Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 octobre 2008
N° CERTA-2008-ACT-042

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-42

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-042`

Gestion du document

Référence	CERTA-2008-ACT-042
Titre	Bulletin d'actualité 2008-42
Date de la première version	17 octobre 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-042.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-042/

1 Vigilance SMB

Le protocole SMB (*Server Message Block*) permet d'échanger des ressources (fichiers, imprimantes, etc.) sur des réseaux locaux. Il fonctionne sous la forme « client / serveur » et est déployé dans la majorité des environnements Microsoft.

Selon les versions de Windows, il s'appuie sur différents protocoles (l'API NetBIOS sur TCP/IP ou directement via TCP).

Cette semaine, plusieurs publications ont mentionné des vulnérabilités associées à ce protocole. Certaines sont corrigées par des mises à jour de Microsoft mais ont été intégrées dans des outils d'exploitation automatiques.

Le CERTA recommande donc de porter une très grande vigilance au trafic SMB et de vérifier qu'une politique de filtrage rigoureuse est bien mise en place.

2 Incidents de la semaine

2.1 Détournement des outils de statistiques, 6 mois après ...

Il y a un peu plus de six mois, dans son bulletin d'actualité CERTA-2008-ACT-013, le CERTA avait présenté l'utilisation détournée des outils de statistiques afin de promouvoir des sites Internet à l'aspect douteux (sites pour adultes, etc.)

Le principe est simple : insérer une requête complète dans un champ d'un site que l'on sait journalisé (moteur de recherche, formulaire, *Referer*). Si les journaux sont présentés aux internautes sans être nettoyés, quelques essais suffisent alors à un utilisateur malintentionné pour injecter correctement les flux permettant de faire afficher des liens dans la visualisation des statistiques.

Cette semaine, le CERTA a traité un incident de cette sorte. La difficulté dans ce type d'incident réside dans le fait que l'administrateur du site offre les conditions nécessaires à ce genre d'activité. En effet, ce type d'incident est provoqué par un abus de fonctionnalité et non pas par une intrusion classique. Les remèdes sont donc plus complexes.

Pour éviter ce type de « compromission », le CERTA recommande :

- de n'afficher les résultats des outils de statistiques que dans une zone restreinte, non publique, et seulement si l'affichage de ces statistiques est strictement nécessaire ;
- d'interdire le référencement des pages de statistiques à l'aide d'un fichier *robots.txt* ;
- de configurer l'outil de statistiques afin de nettoyer les enregistrements et de n'afficher que ce qui est indispensable.

3 Fausse mise à jour Microsoft

3.1 Présentation

Depuis plusieurs jours, un courriel frauduleux circule avec un exécutable prétendant être une mise à jour de sécurité pour Windows. Ce courriel, dont le sujet est « Security Update for OS Microsoft Windows », est signé du nom de Steve Lipner, personnalité dans le domaine de la sécurité chez Microsoft. Le message arrive à point nommé puisque cette semaine Microsoft a publié 11 mises à jour de sécurité. Chose nouvelle, l'email se termine par une signature PGP pour tenter de paraître plus crédible. Cette signature est évidemment invalide.

L'exécutable est en fait une version du malware `Haxdoor`.

Pour information, la clé PGP utilisée par le MSRC pour ses signatures se trouve à l'adresse suivante :
http://www.microsoft.com/technet/security/bulletin/pgp.mspx

S'il arrive bien que Microsoft envoie des courriels de notification sur ses bulletins de sécurité aux personnes l'ayant demandé, l'éditeur assure toutefois qu'il n'enverra jamais de pièce jointe avec ceux-ci. D'une manière générale, aucun éditeur n'envoie de mise à jour ou d'application par courriel.

3.2 Documentation

- « Microsoft n'envoie jamais de mise à jour par email » - bloc-notes de Pascal Saulière :
  http://blogs.technet.com/pascals/archive/2008/10/10/microsoft-n-envoie-jamais-de-mise-jour-par-email.aspx
- « Microsoft Security E-mail Spoofs with Malware » - bloc-notes du MSRC :
  http://blogs.technet.com/msrc/archive/2008/10/13/microsoft-security-e-mail-spoofs-with-malware.aspx

4 Les vulnérabilités par dépendances

4.1 Présentation

L'avis de sécurité publié par `WinZip` a été repris cette semaine par plusieurs sites spécialisés.

