

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-09

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-009>

Gestion du document

Référence	CERTA-2008-ACT-009
Titre	Bulletin d'actualité 2008-09
Date de la première version	29 février 2008
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-009.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-009/>

1 Augmenter la sécurité de PHP

Cette semaine, le CERTA a traité un incident relatif à la compromission d'un serveur web. Le site web compromis utilisait une version vulnérable d'un composant de Joomla. Les attaquants ont réussi à exploiter la vulnérabilité de type injection de code arbitraire (*Remote File Injection*) pour déposer des fichiers malveillants. Ces fichiers permettaient de prendre la main sur le serveur et d'y exécuter des commandes système. Ces fichiers, qui peuvent être connus sous le nom de *PHP Shell*, utilisent généralement des directives PHP permettant d'exécuter des commandes systèmes envoyées dans un formulaire.

Il existe plusieurs directives du langage PHP permettant d'exécuter des commandes système :
`exec`, `passthru`, `shell_exec`, `system`, `proc_open`, `popen`, `pcntl_exec`, ...

Le fichier `php.ini` contient, par défaut, une variable `disable_functions` qui est vide. Cette variable permet d'interdire l'utilisation de certaines directives PHP. La ligne suivante du fichier `php.ini` permet d'interdire l'exécution de commandes systèmes depuis des pages PHP :

```
disable_functions =  
exec,passthru,shell_exec,system,proc_open,popen,pcntl_exec
```

Ces techniques ne peuvent pas garantir une sécurité maximale, en revanche elles permettent de se protéger un peu plus des attaques triviales.

Pour finir, le CERTA recommande d'être attentif aux mises à jour disponibles et de les appliquer dans les meilleurs délais. De plus, les composants inutilisés doivent être supprimés.

2 Documentation

- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

3 Joomla!, un correctif incomplet ?

Le CERTA a publié cette semaine l'avis CERTA-2008-AVI-104 et mis à jour l'alerte CERTA-2008-ALE-002 en réponse à la sortie de la version 1.0.15 de *Joomla!*. Cette nouvelle version du gestionnaire de contenu corrige une vulnérabilité qui permettait l'exécution de code arbitraire à distance. Dans notre alerte, nous avons indiqué également un contournement de la politique de sécurité comme faisant partie des risques. En effet, dans une configuration particulière, une fonctionnalité permettant l'émulation des variables globales pouvait être activée à l'insu de l'administrateur du serveur et de l'administrateur du site web. L'exécution de code arbitraire à distance découle de cette fonctionnalité.

Le correctif proposé par les développeurs de *Joomla!* a pour effet d'écraser une variable qui peut être manipulée par un attaquant. Cette variable est utilisée pour une inclusion de fichier. Si l'on regarde le contenu de cette donnée, on peut voir qu'elle prend successivement plusieurs valeurs :

- celle contenue dans le fichier de configuration ;
- puis celle donnée par un éventuel attaquant ;
- puis de nouveau celle contenue dans le fichier de configuration (avant inclusion).

Du point de vue de la sécurité, le « cycle de vie » de cette variable présente un danger puisqu'à un moment, celle-ci peut être maîtrisée par un attaquant. D'autre part, d'autres variables peuvent être manipulées par un attaquant, ce qui peut avoir des effets variables en fonction des différents modules optionnels utilisés.

Ces éléments nous amènent à dire que, d'une certaine façon, le correctif de *Joomla!* est incomplet. Si vous administrez un site fonctionnant avec *Joomla!* en version 1.0.15, il est sans doute préférable de réfléchir à une migration vers la dernière version de la branche de développement 1.5 ou vers un autre gestionnaire de contenu.

Documentation

- Avis CERTA-2008-AVI-104 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-104/>
- Alerte CERTA-2008-ALE-002 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-002/>

4 De la mauvaise utilisation des moteurs de recherche

4.1 Les faits

Le CERTA a mentionné dans le précédent bulletin CERTA-3008-ACT-008 la possibilité d'utiliser les moteurs de recherche comme outils de tests de vulnérabilité indirects. Cette possibilité n'est envisageable que par des requêtes particulières adressées au moteur de recherche, qu'il va lui-même appliquer sur l'ensemble des données qu'il connaît et qu'il a indexé. Il faut donc que les pages ciblées par l'outil de vulnérabilité soient indexées.

