



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 juillet 2008
N° CERTA-2008-ACT-027

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-27

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-027>

Gestion du document

Référence	CERTA-2008-ACT-027
Titre	Bulletin d'actualité 2008-27
Date de la première version	04 juillet 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-027.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-027/>

1 Incident de la semaine

1.1 La synchronisation des serveurs

Le CERTA a traité un incident impliquant une application Web. L'architecture de l'application comporte un portail Web, hébergé sur un serveur *Apache* sous Linux, et une base de données, hébergée sur un serveur Windows 2000 Serveur. Lors du traitement de l'incident, le CERTA peut avoir besoin de croiser plusieurs journaux venant des deux serveurs. Le problème est que les serveurs n'étaient pas synchronisés sur une base de temps. Ce défaut de configuration a provoqué au bout d'un certain temps un décalage plus ou moins important même si les serveurs avaient été configurés à la main à la même date à l'origine. Il s'avère finalement que les deux serveurs étaient décalés de 48 minutes et 53 secondes à la date de l'incident. Une des méthodes permettant de supprimer ce décalage consiste à choisir une base de temps et à modifier les journaux.

Prenons la date suivante : « 05/12/2007 14:25:07 ». Le but de l'opération sera de mettre en début de ligne la date modifiée, ou non, dans un format permettant un tri en ordre chronologique de la forme :

[Année][Mois][Jour][Heure][Minute][Seconde]

Dans l'exemple cela donne : « 20071205142507 ».

Voici un exemple de code permettant de décaler cette date de *48 minutes et 53 secondes* :

```
echo "05/12/2007 14:25:07" |
perl -ne 'print "$3$2$1$4$5$6 $_" if /^(\\d+)\\/(\\d+)\\/(\\d+) (\\d+):(\\d
+):(\\d+)/' |
perl -MDate::Manip -ane '@F = (split / /);' \
-e '$F[0] = DateCalc ($F[0], "+48 minutes 53 seconds");' \
-e '$F[0]=~ s/[[:]]//g;' \
-e 'print join " ", @F;'
```

Cette commande donne le résultat : « 20071205151400 05/12/2007 14:25:07 » ; soit la nouvelle date « 20071205151400 » qui équivaut à « 05/12/2007 15:14:00 » (48 minutes et 53 secondes plus tard).

Il ne reste plus qu'à utiliser la commande *sort* pour trier les résultats. Cette commande n'est cependant valable que sur des entrées d'une courte période où l'hypothèse d'un même décalage d'horloge est faite.

Le CERTA rappelle à cette occasion qu'il est important de synchroniser tout son parc sur une même base référentielle afin de croiser les lectures et les interprétations de journaux.

2 Vacances d'été

Le CERTA souhaite aux lecteurs de ce bulletin d'actualité d'excellentes vacances d'été. Il rappelle à cet égard qu'il est important d'identifier au sein de son administration des systèmes d'information une personne suppléante qui pourra prendre en charge les problèmes de sécurité pendant l'été.

Les retours de congés sont une période critique à anticiper. L'utilisateur rallume un poste qui peut présenter des retards dans les mises à jour du système. Cela peut concerner le système d'exploitation, les applications bureautiques ou spécialisées, les logiciels divers comme les antivirus, les utilitaires de transferts, d'archivage ou de sauvegarde ...

Avant et pendant tout le processus de la mise à jour, les vulnérabilités des logiciels ne sont pas encore corrigées. En revanche, elles ont été publiées. Les agresseurs les ont analysées. Ils ont eu le temps de préparer des programmes qui exploitent les faiblesses et leur permettent de prendre éventuellement le contrôle des postes.

L'organisation, la politique des droits, l'architecture et les outils présents sur le réseau de l'organisme permettent de répondre de manière très variée à ce problème. Une solution, peu réaliste hors des très petites structures, consiste à ce qu'un utilisateur présent allume les postes des absents lorsque son propre poste se met à jour et provoque (ou laisse se faire) la mise à jour des postes des absents. L'outillage, par exemple un gestionnaire de configuration, peut forcer la mise à jour du poste dès qu'il est allumé. Une autre stratégie consiste à utiliser un sas virtuel. Tout poste non complètement à jour n'est autorisé à effectuer que des connexions restreintes. Lorsque le poste, rallumé, a fini sa mise à niveau, il recouvre entièrement ses droits de connexion.

