Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 février 2009
N° CERTA-2009-ACT-009

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-09

Gestion du document

Référence	CERTA-2009-ACT-009
Titre	Bulletin d'actualité 2009-09
Date de la première version	27 février 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-009.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-009/

1 Alerte CERTA-2009-ALE-002

Le CERTA a publié cette semaine l'alerte CERTA-2009-ALE-002 concernant l'application de bureautique Excel. Cette vulnérabilité est actuellement exploitée dans certains cas d'attaques dont le scénario consiste à envoyer un courrier électronique contenant une pièce jointe malveillante.

Des codes circulent actuellement sur l'Internet et sont signalés sous le nom `Exploit:Win32:Evenex.gen` par Microsoft et `Trojan.Mdropper.AC` par Symantec. Ils fonctionnent sur certaines versions de langue d'Office 2007 mais Microsoft précise dans son avis de sécurité 968272 que l'ensemble des versions Excel seraient impactées.

Le dysfonctionnement d'Excel à l'ouverture de tels fichiers peut créer une entrée dans les journaux d'événements Windows.

Des contournements provisoires sont recommandés par le CERTA dans son alerte CERTA-2009-ALE-001.

- Alerte CERTA-2009-ALE-002, « Vulnérabilité dans Microsoft Excel », 25 février 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-002/
- Bloc-notes MMPC de Microsoft, "*Detection Added For the New 0-day in Excel*" du 25 février 2009 :
  http://blogs.technet.com/mmpc/archive/2009/02/25/detection-added-for-the-new-0-day-in-excel.aspx

2 Retour sur l'alerte CERTA-2009-ALE-001 concernant Adobe

2.1 La vulnérabilité

Le CERTA a publié la semaine dernière l'alerte CERTA-2009-ALE-001 concernant les fichiers PDF interprétés par les lecteurs Adobe. La vulnérabilité identifiée concerne plus précisément la gestion des flux de type `JBIG2`.

`JBIG2` est une méthode de compression d'images binaires apparue dans les standards internationaux en 2000 et 2001 sous les noms d'ITU T.88 et ISO/IEC 14492. Cette méthode distingue dans une image les zones de texte (les symboles), les zones dites en « demi-teintes » ou même d'autres zones dites génériques qu'elle traite différemment dans le processus d'encodage. Une donnée JBIG2 est ainsi constituée de plusieurs blocs fonctionnels, ou *segments*. La compression obtenue peut être avec ou sans perte.

Les fichiers PDF se présentent sous la forme d'un ensemble d'objets pouvant être encodés suivant plusieurs méthodes. L'une de celles définies est donc `JBIG2`. Le filtre `JBIG2Decode` s'applique aux images monochromes (un bit par pixel) de type `XObject` en manipulant dans le fichier PDF le flux de l'objet. Chaque page ou image encodée en JBIG2 est alors représentée par une image PDF.

Une vulnérabilité a été identifiée dans la manière dont est géré un segment JBIG2 avec une page ou image, et en particulier l'association qui existe entre les deux : les pages sont identifiées par leur numéro et le segment JBIG2 précise normalement à quelle page il est associé.

Cette vulnérabilité peut être assez simplement exploitée pour perturber l'application (déni de service) ou exécuter du code arbitraire à distance. L'une des techniques d'exploitation consiste à exploiter la vulnérabilité par du JavaScript (remplissage de tas ou *heap spray*). C'est cette méthode qui est actuellement utilisée par les différents codes diffusés sur l'Internet dont le CERTA a connaissance.

Le CERTA préconise dans son alerte CERTA-2009-ALE-002, comme contournement provisoire, de désactiver l'interprétation du JavaScript dans les lecteurs PDF Adobe. Il y a deux raisons principales à cela :

- cette opération empêche les codes actuellement connus d'exécuter du code à leur ouverture par une application vulnérable ;
- il s'agit d'une bonne pratique générale, compte-tenu des risques associés au format PDF rencontrés depuis plusieurs mois.

Il faut noter que d'autres lecteurs semblent perturbés par un fichier ayant un flux JBIG2 particulier. A titre d'exemple, `Aperçu` sous Mac0S X se ferme inopinément, de même que `xpdf` ou `kpdf` sous certaines conditions. La possibilité d'exécuter du code arbitraire n'est pas encore vérifiée.

Foxit Reader n'est pas fourni par défaut avec le composant pour JPEG2000 et JBIG2, et de fait n'est pas vulnérable.

2.2 Les méthodes de détection

Les méthodes de détection ne sont pas triviales du fait de la complexité du format PDF. Plusieurs propriétés permettent à une personne malveillante de construire un fichier trompant la vigilance des outils de sécurité, ceux-ci n'ayant pas toutes les capacités d'interprétation d'un véritable lecteur (ou bien alors ils pourraient souffrir des mêmes vulnérabilités).

