

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-31

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-2009-ACT-031>

Gestion du document

Référence	CERTA-2009-ACT-031
Titre	Bulletin d'actualité 2009-31
Date de la première version	31 juillet 2009
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

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

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-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-2009-ACT-031/>

1 Avis remarquables de la semaine

Cette semaine, le CERTA a publié plusieurs avis de sécurité. Certains revêtent un caractère particulier et nécessitent une attention soutenue malgré la période estivale. Il sont détaillés dans la section suivante.

1.1 Mises à jour Microsoft

Cette semaine, Microsoft a émis deux correctifs hors de son cycle mensuel habituel de mises à jour. Ces deux bulletins sont détaillés dans les avis CERTA-2009-AVI-299 et CERTA-2009-AVI-300.

La sortie exceptionnelle de ces deux bulletins est liée à l'existence de trois vulnérabilités d'une bibliothèque (*Active Template Library* ou *ATL*). Celle-ci est utilisée dans la création d'objets COM (*Component Object Model*) et donc dans de nombreux contrôles *ActiveX*.

La mise à jour décrite dans le bulletin MS09-035 corrige ces trois vulnérabilités dans les bibliothèques publiques fournies avec les produits Microsoft Visual Studio. Il ne s'agit donc pas d'une faille des produits Visual Studio.

L'exploitation de ces vulnérabilités permet l'exécution de code arbitraire et le contournement du système de liste noire utilisé par Microsoft pour désactiver des contrôles *ActiveX* dangereux (les « kill-bits »).

Le correctif détaillé dans le bulletin MS09-034 corrige également trois vulnérabilités dans Microsoft Internet Explorer. Celles-ci permettent l'exécution de code arbitraire à distance au moyen de pages web spécialement conçues, et ne sont pas liées aux failles de ATL. Toutefois, cette mise à jour inclut également deux mécanismes de protection dans Internet Explorer permettant de se protéger de contrôles ActiveX vulnérables compilés avec la bibliothèque incriminée. C'est pour cette raison que ce correctif est également émis hors du cycle mensuel.

Le premier mécanisme de protection, activé par défaut, filtre selon l'éditeur des « modèles d'appel spécifiques qui sont problématiques ». Le deuxième mécanisme permet, au moyen de clés dans la base de registre, de désactiver les contrôles potentiellement vulnérables. Il est, en revanche, désactivé par défaut car il peut avoir des effets de bord non négligeables.

Il est important de noter que ces deux mécanismes de protection ne fonctionnent que pour les cas potentiels d'exploitation au travers d'Internet Explorer. Les contrôles ActiveX peuvent être utilisés dans d'autres situations (documents Microsoft Office, par exemple).

Les vulnérabilités se trouvant dans une bibliothèque, il appartient également aux développeurs de mettre à jour leurs produits potentiellement affectés. A cette fin, Microsoft a détaillé une méthodologie permettant de déterminer si une application est vulnérable (cf. section Documentation). Un outil est également disponible pour faciliter cette démarche sur le site <http://www.icas.org>. Adobe et Cisco ont, d'ores et déjà, émis des bulletins de sécurité pour certains de leurs produits qui sont concernés.

Davantage de détails sur les deux bulletins sont disponibles sur les sites de Microsoft.

1.1.1 Documentation

- Avis de sécurité Microsoft 973882 du 28 juillet 2008 :
<http://www.microsoft.com/france/technet/security/advisory/973882.msp>
- Méthodologie pour déterminer si une application est vulnérable :
<http://msdn.microsoft.com/en-us/visualc/ee309358.aspx>
- Bloc-notes « Security Research and Defense » :
<http://blogs.technet.com/srd/>
- Bloc-notes « Security Development Lifecycle » :
<http://blogs.technet.com/sdl/archive/2009/07/28/atl-ms09-035-and-the-sdl.aspx>
- Avis du CERTA-2009-AVI-299 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-299/index.html>
- Avis du CERTA-2009-AVI-300 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-300/index.html>

1.2 Vulnérabilité de ISC BIND

Cette semaine, tandis que Microsoft publiait ses correctifs en dehors de son cycle traditionnel, l'Internet Systems Consortium (ISC) publiait bien plus discrètement un correctif pour le serveur de nom de domaine BIND.

La vulnérabilité corrigée a fait l'objet de l'avis CERTA-2009-AVI-302. Elle peut être exploitée par le biais d'un paquet UDP pour perturber le service de noms. Il s'agit de l'interprétation de requêtes de mises à jour dynamiques concernant une zone pour laquelle le serveur est autorisé (*master*) et qui contient des données d'enregistrement de type ANY.