Dans tous les cas, l'utilisateur doit être informé de la fragilité de son poste lorsqu'il rentre d'une absence prolongée. La navigation sur Internet doit être limitée ou retardée. La vigilance doit être renforcée lors de la lecture des courriels qui se sont accumulés dans la boîte aux lettres. Il vaut ainsi mieux attendre la fin des mises à jour pour ouvrir les pièces jointes des courriels.

3 Retours sur quelques navigateurs

3.1 Les versions de navigateurs

Le navigateur étant l'élément le plus exposé d'un poste de travail, l'importance de le maintenir à jour n'est plus à démontrer, mais qu'en est-il réellement ? Une étude récemment publiée fait le point sur les versions des navigateurs utilisées en se basant sur les statistiques du moteur de recherche *Google* et plus précisément sur les versions visibles dans les champs *USER-AGENT* de l'en-tête *HTTP*¹.

Elle a porté sur des données collectées entre janvier 2007 et juin 2008 et a fourni les résultats suivants :

- En juin 2008, 78% des navigateurs vus par *Google* étaient identifiés comme *Internet Explorer* (IE), 16% comme *Firefox*, 3.4% comme *Safari* et 0.8% comme *Opera* ;
- parmi ceux-ci, les navigateurs à jour représentaient 47,6% pour *IE*, 58,1% pour *Opera*, 85,3% pour *Safari* et 83,3% pour *Firefox*.

¹Cette visibilité est cependant plus ou moins évidente selon les navigateurs

- Les dernières versions majeures d'*Internet Explorer* (IE7) et *Firefox* (FF2), au moment de l'étude, sont disponibles depuis octobre 2006, et représentent respectivement, en juin 2008, 52,5% des *IE* et 92,2% des *Firefox*.

Le propos n'est pas ici de discuter de la qualité ni des hypothèses de l'expérimentation mais d'en extraire quelques faits marquants. On remarque une disparité dans le niveau de mise à jour des différents navigateurs utilisés, certainement liés au principe de mise à jour automatique : un grand nombre de personnes utilisent encore une version obsolète de navigateur. L'information n'étant pas disponible dans les données de *Google*, l'étude ne prend pas en compte les vulnérabilités liées à l'utilisation de modules tiers vulnérables. La proportion des navigateurs vulnérables peut donc être supérieure à celle constatée ici.

Le CERTA rappelle qu'il est important de mettre à jour son navigateur et tous les programmes tiers associés.

- S. Frei, T. Duebendorfer, G. Olmann, M. May, "Understanding Web browser threat : Examination of vulnerable online Web browser population and the "insecurity iceberg", rapport technique de l'ETHZ 288 : <http://www.techzoom.net/publications/insecurity-iceberg/>

3.2 Mozilla Firefox

Cette semaine, le CERTA a émis l'avis CERTA-2008-AVI-350 concernant *Firefox2*. La mise à jour 2.0.0.15 corrige plusieurs vulnérabilités dont quatre indiquées comme critiques par Mozilla et certaines permettant l'exécution de code arbitraire à distance. La version 2 du navigateur sera maintenue jusqu'à la fin de l'année mais l'éditeur préconise de passer à la version 3, version présentée dans le bulletin d'actualité du CERTA du 20 juin 2008. À propos de cette dernière, aucune information supplémentaire concernant la vulnérabilité annoncée peu après sa mise à disposition n'est encore disponible.

- Mise à jour de sécurité Firefox : <http://www.mozilla.org/projects/security/known-vulnerabilities.html#firefox2.0.0.15>
- Firefox 3 : <http://www.mozilla-europe.org/fr/firefox/>

3.3 Vulnérabilité dans *Internet Explorer*

3.3.1 Présentation

Une vulnérabilité non corrigée de type *Cross-Domain Scripting* affecte le navigateur *Internet Explorer*. L'exploitation de cette vulnérabilité semble possible pour les versions 6 et 7 du navigateur.

