

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-44

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-044>

Gestion du document

Référence	CERTA-2008-ACT-044
Titre	Bulletin d'actualité 2008-44
Date de la première version	31 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-044.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-044/>

1 Mauvaise gestion d'un incident

Cette semaine, le CERTA a traité le cas d'une défiguration classique suite à l'exploitation d'une vulnérabilité de Joomla! 1.5 (réinitialisation du mot de passe de l'administrateur du site Web). L'intrus ne s'est pas contenté de modifier la page d'accueil du site, il a également installé un *phpshell* (interpréteur de commandes écrit en PHP) dans le but de revenir facilement sur le site compromis.

La réaction du webmestre à cet incident a été assez inhabituelle. En effet, il a modifié les droits du *phpshell* pour en empêcher son exécution. Cette réaction est inappropriée pour les raisons suivantes :

- il est généralement déconseillé de modifier l'état d'une machine compromise pour ne pas perturber une éventuelle analyse ;
- le *phpshell* n'est pas exécuté directement, il est appelé en lecture par l'interpréteur PHP ;
- le *phpshell* reste disponible en téléchargement, et peut être utilisé pour d'autres intrusions. Un des schémas d'intrusion possible est la réutilisation de ce *phpshell* par une faille permettant une inclusion « locale », c'est-à-dire des fichiers déjà présents sur le serveur attaqué.

Les recommandations du CERTA pour les incidents de ce type sont toujours :

- de réaliser une copie physique du disque dur en vue de préserver les traces et indices ;
- de déconnecter du réseau la machine attaquée ;
- de réinstaller complètement le serveur compromis.

2 MS08-062 pour Windows Vista

Cette semaine, les utilisateurs de Windows Vista ont pu remarquer l'apparition de deux nouvelles mises à jour automatiques, ayant pour références KB957200 et KB953155. La première correspond à une mise à jour de fiabilité. Chose plus étrange, la deuxième correspond en fait au bulletin MS08-062 qui a fait l'objet de l'avis CERTA-2008-AVI-503, donc à une faille corrigée il y a plus de deux semaines.

Si le correctif était bien disponible en téléchargement manuel sur le site de Microsoft le 14 octobre 2008 pour les utilisateurs de Windows Vista, il n'était pas délivré en mise à jour automatique (Windows Update, Microsoft Update, WSUS, etc.). Les utilisateurs de Windows Server 2008 version Itanium ont semble-t-il eu le même problème.

Ce phénomène illustre un problème apporté par l'automatisation des mises à jour. Si le principe de mise à jour automatique est une valeur ajoutée pour la sécurité, cela ne doit toutefois pas remplacer les bonnes pratiques d'administration de systèmes :

- vérifier régulièrement l'existence possible de failles non corrigées et de contournements ;
- vérifier régulièrement la disponibilité de mises à jour ;
- vérifier quelles mises à jour sont téléchargées automatiquement et si elles ont été correctement installées.

Pour conclure, les mises à jour automatiques ne signifient pas qu'un système est automatiquement protégé. Elles ne doivent pas dispenser des bonnes pratiques en matière d'information sur les vulnérabilités et leurs correctifs.

2.1 Documentation

- Bulletin de sécurité Microsoft MS08-062 :
<http://www.microsoft.com/france/technet/security/bulletin/ms08-062.msp>
- Bulletin Microsoft KB957200 :
<http://support.microsoft.com/kb/957200>
- Avis CERTA-2008-AVI-503 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-503/index.html>

3 Les extensions Firefox malveillantes

Le navigateur de la fondation Mozilla offre la possibilité d'ajouter des fonctionnalités via des extensions (classiques, packs de langues, thèmes). Afin de limiter les risques d'installation d'une extension malveillante, le CERTA tient à revenir sur quelques bonnes pratiques et sur les moyens de détecter une extension potentiellement malveillante.

