Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 octobre 2008
N° CERTA-2008-ACT-040

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-40

Gestion du document

Référence	CERTA-2008-ACT-040
Titre	Bulletin d'actualité 2008-40
Date de la première version	03 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-040.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-040/

1 Incidents traités cette semaine

1.1 Défiguration invisible

Cette semaine, le CERTA a traité un cas de défiguration « invisible ». L'apparence de la page compromise n'avait subi aucune modification, cependant du code avait bel et bien été inséré dans le code source de la page HTML.

L'insertion de code se présentait sous la forme de liens hypertexte intégrés dans un paragraphe. La balise associée au paragraphe avait un attribut désactivant son affichage. L'interêt d'une telle défiguration est à rechercher du côté de l'indexation par les moteurs de recherche. En effet, le fait d'ajouter une multitude de liens vers un même site permet d'améliorer la position de ce dernier dans les résultats des moteurs de recherche.

Cet incident montre l'interêt pour un administrateur de vérifier régulièrement les journaux d'événements de son serveur web mais également de contrôler l'intégrité des fichiers présents sur le serveur afin de détecter rapidement toute compromission. Cette compromission était en effet invisible à l'oeil nu et seul un contrôle des journaux ou de l'intégrité de la page permettait une détection efficace de cette intrusion.

1.2 Application des correctifs et contrôles

Début août, le CERTA avait prévenu l'administrateur d'un site Web de la présence d'une page illicite sur son site. L'administateur en congés a rapidement supprimé la page indésirable et a mis à jour à son retour certaines applications dont le gestionnaire de contenu Joomla!. Cette semaine, le CERTA a recontacté cette personne pour l'informer de la présence d'une autre page défigurant son site. Le problème est que cette page était déja présente sur le site lors du premier avertissement. Une analyse un peu plus poussée a permis de découvrir d'autres pages illicites, des `shell scripts` et des utilisateurs aux droits élevés illégitimement inscrits dans Joomla!. La faille de sécurité exploitée concerne la page de changement de mots de passe de la version 1.5.6 de Joomla! et a fait l'objet de l'avis CERTA-2008-AVI-214 et d'un article du bulletin d'actualité CERTA-2008-ACT-033.

Lorsqu'un système est compromis, il doit être entièrement vérifié. En effet, lorsqu'un attaquant réussit à s'introduire dans un système, sa première action est souvent de pérenniser son contrôle sur la machine en installant d'autres portes dérobées.

Le CERTA recommande la mise en place d'une vérification régulière de l'intégrité des systèmes. Cela permet de détecter d'éventuelles modifications non désirées, mais aussi en cas de compromission d'avoir une methodologie et une empreinte du système dans un état sain, ce qui permet de retrouver rapidement ce qui a été changé. Il existe des outils dédiés à ce type d'opérations, la difficulté étant de définir les limites de la surveillance. Il est important de sauvegarder sur un support séparé les résultats des prises d'empreintes, afin qu'elles ne soient pas compromises et restent utilisables.

1.3 Le site précédent oublié

1.3.1 Description

Cette semaine le CERTA a informé le propriétaire d'un site d'un contenu frauduleux présent sur ce dernier. Le site hébergeait des pages de filoutage (ou *phishing*). Une fois prévenu, le responsable du site a pris la décision de supprimer les pages frauduleuses et n'a pas cherché à en comprendre l'origine. Un tel comportement est rarement sans conséquence, en effet deux jours plus tard de nouvelles pages frauduleuses sont apparues. Cette fois l'administrateur a pris la décision de fermer définitivement le site, celui-ci étant une ancienne version non-utilisée d'un site qu'il administre sur un autre serveur.

Cet incident soulève plusieurs problèmes :

- un site laissé à l'abandon, n'étant pas mis à jour , devient facilement la proie d'individus malveillants ;
- en ne cherchant pas à comprendre l'origine de la compromission, l'administrateur expose son nouveau site restauré à une attaque identique à la première ;
- se contenter de supprimer des pages frauduleuses n'apporte pas une solution pérenne à un incident de sécurité. Il faut trouver le chemin d'attaque et colmater la brèche.