Une vulnérabilité de type *Cross-Domain Scripting* permet à une personne malintentionnée d'obtenir des informations concernant les pages de navigation appartenant à une autre zone de sécurité.

En effet, *Internet Explorer* cloisonne les données relatives à des cadres (ou *FRAME*) provenant de différentes sources. Afin de différencier les sources, une notion de « zone de sécurité » a été introduite. Ce modèle de sécurité est présent afin d'empêcher le code issu d'un domaine d'accéder à des informations appartenant à un autre domaine.

Cette vulnérabilité est à rapprocher des vulnérabilités de type injection de code indirecte (*Cross-Site Scripting* - *XSS*). Une personne malveillante, en forçant la visualisation d'une page spécialement conçue, peut accéder des informations de l'utilisateur entrées pour d'autres zones. Une exploitation de cette vulnérabilité pourrait même, par exemple, permettre l'enregistrement des frappes clavier dans les formulaires des autres zones, et cela via un simple lien.

Des codes d'exploitation de cette vulnérabilité sont disponibles sur l'Internet. Le CERTA recommande donc une grande prudence quant à l'utilisation d'*Internet Explorer* :

- filtrage de balises de types *FRAME* et/ou *IFRAME* lorsque cela est possible ;
- désactivation de l'interprétation des langages dynamiques (*JavaScript*, *Flash*, ...) dans le navigateur par défaut ;
- navigation sur des sites de confiance ;
- utilisation d'un navigateur alternatif dans l'attente d'un correctif de l'éditeur.

3.3.2 Documentation

- Base de connaissances Microsoft, référence 174360, « Comment utiliser les zones de sécurité dans *Internet Explorer* » : <http://support.microsoft.com/kb/174360/fr>

4 Injections SQL : vérification des pages ASP

4.1 Présentation des faits

Le CERTA a publié depuis le début d'année différents articles concernant des corruptions de bases de données via des variables de codes ASP incorrectement contrôlées. Parmi eux :

- Bulletin d'actualité CERTA-2008-ACT-003, « Les rumeurs d'activités malveillantes » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-003.pdf>
- Bulletin d'actualité CERTA-2008-ACT-012, « Attaques massives de type *SQL Injection* » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-012.pdf>
- Bulletin d'actualité CERTA-2008-ACT-016, « Attaques massives de type *SQL Injection* - Suite » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-016.pdf>
- Bulletin d'actualité CERTA-2008-ACT-019, « Incidents traités cette semaine : attaque par injection SQL » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-019.pdf>

Les incidents utilisant de telles méthodes sont relativement courants depuis le début d'année.

Il est donc important d'auditer avec attention son code afin de vérifier que les valeurs passées aux variables sont correctement filtrées. Ces incidents ont motivé l'apparition de nouveaux outils de vérification de code. L'objet n'est pas ici de les comparer avec d'autres qui existent mais de signaler au lecteur leur existence.

- *Microsoft Source Code Analyzer for SQL Injection*
- *Scrawlr* (produit conjointement par HP et Microsoft)
- *URLScan* (version 3.0 Beta)

Il faut bien comprendre que les outils présentés ne sont pas des outils complets d'audit d'injection SQL mais ils effectuent des tests à la recherche de défauts dans les pages souvent indexés par les moteurs de recherche. Leur utilisation peut donc réduire les risques et limiter les injections SQL massives mais doit être complétée par une analyse directe du code pendant et après la phase de développement.

