

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2009-46

---

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-046>

---

### Gestion du document

Référence	CERTA-2009-ACT-046
Titre	Bulletin d'actualité 2009-46
Date de la première version	13 novembre 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-046.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-046/>

## 1 Bulletins Microsoft du mois de novembre

Cette semaine, Microsoft a émis six nouveaux bulletins de sécurité corrigeant 15 vulnérabilités, dont trois ont un niveau critique et trois important selon la métrique définie par l'éditeur :

- une faille dans WSDAPI (*Web Service on Devices API*) présent dans Windows Vista et Server 2008 permet à une personne sur le même sous-réseau d'exécuter du code arbitraire (MS09-063) ;
- une vulnérabilité dans le serveur de licences d'enregistrement sous Windows 2000 permet l'exécution de code arbitraire à distance au moyen d'un paquet RPC spécialement conçu (MS09-064) ;
- des vulnérabilités dans les pilotes en mode-noyau de Windows permettent l'exécution de code arbitraire à distance (MS09-065) ;
- une faille dans Active Directory permet de provoquer un déni de service à distance (MS09-066) ;
- plusieurs vulnérabilités dans Excel et dans Word permettent à une personne malintentionnée de provoquer l'exécution de code arbitraire en incitant une victime à ouvrir un fichier spécialement conçu (MS09-067, MS09-068).

Des preuves de faisabilité pour certaines des vulnérabilités sont déjà disponibles sur l'internet et il est donc indispensable d'appliquer les correctifs dès que possible.

## 2 Retour sur la vulnérabilité TLS/SSL

### 2.1 Introduction

SSL (*Secure Socket Layer*) est un protocole mis au point par Netscape à partir de 1995 pour permettre l'établissement d'une connexion sécurisée (chiffrée, intègre et authentifiée). Suite à une normalisation par l'IETF en 2001, le protocole a changé de nom pour s'appeler TLS (*Transport Layer for Security*).

Les différentes versions de ces protocoles sont :

- SSLv2 qui est une version obsolète, vulnérable à de nombreuses attaques et qui ne doit plus être utilisée ;
- SSLv3 qui est une version de compatibilité, à éviter ;
- TLSv1.0, correspondant à SSLv3.1, qui est la première version formellement définie par l'IETF (RFC 2246) ;
- TLSv1.1, la version la plus déployée aujourd'hui (RFC 4346) ;
- TLSv1.2, standard défini depuis août 2008 (RFC 5246), mais qui n'est pas encore largement déployé.

Afin de permettre l'établissement d'un canal de communication chiffré et intègre, les deux parties doivent s'entendre sur les algorithmes et paramètres à utiliser : on parle de négociation. Durant cette étape de négociation, le serveur présente un certificat au client. Ce certificat permet au client d'authentifier le serveur. Il est également possible pour le serveur de demander au client de s'authentifier de la même façon à l'aide d'un certificat.

Par la suite, il est possible aux deux parties de renégocier les algorithmes et les paramètres cryptographiques. Parmi les raisons légitimes d'une telle renégociation, on peut citer :

- le rafraîchissement des clés cryptographiques avant leur usure ;
- la demande tardive par le serveur d'un certificat de la part du client (en cas de tentative d'accès à du contenu protégé) ;
- la nécessité d'employer des algorithmes différents en fonction des données échangées (notons que ce dernier cas est généralement une mauvaise raison).

C'est ce mécanisme de renégociation du protocole TLS qui présente une faille décrite ci-dessous.

### 2.2 Description de l'attaque

Remarquons que dans le cadre de cet article, les termes SSL et TLS sont interchangeable. En effet, la vulnérabilité mise en évidence affecte toutes les versions des protocoles SSL et TLS existantes à ce jour.

Le 4 novembre dernier, deux chercheurs, Marsh Ray et Steve Dispensa, ont publié des éléments démontrant l'existence d'une faille conceptuelle dans la gestion de la renégociation des sessions TLS. Plusieurs scénarios ont été décrits, mettant en jeu un client et un serveur légitimes, ainsi qu'un attaquant se plaçant « au milieu », c'est-à-dire capable d'intercepter, de modifier et d'injecter tout trafic entre les deux parties légitimes.