Le CERTA rappelle que lors d'une compromission il est impératif d'en comprendre la cause et de ne pas se limiter à traiter les conséquences. De plus lorsqu'un site Internet n'est plus utile, il est plus prudent de le fermer afin de ne pas permettre à des tiers de profiter de ses ressources.

1.3.2 documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information : http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

1.4 Nom de domaine et machine compromise

1.4.1 Présentation

Le CERTA a rencontré, cette semaine, le cas d'une machine compromise semblant appartenir à une administration. Celle-ci hébergeait un gestionnaire de contenu (`CMS`) dont la version non mise-à-jour comportait sans doute une vulnérabilité. Par ailleurs, le `CMS` n'était pas configuré et laissait voir son type et l'accès à son interface d'aministration.

Après analyse, le CERTA a pu mettre en évidence que l'enregistrement `DNS` pointant vers cette machine, n'avait plus lieu d'être depuis plusieurs mois. En effet, l'adresse `IP` associée à la machine a été réatribuée à une autre entité ne faisant pas partie de l'administration. Pourtant l'enregistrement `DNS` et l'autorité pour la zone est toujours l'administration.

Dans le cas présent, on a donc un domaine pointant sur une machine et une `IP` qui n'appartient plus à l'entité responsable de la zone `DNS`. De surcroit, l'enregistrement dans la base `RIPE` (interrogeable par la commande «

whois » ou via `http://www.ripe.net`) lui aussi référençait encore l'ancien propriétaire de la classe d'adresse `IP` donc l'administration.

Ceci soulève deux problèmes : le premier est que le contenu légitime du site n'a plus aucun rapport avec le domaine recherché. Il est tout à fait envisageable que cette machine héberge dans le futur un contenu pouvant nuire à l'image de l'administration concernée. Le second est que dans le cas d'une compromission comme ici, c'est l'image du propriétaire du domaine (donc de l'administration) qui est mise en cause et pas nécessairement celle du popriétaire réel de la machine.

Cette situation s'apparente à celle du « déménagement d'un site » évoquée dans le bulletin d'actualité CERTA-2007-ACT-037 du 14 septembre 2007.

1.4.2 Recommandations

Lorsqu'une classe d'adresses IP publique est abandonnée suite à une fin de contrat ou autre, il est nécessaire d'entreprendre les démarches suivantes :

- s'assurer que plus aucun enregistrement `DNS` ne pointe sur ces anciennes adresses et que l'autorité pour la zone soit changée ;
- s'assurer que l'enregistrement dans la base `RIPE` soit mis à jour, en particulier les contacts techniques, administratifs ainsi que le *netname*.

1.5 WebDAV

1.5.1 Présentation

Cette semaine, le CERTA a traité un incident relatif à la défiguration d'un site Internet de l'administration, une personne ayant ajouté plusieurs pages à la racine du site web. L'analyse des journaux a révélé que les fichiers ont en fait été ajoutés au moyen d'une requête PUT après identification par l'attaquant du service `WebDAV` sur le serveur. Ce service qui est une extension du protocole HTTP 1.1 est supposé faciliter la publication de documents sur des sites. Il est notamment installé et activé par défaut dans IIS 5.0, contrairement aux versions plus récentes pour lesquelles il est désactivé. Le CERTA recommande la désactivation de ce service quelle que soit la version d'IIS utilisée.

Il est possible de désactiver `WebDAV` dans IIS 5.0 en ajoutant la valeur suivante dans la base de registre :

```
Clé : HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
Nom de la valeur : DisableWebDAV
Valeur (DWORD) : 1
```

Le CERTA en profite également pour rappeler qu'il existe un outil fourni par Microsoft pour aider à sécuriser des serveurs IIS. Cet outil appelé *IIS Lockdown Tool* est disponible à l'adresse suivante :

http://support.microsoft.com/?scid=kb%3Bfr%3B325864

1.5.2 Documentation

- « Comment faire pour désactiver WebDAV pour les services Internet (IIS 5.0) »
  http://support.microsoft.com/?scid=kb%3Bfr%3B241520