4.2 Documentation

- Base de connaissance Microsoft, KB 954476 du 24 juin 2008 :
<http://support.microsoft.com/?kbid=954476>
- Base de connaissance Microsoft, KB 954462 du 24 juin 2008 :
<http://www.microsoft.com/technet/security/advisory/954462.msp>
- Forum de discussion sur les fonctionnalités de l'outil :
<http://forums.microsoft.com/msdn/ShowForum.aspx,ForumID=92&SiteID=1>
- HP Security Laboratory, "Finding SQL Injection with Scrawlr", 24 juin 2008 :
<http://www.communities.hp.com/securitysoftware/blogs/spilabs/archive/2008/06/23/finding-sql-injection-wih-scrawlr.aspx>
- Bloc-notes MSDN associé à la sécurité de SQL Server :
<http://blogs.msdn.com/sqlsecurity/>
- Article Microsoft MSDN, « prévenir les injections SQL en ASP » :
<http://msdn.microsoft.com/en-us/library/cc676512.aspx>
- Bloc-notes de Microsoft MSRC, "SQL Injection Attacks Exploiting Unverified User Data Input", 24 juin 2008 :
<http://blogs.technet.com/msrc/archive/2008/06/24/rise-in-sql-injection-attacks-exploiting-unverified-use-data-input.aspx>
- Article et page de téléchargement de l'utilitaire URLScan :
<http://technet.microsoft.com/en-us/security/cc242650.aspx>
<http://learn.iis.net/page.aspx/473/using-urlscan>
- Projet annexe de test de vulnérabilité de serveur, w3af :
<http://w3af.sourceforge.net/>

5 Vulnérabilités Ruby

5.1 Présentation

Le CERTA a publié le 27 juin 2008 l'avis CERTA-2008-AVI-342 sur des vulnérabilités présentes dans le langage Ruby. Certaines de ces vulnérabilités permettent à un utilisateur distant d'exécuter du code arbitraire. Hormis le fait que le CERTA recommande d'appliquer les correctifs associés dans les plus brefs délais, il tient à préciser quelques points supplémentaires.

Il convient, tout d'abord, de bien différencier les langages dits interprétés des langages compilés. Dans le premier cas, on utilise un interpréteur qui lira un fichier texte dit « de script » pour réaliser des tâches. Dans le second cas, on utilise un compilateur qui transforme un ou plusieurs fichiers de texte ou « code source » en fichier(s) binaires exécutables compréhensibles uniquement par le système d'exploitation ou l'ordinateur lui-même. Ainsi dans le cas de Ruby, il s'agit, en fait, d'un langage interprété utilisant un interpréteur de commandes : *ruby*. Il n'est pas rare que cet interpréteur de commande soit programmé dans un autre langage souvent compilé. Pour *ruby*, une partie des fonctions de base sont écrites en utilisant le langage *ruby* lui-même mais l'interpréteur est programmé avec un langage compilé : C. C'est pourquoi, dans le bulletin de sécurité de *ruby*, on parle de vulnérabilités touchant l'interpréteur *ruby* affectant des fonctions en C présentes dans le code source de l'interpréteur (fichiers en `.c`).

Ces familles de langages ont chacune leurs avantages et leurs inconvénients et il n'appartient pas au CERTA de définir quel autre langage il faut utiliser dans tel ou tel cas. Il tient simplement à rappeler que pour des langages interprétés et lorsqu'une vulnérabilité est publiée à leur sujet, il conviendra de bien dissocier les failles relatives à l'interpréteur de celles relatives aux extensions ou aux fonctions mises en œuvre dans ce langage.

Ainsi, si l'on prend comme exemple `php`, il faudra faire la différence entre la vulnérabilité de l'interpréteur (`php.exe` sous `windows`) de la vulnérabilité résultant d'une erreur dans le code d'un fichier `php`. Dans les deux cas, une mise à jour est indispensable mais, si l'interpréteur est vulnérable, tous les programmes basés sur le langage de cet interpréteur peuvent être des vecteurs d'exploitations. Ainsi, si l'on sait qu'une application en *ruby* utilise une fonction *ruby* vulnérable, une attaque sera envisageable via cette application.

5.2 Recommandations

Les failles relatives aux interpréteurs de langage sont donc relativement critiques et devront généralement faire l'objet d'une mise à jour dans les plus brefs délais car il est assez délicat de répertorier l'ensemble des applications s'appuyant sur les fonctions vulnérables de ce langage.

