

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-39

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-039>

Gestion du document

Référence	CERTA-2008-ACT-039
Titre	Bulletin d'actualité 2008-39
Date de la première version	26 septembre 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-039.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-039/>

1 Incidents traités cette semaine

Cette semaine, le CERTA a été informé d'un incident touchant un site Internet de l'administration, hébergé sur plusieurs serveurs pour des raisons de trafic important. Un intrus a pu se connecter à la page d'administration du site car le mot de passe utilisé était faible. La page était normalement accessible uniquement depuis certaines adresses IP via des ACL (*Access Control List*). Toutefois, l'un des serveurs n'était pas configuré correctement et, contrairement aux autres, ne filtrait donc pas les accès via ces ACL.

Cet incident montre tout d'abord l'intérêt de la défense en profondeur : un moyen de protection ne justifie pas de ne pas en avoir d'autres en aval (dans ce cas précis, l'utilisation d'un mot de passe fort même s'il y a un filtrage sur les adresses IP).

De plus, cet incident met l'accent sur des problèmes de configuration dans des systèmes redondants où il faut bien s'assurer que chacun dispose des mêmes moyens de protection.

La problématique associée à cet incident est relativement courante. Le CERTA avait par exemple traité, il y a quelques semaines, un problème lié à l'existence d'un serveur de secours mal sécurisé qui était accessible depuis l'Internet contrairement à ce qui était préconisé par la politique de sécurité de l'organisme.

D'une manière générale, de nombreux organismes ont recours à la réplication de données et/ou de services (serveurs pour supporter la charge, serveur de secours en cas de panne, etc.). Toutefois, les aspects de sécurité sont

parfois absents de ce processus. Lors de la préparation et de la maintenance de tels serveurs, il est donc important de veiller à l'application des règles de sécurité définies par la PSSI, par exemple :

- règles de filtrage ;
- mises à jour ;
- utilisation de mots de passe différents ;
- changement régulier des mots de passe ;
- etc.

2 Mise à jour du navigateur Mozilla Firefox

Le CERTA a publié cette semaine l'avis CERTA-2008-AVI-473 signalant l'annonce de plusieurs avis de sécurité pour des produits Mozilla.

Certains d'entre eux concernent les versions du navigateur de la branche 3.0.X :

- MFSA 2008-40 : une page malveillante peut abuser de l'opération de "clic" sur le bouton d'une souris pour forcer l'utilisateur à télécharger ou déplacer des objets plutôt que de se déplacer à l'adresse du lien. Cette vulnérabilité nécessite l'activation de JavaScript, et en particulier l'option avancée « Autoriser les scripts à : Déplacer ou redimensionner des fenêtres existantes » ;
- MFSA 2008-41 : certaines vulnérabilités permettent à des scripts JavaScript d'exécuter du code arbitraire avec les droits attribués à chrome et donc au navigateur ;
- MFSA 2008-42 : le rendu d'images ne serait pas correctement géré, pouvant entraîner, dans certaines conditions, une corruption de la mémoire ;
- MFSA 2008-43 : la marque d'ordre des octets BOM (*Byte Order Mark*) n'est pas correctement manipulée avec un code JavaScript, pouvant ainsi permettre de contourner certaines politiques de filtrage de scripts ;
- MFSA 2008-44 : le protocole `resource:` n'est pas correctement manipulé. Il pourrait être exploité pour accéder illégalement à des répertoires. Ce protocole avait déjà fait l'objet de correctifs (cf. section 4, CERTA-2007-ACT-020).

La première remarque consiste à rappeler le bon usage d'un navigateur Internet : il faut bloquer par défaut toute exécution de code dynamique et ne l'autoriser que ponctuellement sur des sites de confiance.

La seconde remarque concerne la mise à jour et le passage du navigateur en version 3.0.2. Ce passage semble poser problème à l'outil de gestion de mots de passe, qui n'arriverait pas à récupérer correctement certains d'entre eux pour des sites dont le nom de domaine associé contiendrait des caractères autres que ceux appartenant au jeu ASCII.

Cette vulnérabilité incite les développeurs Mozilla à publier une nouvelle version, la 3.0.3 dans les prochains jours. Celle-ci fera l'objet d'un nouvel avis du CERTA.

