Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mai 2008
N° CERTA-2008-ACT-020

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2008-20**



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2008-ACT-020 |
| Titre | Bulletin d'actualité 2008-20 |
| Date de la première version | 16 mai 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-020.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-020/

## 1 Vulnérabilités OpenSSL et OpenSSH de Debian et ses dérivés

Cette semaine, l'équipe de sécurité du projet Debian a publié un bulletin de sécurité relatif à une faiblesse dans le générateur de pseudo-aléa mis en œuvre dans le paquetage OpenSSL. Celui-ci s'applique à la version stable (*Etch*) de la distribution Debian ainsi qu'aux versions de développement : *testing* et *unstable*. Par ailleurs le CERTA a publié l'avis CERTA-2008-AVI-239 sur le même sujet.

Dans les faits, l'aléa utilisé pour générer les clefs ne serait qu'un simple dérivé du PID (Process Identifier), donc aisément prévisible. Ceci constitue, très clairement, une grave faiblesse dans le système cryptographique fourni par Debian dans OpenSSL. Il est à noter que toutes les distributions dérivées de Debian Etch sont concernées. Ainsi, le présent article et les recommandations associées sont applicables également à Ubuntu, Xandros, MEPIS, KNOPPIX....

Les implications en terme de sécurité sont assez importantes car les clefs privées ou les certificats utilisés par des services réseaux s'appuyant sur SSL pour leur chiffrement (FTPS, HTTPS, DNSSEC, OpenVPN, ...) doivent être considérés comme non-fiables. Dans ce contexte, il est possible pour un attaquant de prédire et de réutiliser les clefs privées utilisées lors d'échanges chiffrés entre clients et serveurs et de réaliser ainsi des attaques de type « homme au milieu » (« *Man in the middle* »).

Un deuxième bulletin de sécurité a été publié par Debian et par le CERTA expliquant que la vulnérabilité présente dans OpenSSL s'appliquait aussi à OpenSSH. Ce dernier s'appuyant également sur cet aléa faible. En d'autres termes, tout bi-clef (couple clef publique / clef privée) généré à partir de la commande *ssh-keygen* (incluse dans le paquetage vulnérable) est également à considérer comme non-fiable. Là encore, la vulnérabilité s'applique à toutes les distributions dérivées de Debian.

Un autre cas concerne l'utilisation de certificats utilisés dans le contexte d'une IGC (Infrastructure de Gestion de Clef). En effet, un certificat client produit de façon fiable mais signé par une autorité de certification utilisant des clefs de signature non-fiables devient, *de facto*, non-fiable lui aussi. Le cas le plus grave serait une autorité de certification racine non-fiable.

### Recommandations :

Cette vulnérabilité est considérée comme critique en particulier si vous avez mis en œuvre des services s'appuyant sur SSL pour le chiffrement sur une plate-forme Debian ou assimilée. Une mise à jour des paquetages *ssh* et libssl ne sera pas suffisant. Il conviendra de s'assurer que les paquetages suivants ont été correctement mis à jour :

- openssh-client ;
- openssh-server ;
- openssh-blacklist.

http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-239/
http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-246/
Le dernier paquetage contient la liste des clefs reconnues par Debian comme étant non-fiables.

Toute clef produite avec OpenSSL ou OpenSSH par un système d'exploitation Debian stable entre le 8 avril 2007 (date de sortie de la version stable actuelle *Etch*, mais septembre 2006 pour la version *testing*) et la date de sortie de la mise à jour OpenSSL ou OpenSSH est non-fiable. Les clefs présentes dans */etc/ssh* devront été remplacées par de nouvelles. Il faudra également examiner les bi-clefs présents dans les répertoires *.ssh/* des utilisateurs. Généralement ses clefs sont de la forme : *id_dsa* ou id_rsa pour les clefs privées et id_dsa.pub ou id_rsa.pub pour les clefs publiques. Il est à noter que le chemin d'accès et le nom de ces clefs est entièrement paramétrable. Ces informations ne sont donc données qu'à titre indicatif.

Le projet Debian met à disposition un outil nommé *ssh-vulnkey* permettant de faire une recherche rapide des bi-clefs ssh présents sur une machine et de déterminer si ceux-ci sont fiables. Cette outil n'est pas parfait et peut ne pas trouver certaines clefs. Dans le doute, il est plutôt recommandé de remplacer tous les bi-clefs existants (SSL/SSH) par de nouveaux une fois les mises à jours appliquées.