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 26 juin et le 03 juillet 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 27 juin au 03 juillet 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-341 : Vulnérabilités dans Mambo
- CERTA-2008-AVI-342 : Multiples vulnérabilités dans Ruby
- CERTA-2008-AVI-343 : Multiples vulnérabilités dans Apple Mac OS X
- CERTA-2008-AVI-344 : Vulnérabilité dans D-Bus
- CERTA-2008-AVI-345 : Vulnérabilités dans Python
- CERTA-2008-AVI-346 : Vulnérabilité dans Novell Client

Pendant la même période, les avis suivants ont été mis à jour :

- CERTA-2008-AVI-277-001 : Vulnérabilités dans OpenSSL (ajout des références aux bulletins de sécurité Nortel)
- CERTA-2008-AVI-323-001 : Vulnérabilités dans Horde (ajout des références aux bulletins de sécurité Fedora)
- CERTA-2008-AVI-334-001 : Vulnérabilité dans phpMyAdmin (ajout des références aux bulletins de sécurité Fedora)

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 réglementaire, 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 inexplicables 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.

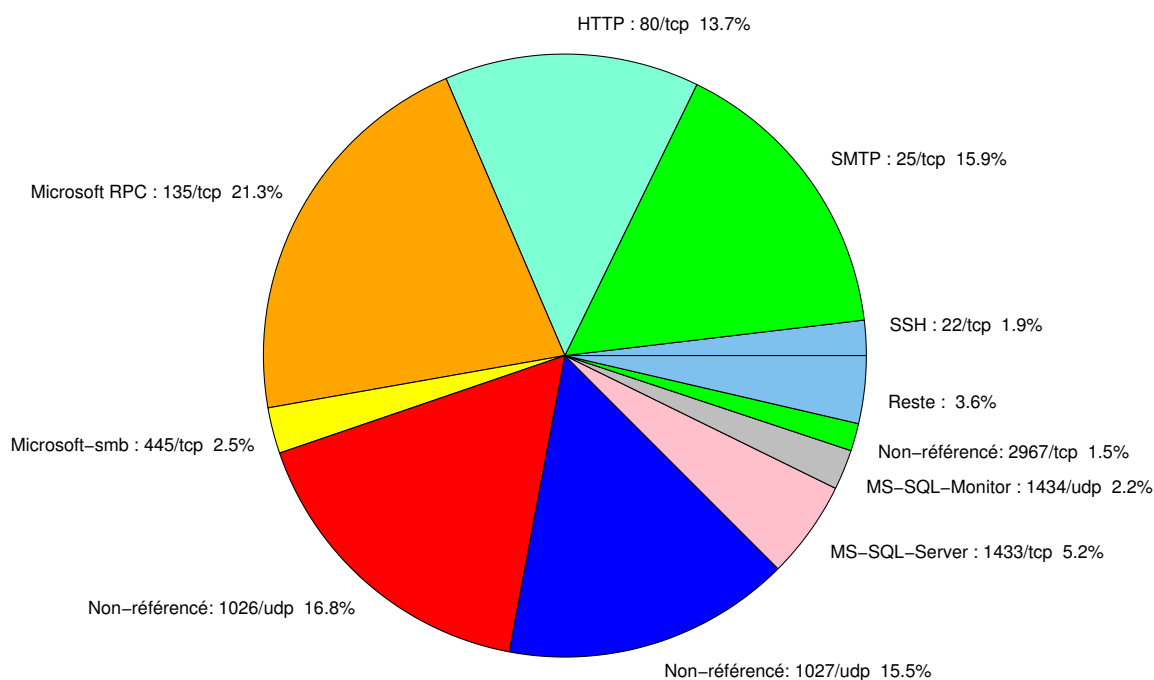


FIG. 1: Répartition relative des ports pour la semaine du 26.06.2008 au 03.07.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	-	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	-	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	-	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	-	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	-	CERTA-2007-AVI-320
80	TCP	HTTP	-	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	-	- CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	-	CERTA-2003-AVI-052
119	TCP	NNTP	-	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	-	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	-	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	-	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051

				CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183

6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	21.32
1026/udp	16.8
25/tcp	15.9
1027/udp	15.45
80/tcp	13.7
1433/tcp	5.24
445/tcp	2.46
1434/udp	2.15
22/tcp	1.88
2967/tcp	1.47
23/tcp	0.98
139/tcp	0.85
4899/tcp	0.76
137/udp	0.53
3389/tcp	0.22
3128/tcp	0.17
3306/tcp	0.08
143/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	10
3	Paquets rejetés	11

Gestion détaillée du document

04 juillet 2008 version initiale.