Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2007
N° CERTA-2007-ACT-041

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-41

Gestion du document

Référence	CERTA-2007-ACT-041
Titre	Bulletin d'actualité 2007-41
Date de la première version	12 octobre 2007
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-2007-ACT-041.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-2007-ACT-041/

1 Les sites épaves, écueils pour la navigation sur l'Internet

Deux incidents traités par le CERTA rappellent que l'abandon d'un site web n'est pas si simple.

1.1 Les mésaventures

Le schéma est le même dans les deux cas, malgré la différence d'environnement technique et organisationnel. Un organisme a développé un site web sur une première infrastructure. À la suite de diverses évolutions, il décide de faire migrer ce site vers un nouvel environnement. Cette migration se traduit par plusieurs changements, dont l'hébergeur, le nom de domaine et l'adresse réseau. Le nouveau site est mis en service avec succès, mais l'ancien est oublié . . . Sauf pour des internautes peu scrupuleux. Ne faisant plus l'objet de surveillance et sans mise à jour des logiciels, l'ancien site resté en ligne est une proie facile. De surcroît, les journaux de l'ancien site ne sont plus du tout consultés, ce qui contribue à maintenir les intrus plus longtemps sur le système. Selon les incidents traités, l'ancien site héberge des codes malveillants ou sert à des cyber-affrontements.

Dans chacun des incidents traités par le CERTA, l'ancien site ayant gardé un nom en rapport étroit avec l'organisme français, les méfaits commis par les intrus entachent l'image de l'organisme. La rupture de liens, contractuels ou techniques, rend difficile la gestion de l'incident.

1.2 Des recommandations

Lors d'un changement d'infrastructure, plusieurs précautions sont utiles :

- attendre la mise en service du nouveau site avant d'abandonner l'ancien ;
- sur l'ancien site et selon la configuration, ôter tout accès, logiciel ou script susceptible de faciliter une intrusion, par exemple :
  - accès réseau vers l'ancien serveur supprimé (ajout de filtrage, DNS, suppression d'adresse ou de machine...) ;
  - logiciel serveur web, PHP, SQL désinstallé du serveur ;
  - configuration du serveur web adaptée (nom de l'hôte virtuel retiré, port fermé...) ;
  - pages en PHP, CMS, remplacés par une page HTML statique. Cette page, qui peut contenir une directive de redirection vers le nouveau site, permettra en même temps d'informer le public légitime ;
- une fois ce serveur « ancien » ainsi nettoyé, le nom d'hôte doit pointer vers l'adresse IP du nouveau site ;
- une fois ce routage modifié, le nom d'hôte peut être moins surveillé et le site ancien réellement abandonné.

2 Nouveautés du côté d'Internet Explorer

2.1 Le téléchargement d'Internet Explorer 7 évolue

Depuis le 4 octobre 2007, Internet Explorer 7 de Microsoft est disponible pour tous les utilisateurs de Windows XP. Cette annonce a été publiée sur le blog du butineur de Microsoft. La mise à jour du navigateur ne requiert plus de validation de Windows Genuine Advantage (`WGA`). Cette mise à jour est disponible en téléchargement sur le site de Microsoft ou *via* les mises à jour automatiques. Jusqu'à présent l'installation d'Internet Explorer 7 n'était possible qu'après vérification de l'authenticité de la copie de Windows XP. La nouvelle version du navigateur est désormais disponible pour l'ensemble des utilisateurs de Windows XP SP2.

2.2 Microsoft : une mise à jour facultative

Microsoft publie des mises à jour prioritaires le deuxième mardi de chaque mois. L'éditeur peut également publier d'autres mises à jour à la même date. Ce fut le cas en octobre. Une mise à jour non prioritaire ajoute des certificats d'autorités de certification dans le navigateur Internet Explorer. Cinq autorités sont concernées : deux espagnoles, une finlandaise, une lettone et une turque.

