM peut être configuré dans les *Options de sécurité*. Sous Windows 2000, le paramètre s'appelle « *Niveau d'authentification LAN Manager* » et à partir de Windows XP « *Sécurité réseau : niveau d'authentification LAN Manager* ».

Il est recommandé de positionner la valeur au niveau 3 ou plus. Dans ce cas, le système utilise uniquement le protocole NTLMv2 pour s'authentifier (mais il accepte toujours les protocoles LM ou NTLM). La valeur 5 renforce encore la sécurité en permettant d'accepter uniquement le protocole NTLMv2.

De Windows 2000 à Windows 2003, le niveau de compatibilité est par défaut positionné à la valeur 0. En revanche, à partir de Windows Vista, ce niveau est porté à la valeur 3.

Par ailleurs, il est conseillé d'appliquer ce paramètre sur un premier échantillon de systèmes pour détecter une éventuelle incompatibilité, puis de généraliser cette configuration si aucun problème n'est détecté.

Pour plus d'informations, reportez-vous aux articles suivants sur le site Internet de Microsoft :
`http://support.microsoft.com/kb/239869/fr`
`http://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx`

3 Arnaque aux SMS sur téléphones mobiles

Les courriers électroniques non sollicités (*SPAM*) sont malheureusement, depuis plusieurs années, monnaie courante sur Internet ; quiconque utilise un compte de messagerie a appris depuis longtemps à trier ces courriers, en écartant les publicités et autres tentatives de filoutage... Mais depuis quelques temps, les personnes malhonnêtes qui utilisaient ce média ont bien compris que d'autres supports pouvaient être intéressants. Ainsi sont apparus les *SMS* publicitaires. Dans ce domaine, l'imagination des attaquants est très forte. Ainsi, le CERTA est fréquemment informé de l'utilisation de scénarios plus évolués, destinés à tromper l'utilisateur, et si possible à lui soutirer de l'argent. Parmi eux, citons :

- le *ping call* : le téléphone portable sonne une seule fois, l'usager n'a généralement pas le temps de prendre l'appel. Le numéro de l'appelant restant affiché, l'utilisateur est tenté d'utiliser les fonctions automatiques de son téléphone afin de rappeler aussitôt le numéro. Problème, ce numéro est fortement surtaxé (par exemple de la famille des 08 99 xx xx xx) et mis à part un peu de musique, ou des messages enregistrés, aucun interlocuteur humain ne sera présent derrière ce numéro ;
- le faux *SMS* de messagerie : vous recevez un *SMS* vous indiquant qu'un message vous attend sur une boîte vocale externe. Pour le lire, il faut à votre tour envoyer un *SMS* vers un numéro surtaxé. Là encore, les attaquants ciblent votre portefeuille.

3.1 Un cas intéressant

Récemment, le CERTA a été informé d'une arnaque au *SMS* mettant aussi en œuvre un faux serveur web : l'utilisateur a reçu sur son téléphone portable un *SMS* de la forme :

```
<< Messagerie Multimédia : le 06xxxxxxxx a reçu 1 nouveau SMS vidéo à 8h03.
Pour le lire : http://tinyurl.com/xxxxxxxx >>
```

L'astuce ici repose sur l'utilisation du service « *tinyurl* » qui va cacher le nom du vrai serveur accédé, *Tinyurl* étant un simple service de redirection et de « raccourcissement » des URL. Si l'utilisateur clique sur le lien, il accède à une page contenant un lien actif qui, une fois activé, va, à l'insu de l'utilisateur, émettre un *SMS* surtaxé (dans le cas présent, il coûte 4,5 euros !).

FIG. 1 – *Exemple d'un SMS frauduleux*

Dans ce scénario, plusieurs éléments sont enchainés afin de tromper la vigilance de l'utilisateur, pour finalement l'amener à commettre la faute qui entrainera la facturation.