Ce problème permet néanmoins de rappeler qu'il est préférable de ne pas stocker les mots de passe localement sur le poste. Celui-ci peut être compromis et fournir l'accès à toute la liste de mots de passe. Une note d'information abordant la gestion des mots de passe se trouve sur le site du CERTA : CERTA-2005-INF-001.

Pour conclure cet article, le CERTA rappelle également que Mozilla a annoncé ne plus maintenir les correctifs de sécurité et de stabilité de la branche 2.0.0.X du navigateur à partir de mi-décembre 2008. La migration doit d'ores et déjà être préparée.

- Page de téléchargement et d'avertissement de Mozilla pour la branche 2.0.0.X :
<http://www.mozilla.com/en-US/firefox/all-older.html>
- CERTA-2008-ACT-018, « Interprétation d'URI », 02 mai 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-018/>
- CERTA-2007-ACT-020, « Fuite d'informations sous Mozilla Firefox », 18 mai 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-020/>
- CERTA-2008-ACT-022, « Des problèmes avec Mozilla Firefox », 01 juin 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-022/>
- Note d'information, CERTA-2005-INF-001, « Les mots de passe » :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>

3 Les publications de sécurité Cisco

Le CERTA a publié cette semaine l'avis CERTA-2008-AVI-474. Ce dernier reprend l'ensemble des avis de correctifs de sécurité des produits Cisco publiés le 24 septembre 2008. Les correctifs sont relativement nombreux.

Comme cela avait été annoncé dans le bulletin d'actualité CERTA-2008-ACT-011 du 14 mars 2008, les mises à jour de sécurité pour Cisco *Internetwork Operating System* (IOS) s'effectuent maintenant deux fois par an, dont l'une dans le courant du mois de septembre (le quatrième mercredi de mars et de septembre pour être précis).

Ce mois-ci douze avis de sécurité ont ainsi été publiés, corrigeant seize vulnérabilités. L'exploitation de ces vulnérabilités se fait au moyen de paquets spécialement construits puis émis à distance. Il s'agit de vulnérabilités associées à la gestion de protocoles de voix sur IP (Skinny SCCP, SIP) mais aussi de plus courants comme DNS, HTTP ou SSL, ainsi que le mécanisme d'encapsulation et de commutation de données MPLS dans une architecture VPN.

Les conséquences des exploitations sont principalement des dénis de service.

La vulnérabilité CVE-2008-3803 peut quant à elle provoquer une fuite d'information. Certains équipements PE (*Provider Edge*) configurés pour des VPN MPLS ou VRF Lite (*Virtual Routing and Forwarding*) ne gèrent pas correctement les communautés étendues BGP. Lorsque celles-ci sont utilisées, le trafic peut être détourné vers une cible de routage (RT ou *Route Target*) différente.

Le CERTA rappelle à cette occasion que les équipements de réseau dits *Intrusion Prevention Systems* (IPS) et les filtres des couches applicatives (comme Cisco *Application Inspection Control*) peuvent être exposés aux trames malveillantes et ne sont pas moins vulnérables que d'autres systèmes. Dans le cas d'un déni de service, c'est non seulement le service de filtrage/détection qui n'est plus rendu, mais c'est potentiellement tout le trafic transitant par l'équipement qui peut être ainsi bloqué.

Il est donc important de considérer ces équipements de sécurité comme des éléments pouvant aussi avoir un impact sur l'accès à plusieurs services en aval.