Documentation

http://support.microsoft.com/kb/931125

3 Les risques des clés USB

Le CERTA rappelait la semaine dernière dans son bulletin d'actualité les risques liés à l'utilisation d'applications placées sur des supports de stockage amovibles. Le 8 octobre dernier, la région Ile de France a distribué 173 000 clés USB (Universal Serial Bus) aux lycéens et apprentis de la région. Ces clés sont présentées comme un « bureau mobile » ou un « cartable électronique ». Ce projet est observé à l'éclairage de la mise en garde publiée la semaine dernière par le CERTA dans son bulletin d'actualité. Ces clés offrent la possibilité d'utiliser des logiciels libres sous Windows comme[1] :

- OpenOffice 2.1 (version actuelle 2.3) ;
- Sumatra 0.7 ;
- Mozilla Sunbird 0.5 ;
- Firefox 2.0.0.6 (version actuelle 2.0.0.7) ;
- Thunderbird 2.0 version actuelle 2.0.0.6 ;
- Wengophone 2.1 ;
- Filezilla ;

[1] les versions des logiciels installés sur les clés sont celles signalées sur le site http://www.campusb.fr

– Miranda 0.4 (version actuelle 0.7);
– VLC Média Player 0.8 (version actuelle 0.8.6) ;
– Coolplayer ;
– Comice ;
– Juice 2.1 (version actuelle 2.2) ;
– 7zip ;
– Fullsync 0.9 (version actuelle 0.9.1) ;
– InfraRecorder 0.4 (version actuelle 0.43.1) ;
– ClamWin ;
– Truecrypt 4.3 ;
– Keepass 1.0.8 ;
– Locknote 1.0 (version actuelle 1.0.3).

Le CERTA attire donc l'attention sur la nécessité de mettre à jour les applications.

Ces objets peuvent être facilement perdus ou volés. Le CERTA rappelle qu'il existe des applications capables de copier l'intégralité de la mémoire de ces supports de stockage afin d'y retrouver des données, même si celles-ci ont été préalablement effacées (traces résiduelles possibles). Ces logiciels sont également capables d'insérer des codes malveillants sur le support, afin de les utiliser comme vecteur de propagation.

Il est donc nécessaire d'utiliser les outils de chiffrement des données disponibles et de minimiser les données personnelles présentes sur le support.

Les clés USB de ce projet ayant pour vocation à être utilisées sur plusieurs ordinateurs, il est important d'attacher une attention toute particulière à la non compromission de celles-ci et des systèmes sur lesquels elles sont montées.

Le CERTA tient à rappeler les précautions à prendre quant à l'utilisation de ces périphériques :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-040.pdf

4 Vulnérabilité dans le traitement des URI

Cette semaine le CERTA a diffusé l'alerte CERTA-2007-ALE-015. Celle-ci concerne une vulnérabilité de *Microsoft Windows* dans le traitement d'URIs, et ne fonctionne que sur les systèmes *Windows XP* et *Windows Server 2003* ayant *Internet Explorer 7*. Windows Vista n'est pas impacté. Comme pour certaines vulnérabilités récentes, la vulnérabilité est en réalité double et concerne à la fois les éditeurs d'applications et Microsoft.

En juillet 2007, l'alerte CERTA-2007-ALE-013 portait sur cette même vulnérabilité liée à *Mozilla Firefox*. Il était ainsi possible, via un lien ou même un `iframe` spécifiquement construit, d'exécuter des commandes arbitraires sur le poste de l'utilisateur. Mozilla a rapidement corrigé le problème de son côté, du moins en partie (cf. l'article « Traitement des URI par Mozilla Firefox » du bulletin CERTA-2007-ACT-036).

Plus précisément, la vulnérabilité concerne la fonction de Windows `ShellExecute()` appelée par diverses applications. Cette fonction traite la chaîne qui lui est passée en argument et en extrait soit un protocole soit une extension, pour lancer ensuite le programme associé spécifié dans la base de registres. Voici deux exemples pour illustration :

1° exemple : protocole
- la chaîne « http://www.certa.ssi.gouv.fr » est passée en argument par l'application ;
- la sous-chaîne « http:// » est reconnue comme protocole valide ;
- `ShellExecute` va donc visualiser la clé `HKEY_CLASSES_ROOT\http\shell\open` pour connaître le programme à lancer, par exemple, *Internet Explorer*.

2° exemple : extension de fichier
- la chaîne « index.htm » est passée en argument par l'application ;
- la sous-chaîne « .htm » est reconnue comme extension ;
- la clé `HKEY_CLASSES_ROOT\.htm` est alors visualisée, qui redirige vers `HKEY_CLASSES_ROOT\htmlfile\shell\open` pour connaître le programme à lancer.

