

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2009-33

---

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-033>

---

### Gestion du document

Référence	CERTA-2009-ACT-033
Titre	Bulletin d'actualité 2009-33
Date de la première version	14 août 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-033.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-033/>

## 1 Élévation de privilège dans le noyau Linux

Une vulnérabilité a été récemment rendue publique. Elle concerne un déréférencement de pointeur NULL à la création de *sockets* pour quelques protocoles (PF\_BLUETOOTH, PF\_ISDN, PF\_APPLETALK, PF\_IRDA, PF\_INET6 avec IPPROTO\_SCTP, PF\_PPOX, PF\_IUCV, ...). Les opérations non disponibles ne sont pas correctement gérées, en particulier par la fonction `sock_sendpage`.

La plupart des noyaux Linux actuels sont concernés par cette vulnérabilité (branche 2.4 y compris 2.4.37.4 et branche 2.6 y compris 2.6.30.4).

Le CERTA a publié à ce sujet l'avis CERTA-2009-AVI-337. Des correctifs pour chaque distribution devraient apparaître dans les prochains jours.

### Documentation

– Avis CERTA CERTA-2009-AVI-337 :

<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-337/>

## 2 Les bulletins mensuels de Microsoft

Cette semaine, Microsoft a publié ses bulletins mensuels de sécurité. Le CERTA revient sur ces différents bulletins :

- **MS09-036** : ce bulletin fait état d'une vulnérabilité dans l'environnement d'exécution Microsoft .NET Framework dans leurs versions 2.0 avec sans le service pack 1 ou 2 et 3.5 avec sans le service pack 1. Une gestion incorrecte des files de requêtes, lorsque *Internet Information Services (IIS) 7.0* est installé, permet d'effectuer un déni de service lorsque *ASP.NET* est configuré pour utiliser le mode « intégré » et non le mode « classique » ;
- **MS09-037** : plusieurs vulnérabilités dans la bibliothèque *ATL (Active Template Library)*, de Microsoft Windows permettent d'exécuter du code arbitraire à distance ;
- **MS09-038** : deux vulnérabilités dans le traitement de fichiers Windows Media permettent à une personne malintentionnée via un fichier *AVI* spécialement conçu d'exécuter du code arbitraire à distance ;
- **MS09-039** : deux erreurs dans Microsoft Windows Internet Name Service permettent à une personne malintentionnée d'exécuter du code arbitraire à distance via un paquet de réplication spécialement conçu envoyé au service WINS vulnérable ;
- **MS09-040** : un problème a été identifié dans le service, non activé par défaut, de mise en file d'attente *MSMQ* de Microsoft Windows. Le service vérifie de façon incorrecte les données en entrée avant de les transmettre au tampon et permet à un utilisateur d'élever ses privilèges ;
- **MS09-041** : une vulnérabilité a été identifiée dans le *Service Station de Travail* de Microsoft Windows. Celui-ci alloue et libère la mémoire de manière incorrecte lors de la réception de messages RPC spécialement conçus. L'exploitation de cette vulnérabilité permet d'exécuter du code arbitraire avec des privilèges élevés ;
- **MS09-042** : le service *Telnet* ne souscrit pas correctement aux protections contre la réflexion des informations d'identification *NTLM*. Une exécution de code arbitraire est possible via cette vulnérabilité ;
- **MS09-043** : un ensemble de contrôles *COM (Component Object Model)* utilisés pour la publication de feuilles de calcul, de graphiques et de bases de données sur le Web ainsi que pour l'affichage de composants publiés sur le Web sont vulnérables et permettent une exécution de code arbitraire à distance. Ce correctif clôt l'alerte CERTA-2009-ALE-011 ;
- **MS09-044** : deux vulnérabilités ont été identifiées dans la *Connexion Bureau à distance* de Microsoft Windows. La première est due aux paramètres renvoyés par le serveur *RDP* qui ne sont pas correctement traités. La seconde concerne le contrôle *ActiveX* du client. Dans les deux cas, seuls les clients *RDP* sont donc affectés et une exécution de code arbitraire à distance est possible.

Le CERTA rappelle l'impérative nécessité d'appliquer au plus vite ces correctifs afin de protéger son système d'information.