4 Mandataire transparent et serveurs DNS publics

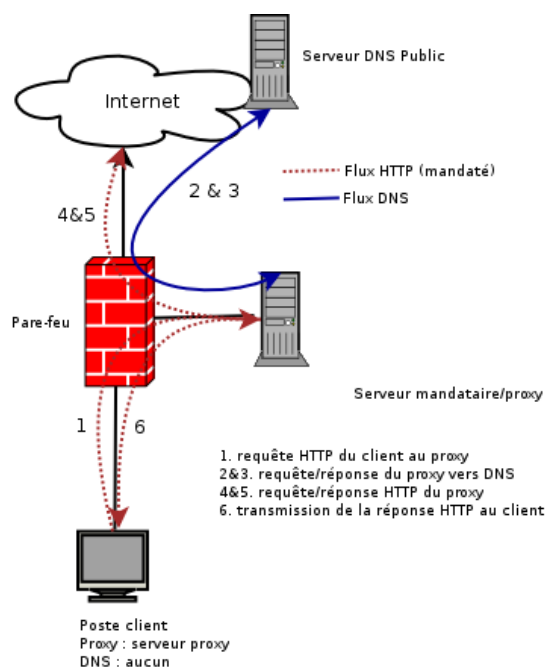


FIG. 1: Fonctionnement classique d'un mandataire avec DNS public

Le principal avantage d'un serveur mandataire web (*proxy*) est de se substituer aux clients réels d'un réseau local pour effectuer des requêtes, généralement HTTP vers des serveurs publics de l'Internet (cf. 1).

L'inconvénient de ce genre de technologie est l'obligation pour le navigateur (ou le client de manière générale) de supporter cette fonctionnalité et l'obligation d'indiquer au navigateur l'adresse de ce mandataire pour commu-