3.1 L'installation des extensions

Tout d'abord, il est nécessaire de vérifier que l'installation d'extensions ne puisse pas se faire de manière silencieuse. En effet une option, activée par défaut, permet que l'utilisateur soit averti lorsqu'une extension est installée sur le navigateur. Cette option se situe dans l'onglet *sécurité* du menu *options* ou *préférences*, selon les systèmes d'exploitation. Cependant, une liste blanche de sites est disponible en cliquant sur le bouton « exceptions... », il est donc primordial de vérifier que seuls des sites de confiance apparaissent dans cette liste. Par défaut, seuls les sites *addons.mozilla.org* et *update.mozilla.org* y figurent. Cette option permet l'installation des extensions dans le navigateur par simple clic sur le bouton « installer » du site proposant l'extension. Une barre jaune apparaît en haut de la fenêtre lorsque Firefox bloque l'installation d'une extension.

Il est également possible d'installer une extension en la téléchargeant, puis en l'ouvrant avec le navigateur ou en faisant un glisser/déposer dans une fenêtre de Firefox.

Afin de contrôler la présence d'extensions installées sur le navigateur, il faut vérifier dans le répertoire d'installation les extensions présentes. Il est important de noter qu'il reste envisageable d'installer des extensions par profil (par défaut) mais également pour tous les utilisateurs de la machine et du navigateur.

3.2 Les risques

Le principal risque lié aux extensions Firefox est qu'elles sont multi-plateformes. Ces extensions sont développées en *JavaScript*, *Java*, *Python* ou *C/C++*. Une extension malveillante permet alors de compromettre différents systèmes d'exploitation : l'activité d'une extension est confondue dans celle du navigateur. Elle n'est pas forcément distinguée du navigateur et peut profiter des accès octroyés à ce dernier. Les extensions peuvent également contenir des *dll* ou des exécutables bien que ces possibilités nuisent à la compatibilité entre les différents systèmes d'exploitation.

Les extensions peuvent intégrer tous les concepts des programmes malveillants modernes comme le polymorphisme, l'obfuscation de code ou l'infection d'autres extensions. Elles sont capables d'ouvrir des connexions réseau, d'enregistrer les frappes du clavier et même de manipuler des données avant leur envoi. De plus, une *API* nommée *XPCOM* (*Cross Platform Object Model*) permet de développer facilement des extensions. Il est également possible, par différents moyens, de rendre des extensions installées invisibles dans la fenêtre de gestion des modules complémentaires.

Pour toutes ces raisons, elles en font une piste de recherche très intéressante pour les développeurs de code malveillant.

3.3 Les bonnes pratiques

Afin de limiter les risques d'infection par une extension malveillante, le CERTA fait un petit rappel des bonnes pratiques en la matière :

- ne pas utiliser de navigateur avec un utilisateur ayant des droits élevés ;
- installer des extensions strictement nécessaires sans en abuser et après avoir audité le code ;
- n'installer des extensions qu'à partir de sites de confiance ;
- contrôler régulièrement l'intégrité des répertoires d'installation des extensions ;
- s'assurer de la mise à jour des extensions et du navigateur ;
- contrôler la signature de l'extension lorsque celle-ci est disponible.

Il est important de noter que les mises à jour d'extensions se font normalement par le biais du site *addons.mozilla.org* via le protocole *HTTPS*. La signature des extensions est vérifiée à l'installation et à chaque mise à jour. Il est intéressant de faire des captures réseau afin de vérifier si les trames échangées à la mise à jour forcée des extensions respecte bien ces principes. À valeur d'exemple, la version 3.1 Bêta de Firefox ne les respecte pas encore pour les quelques extensions déjà mises à disposition. Les mises à jour se font directement vers les sites des éditeurs.

4 Les mises à jour

4.1 Mise à jour importante de OpenOffice.org 2.x

Une mise à jour importante concernant les versions antérieures à la 2.4.2 a été publiée cette semaine. Elle corrige des vulnérabilités concernant le traitement des fichiers au format *WMF* (*Windows Media File*) et *EMF* (*Enhanced Meta File*) dont l'exploitation permet d'exécuter du code sur le poste de l'utilisateur au moyen de fichiers spécialement construits. Cette mise à jour ne concernant pas la dernière version (3.0) de la suite bureautique, certains peuvent se poser la question de l'utilité de ce correctif, vu qu'il "suffit" de passer à la version 3.0.