### Documentation

- Synthèse des bulletins de sécurité Microsoft d'août 2009 :  
<http://www.microsoft.com/france/technet/security/bulletin/ms09-aug.mspx>

## 3 Administrer Adobe Flash sur un poste Windows

### 3.1 Introduction

Le CERTA a publié dans le courant du mois de juillet l'alerte CERTA-2009-ALE-013 concernant Adobe Shockwave Flash. D'autres vulnérabilités avaient fait l'objet en mars 2009 de l'avis CERTA-2009-AVI-076.

Le CERTA a traité cette semaine un incident relatif à une compromission associée à l'exploitation de l'une de ces vulnérabilités. Des codes circulent actuellement, insérés dans des pages Web de sites Internet ou dans des documents au format PDF.

Le CERTA revient donc dans les sections suivantes sur quelques pratiques associées avec cette application.

### 3.2 Quelques précisions utiles

Adobe Flash Player se présente sous la forme d'un module (ou *plugin*) pour navigateur Internet. Il permet d'interpréter des contenus de type vidéo ou animation aux formats *SWF* (Shockwave Flash) ou *FLV* (*Flash Video*).

L'installation n'est cependant pas unique sur chaque machine. Elle peut être effectuée sous une forme ActiveX par exemple pour Internet Explorer et comme module additionnel dans un autre navigateur (Mozilla Firefox, Safari, etc.). Une machine peut donc avoir plusieurs installations distinctes d'Adobe Flash, avec des configurations et des niveaux de mises à jour propres.

Pour connaître les versions actuellement utilisées, il existe deux méthodes :

- en ligne, en visitant pour un navigateur donné une page comme :  
<http://www.adobe.com/software/Flash/about/> S'il y a plusieurs navigateurs installés, il faut donc réitérer l'opération (par exemple Internet Explorer puis Firefox).
- hors ligne, en cherchant l'information dans la configuration même du navigateur :
  - Sous Internet Explorer : clic droit sur l'icône d'IE et sélection de « Propriétés », puis ouverture de l'onglet « Programmes » et de l'option « Gérer les modules complémentaires » ;
  - Sous Firefox : l'adresse « about:plugins » dans la barre d'adressage retourne la liste des modules installés ;
  - Sous Safari : sélection de l'onglet « Modules installés » dans le menu « Aide » ;
  - Sous Opera : le navigateur ne retourne pas la version précise, mais seulement sa présence en interrogeant « opera:plugins » dans la barre de navigation.

Pour conclure cette section, le CERTA tient également à rappeler que les lecteurs Adobe Flash installés sur une machine ne sont pas configurables de manière simple. La seule méthode proposée par Adobe se fait en mode connecté, en se rendant avec un navigateur sur une page donnée du site Internet d'Adobe. C'est à partir de celle-ci qu'une interface de configuration est possible.

La page d'accueil se trouve à l'adresse :

[http://www.macromedia.com/support/documentation/fr/flashplayer/help/settings\\_manager.html](http://www.macromedia.com/support/documentation/fr/flashplayer/help/settings_manager.html)

Le CERTA avait longuement abordé la problématique des fichiers de session propres à Adobe, aussi appelés *Local Shared Objects* ou LSO dans le bulletin d'actualité CERTA-2008-ACT-034. Les paramètres de configuration se trouvent dans un fichier au même format, `settings.sol` et peuvent être modifiés localement avec un éditeur adapté.

Enfin, toutes les mesures citées ci-dessous s'appliquent au lecteur Adobe Flash mais restent valables pour le lecteur Adobe Shockwave.

### 3.3 Procédures de mises à jour

#### 3.3.1 En ligne

Il faut utiliser l'une des pages de l'interface de configuration en ligne Adobe :

[http://www.macromedia.com/support/documentation/fr/flashplayer/help/settings\\_manager05.html](http://www.macromedia.com/support/documentation/fr/flashplayer/help/settings_manager05.html)

Il est possible de préciser dans cette interface :

- un avertissement doit être émis si une nouvelle mise à jour est disponible ;
- la fréquence de vérification des mises à jour. La valeur par défaut, de 14 ou 30 jours, est excessive. La valeur la plus petite proposée est de 7 jours. L'interface permet de l'augmenter au maximum à 7 jours. Cela reste trop important dans les faits, étant donné que des codes d'exploitation apparaissent très rapidement après des mises à jour, voire avant dans les cas les plus récents.

Le CERTA recommande vivement de ne pas se reposer sur le fonctionnement de mise à jour automatique du lecteur Adobe Flash Player. En cas de vulnérabilité critique, une mise à jour manuelle s'impose.