Plusieurs solutions existent actuellement pour spécifier aux moteurs de recherche les plus précautionneux quelles pages doivent être recensées. C'est par exemple l'objectif des fichiers `robots.txt`. D'autres méthodes consistent à construire des cartes de sites (`map`) et à les fournir au moteur de recherche pour orienter son indexation.

4.2 le problème

Il faut bien comprendre ici que ce n'est pas suffisant qu'une page ne soit pas mentionnée dans une map ou soit une exception du fichier `robots.txt` pour avoir la garantie que la page ne sera pas indexée.

Ainsi, des personnes malveillantes peuvent forcer l'opération d'indexation (*spidering*).

Le procédé n'est pas très sophistiqué. Elles collectent les adresses IPs de l'organisation ou l'administration ciblée, puis construisent à partir de celles-ci et de ports courants (80, 8080, 443, 1080, etc.) des listes d'adresses, de la forme :

```
http://Adresse_IP:Port
```

Ces adresses sont ensuite diffusées sur des sites connus, afin d'inciter les robots des moteurs de recherche à interroger cette adresse.

Des moteurs de recherche particuliers ne prennent en compte que ces « nouvelles pages » pour trouver des informations intéressantes, et souvent dangereuses pour la sécurité du site, comme :

- schémas de bases de données ;
- fichiers de configuration ;
- arborescence de fichiers ;
- interfaces Web de produits comme les imprimantes, les appareils de téléphonie sur IP, d'équipements réseaux, etc.

4.3 Les recommandations du CERTA

Il est plus facile de se rendre compte qu'une page est indexée, que de savoir comment elle l'a été (indexation forcée par une personne malveillante, robots peu scrupuleux, etc.) :

- des recherches dans les mêmes moteurs de recherche permettent de vérifier la présence ou non d'informations. C'est une bonne pratique qui offre la possibilité de vérifier si des informations qui ne devraient pas paraître sont malheureusement présentes. Il faut cependant prendre garde à ne pas diffuser l'intégralité de ces informations au moteur de recherche même, pour les mêmes raisons de limiter leurs diffusions. Des expressions régulières ou de courts extraits sont très souvent suffisants.
- surveiller le trafic à destination de ces adresses. Les journaux de connexion peuvent montrer des valeurs comme le site d'origine (`referer`). Une trop grande variété et diversité de ces derniers peut paraître suspect.

Le lecteur comprendra ici que l'erreur n'est pas de faire confiance en la procédure d'indexation des moteurs de recherche. A partir du moment où une interface est accessible publiquement, les données auxquelles elle donne accès sont publiques et risquent d'être lues tôt ou tard. La meilleure pratique consiste à vérifier que les règles de filtrage en amont sont correctement configurées, que les services inutiles sont désactivés et que les listes de contrôle d'accès sont bien mises en vigueur.

5 Vulnérabilité dans Thunderbird

Mozilla a publié cette semaine un bulletin de sécurité, MFSA2008-12 ayant fait l'objet de l'avis CERTA-2008-AVI-105. Il détaille une vulnérabilité du client de messagerie, permettant à une personne malveillante d'exécuter du code arbitraire sous certaines conditions.

La vulnérabilité, identifiée par sa référence CVE-2008-0304, concerne le traitement par Thunderbird de certains documents encodés par MIME. Le standard MIME permet d'encapsuler plusieurs types de données dans un même document Internet, ici le courrier électronique. Dans le cas présent, Thunderbird allouerait moins de mémoire, pouvant conduire à un débordement de pile.

MIME fait appel à la bibliothèque `libsmime3.dylib`.

L'exploitation de cette vulnérabilité peut être déclenchée par la simple pré visualisation de la pièce jointe dans la fenêtre du client (zone *Panneau d'affichage des messages*).

Parmi les bonnes pratiques envisageables pour la lecture d'un courrier, il est préférable de ne pas pré visualiser les pièces jointes, et de n'ouvrir ces dernières que pour des mails de confiance. Un rapide coup de téléphone à l'expéditeur est toujours possible, ainsi qu'un balayage de la pièce jointe par un antivirus à jour. Cette étape de visualisation est souvent mise en oeuvre par des modules peu robustes, et souffrants d'au moins autant de vulnérabilités que leurs grands frères.