3.2 Comment se protéger

Face à ces nouvelles menaces, il convient avant tout de conserver une attitude prudente et de ne jamais répondre à un *SMS* inconnu, ou rappeler un numéro étrange. Typiquement, les 08 9x xx xx xx doivent attirer votre attention.

Enfin, depuis un peu plus d'un an, les opérateurs télécom français ont mis en place une plateforme de signalement destinée à remonter ce type de problèmes survenant dans les environnements mobiles. Il est possible de faire suivre les *SMS* suspects au 33 700 afin que votre opérateur puisse les traiter et éventuellement engager des poursuites judiciaires. De plus amples informations sont disponible sur le site web du 33700, `http://www.33700-spam-sms.fr/`

4 Conférence CanSecWest 2010

La conférence *CanSecWest* 2010 qui se tient à Vancouver du 24 au 26 mars 2010, a annoncé le début du concours *Pwn2Own*. Ce concours, créé dans le contexte du *Zero Day Initiative* fondé par la société *Tipping Point*, a pour objectifs l'exploitation de vulnérabilités des navigateurs Internet et la découverte de vulnérabilités affectant divers téléphones mobiles.

Les navigateurs choisis pour ce concours sont les suivants :

- Microsoft Internet Explorer 8 pour Windows 7 ;
- Mozilla Firefox 3 sur Windows 7 ;
- Google Chrome 4 pour Windows 7 ;
- Apple Safari 4 pour MacOS X Snow Leopard.

Parmi les solutions de téléphones mobiles sélectionnées pour ce concours on peut citer :

- Apple iPhone 3GS ;
- RIM Blackberry Bold 9700 ;
- Nokia E72 fonctionnant sous SymbianOS ;
- HTC Nexus One fonctionnant sous Android.

À ce stade du concours, plusieurs vulnérabilités affectant ces solutions ont été annoncées. Ces vulnérabilités, dont les détails techniques ont pu être publiés, devront être confirmées par les éditeurs respectifs. Il ne peut être exclu qu'une ou plusieurs vulnérabilités annoncées fassent l'objet d'un code d'exploitation avant la publication d'un correctif de sécurité.

Les vulnérabilités suivantes ont d'ores et déjà été annoncées :

- exécution de code arbitraire dans `Internet Explorer` :
  http://www.securityfocus.com/bid/38951
- exécution de code arbitraire dans `Mozilla Firefox` :
  http://www.securityfocus.com/bid/38952
- exécution de code arbitraire dans `Safari 4` pour `MacOS` :
  http://www.securityfocus.com/bid/38955
- exécution de code arbitraire dans `Safari` pour `iPhone` :
  http://www.securityfocus.com/bid/38957

Le CERTA recommande à ses lecteurs la plus grande vigilance sur ces produits et une veille active quant à la publication des correctifs les concernant.

Documentation

- Site web de la conférence CanSecWest 2010 :
  http://cansecwest.com/index.html
- Annonce du concours Pwn2Own par Tipping Point / DVLabs :
  http://www.dvlabs.tippingpoint.com/blog/2010/02/15/pwn2own-2010

5 Problème avec BitDefender

Le 20 mars 2010, une mise à jour automatique de *BitDefender* (versions 2008, 2009 et 2010) a posé de nombreux problèmes aux utilisateurs. En effet, après installation de cette mise à jour, l'antivirus considère que plusieurs fichiers de *Windows* et de *BitDefender* sont infectés par un code malveillant appelé `Trojan.FakeAlert.5`. Par conséquent, certains programmes -voire tout le système- deviennent inutilisables.

Une nouvelle mise à jour automatique de *BitDefender* a été proposée afin de remédier à ce problème. Toutefois, pour les utilisateurs qui rencontreraient des problèmes persistants, *BitDefender* a publié un lien vers un CD de restauration qui devrait remettre le système en état de marche.

