

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-31

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-031>

Gestion du document

Référence	CERTA-2008-ACT-031
Titre	Bulletin d'actualité 2008-31
Date de la première version	01 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-031.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-031/>

1 Vulnérabilité DNS, suite

1.1 Description

La semaine prochaine auront lieu les conférences annuelles en sécurité Blackhat et Defcon. Plusieurs présentations sont attendues, l'une d'elles concernant le DNS et étant à l'origine de nombreux écrits dans la presse spécialisée ces dernières semaines. L'objet de cet article n'est pas de présenter la vulnérabilité qui sera prochainement annoncée ni les évolutions futures de l'architecture DNS. Il propose de modérer certaines solutions qui sont proposées par certains et qui peuvent s'avérer dangereuses. Les décisions correctives doivent être prises avec réflexion et maturité et non sur le coup de la panique ou de la pression.

1.2 Solutions dangereuses

Les mises à jour des serveurs DNS s'effectue plus ou moins vite, compte-tenu des difficultés de mise à jour des machines. De nombreux problèmes sont en particulier apparus comme des incompatibilités entre les mises à jour (qui ajoutent un aléa au choix des ports sources des transactions DNS) et certains équipements de filtrage réseau.

Une solution alternative à cette mise à jour a été évoquée : elle consiste à modifier sa configuration DNS et la faire pointer vers d'autres serveurs tiers dits « non vulnérables » qui se chargeront de faire les résolutions de noms. Des sociétés ont déployé des serveurs DNS hébergés dans différents endroits du globe et offrent les services suivants :

- des serveurs récursifs ouverts prenant en charge toute résolution de noms ;
- des possibilités de filtrage basés sur des domaines (listes noires et catégories de domaines).

Ces services sont parfois vantés comme « LA » solution pratique et simple aux problèmes actuels DNS.

Choisir de rediriger toutes ses transactions DNS vers des serveurs inconnus est une décision qui ne peut être prise dans la panique. Pour s'en assurer, il suffit de lister les informations qui sont alors disponibles par simple examen du trafic DNS d'un organisme :

- modèle d'antivirus déployé ;
- périodes d'activités de la machine ;
- états des mises à jour du système d'exploitation et des applications installées ;
- activités des utilisateurs (lecture de messagerie, navigations...) ;
- données personnelles (sites bancaires, sites de type webmail, réseaux sociaux...) ;
- etc.

Changer de serveurs DNS n'est donc pas innocent. Il revient à rediriger un important volume d'informations vers une source tierce méconnue.

Le CERTA déconseille le recours à de telles solutions.

Si l'application des correctifs s'avère impossible, voici quelques éléments à considérer :

- l'aléa des ports sources peut s'effectuer par des équipements de filtrage. Plusieurs exemples ont ainsi été donnés dans la note d'information CERTA-2008-INF-002 (section 4.3.2) ;
- une nouvelle version du correctif BIND a été annoncée et sera publiée dans les prochains jours ("P2"). Un avis du CERTA sera alors émis pour signaler sa disponibilité ;
- la fonction récursive des serveurs DNS doit être une exception maîtrisée. Cette précaution doit être prise quelle(s) que soi(en)t la(es) vulnérabilité(s) à paraître.

1.3 Documentation associée

- Note d'information CERTA-2008-INF-002, « Du bon usage du DNS » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-INF-002/>

2 Retour sur les incidents traités cette semaine

2.1 Machines en cours d'installation

Ces derniers temps, de nombreuses machines victimes de compromissions (phishing, remplacement de la page d'accueil, hébergement de code ou de script malveillant...) s'avèrent être des sites en cours de création. Ces sites, partiellement construits, sont laissés en libre accès sur l'Internet et présentent de nombreuses faiblesses :

- identifiants d'administration triviaux : afin de simplifier les accès à la machine pendant son installation, certains administrateurs peu vigilants se contentent d'un couple d'identification très faible, comme *test/test* ou *admin/admin* ;
- fichiers d'installation et/ou de configuration encore présents : après une installation d'un service, comme un CMS (*Content Management System*), les fichiers servant à l'installation ou à la configuration restent présents sur le serveur. Une personne malintentionnée peut alors s'en servir pour réinstaller le site « à sa manière » ;
- absence de mise à jour : on observe que peu d'administrateurs se soucient malheureusement des mises à jour pendant la phase d'installation et de configuration d'une machine.

Toutes ces faiblesses regroupées sur un seul système sont une aubaine pour les personnes malveillantes.