Enfin le CERTA vous engage fortement à être très attentif aux journaux d'événements des serveurs utilisant du chiffrement basé sur OpenSSL ou disposant d'un serveur sshd.

# 2 Les incidents traités cette semaine

## 2.1 Fausse alerte ?

Un correspondant du CERTA lui a signalé que son antivirus levait une alarme lors de la navigation sur un site. Le fichier en cause ne s'est pas révélé agressif à l'encontre du poste de l'internaute. Toutefois, ce fichier, un javascript, avait des traits inhabituels. La manière dont il était invoqué et d'autres aspects du sites semblaient anormaux. Le CERTA a contacté l'administrateur qui s'est montré surpris de la présence de ce script. Son analyse des journaux de connexion lui a permis de détecter des compromissions par attaques classiques, de type *PHP-include*. Les mesures correctives ont alors été prises.

Dans cet incident, l'alarme n'est pas pertinente vis-à-vis de l'ordinateur de l'internaute. Par contre, son signalement s'est montré très utile à l'administrateur du serveur web.

Cette attitude constructive de l'internaute ne dispense évidement pas l'administrateur d'un serveur de procéder à une analyse régulière des journaux de son serveur.

## 2.2 Les métadonnées... encore

Cette semaine, dans le cadre d'un incident, le CERTA a analysé un serveur web. Il s'est avéré que celui-ci contenait de nombreux fichiers de bureautique (Word, Excel, PDF...). Ils étaient mis à disposition des internautes par les auteurs qui pensaient, ayant vérifié le contenu des documents, ne pas divulguer d'informations confidentielles. Ces fichiers ont été par ailleurs indexés par des moteurs de recherche. L'analyse des métadonnées contenues a

permis de récupérer des informations telles que des adresses de courriels, des noms et des informations réseau (y compris des adresses MAC). La définition des métadonnées est abordée dans l'article « Les métadonnées surprennent encore » du bulletin d'actualité CERTA-2008-ACT-001 du 4 janvier 2008. L'existence de ces informations est de plus en plus connue et elles sont faciles d'accès. Des outils reposant sur des moteurs de recherche permettent de synthétiser automatiquement un rapport HTML de toutes les métadonnées disponibles sur un site et elles peuvent par exemple être utilisées pour des attaques en ingénierie sociale.

La présence d'informations réseaux dans les documents de bureautique peut, à valeur d'illustration, être due à la méthode employée par Microsoft pour créer un identifiant unique du système sur lequel a été créé le fichier, le GUID (*Globally Unique IDentifier*). En effet, dans une machine, l'une des informations globalement unique est l'adresse physique d'une carte réseau. Cette adresse est concaténée telle quelle à d'autres informations pour créer le GUID. Elle ne permet d'identifier que la machine à partir de laquelle le document a été créé, le GUID n'étant pas touché par les modifications du contenu. L'auteur du virus Melissa, qui se propageait via un document Word malveillant, a été identifié par corrélation entre le GUID du document infecté et celui de documents publiés sur un site internet et dont la source était traçable.

### 2.3 Documentation

- Bulletin d'actualité CERTA-2008-ACT-001 du 4 janvier 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-001.pdf
- «Document Metadata and Computer Forensic» de *Jeffrey R. Jones* :
  http://www.infosec.jmu.edu/reports/jmu-infosec-tr-2006-003.pdf

## 3 Compromissions de machines par un fichier PDF

### 3.1 Précisions sur les publications du CERTA

Le CERTA a mis à jour l'avis CERTA-2008-AVI-053 concernant des vulnérabilités liées au lecteur Adobe Reader. Certaines de ces vulnérabilités ont fait l'objet d'un article dans le bulletin d'actualité CERTA-2008-ACT-007 du 15 février 2008. Celui-ci précisait que les corrections apportées par Adobe ne concernaient que la branche 8 du lecteur. La branche 7 a été délaissée et les utilisateurs ont été fortement incités par l'éditeur à changer de version.

Une mise à jour a été publiée par l'éditeur le 06 mai 2008 et corrige également les vulnérabilités pour cette branche 7 délaissée.