4.2 Les différentes mises à jour

Il faut bien comprendre la différence entre les mises à jour fonctionnelles qui apportent des changements au niveau utilisateur, voir au niveau des compatibilités, par exemple lors de l'utilisation de macros et entre les documents produits, et les mises à jour de sécurité qui corrigent des vulnérabilités sans, normalement, rien changer aux fonctionnalités. Les premières sont souvent désignées comme « majeures » par les éditeurs. Les secondes sont parfois considérées comme « mineures », mais peuvent être critiques pour la sécurité. À la vue de ces différences, il apparaît évident que la politique de déploiement n'est pas, ou en tout cas ne devrait pas être la même dans les deux cas. Certains éditeurs tendent à mélanger les deux aspects (fonctionnalité/sécurité) dans des mises à jour communes, la décision de mettre en place le correctif n'est pas toujours simple à prendre.

4.3 Les recommandations

Le CERTA recommande aux administrateurs de connaître et de suivre les « branches » des versions majeures des logiciels utilisés afin de mettre en place les correctifs de sécurité, mais aussi d'avoir une politique de changement de versions majeures, afin que celui-ci ne se fasse pas dans l'urgence. Dans le cas présent, il faut appliquer le correctif de sécurité `OpenOffice.org 2.4.2`, mais cette branche ne sera pas maintenue de nombreux mois et il faut donc commencer à tester le déploiement de la version 3.0.

4.4 Documentation

- Bulletin de sécurité CERTA-2008-AVI-530 du 29 octobre 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-530/index.html>
- Bulletins de sécurité de OpenOffice.org correspondant aux CVE CVE-2008-2237 et CVE-2008-2238 :
<http://www.openoffice.org/security/cves/CVE-2008-2237.html>
<http://www.openoffice.org/security/cves/CVE-2008-2238.html>

5 Article 323-3-1

Il apparaît, ces derniers temps, que beaucoup s'interrogent sur le champ d'application de l'article 323-3-1 du Code Pénal. Cet article prévoit en effet que « le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 (atteintes aux systèmes de traitement automatisé de données) est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ». Afin de comprendre la portée de cet article, il suffit de se référer aux séances de travail relatives à la rédaction de cet article, au cours desquelles M. René TREGOUET explique qu'« il convient de rappeler que cet article n'a ni pour vocation ni pour effet de permettre la sanction pénale d'internautes non avertis qui détiendraient malgré eux un virus informatique ou qui utiliseraient à des fins licites des logiciels d'accès à des ordinateurs distants. En effet, aux termes du 1er alinéa de l'article 121-3 du Code Pénal, tout délit suppose une intention de le commettre si bien que la détention involontaire de programmes malveillants ne peut être poursuivie ».

Concernant des informaticiens, chercheurs, professeurs en SSI... qui souhaiteraient mettre à disposition de leur communauté certains éléments de leurs recherches, ces éléments étant susceptibles d'être utilisés non pour réaliser de la sécurité mais pour exécuter des « attaques », même si leur motif est légitime comme le stipule le texte, il est fortement recommandé d'user, voire d'abuser, du principe de précaution.

6 « Statification » de site web

Le CERTA traite régulièrement des cas de défigurations impliquant des sites web utilisant un gestionnaire de contenu dynamique ou *CMS*. Ce gestionnaire de contenu s'appuie généralement sur le langage PHP pour fonctionner. Or, la plupart du temps l'utilisation de contenu dynamique est superflue. En effet, ces sites ne sont souvent pas des « blogs » mais bien des portails de type informatif dont le contenu évolue peu.

Le fait d'utiliser un langage dynamique n'est pas sans conséquence sur la sécurité globale du site. Il suffit pour s'en convaincre de faire l'inventaire des vulnérabilités pour l'un d'entre eux. Pour la seule année 2008, Drupal a ainsi fait l'objet de 7 avis du CERTA : CERTA-2008-AVI-021, CERTA-2008-AVI-201, CERTA-2008-AVI-365, CERTA-2008-AVI-377, CERTA-2008-AVI-418, CERTA-2008-AVI-488, CERTA-2008-AVI-525. Il n'est cité, ici, que comme exemple ; d'autres ne sont pas en reste : Wordpress (4), Joomla! (6), ... Il s'agit ici des vulnérabilités publiques de ces gestionnaires de contenus : les modules tiers ne sont pas pris en compte sinon la liste s'allonge...

