Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mars 2010
N° CERTA-2010-ACT-010

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-10

Gestion du document

Référence	CERTA-2010-ACT-010
Titre	Bulletin d'actualité 2010-10
Date de la première version	12 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-010.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-010/

1 Actualités Microsoft

1.1 Bulletins du mois de mars

Cette semaine, Microsoft a émis deux bulletins de sécurité :

– MS10-016 concerne une vulnérabilité dans `Windows Movie Maker` et `Microsoft Producer 2003` permettant l'exécution de code arbitraire à distance ;
– MS10-017 concerne plusieurs vulnérabilités dans les produits `Microsoft Excel` et `Microsoft Office Sharepoint Server`. Leur exploitation permet également l'exécution de code arbitraire à distance.

Le CERTA recommande l'application des correctifs dès que possible.

1.2 Vulnérabilité non corrigée dans Internet Explorer

Cette semaine, le CERTA a également émis une alerte concernant les navigateurs `Internet Explorer 6` et `Internet Explorer 7`. La faille est actuellement exploitée sur l'Internet et il est donc impératif d'appliquer les mesures détaillées dans la section « contournement provisoire » de l'alerte pour se protéger.

Le CERTA rappelle que la vulnérabilité est exploitable au moyen de plusieurs vecteurs d'attaque, notamment des sites *Web* spécialement conçus mais également des documents `Microsoft Office`. Dans ce sens, l'utilisation d'un navigateur alternatif n'est pas suffisante pour se protéger contre tous les vecteurs. En effet, cela protège un utilisateur lors de la navigation Internet mais pas lors de l'ouverture d'un document spécialement construit, par exemple. La restriction d'accès sur la bibliothèque vulnérable ou la mise à jour vers `Internet Explorer 8` sont donc nécessaires pour se protéger totalement contre cette faille.

1.3 Documentation

– Alerte CERTA-2010-ALE-004 du 10 mars 2010 :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-004/

2 Durcissement de la configuration des systèmes Windows : restriction des accès anonymes (3/8)

Les sessions nulles, c'est-à-dire des accès non authentifiés (le client n'a pas besoin de fournir un identifiant et un mot de passe), ont toujours été source d'accès illégitimes aux systèmes Windows. Elles doivent donc être restreintes ou désactivées, afin de se protéger contre la fuite d'information (comptes utilisateurs, partages réseau, etc.). En effet, parmi les fonctions natives d'un système Windows, les fonctions d'énumération accessibles *via* des interfaces RPC étaient historiquement appelables sans authentification. Ces interfaces RPC sont généralement accessibles par le mécanisme des canaux nommés (*named pipes*) et transportées sur le réseau au moyen du protocole SMB.

Cette recommandation s'applique tant pour les postes de travail que pour les serveurs. Il existe plusieurs dispositifs de sécurisation suivant les différentes versions de Windows.

2.1 Windows 2000

La valeur `RestrictAnonymous` de la clef de registre `HKLM\SYSTEM\CurrentControlSet\Control\Lsa` permet de définir des restrictions d'accès pour les connexions anonymes. Elle peut prendre une valeur allant de 0 à 2 :

0 : aucune protection n'est activée. Il est alors possible d'accéder anonymement à de nombreuses interfaces RPC. Il s'agit de la valeur par défaut ;

1 : certaines fonctions RPC, telles que celles permettant l'énumération des comptes utilisateurs et les partages réseau ne sont pas autorisées si le client ne s'est pas préalablement authentifié ;

2 : aucune interface RPC accessible au moyen des canaux nommés ne peut être appelée si le client n'est pas authentifié. Cette option a posé de nombreux problèmes de compatibilité, en particulier avec des applications tierces. Elle n'a donc pas été maintenue dans les versions ultérieures de Windows.

Ce paramètre peut être configuré au travers des *Options de sécurité*. Sous Windows 2000, le paramètre s'appelle « *Restrictions supplémentaires pour les connexions anonymes* » et doit être positionné à la valeur « *Ne pas permettre l'énumération des comptes et partages SAM* », ce qui correspond au niveau 1 du tableau ci-dessus.