Un objet suspect peut apparaître dans le code source du fichier PDF en appelant le filtre `JBIG2Decode` comme :

```
<</Subtype/Image/Width xx/Height yy/ColorSpace/DeviceGray/BitsPerComponent 1
/Decode[1 0]/Interpolate true/Length zz/Filter/JBIG2Decode>>
stream
```

2.3 Documentation

- Site du standard JBIG2 pointant vers plusieurs ressources :
  http://jbig2.com
- Les caractéristiques techniques du format JBIG2 :
  http://www.jpeg.org/public/fcd14492.pdf
- Alerte du CERTA CERTA-2009-ALE-001 du 20 février 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-001/

3 Complément d'information sur l'*autorun*

A la date du 11 février 2009, le CERTA avait complété sa note d'information CERTA-2006-INF-006 liée au « Risques associés aux clés USB » et publié un avis sur une vulnérabilité affectant le mécanisme d'autorun de Microsoft Windows (cf. CERTA-2009-AVI-064).

La mise à jour de sécurité proposée par l'éditeur est depuis sa parution uniquement disponible en mise à jour automatique pour les systèmes d'exploitation Windows Vista et Windows Server 2008, comme le précise la section 3 du bulletin CERTA-2009-ACT-007.

Pour les autres systèmes d'exploitation, cette mise à jour devait être appliquée à l'initiative de l'utilisateur.

Depuis le 24 février 2009, ce correctif de sécurité, associé au numéro de la base de connaissances Microsoft KB967715, est disponible en mise à jour automatique pour les autres versions maintenues du système d'exploitation Windows.

Documentation

- Bloc-notes de Pascal Saulière :
  http://blogs.technet.com/pascals/archive/2009/02/24/mise-jour-pour-la-d-sactivation-de-l-autorun-de-windows.aspx
- Bulletin d'actualité CERTA-2009-ACT-007, « Vulnérabilité dans l'autorun de Windows », 13 février 2009 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-007.pdf

4 Vulnérabilité Mozilla Firefox

Cette semaine, un code d'exploitation permettant d'effectuer un déni de service à distance sur le navigateur Mozilla Firefox a été publié sur l'Internet. Cette vulnérabilité non corrigée n'a pas fait l'objet d'une alerte CERTA en raison du risque limité de cette faille. La fondation `Mozilla` est également restée muette à ce sujet pour l'instant. L'exploitation est très simple et rendue possible via le paramètre *OnLoad* de la balise *BODY* d'une page *HTML*. Le déni de service nécessite cependant que l'interprétation du *JavaScript* soit activée.

Il est important de garder à l'esprit que les navigateurs internet restent des applications critiques pour les machines des utilisateurs. Le CERTA rappelle donc quelques bonnes pratiques afin de limiter les risques de compromission d'une machine via le navigateur Internet :

- naviguer avec un compte utilisateur aux droits limités ;
- ne pas activer par défaut l'exécution de codes dynamiques (*Flash*, *JavaScript*, ...) sur les sites qui ne sont pas de confiance ;
- limiter et même bannir l'installation de modules complémentaires ou extensions ;
- maintenir constamment à jour l'application et ses modules complémentaires.

5 Les *TinyURL*, de quoi s'agit il ?

Ce terme couramment utilisé est dérivé du premier site ayant offert le service en 2002, *tinyurl.org*. Il désigne maintenant un principe de redirection d'une adresse longue et complexe via une plus petite (*Tiny*). Cette technique est utilisée pour faciliter l'utilisation des URLs ou les rendre plus explicites. Par exemple :

`www.monsite.tld/page.php?section=zdilksndifjz&page=13983&titre=MaPAGE`

pourrait devenir :

`www.siteDeRenommage.tld/IdMaPAGE`

Ces petites adresses fonctionnent sur un principe d'association d'un identifiant unique (`IdMaPage` dans l'exemple) à une adresse. Lorsqu'un visiteur demande un identifiant, il est automatiquement redirigé vers la page associée. Si l'utilisation d'un tel procédé peut se justifier, il convient de se montrer prudent s'il repose sur un tiers pour gérer les associations.

En effet, plusieurs sites offrant ce service ont fermé, invalidant ainsi tous les liens reposant dessus. De plus, l'action, par l'internaute, d'interroger le site de redirection introduit un intermédiaire. Il est important de bien le connaître pour définir le niveau global de confiance de la connexion.