Dans tous les cas, l'attaquant a besoin que le client démarre une connexion SSL ou TLS. Le premier message du client (« Client Hello ») est conservé par l'attaquant dans un premier temps, pendant qu'il entame une session SSL avec le serveur. Une fois cette première négociation effectuée entre l'attaquant et le serveur, il est possible au premier d'injecter des commandes auprès du serveur. Lorsqu'il a envoyé tous les éléments nécessaires à son attaque, l'attaquant transmet le message initial du client au serveur, puis relaie de part et d'autre les messages de la renégociation qui a lieu entre le client et le serveur (qui se trouve être la négociation initiale du point de vue du client), en chiffrant/déchiffrant les messages côté serveur. A l'issue de cette négociation, il existe un canal chiffré entre le client et le serveur, auquel l'attaquant n'a plus accès. Le client commence alors à envoyer des messages, sans se douter que l'attaquant a déjà émis des données avant la renégociation. Il est donc possible à l'attaquant d'émettre en clair n'importe quelle quantité de données avant que le client démarre réellement sa connexion et émette ses requêtes, et ce sans qu'aucune des parties légitimes ne puisse le détecter.

Il existe des variantes de cette attaque : par exemple, l'attaquant peut entamer une session HTTPS non authentifiée (côté client), et demander à avoir accès à une page web sécurisée demandant une modification de mot de passe par exemple. Le serveur arrête alors la communication applicative pour demander un certificat au client qui le fournira sans se douter qu'une requête a déjà été émise en son nom. Enfin, la requête sera exécutée par le serveur une fois la renégociation terminée, même si la requête provenait d'un échange alors non authentifié !

### 2.3 Impact de l'attaque

A priori, seul HTTPS est vulnérable

Cette attaque permet à l'attaquant d'injecter des messages précédant les requêtes d'un client légitime auprès d'un serveur, dans toute connexion TLS permettant la renégociation. Cependant, cela ne semble pas avoir d'impact sur un grand nombre de protocoles utilisant SSL : SMTPS, IMAPS, POPS, etc. En effet, si l'utilisateur veut

bénéficier des privilèges d'un utilisateur, il a besoin que celui-ci s'authentifie ; or ces protocoles réalisent l'authentification avant l'exécution des requêtes, ce qui rend inefficace l'injection préalable de trafic, lequel serait perçu comme un ensemble de requêtes non authentifiées.

Il existe toutefois une exception majeure, HTTPS. En effet, il s'agit d'un protocole sans état, dans lequel le contenu de la requête précède l'envoi des éléments d'authentification. Par exemple, on peut voir des échanges légitimes de la forme:

```
GET /change-mot-de-passe.php?mdp=secret
Cookies: login=georges;session=03462f4a47cd67f
```

où la première ligne correspond à la requête, alors que la seconde contient les éléments d'authentification. On peut dès lors imaginer des attaques où injecter des lignes permet à l'attaquant d'obtenir des accès privilégiés. Par exemple, s'il injecte le contenu suivant :

```
GET /change-mot-de-passe.php?mdp=secret
X-Forget-This:
```

sans terminer la seconde ligne, et que le client légitime envoie la requête :

```
GET /index.php
Cookies: login=georges;session=03462f4a47cd67f
cela donne au final, vu du serveur:
```

```
GET /change-mot-de-passe.php?mdp=secret
X-Forget-This: GET /index.php
Cookies: login=georges;session=03462f4a47cd67f
```

où l'en-tête spécifique X-Forget-This rend inopérante la requête réelle du client.

La vulnérabilité n'est cependant pas critique

Bien que les implémentations actuelles de SSL et de HTTPS soient vulnérables aux attaques ci-dessus, puisqu'elles acceptent les renégociations, cette attaque ressemble à une autre classe d'attaques déjà bien connues, les CSRF (*Cross-Site Request Forgeries*). Ces dernières consistent par exemple à utiliser le fait qu'un utilisateur se soit authentifié sur un site donné pour essayer de faire une requête vers ce site depuis une autre page contrôlée par l'attaquant, en bénéficiant des cookies d'authentification.

Dans les deux cas, il s'agit d'attaques « en aveugle » : l'attaquant ne récolte jamais la réponse de la requête qu'il a effectuée, il n'y a pas d'atteinte à la confidentialité de l'échange entre le client et le serveur. L'attaquant ne dispose que d'une seule requête authentifiée pour déclencher son attaque.