Pour contrôler ce qui doit être affiché à l'ouverture d'un courriel, il existe la variable suivante, définie dans le fichier de configuration `mailnews.js` :

```
mailnews.display.disallow_mime_handlers
    valeur 0 : tout est affiché
    valeur 1 : presque tout est affiché, mais il n'y a pas de rendu HTML
    valeur 2 : ... ni d'image insérée
    valeur 3 : ... ainsi que d'autres types moins courants.
```

Le fait de ne pas lire son courriel au format HTML est une excellente chose, mais n'est pas suffisant. Des pièces jointes peuvent être ouvertes dans l'aperçu du courriel.

Il existe la valeur 100 pour cette variable, qui évite l'interprétation de la totalité des pièces jointes, à l'exception de celles explicitement mentionnées. Cette option est donc relativement intéressante.

Le CERTA rappelle à cette occasion que la note d'information CERTA-2000-INF-002 aborde les mesures de prévention relatives à la messagerie.

- CERTA-2000-INF-002, « Mesures de prévention relatives à la messagerie » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/>

6 Tricher sur la valeur du *User-Agent*

Certains navigateurs Internet offrent la possibilité aux utilisateurs de modifier la valeur de leur *User-Agent*. Le fait de modifier cette valeur ne doit pas offrir à l'utilisateur une impression de sécurité de par la pseudo-anonymisation de son navigateur Internet.

Cela est d'autant plus vrai avec le navigateur Internet Mozilla Firefox du fait qu'il existe sur l'Internet le savoir-faire nécessaire pour contourner ce type de dissimulation. La méthode consiste à exécuter un code javascript légitime qui tente de vérifier l'information du *User-Agent* (rempli par l'utilisateur) avec des valeurs accessibles et disponibles dans le répertoire d'installation de Mozilla Firefox. Le code JavaScript peut accéder au répertoire de `resource:///` (comme `resource:///defaults/pref/firefox.js`), et ces valeurs ne sont pas réécrites par les outils classiques de triche, ou par les passerelles Web.

Il est à noter que la désactivation de l'interprétation du javascript par le navigateur Internet permet de contourner ce mécanisme de vérification. La modification de la valeur du *user-agent* de son navigateur Internet peut être utilisée pour contourner les vérifications de certains sites web obligeant, par exemple, l'utilisation d'un navigateur spécifique, et ne doit pas être mise en oeuvre comme une mesure de sécurité efficace.

7 Des vulnérabilités typiques

Une récente publication présentait des vulnérabilités touchant une gamme de routeur ADSL à destination des particuliers et des PME. Finalement, cette liste ne présente que des problèmes couramment rencontrés.

7.1 Des interfaces HTTP qui gèrent mal les droits

Il y a souvent un compte *utilisateur* et un compte *administrateur*, nécessitant tous les deux un mot de passe. Le premier donne accès à une interface restreinte de consultation de statistiques. Les données ne semblant pas sensibles, le mot de passe par défaut est souvent laissé. Le second compte permettant de configurer l'appareil, un message alerte l'administrateur qu'il doit penser à changer le mot de passe. Le problème est qu'une personne utilisant le compte *utilisateur* peut accéder aux pages d'administration en saisissant directement les URL. Ces adresses sont largement documentées, ne serait-ce que par les captures d'écran présentes dans la documentation de l'appareil.

7.2 Le trafic d'administration circule en clair

Les interfaces d'administration sont souvent en HTTP, et les mots de passes sont stockés en clair dans l'appareil. Ainsi, l'écoute d'un réseau permet de capturer les identifiants, que cela soit à la saisie de ceux-ci, ou à leur affichage dans un navigateur.

7.3 Les IP comme identifiants de session

L'équipement identifie les sessions par leur adresse IP d'origine. Ainsi un administrateur qui s'identifie sur l'interface HTTP, depuis une machine avec l'adresse 192.168.0.3, pourra revenir à l'interface sans ressaisir le mot de passe, et cela pendant temps inférieur au *time out*, configurable via l'interface. Ainsi toute personne dans le même réseau local qui configurerait manuellement l'adresse IP de sa machine à 192.168.0.3 pourrait accéder à l'interface sans saisir de mot de passe, pendant la durée du *time out*.

7.4 Les services activés par défaut

Leur présence est souvent ignorée et ils sont rarement utilisés, mais malgré tout, les équipements sont livrés avec des services actifs et configurés par défaut. A l'administrateur de les désactiver. Dans le cas présent, les appareils peuvent être configurés par SNMP (*Simple Network Management Protocol*) en utilisant des mots de passe dédiés largement documentés. Le protocole SNMP permet d'accéder et de modifier des informations confidentielles telles que les mots de passe utilisés pour l'interface HTTP ou les clefs du réseau sans fil.