De manière générale, les gestionnaires de contenu, du fait de leur complexité intrinsèque, sont sujets à de nombreuses vulnérabilités : ils comportent de nombreuses lignes de code pour mettre en œuvre de nombreuses fonctions pas toujours indispensables.

Trois solutions peuvent être envisagées pour remédier à ce problème. La première consiste à développer et à maintenir un site statique « maison ». Cette solution peut être adoptée pour de petits sites ne nécessitant que peu de mises à jour.

Une autre solution peut être de conserver un site dynamique « classique » en pré-production et de le « statifier », c'est à dire de le rendre uniquement composé de pages en HTML statiques. Là encore, plusieurs techniques sont possibles. On peut, par exemple, utiliser un analyseur de code transformant les pages PHP en pages HTML. Cette solution est complexe et relativement rare.

Une dernière solution est d'aspirer le site de pré-production avec des outils comme `wget` ou `httrack` puis d'adapter le contenu obtenu pour le mettre en production. Cette dernière méthode est la plus efficace et la plus simple. Elle nécessitera donc tout de même quelques adaptations et post-traitements pour rendre le site statique semblable à son original dynamique. Quelques `scripts` seront sans doute nécessaires pour changer ou éliminer des balises ou des éléments superflus.

Mais, *in-fine*, le jeu en vaut la chandelle car le site mis en production sera exclusivement constitué de pages statiques en HTML « pur » exemptes de tout `javascript` ou autres balises inutiles. Par ailleurs avec une procédure fiable et un ensemble d'outils et de `scripts` adaptés, il sera tout à fait possible de tenir une cadence d'une dizaine de mises à jour par jour avec un site contenant une centaine de pages. L'intérêt est double : une sécurité accrue et une facilité de rédaction conservée puisque l'on utilise le *CMS* pour cela.

7 Des protocoles méconnus

7.1 Présentation de HSRP

HSRP, ou *Hot Standby Router Protocol*, est un protocole propriétaire de Cisco décrit dans le standard RFC 2281. Il a été développé afin de garantir une continuité de service dans le cas d'un dysfonctionnement (cf. figure 1). Pour cela, deux ou plusieurs routeurs physiques présentent un routeur virtuel qui sera celui vu par les machines du réseau (l'adresse IP de la passerelle de leur configuration réseau). Un seul des routeurs physiques sera effectivement actif et transfèrera les paquets dans le réseau, les autres se mettant en attente. Cette opération est transparente pour les machines du réseau. L'activité des routeurs se fait en définissant des priorités (la valeur 100 étant attribuée par défaut et 255 étant la valeur maximale). Pour deux priorités de valeur équivalente, c'est le routeur ayant une adresse IP la plus « élevée » qui l'emporte.

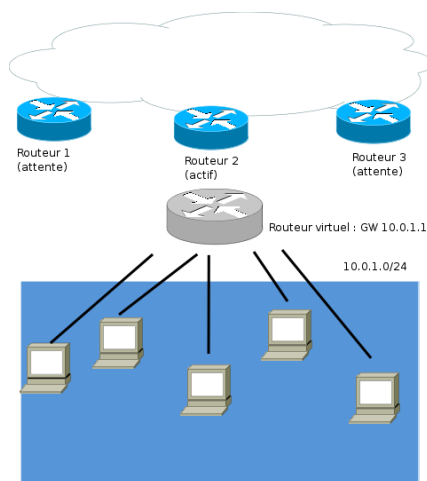


FIG. 1: Présentation générale d'une configuration pouvant exploitée HSRP

Les priorités sont en principe annoncées par des trames *multicast* à destination de l'adresse 224.0.0.2 et du port par défaut 1985/UDP (champ *Time-To-Live* TTL de valeur 1 normalement). Ces trames, dites `Hello`, sont envoyées par défaut toutes les trois secondes. Elles contiennent toutes les informations nécessaires pour construire un faux routeur qui souhaite devenir actif ou forcer les routeurs existants à se mettre tous en mode d'attente et ainsi effectuer un déni de service.