La réponse classique pour contrer les CSRF est l'utilisation de jetons liant un formulaire sensible (changement de mot de passe) lorsqu'il est affiché à l'utilisateur à la réponse qu'envoie ce client. Si l'affichage du formulaire n'a jamais eu lieu, comme dans les attaques décrites, aucun jeton n'a été généré et il ne peut y avoir correspondance : la requête sera rejetée.

Ainsi, la vulnérabilité existe mais est atténuée par les contre-mesures souvent déjà existantes qui ont été mises en place pour lutter contre une classe d'attaques voisine.

## 2.4 Contre-mesures

Nous l'avons vu, des contre-mesures au niveau applicatif permettent de limiter l'impact d'une telle attaque. Il n'en reste pas moins qu'un problème structurel a été mis en évidence dans le protocole SSL : à l'heure actuelle, il n'est pas possible de vérifier que les différentes négociations qui ont lieu au sein d'une même connexion ont été réalisées avec les mêmes interlocuteurs.

Une contre-mesure efficace est d'ores et déjà possible aujourd'hui : elle consiste à simplement refuser toute renégociation côté serveur. C'est le comportement par défaut de la version 0.9.8l de la bibliothèque OpenSSL, publiée le 5 novembre dernier. Cela assure alors au serveur qu'aucun client ne sera attaqué. Cependant, le client n'a toujours aucun moyen de s'assurer de son côté que sa connexion n'a pas été altérée. Cette contre-mesure a des effets secondaires. Elle remet en cause la configuration d'un serveur HTTPS qui fait dépendre les options SSL du répertoire visé. La faille décrite ici peut avoir un impact réel sur la sécurité, d'où la difficulté pour gérer correctement la transition en attendant la nouvelle extension. Il est cependant essentiel de comprendre que l'impact est très dépendant de la couche applicative.

D'autres implémentations (PostgreSQL, VPN SSL...) peuvent être affectées par la vulnérabilité ou sensibles à la contre-mesure précédente. L'analyse doit être faite au cas par cas, pour confirmer ou infirmer le risque.

Dans le cas particulier où une authentification par certificat client doit avoir lieu, une autre contre-mesure intéressante est que le serveur demande ce certificat dès la première négociation, afin d'éviter qu'un attaquant non authentifié puisse injecter des éléments, puisque sa négociation échouera. Cependant là encore, seul le serveur pourra s'assurer de l'absence d'attaque.

Pour résoudre le problème durablement, un projet de RFC (*Request For Comments*) a été publié (cf. la section Documentation). Ce projet décrit une nouvelle extension TLS, émise à chaque négociation par le client, puis par le serveur (si le client la supporte) et donnant des éléments sur la négociation précédente. Dans l'attaque décrite plus haut, il sera alors possible au client (qui croit réaliser une première négociation) et au serveur (qui pense effectuer une renégociation) de se rendre compte qu'ils ont été dupés, et la négociation échouera.

## 2.5 Conclusion

Une vulnérabilité conceptuelle du protocole SSL a été découverte par des chercheurs début novembre 2009. Son impact est a priori limité au protocole HTTPS, mais est atténué par des contre-mesures déjà existantes en réponse à une classe d'attaque voisine, les CSRF.

Cette attaque ne remet pas en cause l'intérêt de SSL et TLS pour gérer l'authentification des serveurs et des clients sur Internet. Il est cependant aujourd'hui essentiel de supprimer la possibilité de renégocier les paramètres SSL sur tous les serveurs qui le permettent. Dans un second temps, il faudra mettre à jour la bibliothèque gérant la couche TLS dès qu'une version intégrant la nouvelle extension sera disponible.

## 2.6 Documentation

- le site d'OpenSSL :  
<http://www.openssl.org>
- le projet RFC sur la renégociation TLS :  
<https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt>
- Avis CERTA-2009-AVI-482 - Vulnérabilité du protocole SSL/TLS :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-482/>

## 3 Gestion des mots de passe dans les applications

Lors d'une analyse d'incident le CERTA a pu constater que certaines applications stockaient les mots de passe de façon peu sûre ou dangereuse lorsque l'utilisateur utilisait la fonctionnalité de « Favoris » de l'application.

Ainsi certains logiciels, pourtant assez connus comme des clients libres de messagerie instantanée ou de transfert de fichiers (FTP), stockent sur le disque les identifiants et mots de passe en clair lorsqu'on leurs demande de sauvegarder les données de connexions d'un site.

