

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-49

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-049>

Gestion du document

| | |
|-----------------------------|------------------------------|
| Référence | CERTA-2008-ACT-049 |
| Titre | Bulletin d'actualité 2008-49 |
| Date de la première version | 05 décembre 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-049.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-049/>

1 Incidents traités cette semaine

1.1 Présentation des faits

Cette semaine, le CERTA a été informé d'un cas de filoutage ciblant les clients d'une banque française. Le site Internet frauduleux reproduisant celui de la banque était hébergé à l'étranger. Le site frauduleux a été fermé dans les meilleurs délais.

Le site malveillant avait été déposé à la suite d'une compromission d'un site Internet légitime. De plus, ce dernier utilisant un certificat HTTPS, les pages frauduleuses ont donc également « bénéficié » de ce chiffrement. Or le CERTA entend trop souvent la fausse information « *si le site utilise HTTPS, il est légitime* ». En réalité, un tel certificat est associé au domaine (ou *FQDN*) ou à l'adresse IP pour lesquels il a été émis (cf. documentation).

Le CERTA rappelle qu'une des précautions pour ne pas se retrouver sur un site frauduleux est de ne pas cliquer sur un lien présent dans un courrier électronique. Il est préférable, pour se rendre sur un site Internet, de recopier soi-même à la main l'adresse dans le navigateur. Cette précaution et bien d'autres liées à la messagerie sont décrites dans la note d'information CERTA-2000-INF-002.

1.2 Documentation

- Note d'information du CERTA sur les mesures de prévention relatives à la messagerie :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/>
- RFC 2817, "Upgrading to TLS Within HTTP/1.1", mai 2000 :
<http://www.ietf.org/rfc/rfc2817.txt>
- RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", janvier 1999 :
<http://www.ietf.org/rfc/rfc2459.txt>
- RFC 4366, "Transport Layer Security (TLS) Extensions", avril 2006 :
<http://www.ietf.org/rfc/rfc4366.txt>
- S. Bortzmeyer, "Authentifier des serveurs Internet avec X.509 lorsqu'ils ont la même adresse IP", 04 décembre 2008 :
<http://www.bortzmeyer.org/auth-x509-plusieurs-noms.html>

2 De l'intérêt de déployer des solutions de sécurité

2.1 Incidents signalés cette semaine

La société SonicWALL a signalé cette semaine sur son site un problème concernant leurs serveurs en charge de la gestion des licences (*Sonicwall License Manager Server*). Les produits de la société qui ont cherché à établir une connexion vers le serveur de gestion de licences distant ont reçu des réponses erronées provoquant la réinitialisation de leur clé de licence.

Les conséquences de ce dysfonctionnement ne sont pas toutes connues. Certaines passerelles de filtrage de messagerie n'ont plus accompli leur rôle et ont transféré sans contrôle tout trafic de l'Internet vers les serveurs de messagerie. Le même comportement a été signalé pour des équipements de type pare-feu qui ont transféré sans contrôle les trames en transit. Les protections sont ainsi désactivées (anti-spam, antivirus, filtrage liste noire, etc.). Les utilisateurs, eux, ne se rendent pas forcément compte rapidement de ce problème.

2.2 Remarques générales

Cet article n'a évidemment pas pour objectif de jeter la pierre sur des produits en particulier. Cet incident reste envisageable avec d'autres solutions de sécurité et d'autres constructeurs.

Il offre l'occasion de rappeler deux principes fondamentaux à bien vérifier avant de déployer toute solution de sécurité :

- il faut connaître le comportement de l'équipement et sa manière de réagir dans un contexte anormal, y compris en cas de panne : un élément d'analyse de trafic en panne doit-il par défaut tout laisser transiter, ou au contraire, bloquer toute activité afin de protéger le réseau ? En d'autres termes, est-ce que la politique de sécurité prend en compte le dysfonctionnement d'un équipement de sécurité ? Le comportement en cas de défaillance dépend du contexte mais il doit être choisi en connaissance de cause ;
- il ne faut pas pas utiliser d'équipements de sécurité dépendant opérationnellement d'un élément tiers non maîtrisable. De manière plus précise, il faut déterminer si les dépendances fonctionnelles de l'équipement de sécurité nuisent ou limitent la sécurité. C'est par exemple le cas de plusieurs éléments mettant en œuvre des mécanismes de "phone home". La communication dépend de nombreux facteurs externes, comme la disponibilité du serveur distant ou du chemin pour la communication.