2 L'obligation de dénoncer

Un employé d'une société de maintenance informatique s'est vu confier un ordinateur, en vue de réparation. Lors de son intervention, il a découvert sur ce matériel des photos pornographiques à caractère pédophile. Sans hésitation, il a supprimé ces fichiers, effectué le dépannage et restitué l'ordinateur au client. Ce n'est que plus tard qu'il a informé son employeur de sa découverte, lequel l'a alors licencié pour faute grave, en raison de la non dénonciation de ce délit. L'employé s'est alors retourné vers le Conseil des Prud'hommes, considérant que son licenciement s'était effectué sans cause réelle et sérieuse. La Cour de Cassation (Cass soc. n 07-40670 du 21 mai 2008) a confirmé que le licenciement était justifié: « Dès lors qu'un salarié ayant découvert que l'ordinateur qui lui avait été confié avait été utilisé pour recueillir des images à usage pédophile, qui constitue une infraction prévue par l'article 227-23 du Code Pénal, et n'avait pas immédiatement retenu ce matériel, sauvegardé les fichiers litigieux puis informé l'autorité judiciaire et son employeur, mais avait pris l'initiative, avant de prévenir celui-ci, de supprimer ces fichiers et de restituer l'appareil au client, contrevenant ainsi aux dispositions impératives de la loi et ne permettant plus aux services de Police de procéder utilement à la moindre recherche, les juges du fond ont pu caractériser un licenciement pour faute grave. »

Si le cas énoncé se situe dans la sphère privée, la fonction publique est d'autant plus concernée par cette problématique. En effet, l'article 40-1 du Code de Procédure Pénale prévoit que « toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au Procureur de la République... » ; le fait de faire obstacle à la manifestation de la vérité est prévu par l'article 434-4 du Code Pénal.

En conclusion, en cas de découverte d'infractions, quelles qu'elles soient, dans le cadre de vos obligations professionnelles, pensez :

1° à préserver les traces et indices ;

2° à aviser dans les plus brefs délais les services de police. Ces derniers rendront compte au Procureur de la République qui décidera des suites à donner.

3 Rumeurs et TCP

3.1 Les faits

La presse s'est faite l'écho cette semaine d'une vulnérabilité pouvant affecter les mises en œuvre du protocole de transport TCP de certains systèmes. Des chercheurs finlandais ont annoncé avoir trouvé une vulnérabilité qu'ils présenteront au cours d'une conférence mi-octobre, mais aucun détail n'est à ce jour connu. Les rumeurs et suppositions sont apparues et ont été ainsi amplifiées dans la presse.

Les chercheurs ont présenté par ailleurs d'autres travaux en septembre concernant une méthode appelée *"SYN Cookie"*. Le lien entre cette précédente présentation et la future annonce n'est pas établi. Sans participer à ce phénomène d'amplification, devenu courant avant certaines conférences, le CERTA reste attentif aux conséquences de cette annonce.

L'objet de cet article est de clarifier l'usage des SYN Cookies et de préciser l'état actuel des informations disponibles.

3.2 Qu'est-ce qu'un *SYN Cookie* ?

Les attaques visant à perturber les serveurs opèrent de manière très variée et ciblent différentes couches protocolaires. Certaines ont consisté depuis la fin des années 1990 à envoyer plusieurs trames TCP de demande de connexion (SYN). Elles restent encore d'actualité.

Pour se prémunir de celles-ci plusieurs solutions sont possibles. Le standard RFC 4987 (*"TCP Syn Flooding Attacks and Common Mitigations"*) en précise certaines. L'une d'elles s'appelle le `TCP SYN Cookie` et a été proposée par D.J. Bernstein. Elle est mise en œuvre dans la majorité des systèmes d'exploitation Linux et BSD.

La solution consiste à s'assurer de l'adresse émettrice avant d'allouer des ressources système pour la connexion. Il s'agit de ne plus affecter pour chaque nouvelle demande de connexion un numéro de séquence ISN (*Initial Sequence Number*) aléatoire mais une valeur non prévisible prenant en compte certaines caractéristiques de la demande en cours. La machine ne stocke pas toutes les informations. Elle récupère ces informations, dont l'ISN, à la réponse de son correspondant. Si ce dernier n'existe pas, peu de ressources auront été finalement allouées.