Parmi les caractéristiques de l'exploitation :

- les trames UDP peuvent être émises en usurpant des adresses IP sources ;
- les traces correspondantes dans les journaux de l'application indiquent la tentative d'exploitation mais ne précisent pas les éventuels émetteurs ;
- l'attaque fonctionne même si la condition "allow-update { none; }; " est indiquée dans la configuration ;
- plusieurs configurations incluent des zones maîtres pour *localhost.localdomain* pouvant ainsi être vulnérables.

Une mesure préventive ou de surveillance consiste à observer les requêtes de type UPDATE (opcode=5).

A cette occasion, le CERTA rappelle qu'il est important de prendre en compte les serveurs de noms dans le cadre d'une politique de surveillance de son réseau.

1.2.1 Documentation associée

- Avis CERTA-2009-AVI-302, « Vulnérabilité dans ISC BIND » du 29 juillet 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-302/>
- Bloc-notes de Stéphane Bortzmeyer, « Faille BIND permettant une DoS via les mises à jour dynamiques », 29 juillet 2009 :
<http://www.bortzmeyer.org/bind-dos-update.html>
- RFC 2136, « Dynamic Updates in the Domain Name System (DNS UPDATE) », avril 1997 :
<http://www.ietf.org/rfc/rfc2136.txt>

1.3 Vulnérabilité Shockwave Flash

Enfin, le CERTA a également publié l'avis CERTA-2009-AVI-305 relatif à la publication par Adobe du correctif pour la faille détaillée dans CERTA-2009-ALE-013. Pour rappel cette vulnérabilité touchait plusieurs produits Adobe dont Acrobat, Reader et Flash Player. Il est vivement recommandé d'appliquer les correctifs associés. Par ailleurs, la faille étant exploitable par le biais des extensions présentes dans Internet Explorer et Firefox, il faudra bien prendre garde à effectuer la mise à jour pour chaque navigateur : un contrôle ActiveX pour le premier et un module complémentaire pour le second.

Cette semaine a donc vu la publication d'avis touchant des produits très répandus ou d'usagers courants. Malgré un contexte estival peu propice à la chose, il est tout de même très fortement recommandé de porter une attention particulière à toutes ces publications et d'appliquer les correctifs associés dans les plus brefs délais.

2 SSL et les caractères spéciaux

Au cours d'une conférence de sécurité, un chercheur a trouvé un moyen plutôt original de mettre à mal la chaîne de sécurité induite par l'utilisation de SSL. Pour rappel, l'initiation d'une connexion SSL se fait après échange et vérification d'un certificat. Pour que ce certificat soit reconnu par défaut par les navigateurs classiques, il est nécessaire de l'avoir fait vérifier et signer par une autorité de certification "de confiance" (CA).

Pour simplifier, lorsqu'une autorité de certification vérifie un certificat, elle contacte le propriétaire du domaine contenu dans le *Nom Commun* (ou *Common Name*). La vérification faite, l'autorité de certification signe le certificat qui peut alors être utilisé.

Au cours de la conférence, le chercheur a démontré des failles dans la gestion des caractères spéciaux permettant de faire signer des certificats par une autorité de certification, puis d'utiliser ces certificats pour tromper un internaute peu attentif.

Les toutes dernières versions des navigateurs corrigent ce problème. Quoiqu'il en soit, le CERTA tient à rappeler qu'il convient de toujours vérifier scrupuleusement le contenu d'un certificat (et en particulier la concordance du *Nom Commun* avec le site visité) avant d'accepter une connexion SSL et a fortiori avant d'accepter définitivement d'ajouter le certificat dans son magasin. Des caractères spéciaux dans le *Nom Commun* (en particulier un "." à la fin de celui-ci) sont certainement suspects.

3 Cycle de vie du système d'exploitation Debian

Le projet Debian fournissant la distribution homonyme basée sur le système GNU/Linux a annoncé cette semaine une modification dans sa politique de publication de nouvelle version stable.

Historiquement et jusqu'à la version 5.0 (*Lenny*), le projet considérait que la sortie d'une nouvelle version stable ne devait avoir lieu que lorsque la distribution en phase de test (*testing*) avait atteint un degré de maturité suffisant. Peu importait la durée du cycle de développement.