2.2 À partir de Windows XP et Windows 2003

La valeur `RestrictAnonymous` est toujours présente, mais seules les valeurs 0 et 1 sont possibles. En revanche, deux nouveaux paramètres font leur apparition, toujours sous la clef `HKLM\SYSTEM\CurrentControlSet\Control\Lsa` :

– la valeur `RestrictAnonymousSam` (pouvant prendre la valeur 0 ou 1) permet d'activer des restrictions supplémentaires sur certaines fonctions RPC natives de Windows ;
– la valeur `EveryoneIncludesAnonymous` (pouvant prendre la valeur 0 ou 1) permet de séparer le contexte de sécurité des connexions anonymes (`ANONYMOUS LOGON`) de toutes les autres (`Tout le monde`).

Ces paramètres peuvent être configurés au travers des *Options de sécurité*. La liste suivante indique les correspondances entre le nom des valeurs de la base de registre et le nom de l'option dans l'éditeur de stratégie :

- `RestrictAnonymous` → *Accès réseau : ne pas autoriser l'énumération anonyme des comptes SAM* : le paramètre doit être activé ;
- `RestrictAnonymousSAM` → *Accès réseau : ne pas autoriser l'énumération anonyme des comptes et partages SAM* : le paramètre doit être activé ;
- `EveryoneIncludesAnonymous` → *Accès réseau : les autorisations Tout le monde s'appliquent aux utilisateurs anonymes* : le paramètre doit être désactivé.

Par ailleurs, toujours dans les *Options de sécurité*, le paramètre *Accès réseau : Permet la traduction de noms/SID anonymes* autorise ou interdit la conversion anonyme des identifiants de sécurité (SID) vers le nom de l'entité associée. Ce paramètre doit être désactivé.

Enfin, au niveau des contrôleurs de domaine Windows 2003, il convient de vérifier que le groupe spécial `ANONYMOUS LOGON` ainsi que `EVERYONE` ne figurent pas dans le groupe `Pre Windows 2000 Compatible Access`.

2.3 À partir de Windows XP Service Pack 2 et de Windows 2003 Service Pack 1

Les paramètres décrits ci-dessous, bien que déjà présents dans les versions antérieures de Windows ou de Service Pack, ne permettaient pas de contrôler certaines valeurs implicitement positionnées par le système, réduisant ainsi leur utilité.

Ce problème est désormais corrigé, l'ensemble des valeurs étant paramétrable sous la clef `HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\parameters` :

- la valeur `NullSessionsShare` énumère les partages réseau qui sont accessibles de manière anonyme (le partage `IPC$` reste toujours implicite pour des raisons de compatibilité) ;
- la valeur `NullSessionsPipes` énumère les canaux nommés qui sont accessibles de manière anonyme.

Ces paramètres peuvent être configurés au travers des *Options de sécurité*. La liste suivante indique les correspondances entre le nom des valeurs de la base de registre et le nom de l'option dans l'éditeur de sécurité :

- `NullSessionsShare` → *Accès réseau : les partages qui sont accessibles de manière anonyme* : la liste doit être vide ;
- `NullSessionsPipes` → *Accès réseau : les canaux nommés qui sont accessibles de manière anonyme* : la liste doit être vide.

3 La technologie DEP (Data Execution Prevention) : Administration, compatibilité et limites (3/3)

La semaine dernière nous avons détaillé la configuration de *DEP*, notamment avec l'`ACT`. Nous allons maintenant nous intéresser aux moyens disponibles pour détecter si *DEP* est activé. Pour finir, nous aborderons les potentiels problèmes liés à *DEP* ainsi que les limites de la technologie.

3.1 Recenser la configuration de DEP

Nous avons vu que le fichier *boot.ini* (ou l'utilisation de *bcdedit*) permet de définir la configuration de *DEP* au niveau du système. Donc un administrateur voulant connaitre la configuration de *DEP* pourrait créer un script pour lire ce fichier.

Cependant cela pose plusieurs problèmes :

- plusieurs entrées peuvent être présentes dans le fichier *boot.ini* avec des réglages de *DEP* différents ;
- il faut analyser (par code) le fichier *boot.ini*, ce qui n'est pas trivial et est potentiellement source d'erreurs.