L'inconvénient majeur est que toute l'information négociée au moment de la demande de connexion TCP, le *three-way handshake*, se trouve dans le SYN Cookie. Les autres informations qui peuvent être échangées dès l'établissement de la connexion sont perdues.

C'est également un avantage pour une machine attaquante qui voudrait envoyer des trames sans elle-même puiser trop de ses propres ressources.

Le SYN Cookie est construit, comme l'indique le code source *syncookie.c* du noyau Linux 2.6.18 ci-dessous, à partir des données suivantes :

- les adresses IPv4 source et destination de la connexion. Le support pour IPv6 a été proposé en avril 2008 mais n'est pas encore intégré au dernier noyau Linux ;
- les ports TCP source et destination utiles pour la connexion ;
- le numéro de séquence éventuel choisi par le client qui envoie la première trame SYN ;
- un compteur dont la valeur augmente régulièrement (par défaut toutes les minutes) afin de vérifier que le cookie a une validité qui ne dépasse pas une valeur seuil ;
- une valeur secrète rendant difficile la possibilité de reconstruire le SYN Cookie ;
- une valeur donnant une approximation de l'option MSS (*Maximum Segment Size*) indiquée par le client.

L'ensemble de ces valeurs est utilisé pour construire un numéro de séquence non prévisible sous forme d'empreinte irréversible (*hash*). Le condensat s'appuie sur le *Secure Hash algorithm* SHA-1.

La machine utilisant ce SYN Cookie n'allouera temporairement aucune ressource pour la demande de connexion. Si la machine distante répond, alors les données récupérées dans la nouvelle trame, dont le SYN Cookie, seront utilisées pour attribuer les ressources d'une session TCP établie.

```
Test pour vérifier la valeur de la SYSCTL associée :
labo:ven oct 03# cat /proc/sys/net/ipv4/tcp_syncookies
0
```

```
/*  Fichier source syncookie.c
*  Syncookies implementation for the Linux kernel
*  $Id$
*/

static __u32 secure_tcp_syn_cookie(__u32 saddr, __u32 daddr, __u16 sport,
                                   __u16 dport, __u32 sseq, __u32 count,
                                   __u32 data)
{
        /*
         * Compute the secure sequence number.
         * The output should be:
         *   HASH(sec1,saddr,sport,daddr,dport,sec1) + sseq + (count * 2^24)
         *      + (HASH(sec2,saddr,sport,daddr,dport,count,sec2) % 2^24).
         * Where sseq is their sequence number and count increases every
         * minute by 1.
         * As an extra hack, we add a small "data" value that encodes the
         * MSS into the second hash value.
         */

        return (cookie_hash(saddr, daddr, sport, dport, 0, 0) +
                sseq + (count << COOKIEBITS) +
                ((cookie_hash(saddr, daddr, sport, dport, count, 1) + data)
                 & COOKIEMASK));
}
```

Parmi les informations initialement perdues, on retrouve en particulier des options comme :

- les acquittements sélectifs, ou `SACK` ;
- l'ajustement de fenêtre, ou `Window scaling` ;
- etc.

Ces dernières servent à contrôler les problèmes de congestion et de perte. Les mises en œuvre actuelles de SYN Cookies n'activent donc cette méthode que quand le nombre de demandes en cours atteint un nombre important, défini par la variable `net.ipv4.tcp_max_syn_backlog`. Cette dernière vaut 1024 par défaut.