Ainsi, la durée entre deux versions a parfois excédé les deux ans. Or, depuis peu, il a été décidé par ce projet communautaire d'initier un processus de stabilisation (*freeze*) à date fixe. Dorénavant, la version de test entrera en version *freeze* au mois de novembre des années impaires pour que la sortie finale de la nouvelle version stable se fasse au début de l'année paire suivante. La phase comprise entre l'état *frozen* et cette publication est réservée à la correction des bogues résiduels.

En terme de sécurité et de maintenance, ceci peut avoir un effet bénéfique, puisqu'il devient possible d'anticiper et planifier une migration. La phase postérieure au *freeze* peut être d'ailleurs l'occasion de tester la nouvelle version puisque dans cet état, les versions des logiciels ne changent plus. Il devient alors possible, et sans trop de surprise, de tester la migration et l'intégration de ses logiciels métier.

4 Windows 7 et la fonctionnalité *HomeGroup*

4.1 De quoi s'agit-il ?

Il s'agit de faciliter le partage de fichiers entre plusieurs ordinateurs d'un réseau privé, par exemple des photos entre plusieurs ordinateurs d'un domicile. Jusque là, pour accéder aux ressources d'une autre machine, il fallait que celle-ci les partage et que l'utilisateur distant ait les droits de s'y connecter et de lire les fichiers, cela pouvant, bien sûr, poser de nombreux problèmes de configuration. La fonctionnalité *HomeGroup* offre la possibilité aux utilisateurs de partager simplement des ressources (fichiers, répertoires ...) au sein d'un groupe. Il n'est plus question de "droits d'accès" ou "droits en lecture" mais d'appartenance au groupe. Pour en faire partie, chaque utilisateur devra saisir le mot de passe unique et partagé, généré au moment de la création du *HomeGroup* et indiquer ce qu'il désire partager. L'accès aux ressources mises en commun se fait ensuite simplement dans l'explorateur de fichiers qui contient un nouvel élément dans le bandeau de gauche, le *HomeGroup*.

4.2 Comment cela fonctionne-t-il ?

Chaque machine qui fait partie d'un *HomeGroup* dispose d'un compte utilisateur `HomeGroupeUser$` qui fait partie du groupe `HomeUsers`, ce dernier ayant les droits sur les données partagées. L'authentification pour accéder aux ressources distantes est ensuite faite par l'utilisateur `HomeGroupeUser$` et à l'aide du nouveau protocole `Public Key-based User to User (PKU2U)`.

4.3 Conclusion

Attention, l'accès aux ressources n'est protégé que par un mot de passe partagé que chacun possède et peut donner ; on ne sait donc pas *a priori* qui accédera aux données. Le CERTA recommande donc la plus grande prudence lors de l'utilisation de cette fonctionnalité.

4.4 Documentation

- Présentations de la fonctionnalité :
<http://windows.microsoft.com/en-us/windows7/products/features/homegroup>
<http://windows.microsoft.com/en-us/windows7/help/home-sweet-homegroup-networking-the-easy-way>
- Article sur son fonctionnement :
<http://blogs.technet.com/pascals/archive/2009/07/28/homegroups-comment-ca-marche.aspx>
- Introduction à la sécurité de Windows 7 (section "Extending Authentication Protocols") :
<http://technet.microsoft.com/en-us/magazine/2009.05.win7.aspx>
- Introduction du protocole PKU2U dans Windows 7 :
[http://windows.microsoft.com/en-us/library/dd560634\(W.S.10\).aspx](http://windows.microsoft.com/en-us/library/dd560634(W.S.10).aspx)

5 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 2009.

6 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/>

7 Rappel des avis émis

Dans la période du 24 au 31 juillet 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-288 : Multiples vulnérabilités de Common Data Format
- CERTA-2009-AVI-289 : Vulnérabilités dans Joomla!
- CERTA-2009-AVI-290 : Multiples vulnérabilités dans Mozilla Firefox
- CERTA-2009-AVI-291 : Vulnérabilité dans IBM Tivoli Identity Manager
- CERTA-2009-AVI-292 : Vulnérabilités dans HP-UX
- CERTA-2009-AVI-293 : Vulnérabilité dans Novell Privileged User Manager
- CERTA-2009-AVI-294 : Multiples vulnérabilités dans Cisco Unified Contact Center Express
- CERTA-2009-AVI-295 : Vulnérabilité dans Sun Java System Access Manager Policy Agent
- CERTA-2009-AVI-297 : Vulnérabilité dans les produits Kaspersky
- CERTA-2009-AVI-298 : Multiples vulnérabilités dans Squid
- CERTA-2009-AVI-299 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2009-AVI-300 : Multiples vulnérabilités dans Microsoft Visual Studio
- CERTA-2009-AVI-301 : Multiples vulnérabilités dans Cisco WLC
- CERTA-2009-AVI-303 : Vulnérabilité dans des produits CISCO
- CERTA-2009-AVI-304 : Multiples vulnérabilités dans le routage BGP des équipements Cisco