2.3 Documentation associée

- Bulletin de sécurité SonicWALL, "SonicWALL License Server Outage", 02 décembre 2008 :
<http://www.sonicwall.com/us/11087.html>
- ISC SANS, "Sonicwall License Manager Failure", 02 décembre 2008 :
<http://isc.sans.org/diary.html?storyid=5419>
- C. Blancher, "Le logiciel libre pour la SSI - principe d'indépendance", JIA 2005, février 2005 :
http://sid.rstack.org/pres/0502_JIA_Libre_Secu.pdf

3 Apache : des lignes étonnantes dans les journaux

Cette semaine, le CERTA a cherché à détailler l'explication de certaines lignes présentes dans les journaux de serveurs Apache. Ces lignes se retrouvent sous la forme d'une requête GET pour une *URI* absolue (*http://un_url.tld*) qui n'a rien à voir avec le serveur interrogé, et qui obtient pourtant en réponse un code 200 (OK). Par exemple :

```
"GET http://nimportequoi.tld" 200 13 "-" "-"
```

La page servie est en fait l'index par défaut (au niveau des journaux cela peut se vérifier car, quelque soit l'*URI*, la taille ne varie pas et correspond à celle de la page d'index).

Les requêtes d'*URI* absolues sont normalement faites à destination de serveurs mandataires. On peut obtenir des traces similaires en configurant un navigateur avec un serveur mandataire pointant sur un serveur WWW (port 80). Toutes les requêtes arriveront alors sous la forme absolue. Cependant on peut se demander pourquoi Apache, n'étant pas configuré en serveur mandataire, répond avec un code 200. La lecture du code source montre en fait que :

- ce qui se trouve avant `"/"` n'est pas utilisé ;
- ce qui se trouve entre `"/"` et le premier `"/` sert à initialiser une variable `host` (*hostinfo*) ;
- ce qui se trouve ensuite est le chemin d'accès à la ressource.

Donc dans :

```
http://nimportequoi.tld/repertoire/fichier.html
```

- `http:` est tronqué ;
- `//nimportequoi.tld/` initialise la variable `host` à *nimportequoi.tld* ;
- `/repertoire/fichier.html` pointe le fichier demandé.

La variable `host` n'est utilisée qu'avec les requêtes du type CONNECT ou lorsqu'il y a plusieurs *vhost*, sinon elle est ignorée. Donc pour une *URI* de la forme *http://nimportequoi.tld/*, le serveur ne traite que le `"/` final, soit la racine du site et, selon sa configuration, retourne normalement la page par défaut avec un code 200.

Ces lignes sont donc le résultat d'un fonctionnement normal. Cependant, si elles s'avèrent gênantes, par exemple en levant des alertes sur un système de détection d'intrusion, il est possible de contourner le problème en utilisant, entre autres, le module `apache mod_rewrite` pour renvoyer un code 403 (*interdit*) pour les requêtes d'*URI* absolues. Il faut néanmoins garder à l'esprit que ce module peut également souffrir de vulnérabilités.

La RFC HTTP 1.1 définissant les *URI* absolues et précisant la nécessité de traiter (section 5.1.2) est accessible à l'adresse suivante :

```
http://www.ietf.org/rfc/rfc2616.txt
```

4 Fonctionnement de tcpdump

L'outil de capture de trames `tcpdump` offre la possibilité de définir des filtres de capture. Il utilise pour cela la syntaxe des filtres BPF (*BSD Packet Filter*). Cette dernière permet de définir certains critères de filtrage sur le type d'élément à filtrer (machine hôte, réseau, port, etc.), la direction des échanges (source vs. destination) ou le protocole recherché (tcp, ip, arp, etc.).

```
$tcpdump [OPTIONS] ip and not net 192.168
```

Cet exemple permet de récupérer toutes les trames IPv4 qui ne concernent pas les adresses du réseau 192.168.X.X.

Les règles de filtrage demandées sont fournies à l'application de filtrage, qui doit alors construire une décision à partir de celles-ci.

A valeur d'exemple, un article publié récemment sur un bloc-notes fait justement remarquer que le filtre `"ip or vlan"` n'est pas équivalent à `vlan or ip`. L'utilisateur voulait capturer les trames, quelles aient un tag VLAN (IEEE 802.1Q) ou non.

