Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 août 2008
N° CERTA-2008-ACT-033

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2008-33**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2008-ACT-033 |
| Titre | Bulletin d'actualité 2008-33 |
| Date de la première version | 14 août 2008 |
| Date de la dernière version | – |
| Source(s) | |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-033.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-033/

## 1 Incident de la semaine

### 1.1 Joomla! et interface d'administration

Le CERTA a traité cette semaine plusieurs cas de compromission de serveurs Web. Il s'avère que celles-ci ont été réalisées par le biais d'une récente vulnérabilité dans le système de gestion de contenu Joomla!. L'exploitation, relativement simple, permet de modifier le mot de passe de l'interface d'administration. Il est alors possible d'effectuer plusieurs actions : modification, effacement, création ou insertion de contenu, ajout ou suppression de comptes utilisateur.

La vulnérabilité est associée à la page `components/com_user/models/reset.php`. Le CERTA a publié l'avis CERTA-2008-AVI-414 à ce sujet. Le correctif apporté vérifie que le jeton demandé pour réinitialiser le mot de passe administrateur est de la taille attendue :

```
$diff resetOLD.php resetNEW.php
>       if(strlen($token)!=32){
>               $this->setError(JText::_('INVALID_TOKEN'));
>               return false;
>       }
```

Si la fonctionnalité n'est pas souhaitée, il est également possible de limiter le correctif à la seule ligne suivante pour l'appel à la fonction `confirmreset` :

```
return(false);
```

Cette vulnérabilité ne concerne cependant pas la branche 1.0.x de Joomla!.

Il est vivement conseillé :

- de surveiller régulièrement les journaux de connexion afin de détecter toute tentative d'intrusion. Une manifestation du changement de mot de passe peut se visualiser par une ligne ressemblant à :

  ```
  POST /index.php option=com_user&task=confirmreset
  ```

- de vérifier les comptes utilisateur configurés ;
- de limiter l'accès à l'interface d'administration à certaines plages d'adresses IP (voir à la boucle locale 127.0.0.1 uniquement) ;
- de mettre à jour les versions de Joomla! antérieures à 1.5.6.

### 1.2 De l'importance de l'application des correctifs

Cette semaine le CERTA a informé plusieurs responsables de site web de la compromission de ces derniers. Les deux vulnérabilités les plus notables qui ont été exploitées étaient :

- la dernière vulnérabilité de Joomla!, détaillée dans l'article précédent et dans l'avis du CERTA CERTA-2008-AVI-414 ;
- une ancienne vulnérabilité d'une solution Open Source de commerce en ligne dont, dans les anciennes versions, le dossier d'administration n'était pas protégé en lecture, laissant ainsi accessibles des outils d'administration tels que le dépôt de fichier sans authentification ou la modification de page Web.

Le CERTA rappelle l'importance de l'application et du suivi des correctifs de sécurité. De plus, lors du traitement de ces incidents, il fut difficile de joindre les responsables techniques des serveurs ou des sites. Ce problème est malheureusement récurrent pendant les congés scolaires d'été rendant parfois très difficile et long le traitement d'incident.

## Documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information : http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

# 2 Les mises à jour Microsoft de cette semaine

Cette semaine, *Microsoft* a publié son traditionnel pack mensuel de correctifs. Les vulnérabilités corrigées (12 bulletins pour 26 vulnérabilités au total) affectent de nombreux logiciels :

- plusieurs vulnérabilités dans `Microsoft Internet Explorer` permettent d'exécuter du code arbitraire à distance (CERTA-2008-AVI-412) ;
- plusieurs vulnérabilités dans le système d'événements de `Microsoft Windows` permettent à une personne malintentionnée d'exécuter du code arbitraire à distance (CERTA-2008-AVI-409) ;
- une vulnérabilité permet de contrôler `Windows Messenger` en utilisant des scripts afin de manipuler un contrôle *ActiveX* et cela à l'insu de l'utilisateur connecté. (CERTA-2008-AVI-410) ;
- une vulnérabilité dans les clients de messagerie (`Outlook Express` et `Windows Mail`) de certains systèmes `Windows` permet à un utilisateur malveillant de porter atteinte à la confidentialité des données (CERTA-2008-AVI-408) ;
- une vulnérabilité dans la gestion par certains systèmes `Windows` de la politique IPsec permet à un utilisateur malveillant de porter atteinte à l'intégrité et à la confidentialité des données (CERTA-2008-AVI-407) ;
- ue vulnérabilité existe dans un module d'allocation de la mémoire du système de gestion des couleurs de certains systèmes `Windows`. Son exploitation, par le biais d'un fichier image spécialement conçu, permet à un utilisateur malveillant d'exécuter du code arbitraire à distance (CERTA-2008-AVI-406) ;
- de nombreuses vulnérabilités affectent la suite de logiciels de bureautique `Microsoft Office` :
  - une vulnérabilité a été identifiée dans le contrôle *ActiveX Snapshot Viewer* de `Microsoft Access`. Elle a fait l'objet de l'alerte CERTA-2008-ALE-009 le 08 juillet 2008 et est maintenant corrigée (CERTA-2008-AVI-413) ;