Pour certains d'entre eux, les fichiers contenant ces informations sensibles portent un nom très explicite et sont des fichiers au format XML présentant des balises de type `<login>... </login>` ou bien encore `<password>... </password>`. Ces balises, elles aussi très explicites, délimitent pour la première un nom d'utilisateur et pour la seconde un mot de passe en clair. Cette grammaire facilite la recherche des données sensibles par les programmes et les utilisateurs malveillants.

Il existe pourtant des mécanismes permettant de protéger un carnet de favoris intégrant la sauvegarde des identifiants, en s'appuyant sur des fonctions cryptographiques pour protéger ce type d'informations.

### Recommandations :

Lorsque l'on veut utiliser un logiciel, il est indispensable de s'assurer de la manière dont il stocke les données sensibles qu'il aurait à traiter. Dans le cas de la sauvegarde des identifiants de connexion, si cette fonctionnalité doit être utilisée, elle doit garantir, au minimum, la confidentialité des données qu'elle mémorise.

Pour l'utilisateur, une bonne pratique consiste à se souvenir des mots de passe et à ne pas faire confiance en ce genre de fonctionnalité.

## 4 Codes malveillants pour iPhone/iPod Touch déverrouillé

Dans le bulletin d'actualité de la semaine dernière, nous avons parlé des dangers du déverrouillage (*Jailbreak*) sur iPhone et iPod Touch. Cette semaine sont apparus de nouveaux codes malveillants exploitant la même faiblesse : l'accès au serveur SSH en utilisant le mot de passe par défaut du compte administrateur.

Jusqu'à présent, les codes exploitant cette erreur de conception étaient plus ou moins inoffensifs. Ils provoquaient par exemple un changement de fond d'écran. Aujourd'hui, il existe des vers réellement malveillants qui permettent d'avoir accès aux données personnelles de l'utilisateur : courriels, répertoire, SMS, calendrier, photos...

Ces codes malveillants parcourent l'Internet, de façon plus ou moins intelligente, à la recherche de services 22/TCP en écoute. Quand ils en trouvent un, ils essaient d'ouvrir une session administrateur en utilisant une attaque par dictionnaire. Les mots de passe testés sont ceux par défaut des comptes administrateur des iPhone/iPod Touch. Cette attaque fonctionne car les utilisateurs qui déverrouillent leurs téléphones et installent un serveur SSH, changent rarement le mot de passe du compte administrateur de leur système.

D'une façon générale, il est clair que les risques en matière de sécurité informatique sont mal évalués lorsqu'on parle de ce type d'appareil. Les bonnes pratiques d'utilisation des ordinateurs sont applicables de la même façon aux *smartphones* et autres assistants personnels... Comme ne pas surfer sur le Web avec un compte administrateur.

Encore une fois, le CERTA recommande de ne pas effectuer ce type de manipulation, qui a pour conséquence de contourner le modèle de sécurité mis en place dans les iPhone/iPod Touch, et de les rendre plus vulnérables aux attaques informatiques.

## 5 Liens utiles

- Mémento sur les virus :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :  
<http://www.auscert.org.au/render.html?it=1937>
- Note d'information du CERTA sur les risques associés aux clés USB :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

## 6 Rappel des avis émis

Dans la période du 06 au 12 novembre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-479 : Vulnérabilité dans Asterisk
- CERTA-2009-AVI-480 : Vulnérabilités dans Joomla!
- CERTA-2009-AVI-481 : Vulnérabilités dans Google Chrome
- CERTA-2009-AVI-482 : Vulnérabilité du protocole SSL/TLS
- CERTA-2009-AVI-483 : Vulnérabilité dans BlackBerry Desktop Manager
- CERTA-2009-AVI-484 : Vulnérabilité dans PowerHA Cluster Management sous IBM AIX
- CERTA-2009-AVI-485 : Vulnérabilité dans les produits Citrix
- CERTA-2009-AVI-486 : Vulnérabilité dans Sun Virtual Desktop Infrastructure