#### 3.3.2 Hors-ligne

Il faut pour cela télécharger préalablement la nouvelle version du lecteur Adobe Flash sur le site officiel. L'installation peut se faire sur un poste déconnecté. La nouvelle version se charge de désinstaller l'ancienne. Il est néanmoins conseillé de vérifier après cette opération par les procédures précédentes que le changement est effectif.

### 3.4 Procédures de désinstallation

Les accès hors-ligne présentés dans la section précédente pour déterminer la version du module Adobe Flash installé permettent, au mieux, selon les navigateurs, de désactiver le module. Il n'est pas possible, via la configuration du navigateur, de désinstaller complètement l'application.

Pour le système d'exploitation Microsoft Windows, il est possible :

- de désinstaller l'application via l'option « Ajout/Suppression de programmes » du système d'exploitation ;

- de lancer manuellement les programmes de désinstallation fournis par Adobe qui se trouvent sous une des formes suivantes :
  - %WINDIR%\system32\Macromed\F\Flash\UninstFl.exe
  - %WINDIR%\system32\Macromed\F\Flash\genuninst.exe
  - %WINDIR%\system32\Macromed\F\Flash\uninstall\_activeX.exe
  - %WINDIR%\system32\Macromed\F\Flash\uninstall\_plugin.exe
- de télécharger l'application de désinstallation fournie par Adobe sur son site Internet : <http://www.adobe.com/shockwave/download/alternates/>

Adobe fournit également d'autres procédures de désinstallation manuelle sur son site Internet. Des liens sont fournis dans la dernière section de cet article.

### 3.5 Mesures préventives

Les mesures citées dans cette section ne sont pas absolues mais permettent de limiter certains risques liés aux contenus de format Flash sur les postes. Il ne s'agit donc ici que de quelques pistes envisageables.

Une mesure consiste à utiliser des navigateurs avec des configurations distinctes : l'une d'elles restrictive, n'interprète par défaut aucun code particulier dynamique suite à la visite d'une page. La seconde, plus laxiste, permet d'activer cette interprétation, de manière ponctuelle, pour des sites de confiance. Cette procédure peut être aussi appliquée en créant pour un même utilisateur plusieurs profils (Mozilla Firefox).

Une autre mesure consiste à utiliser des lecteurs Flash alternatifs en fonction du système d'exploitation et des navigateurs :

- Projet Gnash (<http://www.gnashdev.org>)
- Swfdec (<http://swdec.freedesktop.org/>)
- Gameswf Library (<http://tulrich.com/textweb.pl?path=geekstuff/gameswf.txt>)
- Flirt (non mis à jour depuis 2006 - <http://flirt.sourceforge.net/>)

Ils n'interprètent cependant pas toutes les particularités du format Flash, mal documenté à l'heure actuelle.

Des modules pour certains navigateurs (ex : Firefox - flashblock, noscript, prefbar, etc.), permettent enfin de bloquer par défaut des contenus Flash sauf autorisation explicite de l'utilisateur. Cette approche repose sur ce nouveau module qui devient de fait une nouvelle surface d'attaque. Il faut donc avoir confiance dans ce dernier (mises à jour fréquentes, code audité, etc.) avant de le déployer.

Enfin, les développeurs de sites Web comprendront ici qu'il n'est pas conseillé de développer un site Web intégralement en Flash sous peine de pénaliser nombre de visiteurs qui ne souhaitent pas installer ou activer un tel module. Un site Web doit être par défaut lisible et accessible par tout navigateur, sans forcer l'utilisateur à installer contre son gré des modules tiers.

### 3.6 Documentation associée

- Note technique Adobe 14526, "How to detect the presence of the Flash Player" : [http://kb2.adobe.com/cps/145/tn\\_14526.html](http://kb2.adobe.com/cps/145/tn_14526.html)
- Site de téléchargement des exécutables d'installation et de désinstallation Adobe pour différents navigateurs et systèmes d'exploitation : <http://www.adobe.com/shockwave/download/alternates/>
- Note technique Adobe, "Désinstallation du plug-in et du contrôle ActiveX de Macromedia Flash Player", février 2003 : [http://www.adobe.com/fr/support/flash/ts/documents/remove\\_player.htm](http://www.adobe.com/fr/support/flash/ts/documents/remove_player.htm)
- Note technique Adobe 12727, "How to remove the Flash Player ActiveX control" : [http://kb2.adobe.com/cps/127/tn\\_12727.html](http://kb2.adobe.com/cps/127/tn_12727.html)
- Note technique Adobe 14157, "How to uninstall the Adobe Flash Player plug-in and ActiveX control" : [http://kb2.adobe.com/cps/141/tn\\_14157.html](http://kb2.adobe.com/cps/141/tn_14157.html)
- Bulletin d'actualité CERTA-2008-ACT-034, "Fichiers de session avec Adobe", 22 août 2008 : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-034.pdf>
- Projet ".sol Editor" (Flash Shared Object) : <http://sourceforge.net/projects/soleditor/>  
[http://sourceforge.net/docman/display\\_doc.php?docid=27026&group\\_id=131628](http://sourceforge.net/docman/display_doc.php?docid=27026&group_id=131628)