L'installation de *Internet Explorer 7* change l'interaction entre le shell Windows et *Internet Explorer* lors du traitement d'URIs. Avec Internet Explorer 5 ou 6, une URI de type mailto:% lançe l'application de messagerie enregistrée dans la base de registre, alors que cette chaîne est mal formée. L'installation d'*Internet Explorer 7* change cela, en rejetant la chaîne avant le lancement du programme associé. Toutefois `ShellExecute` tenterait

ensuite, selon Microsoft, de réparer la chaîne, et lance ainsi une application en fonction de l'extension et non du protocole. Cela n'est cependant pas le cas sous *Windows Vista*.

En remarque,le RFC 2368 est dédié au format des URLs de type `mailto`. On peut y lire que les caractères réservés de type parenthèses, virgule ou signe de pourcentage `%` doivent être traduits (encodage). Ainsi, `%` ne peut apparaître dans une URL de type `mailto` que pour introduire un hexadécimal, ou doit sinon être converti en `%25`.

C'est ainsi que l'URL mailto:%../../../../windows/system32/calc.exe".bat cause le lancement du programme de courriel si *Internet Explorer 6* est installé, mais le programme `calc.exe` si *Internet Explorer 7* est installé. A cause de l'extension `.bat`, `ShellExecute` lance la valeur enregistrée dans `HKEY_CLASSES_ROOT\batfile\shell\open`, c'est à dire `"%1" %*`. La chaîne passée en argument après traitement est difficile à déterminer, mais le résultat final est le lancement de `calc.exe`. Des tests internes au CERTA ont de plus montré qu'il est trivial de passer des arguments au programme exécuté. Fondamentalement toutes les URI sont touchées puisque le facteur déclenchant n'est pas le protocole choisi mais l'extension. Cela dépend toutefois de l'application appelante qui peut elle-même limiter les types d'URI autorisées.

La vulnérabilité concerne donc la fonction `ShellExecute`. Néanmoins toute application convenablement conçue doit également vérifier les chaînes qu'elle passe en argument ; c'est de cette manière que Mozilla a corrigé la faille touchant *Firefox*.

Adobe a reconnu récemment que son logiciel *Adobe Reader* était touché par cette vulnérabilité pour les URI de type `mailto`, et a publié un contournement provisoire. Le 10 octobre 2007, Microsoft a également réagi en annonçant qu'un correctif était en cours de développement, ce qui devrait corriger le problème pour toute application appelant `ShellExecute` sans filtrage préalable.

Documentation

- Bulletin de sécurité Microsoft 943521 du 10 octobre 2007 :
  http://www.microsoft.com/technet/security/advisory/943521.mspx
- Bulletin de sécurité Adobe du 05 octobre 2007 :
  http://www.adobe.com/support/security/advisories/apsa07-04.html
- Description sommaire sur l'utilisation et le fonctionnement de ShellExecute :
  http://support.microsoft.com/kb/224816/
- Alerte CERTA-2007-ALE-015 du 10 octobre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-015/index.html
- « Traitement des URI par Mozilla Firefox », CERTA-2007-ACT-036 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-036.pdf
- RFC 2368, "The mailto URL scheme", juillet 1998 :
  http://tools.ietf.org/rfc/rfc2368.txt

5 Des injections de code indirectes : triche au compteur

5.1 Introduction

Le CERTA a mentionné dans son bulletin d'actualité CERTA-2007-ACT-040 les deux points suivants :

- il existe plusieurs formes d'injections de code dans une page de site Web, pour des finalités différentes, incluant les défigurations, ou modifications visuelles de la page ;
- une injection de code dans une page d'un site Web n'est pas nécessairement une défiguration.

Le CERTA revient donc sur ce dernier point, pour donner l'exemple d'injections de code originales, avec des finalités très particulières.

5.2 La mesure d'audience et la publicité

Plusieurs lignes de codes sont fréquemment ajoutées par les développeurs dans les pages Web, sans que celles-ci soient nécessaires au bon fonctionnement de la page. Les ajouts de la sorte, fréquents, peuvent être utilisés pour compter la fréquentation du site, ou pour activer des liens publicitaires.

5.2.1 Les compteurs de fréquentation

Un compteur se présente souvent sous la forme d'un *webbug*, i.e. d'une image non visible par l'internaute sur la page, qui envoie, à son chargement, des informations vers le site de statistique central, comme : le type de navigateur utilisé (`User-Agent`), la page Web visitée, la date, l'adresse IP du visiteur, etc.

D'autres méthodes existent aussi, comme le JavaScript, pour effectuer une telle opération. Il s'agit d'une forme d'espiogiciel (défini comme un outil de « collecte et transmission d'informations à l'insu de l'utilisateur », dans la terminologie CERTA-2006-INF-002).