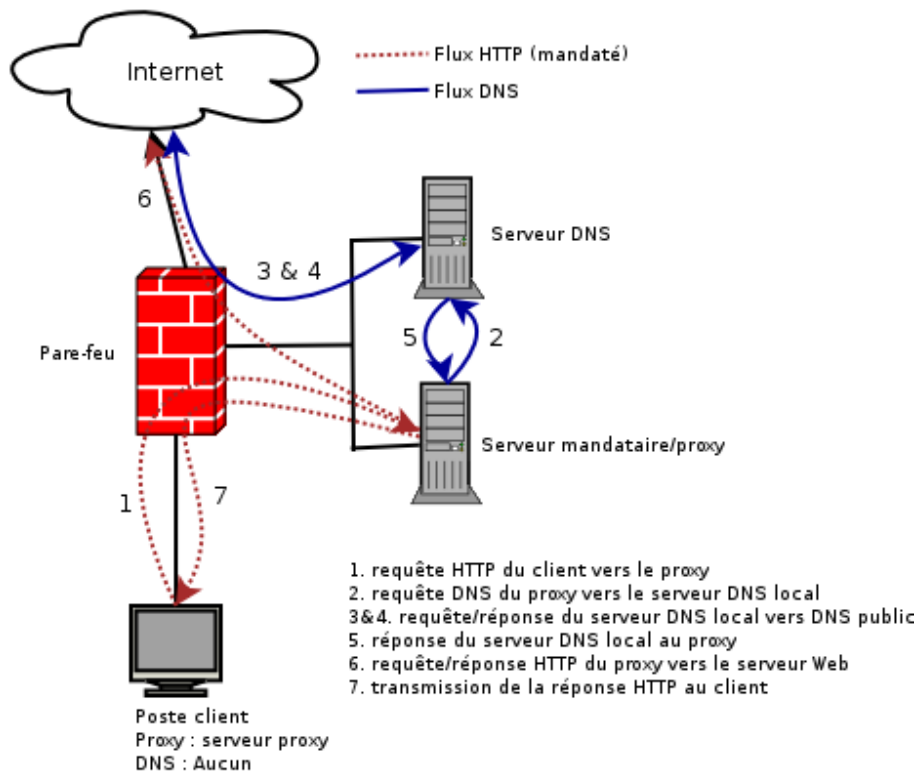


FIG. 2: Fonctionnement classique d'un mandataire avec DNS cache interne

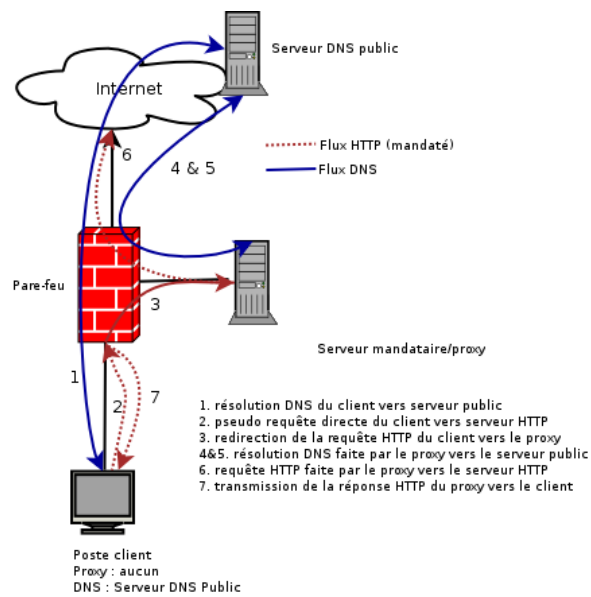


FIG. 3: Fonctionnement d'un mandataire transparent avec DNS public

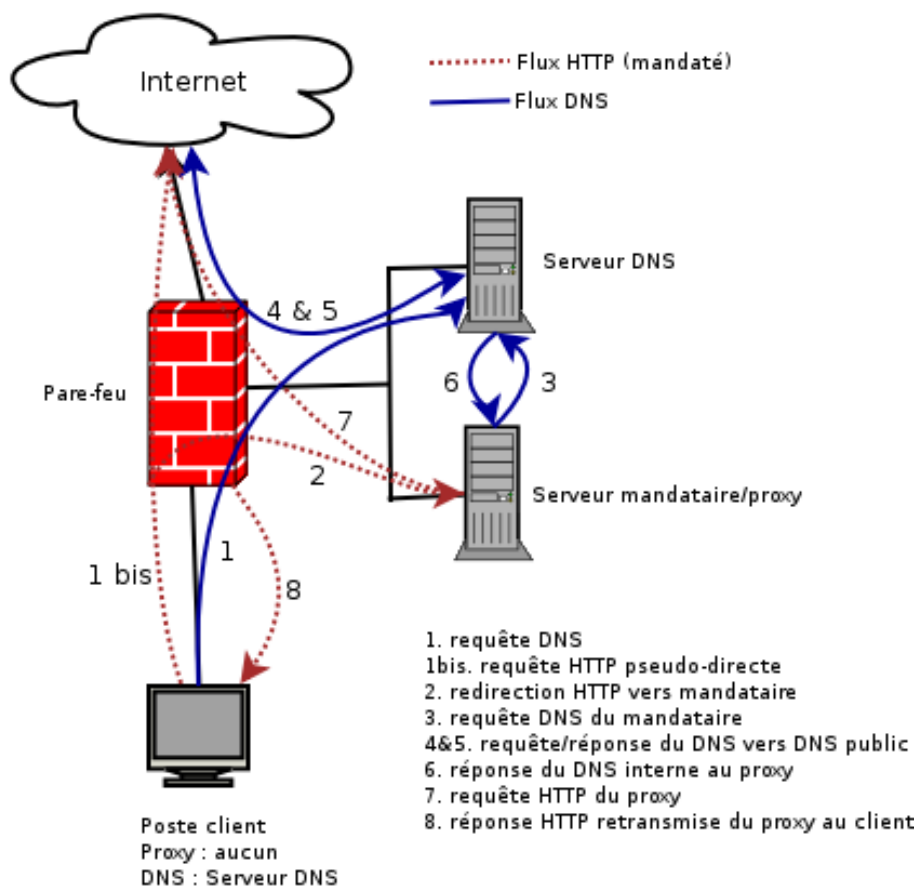


FIG. 4: Fonctionnement d'un mandataire transparent avec DNS cache interne

niquer avec l'extérieur plutôt qu'avec l'extérieur directement. Dans le cas des mandataires HTTP, non seulement la requête vers le serveur web sera effectuée par le « proxy », mais aussi ce dernier s'occupera de la résolution de nom (DNS). Les postes clients n'ont pas besoin de connaître un serveur DNS. Ils doivent simplement disposer de l'adresse du serveur mandataire vers lequel seront envoyées les requêtes. L'idéal consiste à avoir un serveur DNS interne qui mettra en cache les requêtes du serveur mandataire (cf. 2).

Ainsi, sur un parc important, il conviendra de prévoir une politique de diffusion de configuration de navigateur pour qu'ils puissent prendre en compte cet aspect de l'architecture réseau.

Un inconvénient est qu'un utilisateur peut éventuellement modifier la configuration et passer outre le serveur *proxy*. S'il existe une politique de filtrage des flux vers l'Internet, il ne pourra plus surfer mais, en l'absence d'une telle politique, il pourra directement naviguer sur l'Internet sans passer par le mandataire.