Une méthode plus simple à gérer lorsque l'on administre un parc de machines, est d'utiliser un script *WMI* (*Windows Management Instrumentation*). Outre un script on peut aussi appeler *WMI* via l'outil *WMIC.EXE* en ligne de commande.

Dans notre cas, pour savoir quel est le réglage de *DEP* :

```
wmic OS Get DataExecutionPrevention_SupportPolicy
```

Cette ligne de commande renvoie une valeur de 0 à 3 qui correspond au réglage de *DEP* au niveau système.
La fiche technique `http://support.microsoft.com/kb/912923/fr` vous donnera plus de détails.
Outre *WMI*, on peut aussi appeler directement l'*API GetSystemDEPPolicy* depuis un programme.

3.2 Problème de compatibilité

Si vous activez *DEP*, il faudra vous assurer que cela ne pose pas de problèmes aux applications installées sur la machine. Normalement toutes les applications récentes ont été développées pour être compatibles avec *DEP*. Cependant, si vous avez des applications relativement anciennes installées, il se peut que certaines soient instables si vous activez *DEP* (notamment avec les options *AlwaysOn* ou *OptOut*).

Dans ce cas, il faudra vérifier si une nouvelle version de l'application supportant *DEP* n'est pas disponible auprès de l'éditeur. Dans le cas contraire vous pouvez désactiver *DEP* pour cette application, comme nous l'avons vu la semaine dernière.

Dans tous les cas, ces problèmes d'incompatibilité peuvent être réglés, et donc, ne sauraient justifier la décision de ne pas activer *DEP*.

3.3 Limites de DEP

Comme tout mécanisme de protection, *DEP* a ses limites et ne vous protège pas de toutes les formes d'attaques.

Plusieurs méthodes ont été développées pour contourner *DEP*, la plupart utilisent une variante d'une technique appelée «*Return-to-libc*». Le but de cette technique est d'essayer de désactiver *DEP* en réussissant à appeler l'une des ces *API* (liste non exhaustive) :

- *NtSetInformationProcess*
- *SetProcessDEPPolicy*
- *VirtualProtect/ZwProtectVirtualMemory*

Cependant, si *DEP* est couplé à la technologie *ASLR* (*Address Space Layout Randomization*), introduite dans `Vista`, ces techniques de contournement sont rendues plus difficiles à appliquer.

Mais *ASLR* a aussi ses faiblesses, comme l'ont montré les techniques utilisant le «*JIT Spraying*» ...

3.4 Conclusion

Malgré ses limites, la technologie *DEP* (surtout couplée à *ASLR*) rend l'exploitation de vulnérabilités significativement plus difficile. C'est une protection supplémentaire et efficace qui participe à la politique de défense en profondeur.

Le CERTA recommande donc son utilisation, bien que son activation doive être faite avec prudence sur des systèmes opérationnels.

4 Vulnérabilité dans Spamassassin Milter

Cette semaine, une vulnérabilité relative à l'extension `Spamassassin Milter` a été publiée. `Spamassassin Milter` permet d'interfacer le logiciel `Spamassassin` avec des serveurs de messagerie comme `Sendmail` ou `Postfix`. Historiquement cette extension fonctionnait nativement uniquement avec `Sendmail` en utilisant certaines macro-commandes de ce `Sendmail` pour communiquer. `Postfix` utilise d'ailleurs une couche d'émulation de ces macros afin de dialoguer avec `Spamassassin Milter`.

La vulnérabilité concerne l'option *'-x'* qui permet à `spamassassin-milter` de prendre en compte les éventuels *alias* ou utilisateurs virtuels lors du passage de message à `Spamassassin`. Cette option n'est normalement pas activée par défaut et doit faire l'objet d'une configuration spécifique de `Spamassassin Milter`.

Il est à noter que si toutefois cette option est activée, l'exploitation de la vulnérabilité devient triviale et permet l'exécution de code arbitraire à distance.

Recommandation :

En temps normal, un système de filtrage s'appuyant sur `Spamassassin Milter` n'est pas vulnérable car la commande `spamass-milter` ne sera pas appelée avec l'option *'-x'*. Cependant, il convient de bien s'en assurer car si tel n'était pas le cas, une attaque serait facile à réaliser.