Dans le cas d'une installation ou d'une configuration d'un système, le CERTA recommande de procéder à celle-ci de manière totalement déconnectée. Ainsi, la maîtrise du système est conservée tout au long du processus. Les mises à jour doivent se faire autant que possible lorsque la machine n'est pas encore connectée, et, seulement si cela n'est pas possible, dès que la machine est mise en ligne. Le suivi du système doit respecter l'état de l'art en matière de sécurité.

3 Le Service Pack 3 de Microsoft Windows XP

3.1 Présentation

Alors que le *Service Pack 3 de Microsoft Windows XP* était prévu en téléchargement automatique à partir de 10 juillet, il apparaît que cela ne soit pas vrai pour tout le monde !

En effet, la mise à jour n'est pas disponible en mise à jour automatique pour tous. *Microsoft* a pris la décision d'étaler dans le temps la mise à disposition de son nouveau *Service Pack* pour des raisons d'infrastructure. Elle devrait cependant l'être pour la France d'ici la fin de l'été.

Le CERTA rappelle qu'il est nécessaire et important de conserver son système d'exploitation ainsi que l'ensemble des applications installées à jour. Le *Service Pack 3* pour *Microsoft Windows XP* est en revanche disponible via la mise à jour manuelle (interface Web de *Windows Update*).

3.2 Documentation

- Page de mise à jour Windows Update :
<http://v4.windowsupdate.microsoft.com/fr/>

4 Retour sur l'alerte CERTA-2008-AVI-011

Cette alerte concerne une vulnérabilité sur un connecteur *WebLogic* pour *Apache*.

4.1 Les publications

Le 15 juillet 2008, dans son cycle de mises à jour trimestrielles, l'éditeur *Oracle*, nouveau propriétaire de *BEA*, publiait un correctif concernant les connecteurs entre les serveurs *WebLogic* et serveurs HTTP : *Apache*, *Sun* et *Microsoft IIS*. L'éditeur ne donne que peu d'informations sur la vulnérabilité corrigée. Celle-ci est exploitable à distance, sans authentification et en utilisant le protocole HTTP. L'impact n'est pas précis. Il est « partiel » en confidentialité, en intégrité et en disponibilité. La vulnérabilité fait simplement l'objet d'une entrée, CVE-2008-2579, dans le registre de vulnérabilités publiques du MITRE.

Dès le 17 juillet 2008, un code d'exploitation circulait sur l'Internet. La vulnérabilité associée est numérotée CVE-2008-3257. Ce code ne concerne que le connecteur *Weblogic* avec *Apache*. La vulnérabilité réside dans la gestion de requêtes HTTP avec méthode POST de longueur « excessive ». Le code d'exploitation permet de provoquer à distance un déni de service, et, potentiellement, une exécution de code arbitraire. L'éditeur a répondu à cette publication par des mesures de contournement correspondant aux mesures de filtrage préconisées par le CERTA dans son bulletin d'alerte.

4.2 Deux CVE impliquent-ils deux vulnérabilités différentes ?

Le MITRE, qui tient le registre CVE des vulnérabilités, est laconique. Le NIST reprend les CVE dans sa NVD (*National Vulnerability Database*). Le 22 juillet, il a repris le CVE-2008-3257 en ajoutant une mention. Il suggérait un possible recouvrement entre les deux vulnérabilités, voire que la vulnérabilité CVE-2008-3257 pouvait être une résurgence d'une vulnérabilité ancienne. Cette mention a jeté le trouble chez des utilisateurs du produit.

La sortie d'un code d'exploitation peu après une publication de correctif pouvait laisser croire que le code concernait la vulnérabilité qui venait d'être corrigée. Ce scénario est fréquent. Les délinquants informatiques, quand ils manquent d'informations sur une vulnérabilité, attendent la sortie du correctif et, par analyse inverse du correctif :

- découvrent la vulnérabilité qui fait l'objet du correctif ;
- conçoivent et publient le code d'exploitation de cette vulnérabilité.

Cette opération peut être faite en quelques heures parfois. L'exploitant d'un système d'informations peut légitimement s'interroger. Quel est le risque réel ? Suis-je déjà protégé en ayant appliqué les correctifs trimestriels ? Au contraire, doit-on mettre en place des mesures palliatives qui peuvent avoir des effets secondaires ?

Le CERTA a analysé les différentes sources d'information avec certains de ses correspondants et de ses homologues. L'éditeur mentionne dans ses bulletins que la première vulnérabilité concerne tous les connecteurs, pour les trois serveurs Web, antérieurs au 15 juillet, tandis que la deuxième ne concerne que les connecteurs pour *Apache*, mais jusqu'au 28 juillet. Le périmètre et la période diffèrent. Les impacts, tels que définis par le CVSS (*Common Vulnerability Scoring System*), sont beaucoup plus importants pour la deuxième que pour la première. Ces différences militent pour une différence réelle entre les vulnérabilités.