- Bibliothèque pour manipuler les fichiers SWF, MING :  
<http://www.libming.org>  
<http://sourceforge.net/projects/ming/>
- Liste relativement à jour de projets en source ouverte concernant Flash :  
[http://www.osflash.org/open\\_source\\_flash\\_projects](http://www.osflash.org/open_source_flash_projects)
- Documentation Mozilla, "Gestion des profils" :  
<http://support.mozilla.com/fr/kb/Managing+Profiles>

## 4 Serveurs mandataires malveillants et HTTPS

L'objectif de cet article est d'aborder la problématique des serveurs mandataires pour les connexions en HTTPS. En effet, s'agissant d'un protocole cryptographique de bout en bout, la présence d'intermédiaires non de confiance ne devrait pas poser de problème. Voyons ici comment ces *Pretty-Bad-Proxy* (PBP) peuvent être utilisés pour mener des attaques.

### 4.1 Définition du Pretty-Bad-Proxy

Il s'agit d'un serveur mandataire web (*proxy*) utilisé pour mener des attaques de type « *man in the middle* ». Il a accès au trafic brut, mais ne pouvant décrypter le flux HTTPS, il utilise le canal clair associé (HTTP) pour injecter du contenu malveillant et tenter d'accéder à des données sensibles.

### 4.2 Quelques principes

#### 4.2.1 Same Origin Policy (SOP)

Il s'agit d'une sécurité consistant à cloisonner les contenus (pages, scripts, ...) afin d'éviter les interactions. Par exemple, la page d'un site A n'a pas à accéder aux identifiants saisis sur la page d'un site B. L'*origine* est déterminée par trois critères, le protocole, le nom du serveur et le port. Ainsi, <http://unserveur.tld> n'a pas la même *origine* que <https://unserveur.tld>. Il est intéressant de remarquer que les scripts n'ont pas d'*origine* propre, mais celle du cadre ou de la page qui les contient.

#### 4.2.2 HTTPS et proxy

HTTPS est un protocole bout-en-bout, ce qui est contraire au principe du serveur mandataire qui s'intercale dans le flux. Pour réussir à établir une connexion sécurisée au travers d'un proxy il faut utiliser le mécanisme de *tunnel*. Pour cela, le client envoie une première requête HTTP au proxy annonçant le serveur final, et le port, avec lequel il désire établir la session. Le proxy va alors ouvrir et maintenir deux connexions, l'une vers le client, l'autre vers le serveur et servira de relais passif pour le trafic HTTPS.

### 4.3 Les problèmes

#### 4.3.1 Les réponses d'erreur

Lorsque l'utilisateur demande la page (<https://unepage.tld>), le navigateur émet de façon transparente une requête HTTP à destination du proxy. Si ce dernier ne trouve pas la page en question, il retourne une erreur HTTP (ex: 404) qui est interprétée dans le contexte de <https://unepage.tld>. Un proxy malveillant peut donc volontairement répondre une page d'erreur contenant un script malveillant qui aura accès aux données du site sécurisé initialement demandé.

#### 4.3.2 Les redirections et l'absence d'*origine* des scripts

Les pages importent souvent des scripts depuis plusieurs sources. Chacun des scripts externes nécessite une requête à destination du proxy suivant le même schéma, à savoir, une première requête en HTTP afin de définir le tunnel désiré, puis l'établissement de la connexion sécurisée. À la première requête, le proxy peut répondre que le site a été déplacé (message 3xx), et faire établir le tunnel avec un autre serveur. Comme les scripts n'ont pas d'*origine* propre, ils seront exécutés dans le contexte du cadre qui a fait l'import et qui est bien celui du site sécurisé.