L'utilisation des SYN Cookies présente donc des inconvénients. Un contributeur de l'un des premiers correctifs en 1997 se pose d'ailleurs la question de l'intérêt d'ajouter le support pour IPv6, actuellement en débat :

```
http://lwn.net/Articles/277216/
De : Andi Kleen
A : linux-kernel AT vger.kernel.org
Sujet : Re: [PATCH] Add IPv6 support to TCP SYN cookies

(...)
Syncookies are discouraged these days. They disable too many valuable TCP features
(window scaling, SACK) and even without them the kernel is usually strong enough to
defend against syn floods and systems have much more memory than they used to be.

So I don't think it makes much sense to add more code to it, sorry.
(...)
```

3.3 Exploitation d'une méthode approchante dans le cadre de dénis de service

Il n'est pas improbable que la vulnérabilité annoncée exploite la fonctionnalité mentionnée ci-dessus des SYN Cookies, ou du moins une méthode approchante, mise en place par l'attaquant. Sans être révolutionnaire, il s'agit d'utiliser un minimum de ressources du côté du poste attaquant.

Rien n'est cependant sûr à la date de rédaction de cet article. Néanmoins, on peut imaginer le scénario suivant, où la machine cliente parvient à créer par ce biais beaucoup de connexions TCP établies du côté du serveur. La subtilité réside alors dans la facilité à maintenir la connexion ouverte ou d'attendre qu'un minuteur marquant la durée de session n'expire. Certains outils dits *tarpit* emploient de telles techniques (par exemple présenter une taille de fenêtre TCP nulle à une demande de connexion). Des idées ont été également suggérées dans de précédents articles de recherche (cf. section 3.5).

3.4 Que faut-il retenir ?

Il est important, avant de mettre en œuvre des mesures de sécurité, de bien comprendre leur fonctionnement. Dans le cas des SYN Cookies, il s'agit d'une méthode de protection contre une classe d'attaques en déni-de-service qui présente certains avantages mais également des inconvénients. Ces derniers doivent être connus et acceptés.

La faille qui fait actuellement l'objet de rumeurs n'est pas documentée. En tout état de cause, cette faille ne remet pas en cause les bonnes pratiques à mettre en place pour prévenir les dénis de service ainsi qu'une politique de filtrage rigoureuse et précise du trafic autorisé.

3.5 Références pour aller plus loin

- Articles fondateurs de D.J. Bernstein concernant les SYN Cookies :
  http://cr.yp.to/syncookies/idea
  http://cr.yp.to/syncookies/archive
  http://cr.yp.to/syncookies.html
- Soumission d'un correctif pour le support IPv6 des TCP SYN cookies, avril 2008 :
  http://lwn.net/articles/277225/
- F. Westphal, "Add support for TCP-options via timestamps", archive de mailing-list, 31 mars 2008 :
  http://lwn.net/Articles/277219/
- Option synproxy de Packet Filter (PF) :
  http://www.openbsd.org/faq/pf/filter.html
- A. Kuzmanovic, E.W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants), SIGCOMM 2003 :
  http://conferences.sigcomm.org/sigcomm/2003/papers/p75-kuzmanovic.pdf
- Outil LaBrea, présentation et page du projet :
  http://labrea.sourceforge.net/Intro-History.html
  http://labrea.sourceforge.net/labrea-info.html
- Article SecurityFocus, "Slow Down Internet Worms With Tarpits, août 2003 :
  http://www.securityfocus.com/infocus/1723
- F. Gont, Draft IETF, "ICMP attacks against TCP", 14 mars 2008 (date d'expiration du 15 septembre 2008 cependant) :
  http://www.gont.com.ar/drafts/icmp-attacks/draft-ietf-tcpm-icmp-attacks-03.txt
- A. Ramaiah, R. Steward, M. Dalal, Draft IETF, "Improving TCP's Robustness To Blind In-Window Attacks", juillet 2008 :
  http://tools.ietf.org/id/draft-ietf-tcpm-tcpsecure-10.txt
- J. Lemon, "Resisting SYN flood DoS Attacks with a SYN cache", FreeBSD Project :
  http://people.freebsd.org/ jlemon/papers/syncache.pdf
- F. Westphal, "Reflections on TCP", 22 juin 2008 :
  http://www.strlen.de/talks/tcp-review.pdf
- A. Zuquete, "Improving the functionality of SYN Cookies", 2002 :
  http://www.ieeta.pt/ avz/pubs/CMS02.ppt
- T. Aura, P. Nikander, J. Leiwo, "DOS-resistant Authentication with Client Puzzles :
  http://research.microsoft.com/users/tuomaura/Publications/aura-nikander-leiwo-protocols00.pdf