`Tcpdump` cherche les deux informations "ip" ou "vlan". Or, en fonction du type de trames, l'information sur le type de protocole dans l'en-tête Ethernet se trouve à l'octet 12 ou l'octet 16 (décalée par la présence du champ "tag" inséré). `tcpdump` cherche dans le second cas ("vlan or ip") s'il trouve un tag à l'octet 12. Si ce n'est pas le cas, il cherche l'information IP à l'octet 16 et non 12. Cela n'est donc jamais le cas si des trames n'utilisent pas IEEE 802.1Q.

Les options `-d`, `-dd` ou `-ddd` de `tcpdump` permettent de mieux comprendre quelles sections du paquet ont correctement validé la requête de filtrage. Elles retournent les différentes instructions appliquées (récupération de valeurs dans la trame et comparaison faite).

Cette option est donc un bon moyen pour vérifier et corriger les erreurs de filtrage.

Cette nouvelle rappelle également qu'un outil de filtrage n'a de valeur que si son fonctionnement est bien compris. Dans les autres cas, cela peut conduire à de mauvaises interprétations ou à des filtres effectifs qui ne correspondent pas à ceux désirés. Il est donc impératif de tester et vérifier par la pratique que les règles appliquées correspondent aux règles attendues.

- S. McCanne, V. Jacobson, "The BSD Packet Filter: A New Architecture for User-Level Packet Capture", décembre 1992 :
<http://www.tcpdump.org/papers/bpf-usenix93.pdf>
- R. Bejtlich, "BPF for IP or VLAN Traffic", 04 décembre 2008 :
<http://taosecurity.blogspot.com/2008/12/bpf-for-ip-or-vlan-traffic.html>
- R. Bejtlich, "Understanding Tcpdump's -d Option, Part 2", 21 décembre 2004 :
<http://taosecurity.blogspot.com/2004/12/understanding-tcpdumps-d-option-part-2.html>
- A. Begel, S. McCanne, S.L. Graham, "BPF+: Exploiting Global Data-Flow Optimization in a Generalized Packet Filter Architecture", SigComm 1999 :
<http://research.microsoft.com/abegel/sigcomm99/bpf+.ps>
- V. Paxson, "Measurements and Analysis of End-to-End Internet Dynamics", avril 1997 :
<ftp://ftp.ee.lbl.gov/papers/vp-thesis/dis.ps.gz>

5 Bulletins Microsoft du mois de décembre

Microsoft a annoncé cette semaine la publication de huit nouvelles mises à jour de sécurité le mardi 9 décembre.

Six vulnérabilités sont considérées comme « critiques » par l'éditeur. Celles-ci concernent Windows, Internet Explorer, Visual Basic, Word et Excel. Les failles permettraient l'exécution de code arbitraire à distance.

Deux vulnérabilités touchant Sharepoint et des composants Windows Media sont considérées comme « importantes » par l'éditeur. La première permettrait une élévation de privilèges et la deuxième une exécution de code arbitraire à distance.

Toutes les versions de Windows, Office et Internet Explorer encore officiellement supportées par l'éditeur semblent concernées par ces mises à jour.

Le CERTA recommande l'application de ces correctifs dès que possible.

5.1 Documentation

- Microsoft Security Bulletin Advance Notification for December 2008
<http://www.microsoft.com/technet/security/bulletin/ms08-dec.msp>

6 Compromission via DHCP

6.1 Rappel sur le protocole

Le protocole *DHCP* (*Dynamic Host Configuration Protocol*) permet de fournir les paramètres de configuration réseau à un ensemble de machines d'un même réseau. Ce système est défini dans la RFC 2131 et fonctionne sur le protocole de transport *UDP*, qui ne fournit donc aucune authentification ni contrôle des données envoyées.

De nombreuses options peuvent être intégrées à une requête *DHCP*, comme *vendor class identifier*, *sname* ou *file* qui permettent de récupérer des informations sur le serveur ou l'infrastructure réseau.

De plus, une interception ou une modification des trames du serveur *DHCP* peut affecter l'ensemble du parc informatique sans que celui-ci ne soit infecté ni même vulnérable à une attaque.

Un exemple parmi beaucoup d'autres peut être l'usurpation d'identité d'un serveur d'annuaire eDirectory dans un réseau Novell Netware.