Il s'avère en fait que ce n'est pas le programme en lui-même qui présente une faiblesse mais les bibliothèques fournies avec. En effet, la distribution contient le fichier Microsoft `gdiplus.dll`. La version précédemment distribuée avec l'outil d'archivage est vulnérable (CERTA-2008-AVI-449) et son exploitation permet une exécution de code arbitraire à distance.

L'inclusion de fichiers et de bibliothèques tierces par les éditeurs servent l'utilisateur et lui permettent de faciliter le processus d'installation. Cela pose néanmoins quelques problématiques de sécurité.

En effet, les mises à jour de ces composants tiers fournis en complément se font toujours avec un temps de retard par rapport à celles officielles. Elles nécessitent une nouvelle version du produit. Il faut également que le programme soit mis à jour par l'utilisateur. Cette opération n'est pas toujours automatique.

L'utilisateur n'a pas nécessairement conscience de disposer d'un logiciel vulnérable. Dans le cas présent, une mise à jour Microsoft effectuée en septembre ne suffit pas pour se protéger de l'exploitation d'une vulnérabilité `gdiplus.dll` via WinZip.

Le CERTA recommande d'éviter autant que possible ces systèmes de dépendances. Certaines installations offrent la possibilité de s'en abstenir. Il est également important de comprendre les intéractions des différents logiciels/systèmes entre eux.

4.2 Documentation

- Bulletin de sécurité CERTA CERTA-2008-AVI-449 du 10 septembre 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-449/
- Bulletin de sécurité Microsoft MS08-052 du 9 septembre 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-052.mspx
- Bulletin de sécurité WinZip 11.2 SR-1 du 25 septembre 2008 :
  http://www.winzip.com/wz112sr1.htm

5 Retour sur l'alerte CERTA-2008-ALE-012

5.1 Présentation

Le CERTA a publié, le 10 octobre 2008, l'alerte CERTA-2008-ALE-012 concernant une vulnérabilité dans Microsoft Windows. Cette vulnérabilité peut être exploitée par un utilisateur malveillant afin d'élever ses privilèges sur le système.

Cette vulnérabilité a fait l'objet d'une publication par Microsoft le 17 avril 2008. Elle n'était cependant pas documentée. La diffusion d'un code de faisabilité (*proof of concept*) pouvant exploiter cette faille a motivé une récente publication de Microsoft sur leur bloc-notes MSRC (Microsoft Security Response Center).

Cette vulnérabilité peut être exploitée en complément d'autres vulnérabilités afin de prendre le contrôle complet du système.

Le CERTA a traité de nombreux incidents pour lesquels les intrus ont associé l'exploitation de vulnérabilités distantes avec des vulnérabilités leur permettant d'élever leurs privilèges.

5.2 Documentation

- Bulletin de sécurité Microsoft 951306 du 17 avril 2008 :
  http://www.microsoft.com/technet/security/advisory/951306.mspx
- Bloc-notes de Microsoft Security Response Center du 09 octobre 2008 :
  http://blogs.technet.com/msrc/archive/2008/10/09/update-1-microsoft-security-advisory-951306.aspx

6 Retour sur les mises à jour Microsoft

Cette semaine, `Microsoft` a publié 11 nouveaux bulletins de sécurité dans le cadre de ses mises à jour mensuelles. Ces bulletins corrigent une vingtaine de vulnérabilités considérées comme importantes ou critiques. Le CERTA tient à revenir sur ces bulletins :