4 Des en-têtes qui vous desservent - Précisions

Le bulletin d'actualité du CERTA de la semaine dernière (CERTA-2008-ACT-039) mentionnait une vague de pourriels (SPAM) construits avec certains champs d'en-tête un peu spéciaux. Pour rappel, ces messages non-sollicités utilisaient l'en-tête *X-Confirm-Reading-To* pour demander au client de messagerie le renvoi d'un accusé de réception à la lecture du mail. Revenons plus en détail sur cette vague de SPAM.

4.1 Les en-têtes

Un lecteur attentionné (que nous remercions) nous a fait remarqué que ce champ s'accompagnait de deux autres :

- *Disposition-Notification-To* : ce champ a la même fonction que le *X-Confirm-Reading-To*, et est défini dans la RFC 3978 ;
- *User-Agent: SquirrelMail/1.4.12* : ce champ détermine a priori le client de messagerie utilisé pour envoyer le message. Ici, il semble s'agir de SquirrelMail, logiciel de type *webmail*.

Dès lors, on peut se demander si cette vague est envoyée depuis des machines compromises. Pour répondre à cette question, il est possible de vérifier les en-têtes de ce message. On remarque la présence de l'en-tête Message-ID, censé servir d'identifiant unique au message. Chaque client de messagerie utilise un algorithme plus ou moins différent afin de générer cet identifiant. Dans le cas des versions de SquirrelMail inférieures à la version 1.4.15, l'identifiant est construit suivant le schéma [port].[adresse IP].[time+rand].squirrel@mondomaine.xxx, avec :

port : le port utilisé pour l'envoi du mail ;
adresse IP : l'adresse IP utilisée pour l'envoi du mail ;
time+rand : une combinaison de temps en millisecondes et d'une graine aléatoire.

Dans le cas des SPAM récoltés, le port et l'adresse utilisés dans la création du *Message-ID* sont totalement farfelus. En voici quelques exemples :

```
64951.651.585.309.759.1304476643.squirrel@xxxxxxx.xxx
57397.740.510.639.891.1169069027.squirrel@xxxxxxx.xxx
```

Nous sommes donc en présence de pourriels dont l'en-tête ont été forgée pour ressembler au plus près à un message envoyé d'un client légitime.

4.2 Durée de la vague

Plusieurs tests, dont certains faits par notre lecteur, montrent que cette vague est très limitée dans le temps. Les premiers courriels forgés de la sorte apparaissent le 20 septembre 2008, et les derniers sont datés du 27 septembre 2008, soit exactement une semaine.

Ce laps de temps relativement court peut être interprété de plusieurs manières différentes, sans aucune certitude :

- phase de test afin de vérifier l'efficacité de la technique ;
- location d'un nouvel outil (ou réseau) de spam ;
- vérification d'un ensemble d'adresses électroniques en préparation de nouvelles vagues ;
- etc.

4.3 Perspectives futures

Comme indiqué dans le bulletin de la semaine dernière, nous pouvons nous attendre à ce que de plus en plus de champs d'en-tête soient utilisés de manière détournée afin de rendre les campagnes de pourriels efficaces.

Il serait trop long de lister ici tous ces champs, mais il existe de nombreuses RFC permettant de se faire une idée, et de mettre en place un système de filtrage efficace au besoin :

- RFC 822 : *Standard for the Format of ARPA Internet Text Messages*
  http://rfc.net/rfc822.html
- RFC 3798 : *Message Disposition Notification*
  http://rfc.net/rfc3798.html
- RFC 2156 : *Mapping between X.400 and RFC822/MIME*
  http://rfc.net/rfc2156.html
- RFC 1327 : *Mapping between X.400 / ISO 10021 and RFC822*
  http://rfc.net/rfc1327.html

– RFC 2076 : *Common Internet Message Headers*
http://rfc.net/rfc2076.html
– RFC 4021 : *Registration of Mail and MIME Header Fields*
http://rfc.net/rfc4021.html

5 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 25 septembre et le 02 octobre 2008.