### 3.2 Les vulnérabilités corrigées

Les vulnérabilités corrigées par cette mise à jour ainsi que celle de février sont :

- CVE-2008-0667 : une fonction de la bibliothèque JavaScript Adobe (`DOC.print`) pourrait être appelée à l'ouverture d'un document spécialement construit afin d'envoyer une ou plusieurs requêtes d'impression à l'insu de l'utilisateur.
- CVE-2007-5666 : le chemin d'accès à des bibliothèques "Security Provider" peut être contourné et permettre de charger un fichier arbitraire dans le répertoire contenant le document PDF malveillant.
- CVE-2007-5663 : la mise en oeuvre de JavaScript dans le module `Escript.api` ne serait pas correcte et permettrait sous certaines conditions d'exécuter du code arbitraire.
- CVE-2008-0726 : les arguments attribués à la fonction Adobe JavaScript `printSepsWithParams` ne sont pas suffisamment contrôlés. L'exploitation de cette vulnérabilité peut conduire à un dépassement d'entier et la corruption d'une zone mémoire afin d'exécuter du code arbitraire.
- CVE-2008-2042 : l'appel à la fonction `app.checkForUpdate` peut entraîner via une fonction de retour (*callback*) un débordement de tampon.
- CVE-2007-5659 et CVE-2008-5663 : plusieurs débordements de tampon seraient possibles, notamment via des méthodes JavaScript comme `Collab.collectEmailInfo`. Ces vulnérabilités ne sont pas toutes documentées.

### 3.3 Les risques associés

Le CERTA signale que plusieurs codes malveillants se propagent actuellement via des documents au format PDF. Ces codes peuvent exploiter l'une des vulnérabilités citées ci-dessous ou des fonctionnalités intrinsèques au format. A valeur d'exemple, le format précise certaines classes d'action :

- `OpenAction` détaille des actions à lancer à l'ouverture du document ;
- `Action` précise des actions à lancer suite à une opération de l'utilisateur via le document (clic sur une adresse réticulaire, formulaire et envoi de courriel, etc.).

Certaines de ces actions se manifestent par la présence de fonctions comme l'envoi d'un formulaire (`SubmitForm`) ou l'accès à une adresse (`URI`).

La combinaison de ces actions peut permettre, à l'ouverture d'un document PDF spécialement construit, de dérober de l'information sur le poste de l'utilisateur ou d'accéder à d'autres ressources.

Un fichier PDF est constitué d'un ensemble d'objets qui se trouvent dans le code source du document. Ces objets permettent de décrire l'apparence des pages, l'interaction avec des données et d'autres objets...

Il s'agit d'un format très riche. Les codes malveillants peuvent se dissimuler dans des objets sous forme de flux (*streams*) compressés et obfusqués de différentes manières. Ces variétés rendent la tâche des antivirus très difficile, et le taux de détection de tels codes malveillants est souvent très faible.

### 3.4 Les recommandations du CERTA

Le CERTA tient donc à rappeler ici quelques bonnes pratiques :

- ne pas ouvrir de fichiers ne provenant pas d'une source de confiance ;
- mettre à jour les lecteurs Adobe Reader ou utiliser un lecteur alternatif aux fonctionnalités moins riches ;
- configurer ces lecteurs au plus strict usage ;
- signaler à son responsable de sécurité (RSSI) tout document suspect.

### 3.5 Documentation

- Documents de référence Adobe sur les formats PDF :
  http://www.adobe.com/devnet/pdf/pdf_reference.html
- Article « Retour sur les vulnérabilités d'Adobe Reader » du bulletin CERTA-2008-ACT-007, 15 février 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-007.pdf

## 4 Sortie de Fedora 9

*Fedora 9* est depuis peu disponible en téléchargement. Cette nouvelle version comporte quelques modifications de sécurité :

- possibilité de stockage des mots de passe sous forme de condensats SHA-256 et SHA-512 ;
- changement du comportement du pare-feu. Désormais, le pare-feu filtre tous les ports dans sa configuration par défaut, à l'exception du port 22/tcp (habituellement utilisé par le service SSH) ;
- améliorations de SELinux pour affiner le contrôle des accès.

De plus, le programme d'installation *Anaconda* prend en charge le chiffrement des systèmes de fichiers. Si ce chiffrement semble une bonne idée de prime abord, notamment pour se protéger d'un éventuel vol de disque dur, il reste une arme à double tranchant. En effet, en cas de panne du disque, de défaillance du système de fichiers, ou de perte du mot de passe, il est très difficile voire impossible de récupérer les données. À noter que le système de fichiers `ext4` (futur remplacement de `ext3`) est reconnu par *Fedora 9*.