Documentation

- Article de BitDefender relatif au problème du 20 mars 2010 :
  http://www.bitdefender.com/site/KnowledgeBase/consumer/#638
- CD de restauration proposé par BitDefender :
  http://www.bitdefender.com/site/KnowledgeBase/consumer/#650

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 19 au 25 mars 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-128 : Multiples vulnérabilités dans CA ARCserve Backup
- CERTA-2010-AVI-129 : Vulnérabilité dans IBM DB2 Content Manager
- CERTA-2010-AVI-130 : Vulnérabilité dans Firefox
- CERTA-2010-AVI-131 : Vulnérabilités dans Opera
- CERTA-2010-AVI-132 : Multiples vulnérabilités dans Qt
- CERTA-2010-AVI-133 : Vulnérabilité dans Samba
- CERTA-2010-AVI-134 : Vulnérabilités dans Cisco Unified Communications Manager Express

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_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.

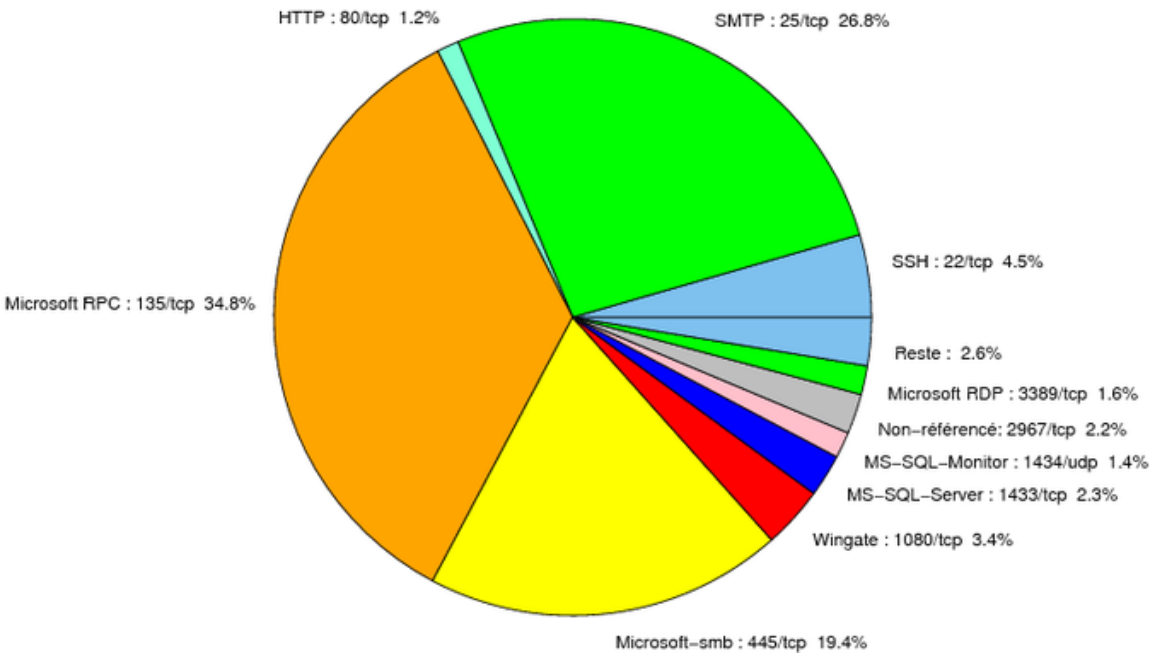

FIG. 2: Répartition relative des ports pour la semaine du 19 au 25 mars 2010

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

				http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT

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	34.77
25/tcp	26.8
445/tcp	19.35
22/tcp	4.46
1080/tcp	3.35
80/tcp	2.38
1433/tcp	2.3
2967/tcp	2.15
3389/tcp	1.56
1434/udp	1.41
23/tcp	0.74
3128/tcp	0.67
4899/tcp	0.29
3306/tcp	0.22

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

26 mars 2010 version initiale.