Le 31 juillet, le NIST a supprimé la mention qui a soulevé les questions.

4.3 Moralité

De manière générale, il faut considérer le système des CVE comme un système d'énumération et non un système de qualification absolue. Le processus de revue avant publication dans le registre limite les risques de doublon mais ne garantit pas leur inexistence. La détection et l'élimination des recouvrements entre deux entrées dans le registre sont bien plus difficiles.

Les CVE sont assez largement utilisés, par exemple pour des vulnérabilités de produits *Apple*, *Cisco*, *OpenOffice.org*, *Oracle*, *Microsoft*, *Mozilla*, et bien d'autres. Cette numérotation répandue facilite les recherches. Il faut profiter de cette qualité sans chercher les propriétés qu'elle ne garantit pas.

4.4 Documentation

- Avis du CERTA CERTA-2008-AVI-367 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-367/index.html>
- Alerte du CERTA CERTA-2008-ALE-011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-011/index.html>
- Bulletin de sécurité Oracle du 15 juillet 2008 :
https://support.bea.com/application_content/product_portlets/securityadvisories/2785.html
- Bulletin de sécurité Oracle du 28 juillet 2008 :
https://support.bea.com/application_content/product_portlets/securityadvisories/2793.html
- Utilisation du CVSS par Oracle :
<http://www.oracle.com/technology/deploy/security/cpu/cvssscoringssystem.htm>
- Référence CVE CVE-2008-2579
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2579>
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2579>
- Référence CVE CVE-2008-3257
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3257>
<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3257>

5 RAID, sauvegardes et plus si affinité

Lors de traitements d'incident, le CERTA peut être amené à intervenir sur des machines équipées de disques configurés en RAID. Ce type d'architecture disque est souvent utilisée pour assurer de la tolérance de panne. Ainsi on pourra trouver, par exemple, du RAID-1 ou *mirroring* consistant en une synchronisation « temps-réel » des informations présentes sur chacun des 2 disques du RAID.

Le RAID-1 est composé de deux disques et autorisera la « perte » d'un des deux disques temporairement sans coupure du service. On trouve également assez fréquemment du RAID-5 plus complexe mais également plus économique en espace disque puisque il consomme (1/N) disque pour fonctionner (où N est le nombre de disques fonctionnant en RAID-5, celui-ci étant toujours au moins égal à 3).

Utiliser ce type de technologie présente un avantage certain puisqu'il rend la machine plus tolérante aux pannes matérielles. Il facilite également les éventuelles copies de disque dans le cas du RAID-1 car il suffit d'extraire un disque du serveur pour avoir une copie immédiate du système.

Les choses deviennent plus problématiques si l'on utilise du RAID-5 puisque la réalisation d'une copie du contenu du serveur nécessitera l'intégralité des disques qui composent le RAID-5.

Ainsi, lorsque du RAID est utilisé, il faudra adapter la manière dont on réalisera la copie. A titre d'exemple, il ne faudra surtout pas enlever « à chaud » un disque si la machine dispose de disques en RAID-0 ou *stripping*. Dans cette configuration les disques étant agrégés dans un seul volume global, si l'un d'entre eux venait à disparaître, c'est tout le volume qui serait perdu. De manière générale et sauf pour le cas particulier du RAID-1, le fait de mettre en œuvre du RAID compliquera la réalisation de copie de disque. De surcroît, le RAID compliquera également la reconstruction des volumes pour une analyse *a posteriori* ou pour récupérer des données.

Dans cet esprit, le RAID ne devra pas être considéré comme une solution remplaçant une véritable politique de sauvegarde mais bien comme un moyen d'éviter les coupures de services dues à une panne de disque. Il conviendra donc de disposer d'une solution de sauvegarde adaptée.

Ainsi, si une machine est compromise, seule une sauvegarde saine permettra éventuellement de repartir sur de bonnes bases.

Enfin, la politique de sauvegarde n'est, elle non plus, pas suffisante car les restaurations ne prendront pas forcément en compte les éléments compromis. Il n'est pas rare que l'on sauvegarde les données présentes sur le système d'exploitation mais pas le système d'exploitation. Or, c'est souvent ce dernier qui sera la cible d'un attaquant ou d'un code malveillant. Les données ne seront, elles, modifiées que plus tard et ce sera souvent à cette occasion que la compromission deviendra visible.