Cette action malveillante peut être effectuée par plusieurs outils d'attaque automatiques, mais aussi par des applications permettant de construire et manipuler simplement des trames.

Pour limiter ce genre d'actions malveillantes, il est possible de :

- regarder les adresses MAC utilisées. Celle annoncée par le « routeur virtuel » est une adresse Cisco, par défaut `00:00:0c:07:ac:01` ;
- filtrer sur les équipements de bordure les trames illégitimes à destination du port UDP 1985 ;
- filtrer sur les équipements de bordure les trames multicast qui n'ont pas raison d'être ;
- mettre en place des interfaces dédiées pour les communications et synchronisations entre équipements ;

- utiliser le mécanisme proposé par Cisco et basé sur une authentification par condensat de type MD5 pour éviter que le mot de passe de groupe transite en clair.

7.2 Au-delà de ce protocole

Il existe des protocoles alternatifs qui ont les mêmes vocations, comme :

- VRRP (*Virtual Router Redundancy Protocol*), décrit dans le standard RFC 3768. Il fonctionne de manière assez similaire à HSRP, l'adresse MAC annoncée par le routeur virtuel étant cette fois de la forme 00:00:5E:00:01:XX et l'adresse multicast étant 224.0.0.18 (TTL de 255). L'authentification peut être absente. Le standard ne donne pas de directive particulière sur les mesures d'authentification, au contraire de sa première version RFC 2338. La phase d'authentification peut sinon se présenter comme un simple échange de mot de passe clair ou une méthode IPsec AH (*Authentication Header*) afin d'apporter une garantie d'intégrité et d'origine des trames.
- GLBP (*Gateway Load Balancing Protocol*)
- CARP (*Common Address Redundancy Protocol*) sous BSD et dérivé sous Linux par le projet UCARP libre et disponible depuis fin 2003. La documentation n'est cependant pas excessivement fournie. Le code source reste le meilleur descriptif du fonctionnement. La variable système `sysctl` associée `net.inet.carp.allow` est activée par défaut. La priorité porte alors le nom de `advskew`. Un mot de passe est utilisé avec une solution SHA1 HMAC pour éviter certaines tentatives d'usurpation de trames.

7.3 Ce qu'il faut en retenir

L'objet n'est pas ici de pointer une solution plutôt qu'une autre, mais de comprendre que chaque service lancé n'est pas « magique », même si ce dernier a pour finalité d'améliorer la disponibilité du réseau. Il est important en terme de sécurité d'en comprendre le mécanisme. Un abus de ces fonctionnalités peut avoir des conséquences dramatiques.

7.4 Documentation associée

- RFC 2281, « Cisco Hot Standby Router Protocol », mars 1998 :
<http://tools.ietf.org/rfc/rfc2281.txt>
- RFC 3768, « Virtual Router Redundancy Protocol », avril 2004 :
<http://tools.ietf.org/rfc/rfc3768.txt>
- Projet UCARP :
<http://ucarp.org>
- Documentation Cisco, « Using HSRP for Fault-Tolerant IP Routing » :
<http://www.cisco.com/en/US/docs/internetworking/case/studies/cs009.html>
- Documentation Cisco, « HSRP MD5 Authentication » :
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gthsrpau.html
- CERT-IST, « Faiblesse du protocole HSRP de Cisco » :
http://www.cert-ist.com/fra/resources/Publications_ArticlesBulletins/Environnementreseau/HSRP_Cisco/
- Documentation OpenBSD concernant CARP :
<http://openbsd.org/faq/faq6.html#CARP>
- Countersiege.com, « Firewall Failover with pfsync and CARP » :
<http://www.countersiege.com/doc/pfsync-carp/>
- Documentation Cisco, "Cisco Guide to Harden Cisco IOS Devices", id 13608 :
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

8 Ports observés

Le tableau 3 et la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 23 et le 30 octobre 2008.