### 4.3.3 Les pages accessibles en HTTPS

Alors que le HTTPS est utilisé pour des transactions sécurisées et le HTTP pour tout le reste, il arrive souvent que les pages non sensibles soient aussi accessibles via HTTPS, elles portent le nom de "*HPIHSL*" (*HTTP-intended-but-HTTPS-loadable*). Donc, lorsqu'une page en clair est demandée (ex: <http://unsite.tld>), le *PBP* peut insérer une *IFRAME* qui a comme source une page non sensible du même site (*iframe src=https://unsite.tld/pagenonsensible.html*). Mais demandée via HTTPS et elle-même important un script en HTTP, ce dernier est demandé en clair. Le proxy peut alors le remplacer par un autre, et n'ayant pas d'*origine* propre, il aura celle de l'*IFRAME*. Comme le cadre principal a comme *origine* HTTP, le fait d'accéder à du HTTP dans une *IFRAME*, elle-même en HTTPS, n'engendre pas d'alerte.

### 4.3.4 La mise en cache des certificats

Afin d'optimiser les performances, les navigateurs mettent en cache les certificats. Un *PBP* peut utiliser ce fonctionnement pour servir ses propres pages et apparaître comme sûr (affichage du cadenas). Lorsqu'une page sécurisée est demandée (via HTTP dans un premier temps), le *PBP* répond par une page d'erreur (4xx ou 5xx) qui contient un élément pointant vers le site sécurisé (par exemple une image) et un méta élément qui forcera le rechargement de la page quelques instants plus tard. L'élément pointant vers le site sécurisé va provoquer l'établissement de la connexion sécurisée, et donc la mise en cache du certificat. Lorsque la page se recharge, le *PBP* répond par une page imitant le site sécurisé demandé (toujours au moyen d'une erreur). Le contexte étant celui du site visé et le certificat étant en cache, la page apparaît comme certifiée. Cela ne fonctionne cependant pas avec tous les navigateurs mais cette technique a l'avantage de ne pas utiliser de script.

### 4.3.5 Same Origin Policy pour les cookies

Les *cookies* sont des chaînes de caractères utilisés, entre autres, pour maintenir des sessions ouvertes. Le problème est que l'*origine* des *cookies* ne tient pas compte du protocole. Une page de <http://unsite.tld> pourra accéder aux *cookies* de <https://unsite.tld>. Pour empêcher cela le serveur doit utiliser l'attribut *SECURE* du *cookie*. Dans les faits, une grande proportion de sites dit « sécurisés » ne le font pas. Lorsqu'un utilisateur est connecté à un site « sécurisé » de la sorte, le *PBP* n'a qu'à attendre que la victime demande n'importe quelle page en HTTP de n'importe quel serveur pour y injecter une *IFRAME* malveillante. Cette dernière ayant comme source l'adresse du site sécurisé en HTTP, les *cookies* d'authentification circuleront en clair et seront interceptables par le *PBP*.

## 4.4 Conclusion

Le CERTA recommande de désactiver l'utilisation automatique des serveurs mandataires non maîtrisés. En particulier, il convient de rester prudent lors de la navigation depuis un lieu public (réseau d'hôtel, accès WiFi public, cybercafé, ...).

## 4.5 Documentation

- L'article sur les *Pretty-Bad-Proxy* de Microsoft dont sont tirés ces quelques paragraphes :  
<http://research.microsoft.com/apps/pubs/default.aspx?id=79323>
- Article de "The H security" du 10 août 2009 mettant en avant le problème des *PBP* :  
<http://www.h-online.com/security/Vulnerability-affects-all-major-browsers-/news/113965>