- trois vulnérabilités ont été découvertes dans les différentes versions de `Microsoft PowerPoint` (CERTA-2008-AVI-411) ;
- des vulnérabilités ont été identifiées dans certains filtres `Microsoft Office`. L'exploitation de ces dernières peut conduire à l'exécution de code arbitraire à distance par le biais de documents spécialement construits (CERTA-2008-AVI-405) ;
- plusieurs vulnérabilités ont été identifiées dans l'application bureautique `Microsoft Excel`. Elles peuvent être exploitées à distance via un fichier spécialement construit afin d'exécuter des commandes arbitraires sur le système vulnérable sur lequel le document serait ouvert (CERTA-2008-AVI-404) ;
- une vulnérabilité a été identifiée dans `Microsoft Word` (CERTA-2008-AVI-403). Elle permet à une personne malveillante distante d'exécuter du code arbitraire sur un poste vulnérable par le biais d'un document spécialement construit. Cette vulnérabilité a fait l'objet de l'alerte CERTA-2008-ALE-010 le 09 juillet 2008.

Les vulnérabilités affectant le navigateur et la suite de bureautique `Microsoft Office` vont très certainement faire l'objet, si ce n'est déjà le cas pour certaines, dans les prochains jours, de la publication de code d'exploitation. Le CERTA profite de cette ensemble de mises à jour pour rappeler quelques bonnes pratiques afin de limiter les risques et impacts en cas d'exploitation de vulnérabilité :

- maintenir l'ensemble des applications à jour (système d'exploitation, navigateur, logiciels de bureautique, antivirus, ...) ;
- utiliser un compte aux droits limités lors de la navigation sur l'Internet et plus généralement lorsqu'aucun droit d'administration n'est nécessaire ;
- de pas ouvrir de pièce jointe ou suivre de lien provenant d'une source non sûre ;
- lire les courriels au format texte ;
- éventuellement convertir les fichiers de bureautique par un logiciel tiers afin de prévenir l'exploitation de certaines vulnérabilités.

# 3 Contournement HTTPS

## 3.1 Scénario d'attaques

Des serveurs Web ont recours à HTTPS (SSL/TLS) pour chiffrer les communications avec leurs clients. Cela peut être, par exemple, les services en ligne de messagerie. Par ailleurs, les sites peuvent également déposer chez les postes clients des fichiers de session (`cookies`) qui s'appliquent à un domaine donné. C'est la politique dite de « même origine ». Une visite du site www.certa.ssi.gouv.fr ne peut `a priori` pas déposer de fichier pour un autre domaine en *.com* par exemple.

Ces fichiers de session ont un champ "*secure*" qui, s'il est déployé, signale au navigateur de transmettre les fichiers vers des serveurs utilisant un canal de communication chiffré. Cependant, peu de sites ont recours à ce champ et le transfert de fichiers se fait sans contrôle du contexte de la communication.

Il est alors possible d'imaginer le scénario d'attaque suivant :

1. un utilisateur se connecte et s'authentifie avec son navigateur sur un site via HTTPS : `https://www.MonSiteSecure.tld` ;
2. le site lui communique un fichier de session ;
3. l'utilisateur navigue au même moment sur un autre site `http://www.SiteMalveillant.tld`. Cette action peut provenir id'un clic malencontreux dans un courriel ou d'une redirection (ARP/DNS) de trafic, etc.
4. le site `http://www.SiteMalveillant.tld` retourne un code HTTP de redirection (par exemple "301 Moved Permanently") avec, dans l'en-tête, la valeur `Location:http://www.MonSiteSecure.tld` ;
5. le navigateur de l'utilisateur cherche alors à se connecter à `http://www.MonSiteSecure.tld` et lui envoie une requête HTTP avec le fichier de session en clair.