Pour cette même période le CERTA a mis à jour les avis suivants :

- CERTA-2009-AVI-272-001 : Vulnérabilité de Apache mod_proxy (modification de la solution, ajout des solutions pour les éditeurs : Debian, Ubuntu, RedHat et Mandriva)
- CERTA-2009-AVI-296-001 : Vulnérabilité dans VLC (ajout du lien vers la liste des changements apportés à la version 1.0.1)
- CERTA-2009-AVI-302-001 : Vulnérabilité dans ISC BIND (ajout des bulletins de sécurité Debian, Ubuntu, RedHat, OpenBSD, FreeBSD)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

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

9 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.

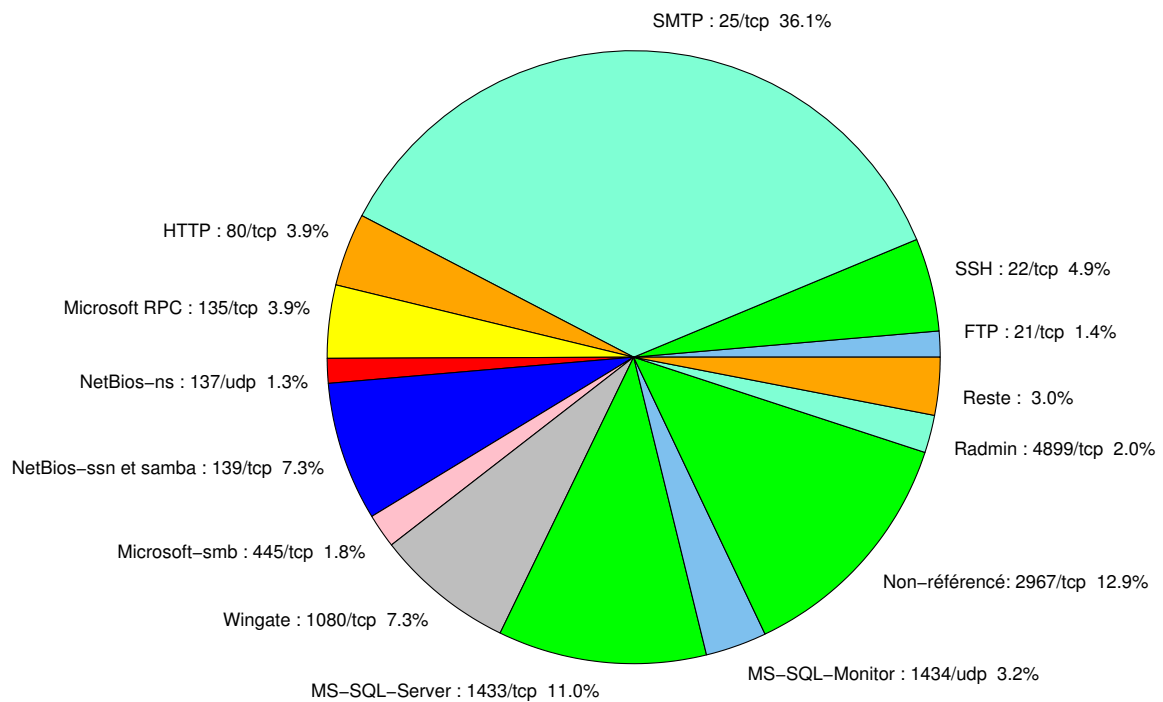


FIG. 1: Répartition relative des ports pour la semaine du 24 au 31 juillet 2009

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
25/tcp	36.08
80/tcp	31.92
2967/tcp	12.91
1433/tcp	10.99
1080/tcp	7.32
22/tcp	4.9
135/tcp	3.85
1434/udp	3.22
4899/tcp	1.98
445/tcp	1.8
3127/tcp	1.36
137/udp	1.3
3306/tcp	0.86
3389/tcp	0.62
3128/tcp	0.43
2100/tcp	0.12

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

31 juillet 2009 version initiale.