6.2 Les risques

Il peut donc être intéressant pour une personne malveillante de compromettre le processus d'envoi des configurations réseau via un serveur *DHCP*. Par exemple, le code malveillant *DNSChanger*, dont nous parlions déjà dans le bulletin d'actualité CERTA-2008-ACT-047, injecte des paquets d'offres *DHCP* sur le réseau avec une option *DNS* falsifiée comme le montre l'exemple ci-dessous :

```
Option : (t=6, l=8) Domain Name Server
  option : (6) Domain Name Server
  Length : 8
  value : 55FF702455FF7024
  IP Address : xxx.xxx.xxx.xxx
  IP Address : YYY.YYY.YYY.YYY
```

Cette pollution a pour effet de rediriger le trafic *DNS* de l'ensemble des machines obtenant leur configuration *DHCP* vers des serveurs illégitimes. Ce type d'attaque permet d'intercepter tout ou partie des requêtes envoyées sur l'Internet. Cela peut être intéressant pour attaquer les utilisateurs de sites commerciaux ou d'organismes bancaires afin d'effectuer des attaques par filoutage en toute discrétion.

6.3 Les recommandations

Afin de limiter les risques liés à une telle modification des paramètres envoyés par un serveur *DHCP*, il est possible :

- de surveiller/filtrer le trafic *DNS* afin de s'assurer que celui-ci s'effectue vers des serveurs légitimes ;
- de contrôler la cohérence des configurations réseau des clients ;
- d'opter pour des systèmes de mise à disposition de configuration réseau plus sûrs nécessitant par exemple une authentification.

6.4 Documentation

- RFC 2131 :
<http://www.ietf.org/rfc/rfc2131.txt>
- Bulletin d'actualité CERTA-2008-ACT-047 du 21 novembre 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-047.pdf>

7 Serveur Web sur téléphone mobile

7.1 Présentation

Un grand constructeur de téléphones mobiles propose depuis peu une solution originale pour transformer certains modèles de téléphones en véritable serveur web. Il suffit d'y installer une application puis d'enregistrer un nom de domaine particulier sur le site du constructeur pour accéder à distance à une interface web complète permettant de réaliser de nombreuses tâches. En fait, l'application installée est un serveur HTTP dérivé d'Apache auquel a été ajouté le support du langage Python (`mod_python`). D'après les développeurs du projet, il est possible, à partir des données personnelles présentes sur le téléphone et par l'intermédiaire du serveur, de publier un site Internet. Outre cette fonctionnalité d'hébergement, il est aussi possible, via une interface d'administration présente sur le serveur, d'exécuter un certain nombre de tâches d'administration sur le téléphone :

- envoi de SMS ;
- prise de photos (si l'appareil en est capable) ;
- gestion et partage de contacts.
- etc.

L'accès à l'interface se fait via le portail du constructeur qui garantit la sécurité du lien entre son portail et le téléphone lors des opérations d'administration. Le serveur web sur le téléphone est, quant à lui, accessible depuis l'Internet de façon très classique.

Cette « fonctionnalité » mise en avant par le constructeur comme une petite révolution n'est pas sans poser certains problèmes de sécurité.

En effet, à partir du moment où le téléphone est utilisé comme serveur web, il devient sujet aux mêmes menaces que tout autre équipement assurant les mêmes fonctions.

On pourra donc, par exemple, imaginer réaliser sur eux des dénis de service assez facilement puisque ils disposent, tout de même, de ressources système bien en deçà de n'importe quel ordinateur PC récent.

De la même façon, le téléphone devra disposer d'une politique de mise à jour rigoureuse pour son serveur HTTP mais également pour le contenu Web (blog, page personnelle, ...) sous peine de subir des attaques (défiguration, hébergement de contenu illicite) à l'insu du propriétaire, voire de participer à des attaques de type *DDoS* (Déni de service distribué).

7.2 Recommandations

La sécurité actuelle de tels services est aujourd'hui inconnue sinon faible. Il faut donc s'assurer de ne pas les interconnecter à des réseaux informatiques et à ne pas augmenter les risques de compromission (de ces derniers ou de leur environnement de synchronisation) en leur installant des services qui les exposent davantage.