- MS08-56 : une vulnérabilité affecte la gestion du protocole *CDO* (*Collaboration Data Objects*) de `Microsoft Office`. Cette vulnérabilité permet à une personne malveillante via une adresse réticulaire *CDO* spécialement conçue de porter atteinte à la confidentialité des données ou d'entreprendre des actions que l'utilisateur pourrait effectuer sur un site Web affecté. Ce correctif ne concerne que `Microsoft Office XP Service Pack 3` ;
- MS08-57 : ce bulletin révèle la présence de trois vulnérabilités dans `Microsoft Excel`. Toutes permettent à une personne malveillante d'exécuter du code arbitraire à distance et affectent la plupart des versions de `Microsoft Excel` ainsi que les visionneuses. Elles sont dues à différentes erreurs liées au traitement du cache de performance *VBA* (*Visual Basic for Application*), à une allocation de mémoire incorrecte lors du chargement d'objets et au traitement de cellules Excel contenant une formule spécifique ;

– MS08-58 : cette mise à jour de sécurité corrige six vulnérabilités d'`Internet Explorer`, toute version. Quatre permettent à un attaquant d'accéder à une fenêtre de navigation dans un autre domaine ou une autre zone d'Internet Explorer. Elles ont pour origine :

  – une vulnérabilité inter-domaines liée à la propriété "emplacement" (*Window Location*) de la fenêtre de navigation ;
  – une vulnérabilité inter-domaines liée à l'élément HTML ;
  – une vulnérabilité inter-domaines liée à la gestion des événements ;
  – une vulnérabilité de divulgation d'informations inter-domaines.

  Les deux dernières concernent l'accès à la mémoire non initialisée ou dans des objets et permettent l'exécution de code arbitraire à distance.
– MS08-59 : ce bulletin fait état d'une vulnérabilité touchant le traitement des requêtes *RPC* (*Remote Procedure Call*) dans `Microsoft Host Integration server`. Ce correctif concerne plus précisément le service *SNA RPC*. L'application de ce correctif nécessite un rédemarrage de la machine. Une désactivation du service ou une diminution des droits de l'utilisateur démarrant ce service permet d'atténuer les impacts de l'exploitation. Ces mesures ne peuvent être que provisoires en attendant une nécessaire installation du correctif.
– MS08-60 : ce correctif traite d'une vulnérabilité affectant l'*Active Directory* de `Microsoft Windows 2000 Server Service Pack 4`. Cette vulnérabilité est due à une mauvaise allocation mémoire et peut être exploitée par une personne malveillante afin d'exécuter du code arbitraire à distance au moyen d'une requête *LDAP* ou *LDAPS* spécialement conçue.
– MS08-61 : trois vulnérabilités affectent le noyau `Microsoft Windows` et permettent une élévation de privilèges sur le système. L'exploitation de ces vulnérabilités est possible au travers d'un problème dans la validation de certaines propriétés de fenêtre transmises lors du processus de création de fenêtre, d'une possible double libération de mémoire et d'une validation incorrecte des entrées transmises au noyau depuis le mode utilisateur.
  La double libération de mémoire est provoquée lorsque le noyau n'effectue pas de capture du code présent dans la zone mémoire utilisateur afin d'exécuter ce dernier avec les privilèges du noyau. Cette pratique existe afin d'eviter de multiples accès au code présent dans l'espace utilisateur. Dans le cas présent, l'allocation mémoire est inadéquat et provoque un dépassement de mémoire avec des privilèges élévés.
– MS08-62 : il y est indiqué qu'une vulnérabilité affecte les systèmes `Microsoft Windows` lorsque ces derniers exécutent *IIS* et que le service d'impression Internet est activé. Des exploitations de cette vulnérabilité ont été constatées et touchent l'ensemble de la gamme des systèmes d'exploitation encore maintenus.
– MS08-63 : ce bulletin détaille une vulnérabilité dans la mise en œuvre protocolaire de `Server Message Block` (*SMB*) dans `Microsoft Windows`. Cette vulnérabilité permet une exécution de code arbitraire à distance via une trame spécialement construite émise par un utilisateur authentifié, y compris l'utilisateur « invité ».
– MS08-64 : une vulnérabilité a été identifiée dans le gestionnaire de mémoire Windows. Cette dernière affecte plus particulièrement la gestion des descripteurs d'adresses virtuelles (*VAD*). Cette vulnérabilité peut être exploitée par un utilsateur local afin d'élever ses privilèges au niveau *ring 0* et affecte toutes les versions de `Microsoft Windows`.
– MS08-65 : le correctif traite une erreur présente dans le service de mise en file d'attente de message dans `Microsoft Windows 2000 Service Pack 4` : *MSMQ* (*Message Queuing Service*). Cette vulnérabilité permet, lorsque le service est activé, d'exécuter du code arbitraire à distance mais la mise en œuvre d'une telle attaque n'est pas triviale et nécessite une modification de mémoire par un autre processus et une coordination, *a priori*, difficile à réaliser.
– MS08-66 : une vulnérabilité est présente dans le pilote de fonction connexe ou *Ancillary Function Driver* de `Microsoft`. Un manque de contrôle des données transmises du mode utilisateur au mode noyau permet à un utilisateur local d'exécuter du code arbitraire avec des privilèges très élevés sur le système.