9 Liens utiles

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

10 Rappel des avis émis

Dans la période du 24 au 31 octobre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-522 : Vulnérabilités dans Cisco PIX et ASA
- CERTA-2008-AVI-523 : Vulnérabilité dans Windows Service Server
- CERTA-2008-AVI-524 : Multiples vulnérabilités du navigateur Opera
- CERTA-2008-AVI-525 : Multiples vulnérabilités dans Drupal
- CERTA-2008-AVI-526 : Vulnérabilité dans la bibliothèque libspf2
- CERTA-2008-AVI-527 : Multiples vulnérabilités dans Moodle
- CERTA-2008-AVI-528 : Multiples vulnérabilités dans VLC media player
- CERTA-2008-AVI-529 : Vulnérabilité dans SquirrelMail
- CERTA-2008-AVI-530 : Multiples vulnérabilités dans OpenOfficeorg
- CERTA-2008-AVI-531 : Vulnérabilité dans ftpd
- CERTA-2008-AVI-532 : Multiples vulnérabilités dans Novell eDirectory
- CERTA-2008-AVI-533 : Multiples vulnérabilités dans IBM Lotus Connections
- CERTA-2008-AVI-534 : Multiples vulnérabilités dans Opera
- CERTA-2008-AVI-535 : Vulnérabilités dans Adobe PageMaker
- CERTA-2008-AVI-536 : Vulnérabilité dans Citrix

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 :

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.

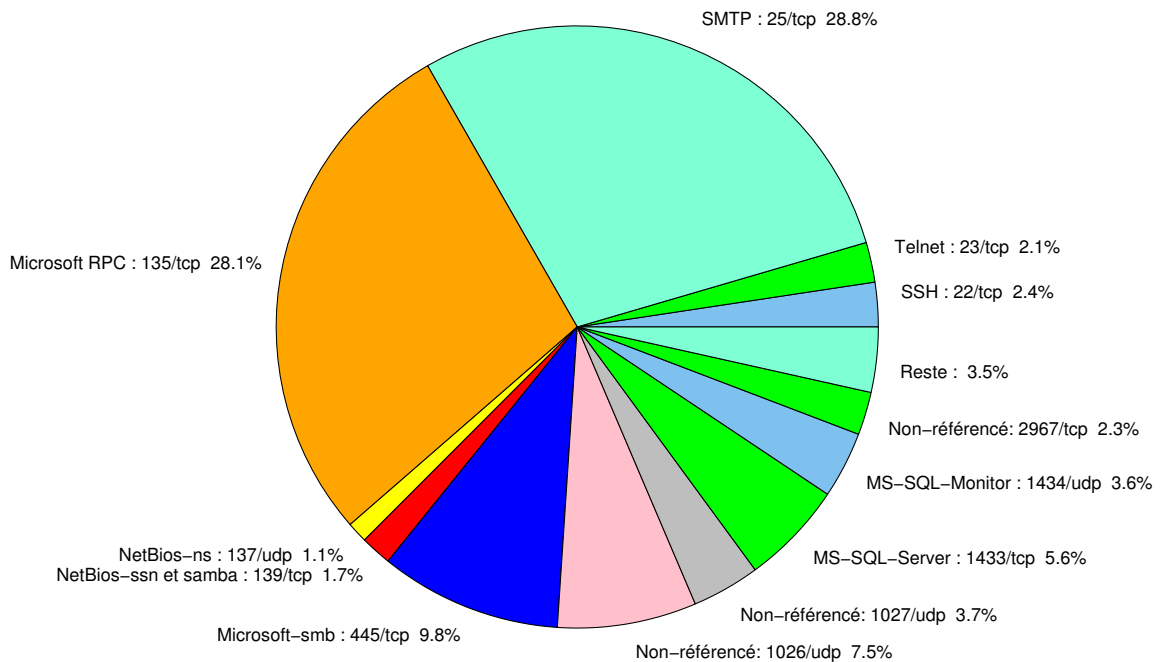


FIG. 2: Répartition relative des ports pour la semaine du 23.10.2008 au 30.10.2008

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	28.75
135/tcp	28.19
445/tcp	9.76
1026/udp	7.46
1433/tcp	5.55
1027/udp	3.65
1434/udp	3.57
22/tcp	2.38
2967/tcp	2.3
139/tcp	1.66
137/udp	1.11
1080/tcp	0.79
4899/tcp	0.55
111/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	11
3	Paquets rejetés	12

Gestion détaillée du document

31 octobre 2008 version initiale.