L'exemple ci-dessous est tiré du code source de certaines pages Web, avec le service `audientia`. D'autres services comme `xiti`, `cybermonitor`, etc. ont une approche très semblable.

```
    <!-- Begin WEBandSTATS Tag ... -->
<!-- COPYRIGHT AUDIENTIA ALL RIGHTS RESERVED. -->
<_script language='javascript1.1' type="text/javascript"><!--
var SITE_ID          = "XXXXXX";
var PAGE_URL         = escape("http://MonSiteWeb");
var PAGE_NAME        = "MonSiteWeb";
(...)

var wasb = '?SITE_ID=XXXXXX&REFERRER='+escape(document.referrer)+
                '&LOCAL_DATE='+(new Date()).getHours();
wasb += '&JS_VERSION=10&PAGE_TITLE='+escape(document.title)+
                '&PAGE_NAME='+escape(PAGE_NAME);
wasb += '&PAGE_URL='+PAGE_URL+'&HANDLE_PARAM='+HANDLE_PARAM+
                '&GALLERY_NAME='+escape(GALLERY_NAME);
        '&PARAMETERS='+escape(PARAMETERS);
(...)

var wasImg = new Image();wasImg.src = wasa+wasb;};//-->
</_script>

<_noscript>
<_img src="http://apu03c0.audientia.net:80/scripts/stats.asp?SITE_ID=XXXXXX&
        PAGE_URL=&HANDLE_PARAM=NO&GALLERY_NAME=&GALLERY_PRODUCTID="
        alt="statistiques de fr&eacute; quentation (audientia)" />
</_noscript>
<!-- End WEBandSTATS Tag -->
```

5.2.2 Les revenus publicitaires

Suivant le même principe, les sites peuvent également servir de vitrine publicitaire. La rémunération se fait en fonction des clics que le site engendre. Plus un site redirige vers l'annonceur, plus sa « contribution publicitaire » est récompensée.

Des services permettent de compter les clics, et servent à des transactions financières. Ils fournissent également les codes à insérer dans les pages Web. Un exemple est le service *Google Adsense*. Le code inséré ressemble à :

```
<_script type="text/javascript"><!--
google_ad_client = "pub-XXXXXXXXXXXXXXXXXXXXX";
google_ad_width = 160;
google_ad_height = 600;
google_ad_format = "160x600_as";
google_ad_type = "text_image";
google_ad_channel = "";
google_color_border = "FFFFFF";
google_color_bg = "FFFFFF";
google_color_link = "0000FF";
google_color_text = "000000";
google_color_url = "191970";
//-->
</_script>
```

```
<_script type="text/javascript"
src="http://pagead2.googlesyndication.com/pagead/show_ads.js">
</_script>
```

5.3 L'injection de code malveillant, comme effet secondaire

Reprenons donc les deux échantillons de code cités ci-dessus. Si une personne peut modifier le code source de la page (hypothèse malheureusement confirmée lors du traitement de défigurations), voici des scénarii possibles d'injection de codes :

- la variable `SITE_ID` prend maintenant pour valeur YYYYYY ;
- l'adresse `apu03c0.audientia.net` est remplacée par `MonSiteMalveillant` ;
- la variable `google_ad_client` a pour nouvelle valeur "pub-YYYYYYYYYYYYYY"
- etc.

L'injection se limite donc à modifier très peu de champs de ces codes tiers dans les pages. Elle risque fort de passer inaperçue aux yeux de l'administrateur du site qui ne vérifie pas l'intégrité du code complet du site. Elle permet en revanche à une personne malveillante d'effectuer les actions suivantes :

- fausser les compteurs de fréquentation des sites ;
- collecter efficacement des informations sur les visiteurs du site à distance ;
- effectuer de la fraude pour les techniques de paiement au « clic » ;
- etc.

Il est également possible d'imaginer des actions plus furtives, qui modifient le code Javascript pour continuer à créditer occasionnellement le vrai site, afin de ne pas trop éveiller les soupçons d'un responsable de communication anxieux.

5.4 Les recommandations du CERTA

Ce type d'activité malveillante repose une nouvelle fois sur la possibilité d'injecter du code dans des pages Web. Elle met donc en évidence la nécessité du contrôle d'intégrité de celles-ci.