Une solution envisageable est d'utiliser un mandataire transparent. Cette technique consiste à rediriger les flux « à mandater » vers le mandataire par le biais d'un pare-feu configuré de façon particulière. Ainsi, un flux (typiquement le HTTP : 80/tcp) sera mandaté, quel que soit la configuration des clients.

Cependant dans ce cas de figure, un cache DNS local devient indispensable pour garantir un bon cloisonnement du réseau. En effet, si les clients utilisent un serveur DNS public pour effectuer la résolution de nom, on aura un double requêtage DNS, l'un fait par le client et l'autre fait par le mandataire (cf. 3). En effet, comme la redirection du flux « mandaté » se fait de façon transparente pour le client, ce dernier devra disposer d'une configuration DNS *a priori* valide car indispensable à une requête HTTP (on doit connaître l'adresse IP de la machine avant de lui demander une page web).

Il est donc indispensable de disposer d'un serveur cache DNS interne pour garantir un bon cloisonnement lorsque l'on met en œuvre un système de mandataire transparent. Certes, le double de requêtes DNS sera nécessaire à un bon fonctionnement (une du client, une du mandataire), mais aucun flux direct vers l'extérieur ne sera nécessaire (cf. 4).

5 Fausse croyance sur les portées du Bluetooth

Dans la note d'information CERTA-2007-INF-003, publié le 01 août 2007, le chapitre 4.2 faisait mention du savoir-faire disponible sur l'Internet et permettant d'augmenter la portée de réception et/ou d'émission d'un équipement Bluetooth initialement limité à 100m dans sa dernière version.

Un équipementier a récemment commercialisé une interface Bluetooth permettant d'obtenir une portée effective de 100m. Dans sa meilleure configuration, la portée peut atteindre environ 30km (selon le type d'antenne, son gain et l'environnement).

Cette information s'inscrit dans la continuité des risques liés à l'usage des technologies sans-fil et surtout Bluetooth, à savoir que le faux sentiment de sécurité créé par la notion de communication de courte portée n'est pas fondé. Ceci oblige l'utilisateur à rester vigilant lors de l'utilisation de la technologie Bluetooth. Il n'a pas (ou très peu) de maîtrise sur les interactions qu'il peut y avoir entre un élément extérieur et son interface. Il doit la désactiver physiquement par défaut.

- Note d'information CERTA-2007-INF-003, « Sécurité des réseaux sans fil Bluetooth » : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/>

6 Des en-têtes qui vous desservent

L'année dernière, le CERTA a publié dans son bulletin CERTA-2007-ACT-014 quelques recommandations concernant la réponse automatique aux demandes d'accusés de réception des courriers électroniques. Il était écrit que le renvoi de ces accusés de réception peut participer à de la fuite d'information.

Un exemple concret de fuite d'information par ce biais vient d'apparaître ces dernières semaines. En effet, quelques *spam* utilisent cette fonctionnalité afin de valider la lecture du courriel par une personne physique. Ceci permet aux auteurs de campagnes de courriels non sollicités de confirmer les adresses destinataires et de créer des statistiques précises sur ces adresses (type de client de messagerie, affichage de code HTML, nom précis de la personne, etc.).

Techniquement, cela repose sur l'insertion d'un champ MIME optionnel dans l'en-tête du message non sollicité : *X-Confirm-Reading-To*. Ce champ est considéré comme champ optionnel dans les différentes RFC caractérisant les en-têtes mail.

Deux solutions peuvent être appliquées. La première, centrée sur le poste de travail, consiste à configurer les clients de messagerie afin de ne pas répondre automatiquement à ce genre de message. Pour cela :

- dans **Microsoft Outlook** : Outils -> Options -> Options de la messagerie -> Option de suivi : vérifier que l'option *toujours envoyer une réponse* n'est pas cochée ;
- dans **Mozilla Thunderbird** : Edition -> Préférences -> Rédaction -> Général -> Accusé de réception : vérifier que l'option *toujours envoyer* n'est pas cochée.

La deuxième consiste à supprimer de l'en-tête l'option *X-Confirm-Reading-To* au niveau du serveur de messagerie entrante. Cette disposition spécifique ayant un impact réel sur la production doit cependant être réfléchie et rester en accord avec la politique de sécurité. Il n'est en effet pas anodin de filtrer ou supprimer un champ pourtant prévu dans une RFC, même s'il s'agit d'un champ optionnel.