7.5 Des attaques indirectes

Toutes ces vulnérabilités sont utilisables directement pour prendre le contrôle du réseau, mais elles permettent aussi d'effectuer une attaque du type XSS persistant. En effet, les paramètres étant affichés via l'interface Web dans le navigateur de l'administrateur et cela sans contrôle préalable, il est possible d'injecter dans l'une d'elle une *iFrame* pointant sur un JavaScript malveillant.

7.6 Conclusion

Les recommandations du CERTA concernant toutes ces vulnérabilités sont classiques :

- maîtriser ses équipements ;
- couper tous les services par défaut et n'activer que ceux utiles ;
- changer les mots de passe par défaut ;
- n'autoriser le JavaScript et les ActiveX qu'à bon escient.

8 Le pare-feu personnel : utile mais pas suffisant

La semaine dernière, dans le bulletin d'actualité CERTA-2008-ACT-008, était fait un retour sur l'activation et la bonne mise en oeuvre des services que propose le pare-feu de Windows Vista. Cette semaine, le CERTA tient à revenir sur les risques d'une sécurité reposant uniquement sur le pare-feu personnel des utilisateurs. Le mode de protection reposant sur un seul et unique rempart ne peut pas être suffisant. Cela reviendrait à un pare-feu extérieur unique, ou un pare-feu sur le poste utilisateur. Cette seule protection si elle est contournée par un individu malveillant laisse sans défense l'intérieur du réseau ou du système d'exploitation. De plus un pare-feu personnel dépend de l'intégrité du système sur lequel il est installé. Une machine compromise par un code malveillant peut se voir reconfigurer et de nouvelles règles de filtrage intégré au pare-feu permettant ainsi au code de s'exécuter et de communiquer avec l'extérieur sans que l'utilisateur ne soit prévenu. Le principal inconvénient du pare-feu personnel est que ses journaux ne sont que très rarement lus ce qui ne devrait normalement pas être le cas des journaux du pare-feu d'un réseau, par exemple. Autrement dit, un pare-feu personnel peut, dans certain cas, retarder la découverte d'un incident. Il est donc préférable dans un système d'information de choisir un mode de protection à plusieurs fonctions indépendantes. Ces dernières constituent plusieurs couches de protection au cas où il serait agressé par un élément extérieur. Il est donc nécessaire de disposer d'un pare-feu personnel correctement configuré sur chaque poste utilisateur. Ce pare-feu offre la possibilité de filtrer les autorisations de sortie ou d'entrée de flux par applications. Il limite aussi des propagations dans le réseau interne d'un quelconque code malveillant. Ces applications sont toutefois vulnérables aux codes malveillants, il est donc important d'y ajouter un autre niveau de protection avec un pare-feu d'entreprise. Ce dernier ne permet pas le filtrage par applications mais par zone et n'est pas sensible aux mêmes codes malveillants.

Le CERTA rappelle qu'il est important d'assurer différents niveaux de protection. Ceux-ci doivent être correctement configurés et conformes à l'application de la politique de sécurité afin d'assurer un maximum de sécurité au système d'information. Ces niveaux de protection, mis en oeuvre dans des logiciels et des boîtiers, doivent être également à jour.

Documentation

:

- Bulletin d'actualité CERTA-2008-ACT-008 du 22 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-008>
- Note d'information CERTA-2006-INF-001 du 10 janvier 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001>
- Portail de la Sécurité informatique, « Pare-feu (firewall) et pare-feu personnel » :
http://www.securite-informatique.gouv.fr/gp_article41.html

9 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 21 et le 28 février 2008.