6 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/

7 Rappel des avis émis

Dans la période du 26 septembre au 02 octobre 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-473 : Multiples vulnérabilités des produits Mozilla
– CERTA-2008-AVI-474 : Multiples vulnérabilités dans Cisco IOS
– CERTA-2008-AVI-475 : Vulnérabilité dans Symantec Veritas NetBackup
– CERTA-2008-AVI-476 : Multiples vulnerabilite dnas Mac OS X Java
– CERTA-2008-AVI-477 : Vulnérabilités dans CA Service Desk Web Forum
– CERTA-2008-AVI-478 : Vulnérabilité dans Tivoli
– CERTA-2008-AVI-479 : Vulnérabilité dans Lighttpd

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

– CERTA-2008-AVI-464-001 : Vulnérabilité dans phpMyAdmin
(Ajout Fedora)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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

9 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.

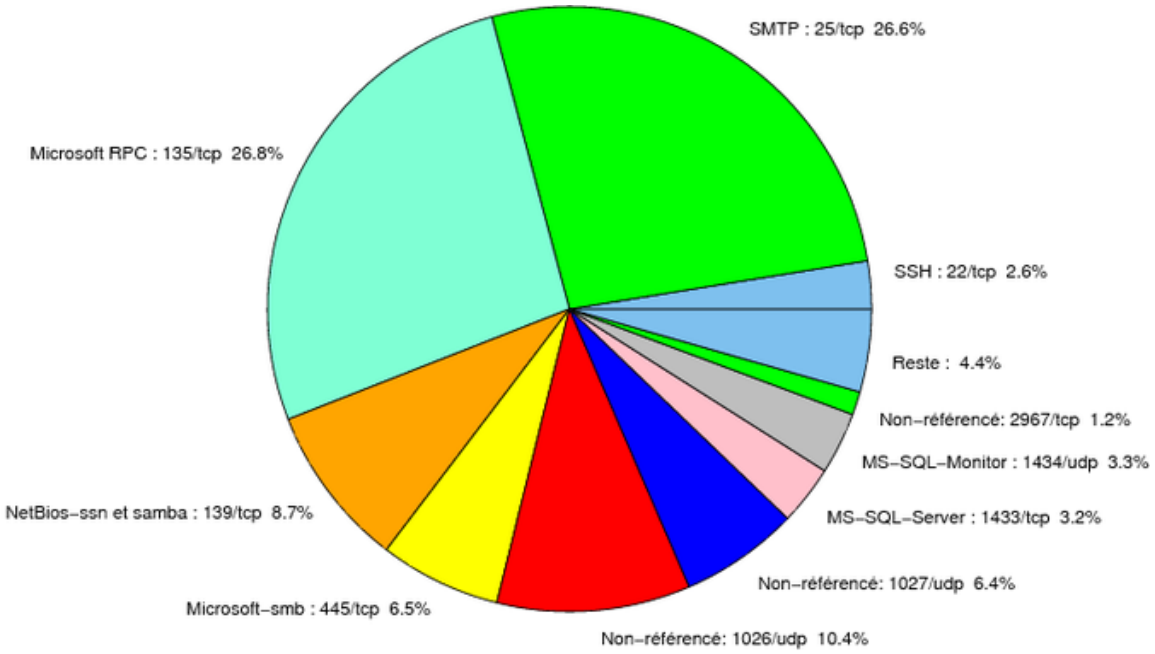

FIG. 1: Répartition relative des ports pour la semaine du 25.09.2008 au 02.10.2008

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	26.79
25/tcp	26.58
1026/udp	10.35
139/tcp	8.7
445/tcp	6.49
1027/udp	6.35
80/tcp	3.45
1434/udp	3.31
1433/tcp	3.17
22/tcp	2.62
2967/tcp	1.24
21/tcp	0.89
4899/tcp	0.82
23/tcp	0.69
137/udp	0.62
3306/tcp	0.55
3128/tcp	0.27
3389/tcp	0.2

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

03 octobre 2008 version initiale.