## 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 07 et le 13 août 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 07 au 13 août 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-314 : Vulnérabilité dans IBM AIX
- CERTA-2009-AVI-315 : Multiples vulnérabilités dans WordPress
- CERTA-2009-AVI-316 : Vulnérabilité dans Fetchmail
- CERTA-2009-AVI-317 : Vulnérabilité dans CA Data Transport Services
- CERTA-2009-AVI-318 : Vulnérabilité dans CA Unicenter
- CERTA-2009-AVI-319 : Vulnérabilités dans Zope
- CERTA-2009-AVI-320 : Multiples vulnérabilités dans Subversion
- CERTA-2009-AVI-321 : Vulnérabilité dans libvorbis
- CERTA-2009-AVI-322 : Multiples vulnérabilités dans Asterisk
- CERTA-2009-AVI-323 : Vulnérabilités dans Apache APR-Utility
- CERTA-2009-AVI-324 : Vulnérabilité dans ASPNET de Microsoft Windows
- CERTA-2009-AVI-324 : Vulnérabilités de la bibliothèque ATL de Microsoft Windows
- CERTA-2009-AVI-326 : Vulnérabilités dans le traitement de fichiers Windows Media
- CERTA-2009-AVI-327 : Vulnérabilités dans Microsoft WINS
- CERTA-2009-AVI-328 : Vulnérabilité dans le service MSMQ Microsoft Windows
- CERTA-2009-AVI-329 : Vulnérabilité dans le Service Station de Travail Microsoft Windows
- CERTA-2009-AVI-330 : Vulnérabilité dans Microsoft Telnet
- CERTA-2009-AVI-331 : Multiples vulnérabilités dans Microsoft Office Web Components
- CERTA-2009-AVI-332 : Multiples vulnérabilités dans la Connexion Bureau à distance Microsoft
- CERTA-2009-AVI-333 : Vulnérabilités de Safari
- CERTA-2009-AVI-334 : Vulnérabilité dans WordPress
- CERTA-2009-AVI-335 : Multiples vulnérabilités dans libxml2

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

- CERTA-2009-AVI-302-002 : Vulnérabilité dans ISC BIND (ajout du bulletin de sécurité IBM AIX)

## **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.

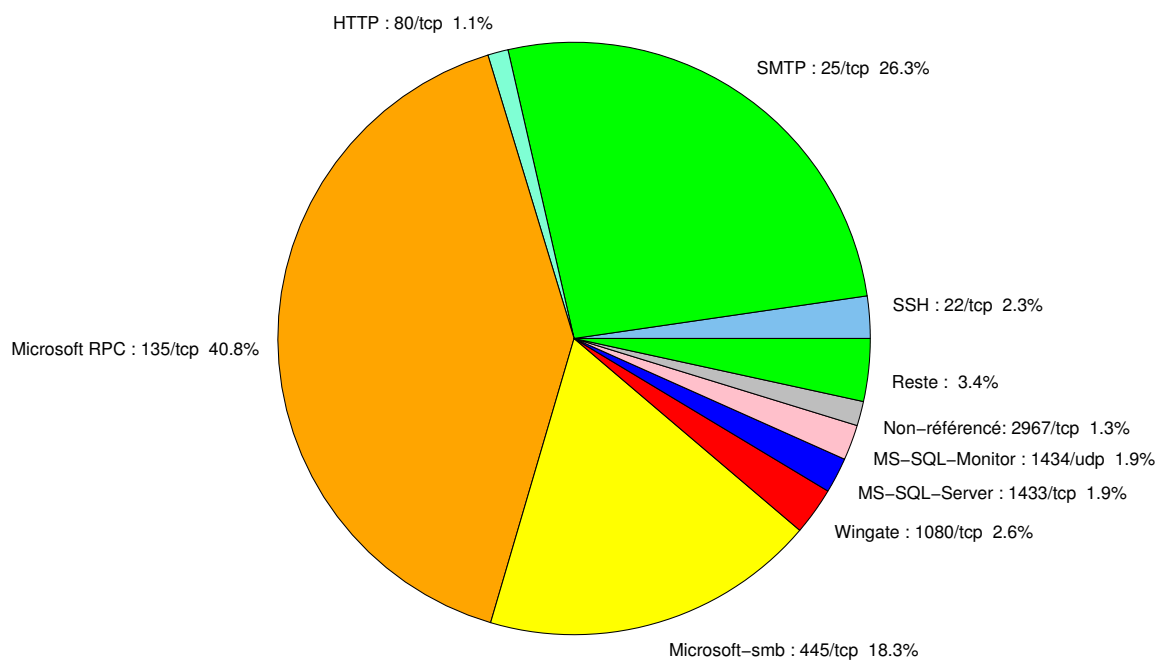


FIG. 1: Répartition relative des ports pour la semaine du 07 au 14 août 2009

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	40.75
25/tcp	26.28
445/tcp	18.33
1080/tcp	2.59
22/tcp	2.3
1434/udp	1.93
2967/tcp	1.33
80/tcp	1.18
4899/tcp	0.89
3128/tcp	0.74
23/tcp	0.59
3306/tcp	0.44
3389/tcp	0.29
143/tcp	0.22

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	11
3	Paquets rejetés . . . . .	12

## Gestion détaillée du document

14 août 2009 version initiale.