Le CERTA rappelle l'importance de l'installation des mises à jour afin de limiter les risques d'intrusion dans le système d'information.

http://blogs.technet.com/swi/

7 Les redirections ouvertes

7.1 Présentation

Les utilisateurs sont parfois redirigés vers des adresses autres que celles initialement demandées. L'intérêt de cette approche est bien souvent d'orienter le visiteur vers un nouveau contenu (nouveau site, nouvelles pages) sans que ce dernier ne s'en rende compte.

Certaines redirections sont dites « ouvertes ». Le site Web ne vérifie pas les paramètres du lien avant de provoquer la redirection. Par exemple :

`http://MonSite.tld/redirect.php?dest=http://siteMalveillant.tld`

En d'autres termes, le script `redirect.php` permet de rediriger l'utilisateur vers une adresse quelconque de l'Internet.

Le site `siteMalveillant.tld` peut héberger des pages ayant un contenu agressif pour le navigateur et ses composants ou des pages de filoutage. Cela peut également être un moyen pour suivre une partie de la navigation de l'internaute.

Bien souvent, l'utilisateur ne voit ou ne prête attention qu'aux premiers caractères. Il risque donc de se laisser duper par une page imitant un contenu légitime. L'adresse peut également être encodée de plusieurs manières afin de rendre la lecture plus complexe. Certaines de ces techniques avaient été présentées dans l'article 4 du bulletin d'actualité CERTA-2007-ACT-004.

La redirection peut s'effectuer de différentes manières. La plus conventionnelle citée par le *World Wide Web Consortium* (W3C) est le `HTTP Redirect`. Cela correspond à un code de retour HTTP de la forme 3XX. Par exemple, le code 301 signifie "*moved permanently*" et peut être associé à une réponse comme :

```
HTTP/1.1  301   Moved Permanently
Location: http://NouveauSite.tld
Content-Type: text/html
Content-Length: ...

<HTML>
....
</HTML>
```

D'autres méthodes existent cependant. Il est par exemple possible d'exploiter la fonctionnalité de rafraîchissement d'une page avec l'attribut `content`. Ainsi la page peut présenter une ligne semblable à :

```
<meta http-equiv="refresh" content=2;url=http://NouveauSite.tld">
```

La valeur 2 représente le nombre de secondes avant que la redirection prenne effet. Sous certaines conditions, l'utilisation de la touche "Reculer d'une page" ne ramène pas à la page précédente.

D'autres méthodes consistent à profiter de l'interprétation de code dynamique JavaScript sur le navigateur de l'utilisateur. La destination de la redirection est alors fournie par le code JavaScript.

Il est possible de distinguer les redirections statiques, qui redirigent systématiquement vers les mêmes ressources, de celles dynamiques, dont la destination peut varier selon certains paramètres :

- de temps ;
- dépendant du poste client et des informations renseignées dans la requête (User-Agent, géolocalisation de l'adresse IP) ;
- le format de l'adresse de redirection sur lequel l'utilisateur clique.

Un article de recherche récent ayant effectué plusieurs tests montre que certaines redirections se comportent différemment en fonction des paramètres de la requête. Plus précisément, faire abstraction de certains champs amènent le serveur à être beaucoup moins regardant au niveau de la redirection !