Comme il est possible d'associer plusieurs *TinyURL* à une même page, il est courant de voir ce service détourné par des attaquants susceptibles de l'utiliser pour multiplier les liens pointant sur un site malveillant (phishing ou autre). Cette solution leur permet d'éviter trop rapidement le *blacklistage*.

Si ce procédé doit être utilisé, le CERTA recommande de se reposer sur un tiers de confiance ou d'utiliser une solution locale. L'utilisateur ne pourra pas apporté la même confiance, dans tous les cas, à un lien réticulaire qui ne correspond pas à celui de forme prévisible et attendue.

6 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 19 et le 26 février 2009.

7 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/

8 Rappel des avis émis

Dans la période du 20 au 27 février 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-073 : Vulnérabilité dans libpng
- CERTA-2009-AVI-074 : Vulnérabilité dans OpenBSD
- CERTA-2009-AVI-075 : Vulnérabilité dans IBM AIX
- CERTA-2009-AVI-076 : Vulnérabilités d'Adobe Flash Player
- CERTA-2009-AVI-077 : Vulnérabilité dans IBM WebSphere MQ
- CERTA-2009-AVI-078 : Multiples vulnérabilités dans Cisco ACE
- CERTA-2009-AVI-079 : Vulnérabilités dans Cisco ANM

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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.ssi.gouv.fr/fr/formation/

10 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.

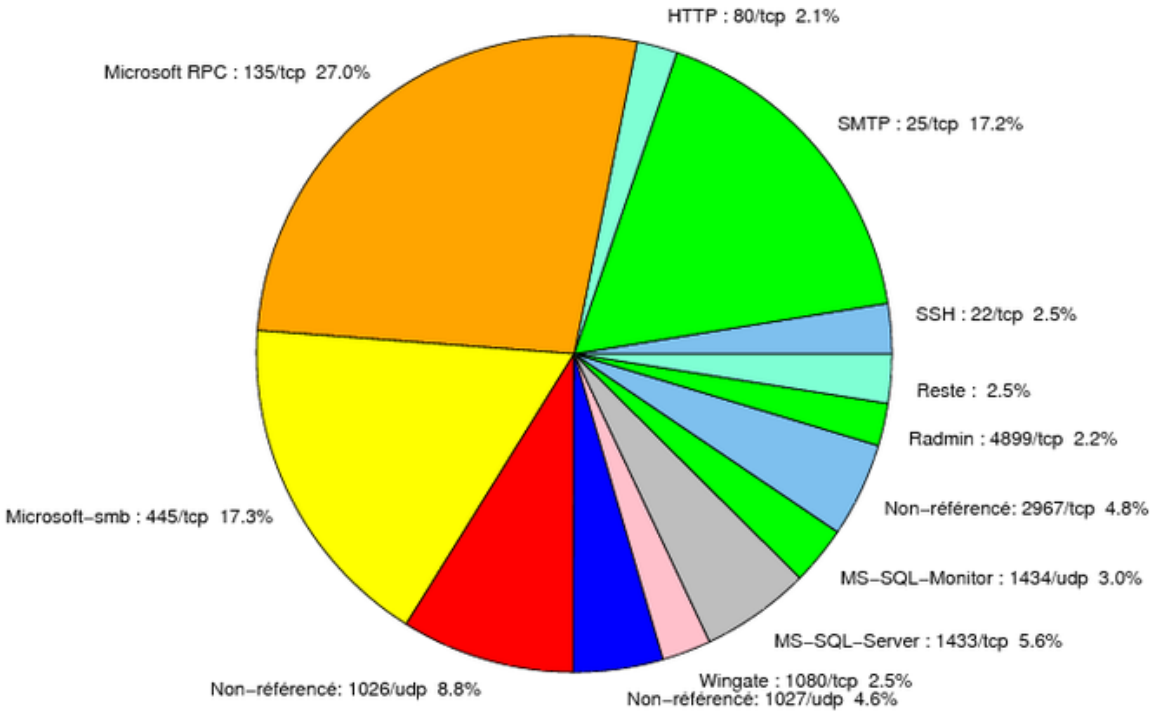

FIG. 1: Répartition relative des ports pour la semaine du 19.02.2009 au 26.02.2009

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	27
445/tcp	17.31
25/tcp	17.21
1026/udp	8.82
1433/tcp	5.56
2967/tcp	4.79
1027/udp	4.55
1434/udp	2.97
22/tcp	2.63
80/tcp	2.58
1080/tcp	2.49
4899/tcp	2.15
21/tcp	0.62
23/tcp	0.57
3389/tcp	0.38
139/tcp	0.28
3128/tcp	0.14
6129/tcp	0.09
1023/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

27 février 2009 version initiale.