Cette attaque ne fonctionne bien sûr que sous certaines conditions. Le site distant sécurisé doit également répondre en HTTP et la personne malveillante doit être en mesure de récupérer le fichier de session en *sniffant*. Ce scénario est cependant très envisageable dans le cas de connexions sans-fil libres.

La politique de sécurité est alors contournée, et le seul recours à HTTPS pour se connecter au site n'est pas suffisante.

Une fois le fichier de session obtenu, la personne malveillante peut l'importer dans son navigateur et accéder à la session usurpée pour y effectuer les mêmes opérations que l'utilisateur légitime (lecture ou envoi de courriers par exemple).

Ces attaques sont documentées et des codes d'exploitation ont été publiés. Il a été montré récemment au cours d'une conférence en sécurité que des sites bancaires ainsi que des services de messagerie en ligne assez populaires pouvaient être vulnérables à ce scénario d'attaque.

## 3.2 Recommandations

### 3.2.1 Pour les développeurs

Il est utile de vérifier que l'attribut `secure` est bien utilisé dans le cas de communication en HTTPS. Dans ce cas, le fichier de session ne sera pas transmis si le navigateur est redirigé vers un canal de communication non chiffré.

```
document.cookie="certa=test;expires=Fr, 15-Aug-2008 23:59:59 GMT;secure";
```

Il est également souhaitable de ne pas mixer les échanges via HTTP et HTTPS.

### 3.2.2 Pour les utilisateurs

Il faut éviter de naviguer sur des sites qui ne sont pas de confiance. Le navigateur doit être configuré pour effacer les fichiers de session à chaque fermeture.

Dans le cas de communications chiffrées en HTTPS, il faut :

- se limiter à celles-ci (éviter de naviguer en parallèle sur d'autres sites) ;
- vérifier les certificats reçus ;
- se déconnecter proprement du site.

Enfin, il est vivement déconseillé de naviguer sur des sites sensibles où des échanges de données confidentielles seront faites via des réseaux non maîtrisés, et en premier lieu des réseaux sans-fil ouverts.

# 4 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 07 et le 13 août 2008.

# 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=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/

# 6 Rappel des avis émis

Dans la période du 07 au 14 août 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-392 : Multiples vulnérabilités dans Apache Tomcat
– CERTA-2008-AVI-393 : Vulnérabilité dans HP-UX libc
– CERTA-2008-AVI-394 : Vulnérabilité dans Oracle BEA WebLogic Server
– CERTA-2008-AVI-395 : Vulnérabilité dans IBM Rational ClearQuest
– CERTA-2008-AVI-396 : Vulnérabilité de PowerDNS Authoritative Server
– CERTA-2008-AVI-397 : Vulnérabilités dans Cygwin
– CERTA-2008-AVI-398 : Vulnérabilités dans Adobe Presenter
– CERTA-2008-AVI-399 : Vulnérabilité de McAfee Encrypted USB Manager
– CERTA-2008-AVI-400 : Vulnérabilité de Solaris Trusted Extensions
– CERTA-2008-AVI-401 : Plusieurs vulnérabilités dans des produits CA
– CERTA-2008-AVI-402 : Multiples vulnérabilités dans Ruby
– CERTA-2008-AVI-403 : Vulnérabilité dans Microsoft Word
– CERTA-2008-AVI-404 : Vulnérabilités dans Microsoft Excel
– CERTA-2008-AVI-405 : Multiples vulnérabilités dans des filtres Microsoft Office
– CERTA-2008-AVI-406 : Vulnérabilité dans Windows Color Management System
– CERTA-2008-AVI-407 : Vulnérabilité dans Windows IPsec
– CERTA-2008-AVI-408 : Vulnérabilité dans Outlook Express et Windows Mail
– CERTA-2008-AVI-409 : Multiples vulnérabilités dans le système d'événements de Microsoft Windows
– CERTA-2008-AVI-410 : Vulnérabilité dans Windows Messenger
– CERTA-2008-AVI-411 : Multiples vulnérabilité de Microsoft PowerPoint
– CERTA-2008-AVI-412 : Multiples vulnérabilités dans Internet Explorer
– CERTA-2008-AVI-413 : Vulnérabilité dans le contrôle ActiveX Snapshot Viewer d'Access
– CERTA-2008-AVI-414 : Vulnérabilité dans Joomla!