#### 4.0.1 Documentation

- Notes de version de Fedora 9 :
  http://docs.fedoraproject.org/release-notes/

# 5 Nouvelle attaque via des protocoles de messagerie instantanée

Cette semaine, de nombreux articles ont fait état d'une nouvelle attaque se propageant via les messageries instantanées MSN/Live Messenger et ICQ. Une arnaque du même type avait fait l'objet d'un article dans le bulletin d'actualité CERTA-2008-ACT-007. Ce code malveillant se propage de manière classique via ce type d'outil. Tout d'abord, il est nécessaire que la victime se rende sur un site Internet malveillant pour soit-disant vérifier la liste des personnes ayant bloquée son adresse. Pour avoir cette liste il est nécessaire de fournir l'identifiant et le mot de passe de la messagerie instantanée. Après validation, les données sont ainsi subtilisées et utilisées pour se connecter à l'insu de l'utilisateur à son compte de MSN ou ICQ. Une fois la connexion frauduleuse établie, un message est envoyé à l'ensemble des contacts sous la forme d'un lien vers un site. Ce lien peut avoir plusieurs formats comme :

- m0bil3.info ;
- c-oo-l-st-uff.info ;
- pe0ples.info ;
- bidule.fr.

Ces liens sont généralement précédés du début de l'adresse de l'utilisateur compromis. Par exemple un utilisateur ayant pour adresse prenom.nom@domaine.tld enverra des messages à ces contacts sous la forme d'un lien : http://prenom.nom.c-oo-l-st-uff.info.

Le compte de messagerie compromis, il est alors possible pour les personnes se cachant derrière ces sites d'envoyer des courriels indésirables ou d'usurper l'identité des victimes. Le but principal de ce genre de compromission est de constituer une base de données afin d'envoyer pourriels et codes malveillants.

Le CERTA rappelle qu'il ne faut jamais cliquer sur un lien suspect même si celui-ci semble fourni par une personne de confiance. Il est important de vérifier que l'envoi du lien est volontaire et non fait à l'insu de l'utilisateur propriétaire du compte de messagerie. De plus, il est fréquent que le même mot de passe soit utilisé pour différents comptes. Il est alors possible de compromettre plusieurs comptes en une seule action. Les personnes malveillantes en profitent également pour enregistrer les données personnelles renseignées dans le profil utilisateur. Les clients de messagerie instantanée doivent également être mis à jour car ils sont eux aussi vulnérables comme le rappelait un article du bulletin d'actualité CERTA-2007-ACT-051.

## 5.1 Documentation

- Bulletin d'actualité CERTA-2008-ACT-007 du 15 février 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-007.pdf
- Bulletin d'actualité CERTA-2007-ACT-051 du 21 décembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-051.pdf
- Note d'information sur les mots de passe CERTA-2005-INF-001 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001.pdf

# 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 08 et le 15 mai 2008.

# 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 09 au 15 mai 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-233 : Multiples vulnérabilités dans Mozilla Thunderbird
– CERTA-2008-AVI-234 : Vulnérabilité dans HP-UX LDAP-UX
– CERTA-2008-AVI-235 : Multiples vulnérabilités dans Sun Java System Web Server et Application Server
– CERTA-2008-AVI-236 : Vulnérabilités dans HP-UX WBEM Services
– CERTA-2008-AVI-237 : Vulnérabilité dans MySQL
– CERTA-2008-AVI-238 : Vulnérabilité dans CUPS
– CERTA-2008-AVI-239 : Vulnérabilité dans la version OpenSSL de Debian
– CERTA-2008-AVI-240 : Vulnérabilité dans Tcl/Tk
– CERTA-2008-AVI-241 : Multiples vulnérabilités dans Sun Solaris
– CERTA-2008-AVI-242 : Vulnérabilités dans Microsoft Word et Outlook
– CERTA-2008-AVI-243 : Vulnérabilité dans Microsoft Publisher
– CERTA-2008-AVI-244 : Vulnérabilité dans Microsoft Jet Database Engine
– CERTA-2008-AVI-245 : Vulnérabilités des outils Microsoft de protection
– CERTA-2008-AVI-246 : Vulnérabilité dans OpenSSH pour Debian et Ubuntu