- CERTA-2009-AVI-487 : Multiples vulnérabilités dans Apple MacOS X
- CERTA-2009-AVI-488 : Vulnérabilités dans Xoops
- CERTA-2009-AVI-489 : Vulnérabilité dans CUPS
- CERTA-2009-AVI-490 : Vulnérabilité de Microsoft WSDAPI
- CERTA-2009-AVI-491 : Vulnérabilité dans le serveur d'enregistrement de licences Microsoft
- CERTA-2009-AVI-492 : Vulnérabilités dans le noyau de Microsoft Windows
- CERTA-2009-AVI-493 : Vulnérabilité dans Microsoft Active Directory
- CERTA-2009-AVI-494 : Multiples vulnérabilités dans Microsoft Office Excel
- CERTA-2009-AVI-495 : Vulnérabilité dans Microsoft Office Word
- CERTA-2009-AVI-496 : Multiples vulnérabilités de Apple Safari
- CERTA-2009-AVI-497 : Vulnérabilités dans McAfee IntruShield Network Security Manager

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

- CERTA-2009-AVI-478-001 : Vulnérabilité dans Snort (correction d'une erreur dans les systèmes affectés)

## **7 Actions suggérées**

### **7.1 Respecter la politique de sécurité**

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel 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.

### **7.2 Concevoir une architecture robuste**

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

### **7.3 Appliquer les correctifs de sécurité**

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

### **7.4 Utiliser un pare-feu**

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

## 7.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

## 7.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements 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.

## 7.7 Former et sensibiliser les utilisateurs

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

[http://www.ssi.gouv.fr/site\\_rubrique63.html](http://www.ssi.gouv.fr/site_rubrique63.html)

## 8 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

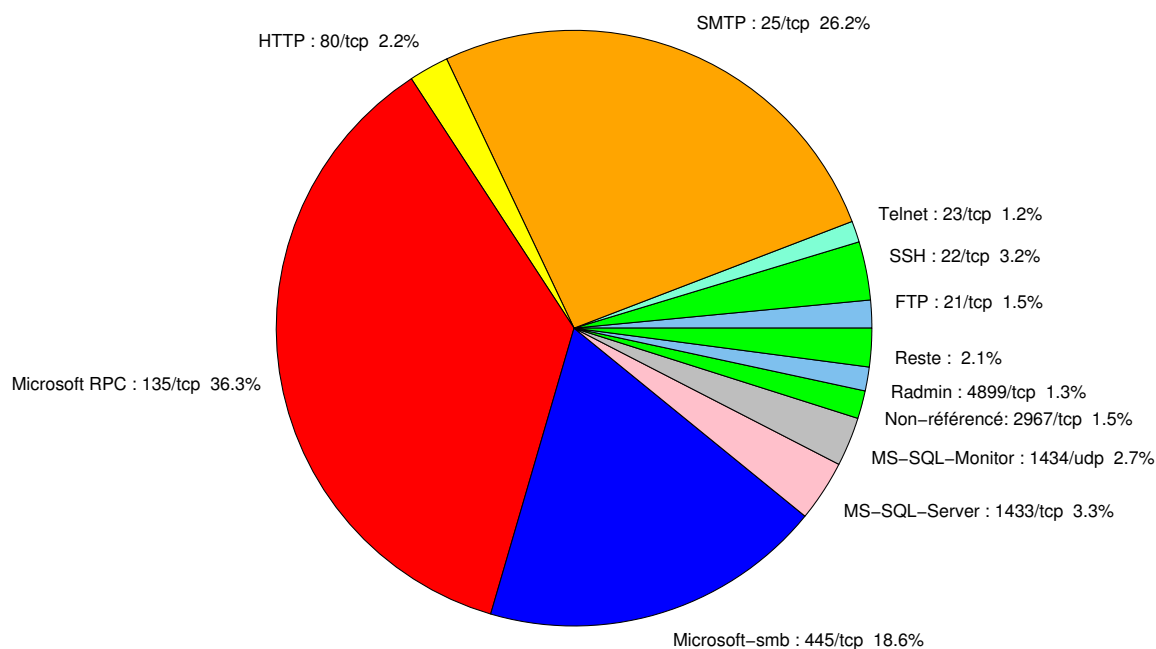


FIG. 1: Répartition relative des ports pour la semaine du 06 au 12 novembre 2009

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
135/tcp	36.28
25/tcp	26.2
445/tcp	18.64
1433/tcp	3.31
22/tcp	3.16
80/tcp	2.73
1434/udp	2.66
21/tcp	1.58
2967/tcp	1.51
4899/tcp	1.29
23/tcp	1.22
3389/tcp	0.71
3128/tcp	0.5
1080/tcp	0.43
2100/tcp	0.14
3306/tcp	0.07

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

13 novembre 2009 version initiale.