De manière générale, laisser une redirection ouverte permet aux personnes de relayer des adresses malveillantes via le site et elle indique une mauvaise maîtrise des actions mises en place. Il appartient au responsable du site Internet de contrôler celles-ci.

7.2 Recommandations

- Pour les administrateurs de sites :
  - regarder avec attention dans les journaux du serveur les tentatives de connexion contenant des chaînes particulières comme `http:` ou `https` ;
  - filtrer au niveau du serveur les champs `referer` pour vérifier une redirection. Cette méthode peut cependant poser problème lorsque le champ n'est pas utilisé ou nettoyé par une passerelle ;
  - utiliser un condensat (*hash*) caractérisant le site destinataire ainsi qu'un secret du serveur. Ce condensat est inclu dans l'adresse de redirection et il est vérifié par le serveur d'arrivée.
- pour les utilisateurs :
  - être sensibilisés ;
  - filtrer les en-têtes HTTP conduisant à des redirections (voire effectuer un test préalable) ;
  - ne pas cliquer sur des liens suspects.

7.3 Documentation associée

- Bulletin d'actualité CERTA-2007-ACT-004, « Filtrage et syntaxe d'URL », janvier 2007 : http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-004.pdf
- MITRE, "CWE-601: URL Redirection to Untrusted Site (aka 'Open Redirect')", octobre 2008 : http://cwe.mitre.org/data/definitions/601.html
- C.A. Shue, A.J. Kalafut, M. Gupta, "Exploitable Redirects on the Web: Identification, Prevalence, and Defense", Woot08, juillet 2008 : http://www.cs;indiana.edu/cgi-pub/cshue/research/woot08.pdf

8 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 09 et le 16 octobre 2008.

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 10 au 17 octobre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-488 : Multiples vulnérabilités dans Drupal
- CERTA-2008-AVI-489 : Multiples vulnérabilités dans Cisco Unity
- CERTA-2008-AVI-490 : Vulnérabilité dans Adobe Flash Player
- CERTA-2008-AVI-491 : Multiples vulnérabilités dans CA ARCserve Backup
- CERTA-2008-AVI-492 : Multiples vulnérabilités dans Mac OS X
- CERTA-2008-AVI-493 : Multiples vulnérabilités dans CUPS
- CERTA-2008-AVI-494 : Vulnérabilité dans Sun Java System Web Proxy Server
- CERTA-2008-AVI-495 : Vulnérabilité dans HP System Management Homepage
- CERTA-2008-AVI-496 : Multiples vulnérabilités dans Avaya Communication Manager
- CERTA-2008-AVI-497 : Vulnérabilité dans Microsoft Office
- CERTA-2008-AVI-498 : Multiples vulnérabiliés dans Microsoft Excel
- CERTA-2008-AVI-499 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2008-AVI-500 : Vulnérabilité dans Microsoft Host Integration Server
- CERTA-2008-AVI-501 : Vulnérabilité dans Active Directory
- CERTA-2008-AVI-502 : Multiples vulnérabilités dans le noyau Microsoft Windows
- CERTA-2008-AVI-503 : Vulnérabilité dans le service d'impression Internet de Microsoft Windows
- CERTA-2008-AVI-504 : Vulnérabilité SMB dans Microsoft Windows
- CERTA-2008-AVI-505 : Vulnérabilité dans la gestion mémoire Windows
- CERTA-2008-AVI-506 : Vulnérabilité du Message Queuing de Microsoft Windows
- CERTA-2008-AVI-507 : Vulnérabilité dans le pilote de fonction connexe de Microsoft
- CERTA-2008-AVI-508 : Vulnérabilités dans les produits Oracle et WebLogic
- CERTA-2008-AVI-509 : Vulnérabilité dans VLC media player
- CERTA-2008-AVI-510 : Vulnérabilité dans HP-UX
- CERTA-2008-AVI-511 : Vulnérabilité du serveur Apache Tomcat
- CERTA-2008-AVI-512 : Multiples vulnérabilités dans Adobe Flash Player