5 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/

6 Rappel des avis émis

Dans la période du 05 au 11 mars 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-107 : Multiples vulnérabilités dans CA SiteMinder
- CERTA-2010-AVI-108 : Multiples vulnérabilités dans Drupal
- CERTA-2010-AVI-109 : Vulnérabilité dans Juniper
- CERTA-2010-AVI-110 : Vulnérabilité dans CUPS
- CERTA-2010-AVI-111 : Vulnérabilité dans des produits Symantec
- CERTA-2010-AVI-112 : Multiples vulnérabilités du serveur HTTP Apache
- CERTA-2010-AVI-113 : Vulnérabilité dans phpBB
- CERTA-2010-AVI-114 : Vulnérabilité dans Windows Movie Maker
- CERTA-2010-AVI-115 : Multiples vulnérabilités dans Microsoft Excel et Office Sharepoint Server
- CERTA-2010-AVI-116 : Vulnérabilité de Dovecot
- CERTA-2010-AVI-117 : Vulnérabilité dans HP Performance Insight
- CERTA-2010-AVI-118 : Vulnérabilité dans Samba

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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

8 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.

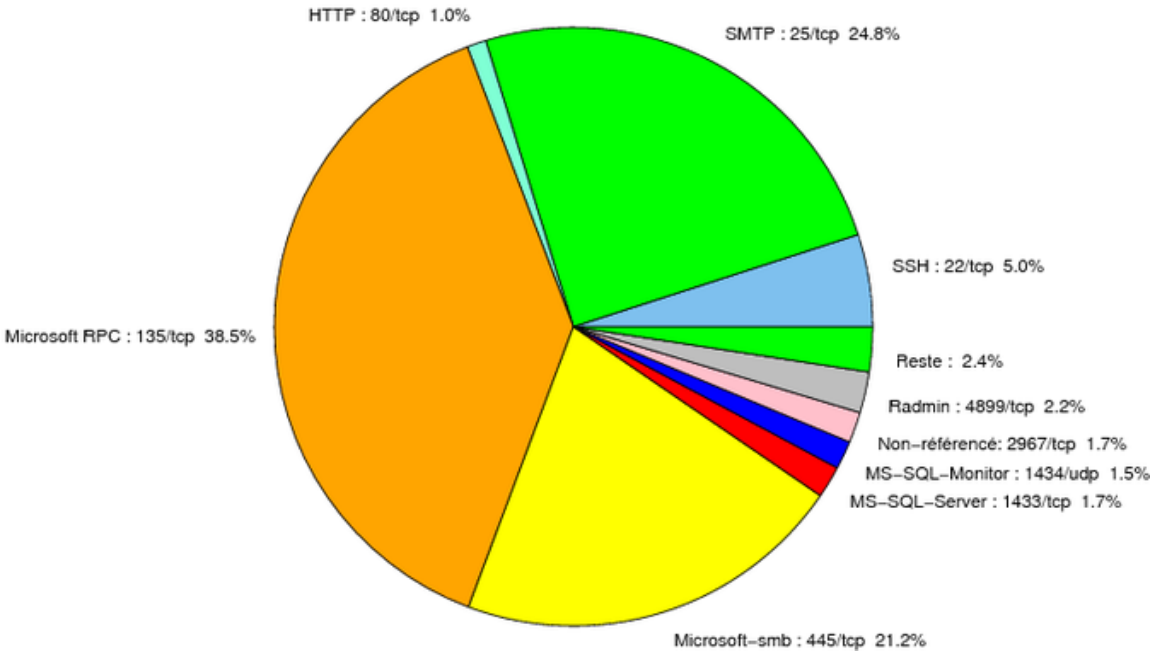

FIG. 1: Répartition relative des ports pour la semaine du 05 au 11 mars 2010

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	38.52
25/tcp	24.75
445/tcp	21.16
80/tcp	5.04
22/tcp	4.97
4899/tcp	2.21
1433/tcp	1.72
2967/tcp	1.65
1434/udp	1.52
23/tcp	0.76
3389/tcp	0.55
21/tcp	0.48
3306/tcp	0.27
1080/tcp	0.2
3128/tcp	0.13
111/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

12 mars 2010 version initiale.