Durant la même période, une alerte et deux avis ont été mis à jour :

– CERTA-2008-ALE-005-002 : Vulnérabilité dans Microsoft Jet Database Engine
(publication du correctif par l'éditeur)
– CERTA-2008-AVI-053-003 : Multiples vulnérabilités dans Adobe Reader
(ajout de références aux CVE et APSB08-13 mentionnant la mise à disposition du correctif pour la branche 7 Adobe Reader)
– CERTA-2008-AVI-239-001 : Vulnérabilité dans la version OpenSSL de Debian
(ajout de Ubuntu dans les systèmes vulnérables, ajout de la non-vulnérabilité de la Debian sarge)

# 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.formation.ssi.gouv.fr

# 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.

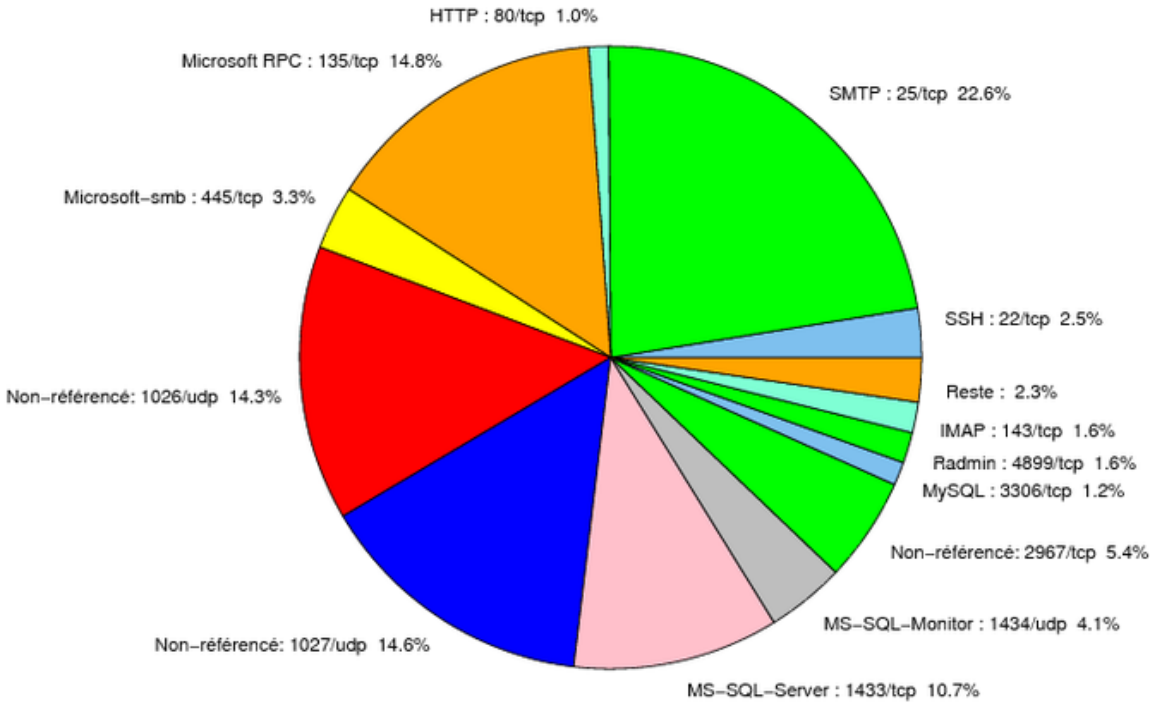


FIG. 1: Répartition relative des ports pour la semaine du 08.05.2008 au 15.05.2008

| 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 |
|---|---|
| 25/tcp | 22.56 |
| 135/tcp | 14.78 |
| 1027/udp | 14.59 |
| 1026/udp | 14.27 |
| 1433/tcp | 10.7 |
| 2967/tcp | 5.41 |
| 1434/udp | 4.07 |
| 445/tcp | 3.31 |
| 22/tcp | 2.54 |
| 143/tcp | 1.59 |
| 3306/tcp | 1.21 |
| 137/udp | 0.82 |
| 139/tcp | 0.38 |
| 21/tcp | 0.25 |
| 3389/tcp | 0.19 |
| 3128/tcp | 0.12 |
| 9898/tcp | 0.06 |

TAB. 3: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**16 mai 2008** version initiale.