Recommandations

Différents moyens peuvent être mis en place sur un serveur pour qu'il puisse assurer un service continu quoi qu'il arrive. Le RAID apportera une tolérance aux défaillances de disques durs. Les sauvegardes garantiront de pouvoir revenir à la version précédente suite à un incident ou une compromission. Mais une précaution supplémentaire pourra encore être prise en compte. Elle consistera en la rédaction complète d'une documentation de configuration et mise en œuvre du serveur permettant la reconstruction complète du service à partir d'une machine vierge. Cette disposition accompagnée d'une politique de sauvegarde efficace des données et de la configuration du serveur garantiront que même en cas de panne ou de compromission majeure, un retour à la normal puisse se faire dans de bonnes conditions.

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 24 et le 31 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 25 au 31 juillet 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-374 : Vulnérabilités de Claroline

- CERTA-2008-AVI-375 : Multiples vulnérabilités dans dnsmasq
- CERTA-2008-AVI-376 : Multiples vulnérabilités du client de messagerie Mozilla Thunderbird
- CERTA-2008-AVI-377 : Vulnérabilité dans Drupal
- CERTA-2008-AVI-378 : Multiples vulnérabilités dans RealPlayer
- CERTA-2008-AVI-379 : Vulnérabilité de openSUSE
- CERTA-2008-AVI-380 : Multiples vulnérabilités dans VMware ESX
- CERTA-2008-AVI-381 : Vulnérabilité dans AVG Anti-Virus
- CERTA-2008-AVI-382 : Multiples vulnérabilités de l'antivirus ClamAV

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.

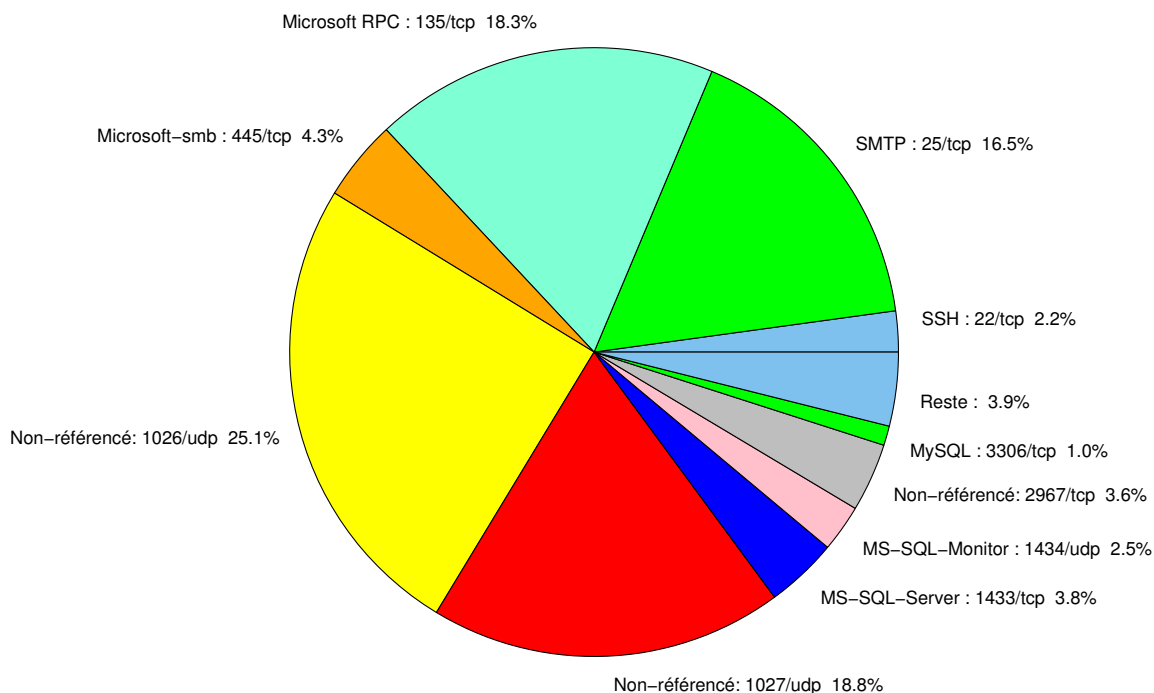


FIG. 1: Répartition relative des ports pour la semaine du 24.07.2008 au 31.07.2008

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
1026/udp	25.08
1027/udp	18.76
135/tcp	18.29
25/tcp	16.5
445/tcp	4.33
1433/tcp	3.81
2967/tcp	3.63
1434/udp	2.49
22/tcp	2.16
3306/tcp	1.03
4899/tcp	0.94
139/tcp	0.89
23/tcp	0.66
137/udp	0.47
21/tcp	0.37
80/tcp	0.33
3389/tcp	0.14
143/tcp	0.09

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	9
3	Paquets rejetés	10

Gestion détaillée du document

01 août 2008 version initiale.