7 Ports observés

Le tableau 3 et la figure 5 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 18 et le 25 septembre 2008.

8 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/>

9 Rappel des avis émis

Dans la période du 18 au 26 septembre 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-468 : Vulnérabilité dans Sun Solaris
- CERTA-2008-AVI-469 : Vulnérabilité dans ISC BIND sous Microsoft Windows
- CERTA-2008-AVI-470 : Vulnérabilité dans des produits VMware
- CERTA-2008-AVI-471 : Vulnérabilité de ProFTPD
- CERTA-2008-AVI-472 : Vulnérabilité dans HP-UX
- CERTA-2008-AVI-473 : Multiples vulnérabilités des produits Mozilla

- CERTA-2008-AVI-474 : Multiples vulnérabilités dans Cisco IOS

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

- CERTA-2008-AVI-453-001 : Vulnérabilités de WordPress
(ajout de références CVE)
- CERTA-2008-AVI-456-001 : Vulnérabilités de Joomla!
(ajout des références CVE)
- CERTA-2008-AVI-464-001 : Vulnérabilité dans phpMyAdmin
(ajout de la référence CVE)

10 Actions suggérées

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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>

11 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.

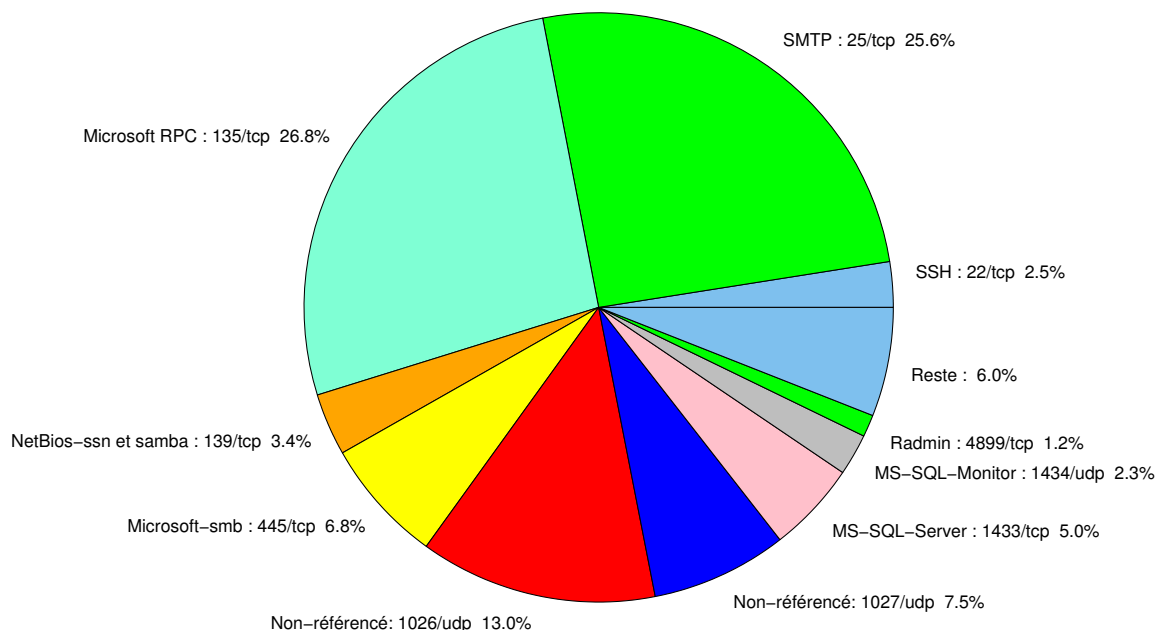


FIG. 5: Répartition relative des ports pour la semaine du 18.09.2008 au 25.09.2008

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
135/tcp	26.76
25/tcp	25.55
1026/udp	13.02
1027/udp	7.47
445/tcp	6.83
1433/tcp	4.98
139/tcp	3.41
22/tcp	2.49
1434/udp	2.27
4899/tcp	1.35
1080/tcp	0.99
80/tcp	0.92
3128/tcp	0.71
3389/tcp	0.64
21/tcp	0.42
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

26 septembre 2008 version initiale.