10 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1935>
- Note d'information du CERTA sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

11 Rappel des avis émis

Dans la période du 22 au 28 février 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-100 : Vulnérabilités dans Symantec Veritas Storage Foundation
- CERTA-2008-AVI-101 : Vulnérabilités dans Netscape
- CERTA-2008-AVI-102 : Multiples vulnérabilités dans IBM AIX
- CERTA-2008-AVI-104 : Vulnérabilité dans Joomla!
- CERTA-2008-AVI-105 : Vulnérabilité dans Thunderbird
- CERTA-2008-AVI-106 : Vulnérabilité dans Sun Solaris
- CERTA-2008-AVI-107 : Vulnérabilités dans Symantec Decomposer

- CERTA-2008-AVI-108 : Vulnérabilités dans Wireshark
- CERTA-2008-AVI-109 : Vulnérabilité de OpenBSD
- CERTA-2008-AVI-111 : Vulnérabilités dans Mambo

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

- CERTA-2008-AVI-103-001 : Multiples vulnérabilités dans VMware ESX Server (correction du lien vers le bulletin de sécurité VMware)
- CERTA-2008-AVI-110-001 : Vulnérabilité dans Cadic Intégrale (Ex-Libris) (prise en compte du changement de nom du logiciel)

12 Actions suggérées

12.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

12.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

12.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

12.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

12.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le COSSI/CERTA peut vous aider dans ce travail d'analyse.

12.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

12.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

<http://www.formation.ssi.gouv.fr>

13 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

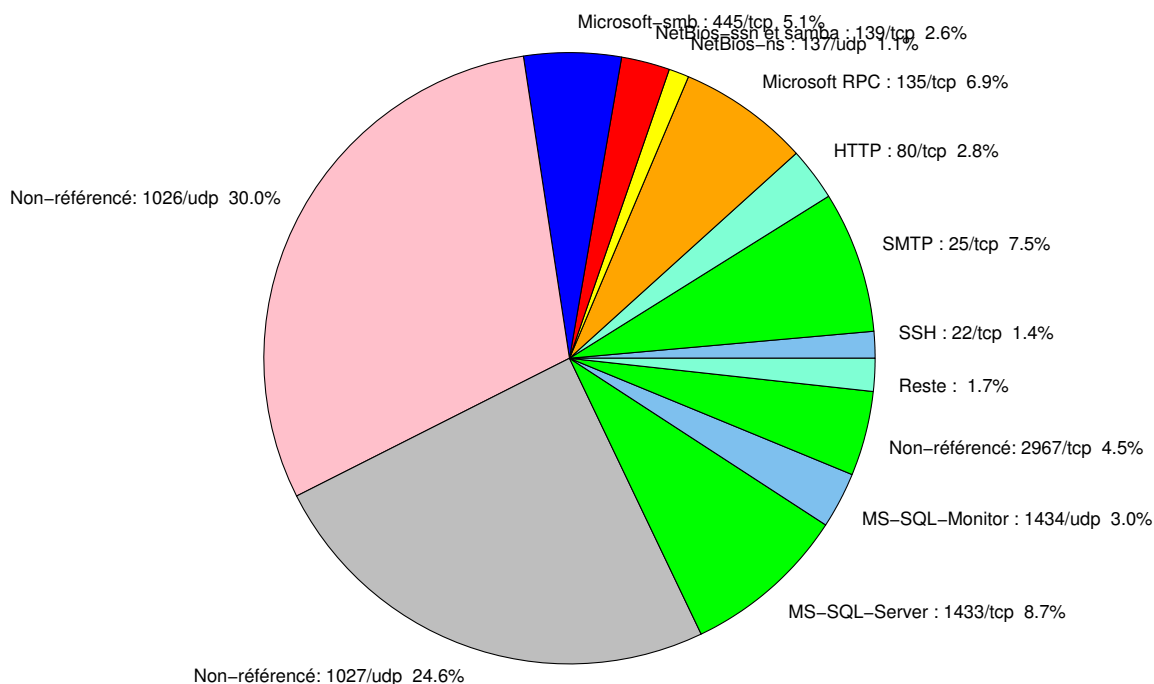


FIG. 1: Répartition relative des ports pour la semaine du 21.02.2008 au 28.02.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283

				CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	–	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	–	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-153
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	CERTA-2007-AVI-183
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310
54345	TCP	HP Mercury	–	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	–	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
80/tcp	83.72
1026/udp	30.03
1027/udp	24.64
1433/tcp	8.73
25/tcp	7.48
135/tcp	6.93
445/tcp	5.14
2967/tcp	4.47
1434/udp	2.96
139/tcp	2.56
22/tcp	1.41
137/udp	1.06
4899/tcp	0.6
3306/tcp	0.36
21/tcp	0.28
3389/tcp	0.1
143/tcp	0.08
3128/tcp	0.06
2100/tcp	0.04
9898/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

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

Gestion détaillée du document

29 février 2008 version initiale.