De manière générale :

- il est préférable de ne pas utiliser ces services. Les statistiques peuvent souvent être directement extraites de l'analyse des journaux du site. Ces journaux fournissent bien plus d'informations, et permettent de faire une première surveillance des activités du site.
- il est vivement recommandé de vérifier régulièrement l'intégrité des pages du site Web. Ce contrôle doit concerner le code source dans son intégralité.

6 Citrix Metaframe

La technologie de Citrix Metaframe permet à un utilisateur distant de se connecter à un bureau Microsoft Windows à distance. Ceci permet à des clients nomades d'obtenir un environnement de travail complet à partir d'une simple connexion à l'Internet. Cette connexion à un bureau se fait grâce à un programme nommé client `ICA` (`Independent Computing Architecture`).

Celui-ci utilise pour se connecter un fichier de configuration d'extension `.ica`. Ce fichier peut être détenu par l'utilisateur sur un support amovible. Souvent, il est mis à disposition sur un site web. Ce problème est que ce fichier de configuration comporte des informations sensibles sur la configuration à la fois du client et du serveur. Ce fichier ne doit donc pas être laissé en libre téléchargement sur un site web. Il doit, au minimum, faire l'objet de contrôles d'accès, d'autant plus que ce fichier de configuration est en texte clair et peut être modifié ou adapté après téléchargement.

Par ailleurs, le CERTA a eu connaissance d'une possible vulnérabilité dans la partie serveur Citrix. En effet, un utilisateur malintentionné, en modifiant de façon particulière un fichier de configuration `.ica`, pourrait contourner la phase d'authentification nécessaire à la connexion au bureau distant. Ce faisant, il obtient une session valide sans s'identifier. Il est donc impératif de bien restreindre l'accès à ce fichier de configuration aux seules personnes auxquelles il est destiné.

7 Safari pour Windows

Dans le bulletin d'actualité du 15 juin 2007 (CERTA-2007-ACT-024), il était fait mention de la version beta du navigateur Internet Safari pour Windows. L'article traitant de cette application signalait de nombreuses vulnérabilités découvertes très peu de temps après la mise à disposition de ce dernier sur l'Internet. Au cours du mois d'août 2007, de nouvelles vulnérabilités ont été corrigées par Apple :

- CVE-2408 : Cette vulnérabilité permet à un utilisateur distant malveillant d'exécuter des *applets* `Java` arbitraires, même si dans les paramètres du navigateur Safari l'option « Activer Java » est désactivée ;
- CVE-3742 : une vulnérabilité dans le traitement des noms internationaux de domaines (International Domain Names) permet à un utilisateur distant malintentionné d'usurper la véritable adresse réticulaire par une autre ;
- CVE-3743 : une vulnérabilité de type débordement de mémoire peut être exploitée par un individu malveillant afin de provoquer un déni de service ou d'exécuter du code arbitraire, en incitant l'utilisateur à rajouter un marque-page (*bookmark*) dont le nom est spécialement construit ;
- CVE-3944 : une vulnérabilité de type débordement de mémoire causée par une erreur dans le moteur Javascript du navigateur permet à un utilisateur malintentionné, au moyen d'une page web spécialement construite, de provoquer un déni de service ou d'exécuter du code arbitraire.

Ces vulnérabilités sont corrigées dans la version 3.0.3 du Navigateur Safari.

Malgré cette mise à jour, le navigateur Internet Safari pour Windows n'est pas encore une version finale, et par conséquent, il est recommandé de ne pas déployer cette application avant la publication d'une version stable.

Documentation

- Avis Apple ID 306174 du 30 juillet 2007 :
  http://docs.info.apple.com/article.html?artnum=306174-fr
- Bulletin d'actualité CERTA-2007-ACT-024 du 15 juin 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-024.pdf

8 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 04 et le 11 octobre 2007.

9 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/

10 Rappel des avis émis

Dans la période du 05 au 11 octobre 2007, le CERTA a émis l'alerte :