# 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, la DCSSI dispose d'un centre de formation :

http://www.formation.ssi.gouv.fr

## 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.

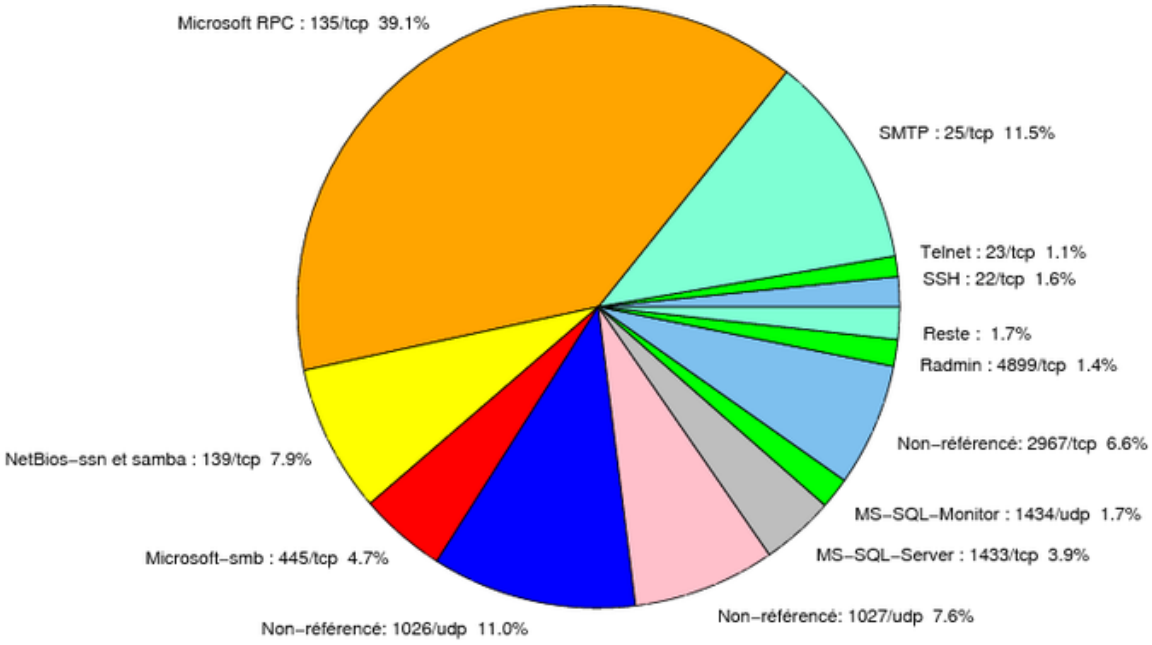


FIG. 1: Répartition relative des ports pour la semaine du 07.08.2008 au 13.08.2008

| Port | Protocole | Service | Porte dérobée | Référence possible CERTA |
|---|---|---|---|---|
| 21 | TCP | FTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 22 | TCP | SSH | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 23 | TCP | Telnet | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>CERTA-2007-ALE-005-001 |
| 25 | TCP | SMTP | – | http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 106 | TCP | MailSite Email Server | – | –<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |
| 445 | TCP | Microsoft-smb | – | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER |

| | | | | |
|---|---|---|---|---|
| | | | | http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>http://www.certa.ssi.gouv.fr/site/CER<br>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<br>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<br>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<br>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 | 39.13 |
| 25/tcp | 11.54 |
| 1026/udp | 10.97 |
| 139/tcp | 8.04 |
| 1027/udp | 7.64 |
| 2967/tcp | 6.6 |
| 445/tcp | 4.83 |
| 1433/tcp | 3.93 |
| 1434/udp | 1.66 |
| 22/tcp | 1.6 |
| 4899/tcp | 1.43 |
| 23/tcp | 1.13 |
| 21/tcp | 0.46 |
| 80/tcp | 0.43 |
| 1080/tcp | 0.26 |
| 137/udp | 0.2 |
| 3128/tcp | 0.13 |
| 3306/tcp | 0.1 |
| 3389/tcp | 0.06 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**14 août 2008** version initiale.