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

- CERTA-2007-AVI-520-001 : Vulnérabilité de Squid
  (Modification des versions affectées, ajout des CVE et des correctifs des distributions Linux)
- CERTA-2008-AVI-413-001 : Vulnérabilité dans le contrôle ActiveX Snapshot Viewer d'Access
  (mise à jour du bulletin de Microsoft)
- CERTA-2008-AVI-465-001 : Vulnérabilité dans libxml2
  (ajout de la référence au bulletin Debian)
- CERTA-2008-AVI-466-001 : Vulnérabilité de OpenSSH pour Debian
  (ajout des bulletins de sécurité Ubuntu et SuSE)
- CERTA-2008-AVI-473-001 : Multiples vulnérabilités des produits Mozilla
  (Ajout des références aux bulletins de sécurité Debian, openSUSE et RedHat)
- CERTA-2008-AVI-493-001 : Multiples vulnérabilités dans CUPS
  (ajout des bulletins Ubuntu, Redhat et Fedora)

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'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 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 oeuvre (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 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.

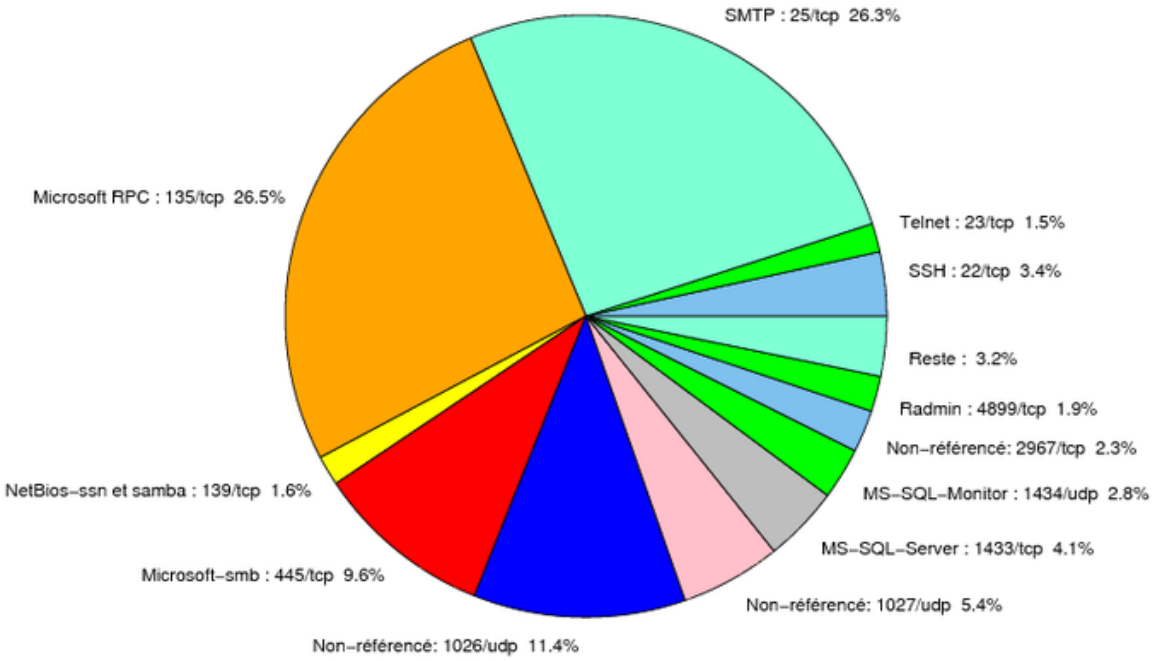

FIG. 1: Répartition relative des ports pour la semaine du 09.10.2008 au 16.09.2008

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
135/tcp	26.51
25/tcp	26.29
1026/udp	11.39
445/tcp	9.56
1027/udp	5.4
1433/tcp	4.09
22/tcp	3.43
1434/udp	2.77
2967/tcp	2.26
4899/tcp	1.89
139/tcp	1.6
137/udp	0.87
21/tcp	0.73
80/tcp	0.65
3306/tcp	0.36
3127/tcp	0.21
3389/tcp	0.14
3128/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

17 octobre 2008 version initiale.