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 27 novembre et le 04 décembre 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 28 novembre au 04 décembre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-570 : Multiples vulnérabilités dans IBM AIX
- CERTA-2008-AVI-571 : Vulnérabilité dans VLC media player
- CERTA-2008-AVI-572 : Vulnérabilité de Samba

- CERTA-2008-AVI-573 : Vulnérabilité de RSA enVision
- CERTA-2008-AVI-574 : Vulnérabilité dans ClamAV
- CERTA-2008-AVI-575 : Vulnérabilité dans imlib2
- CERTA-2008-AVI-576 : Vulnérabilité dans CUPS
- CERTA-2008-AVI-577 : Vulnérabilité des produits VMware ESX et ESXi
- CERTA-2008-AVI-578 : Vulnérabilités de la machine virtuelle Java
- CERTA-2008-AVI-579 : Vulnérabilité dans SquirrelMail

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 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.

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 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.

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.ssi.gouv.fr/fr/formation/>

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.

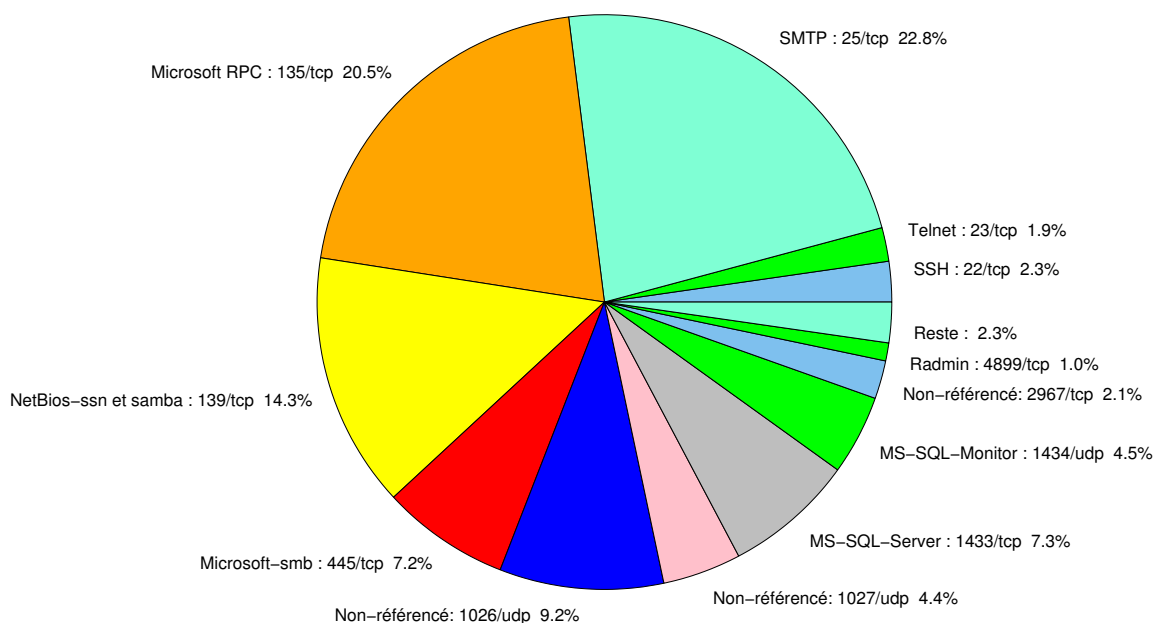


FIG. 1: Répartition relative des ports pour la semaine du 27.11.2008 au 04.12.2008

| 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 |
|----------|-------------|
| 25/tcp | 22.81 |
| 135/tcp | 20.54 |
| 139/tcp | 14.34 |
| 1026/udp | 9.22 |
| 1433/tcp | 7.33 |
| 445/tcp | 7.2 |
| 1434/udp | 4.48 |
| 1027/udp | 4.42 |
| 22/tcp | 2.27 |
| 2967/tcp | 2.14 |
| 23/tcp | 1.89 |
| 4899/tcp | 1.01 |
| 80/tcp | 0.63 |
| 137/udp | 0.5 |
| 3389/tcp | 0.25 |
| 3306/tcp | 0.12 |
| 111/tcp | 0.06 |

TAB. 3: Paquets rejetés

Liste des tableaux

| | | |
|---|--|----|
| 1 | Gestion du document | 1 |
| 2 | Correctifs correspondant aux ports destination des paquets rejetés | 10 |
| 3 | Paquets rejetés | 11 |

Gestion détaillée du document

05 décembre 2008 version initiale.