– CERTA-2007-ALE-015 : Vulnérabilité dans le traitement des URI sous Windows

Pendant cette même période, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-423 : Vulnérabilités d'OpenSSL
– CERTA-2007-AVI-424 : Multiples vulnérabilités dans XOrg
– CERTA-2007-AVI-425 : Multiples vulnérabilités dans libpng
– CERTA-2007-AVI-426 : Vulnérabilité dans AlsaPlayer
– CERTA-2007-AVI-427 : Multiples vulnérabilités d'Internet Explorer
– CERTA-2007-AVI-428 : Vulnérabilité de Windows RPC
– CERTA-2007-AVI-429 : Vulnérabilité dans Windows SharePoint Services 30 et Office SharePoint Server 2007
– CERTA-2007-AVI-430 : Vulnérabilité dans Microsoft Word
– CERTA-2007-AVI-431 : VUlnérabilité dans Microsoft Outlook Express et Windows Mail
– CERTA-2007-AVI-432 : Vulnérabilité dans l'afficheur d'images Kodak
– CERTA-2007-AVI-433 : Vulnérabilité dans Adobe PageMaker
– CERTA-2007-AVI-434 : Vulnérabilité sous HP-UX
– CERTA-2007-AVI-435 : Vulnérabilité dans HP System Management Homepage

11 Actions suggérées

11.1 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.

11.2 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 œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

11.3 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.

11.4 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.

11.5 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.

11.6 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.

11.7 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

12 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.

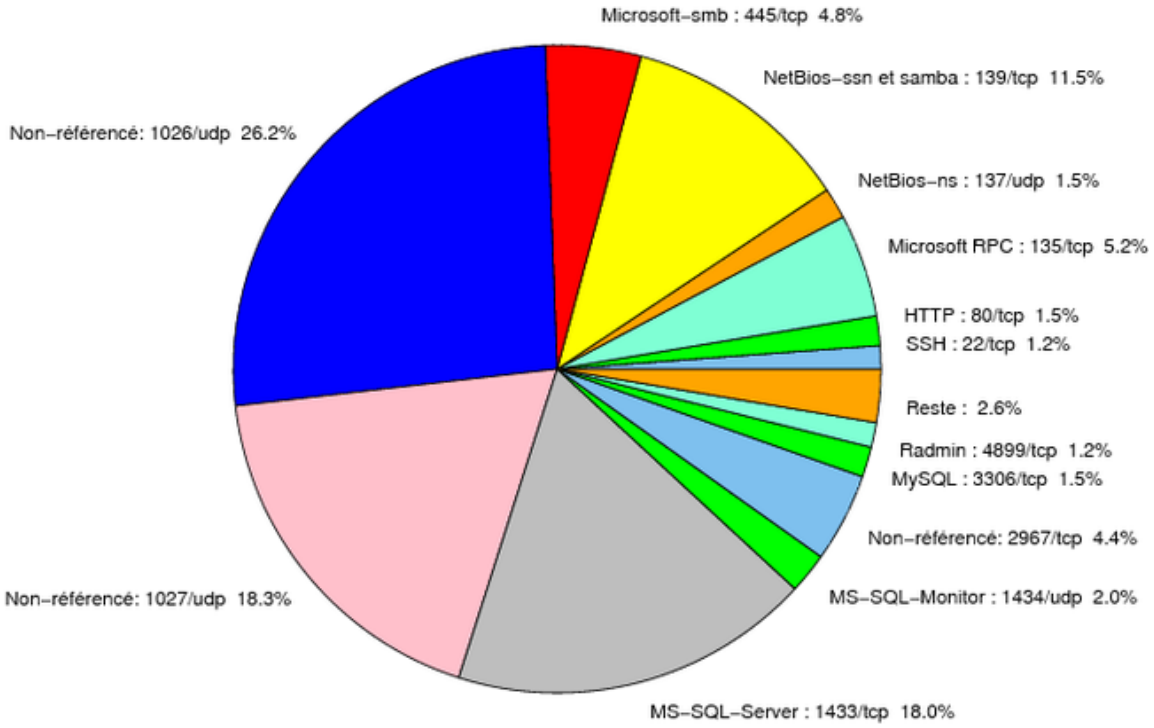

FIG. 1: Répartition relative des ports pour la semaine du 04.10.2007 au 11.10.2007

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/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CERT
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CERT
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CERT
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CERT
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CERT
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CERT

				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
1026/udp	26.23
1027/udp	18.26
1433/tcp	18.04
139/tcp	11.49
135/tcp	5.15
445/tcp	4.75
2967/tcp	4.44
1434/udp	2.03
137/udp	1.54
3306/tcp	1.51
80/tcp	1.47
4899/tcp	1.23
22/tcp	1.15
1080/tcp	0.7
25/tcp	0.57
3128/tcp	0.55
21/tcp	0.27
2100/tcp	0.14
23/tcp	0.07
15118/tcp	0.05
143/tcp	0.03
31511/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

12 octobre 2007 version initiale.