Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 août 2006
N° CERTA-2006-ACT-031

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-31

Gestion du document

Référence	CERTA-2006-ACT-031
Titre	Bulletin d'actualité 2006-31
Date de la première version	04 août 2006
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-2006-ACT-031.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-2006-ACT-031/

1 Activité en cours

1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 27 juillet et le 03 août 2006.

1.2 Injection de code indirecte

Le CERTA a traité plusieurs incidents relatifs à `l'injection de code indirecte` (ou *cross site scripting*) sur certains sites de l'administration. Conformément à la terminologie d'usage au CERTA, le *cross site scripting* est une activité malveillante qui consiste à injecter des données arbitraires dans le code de pages HTML. Un utilisateur malveillant peut faire afficher à un site web vulnérable un contenu agressif ; ce contenu peut rediriger l'utilisateur vers d'autres sites, ou transmettre des informations (jetons de sessions, aussi appelés cookies, etc) ou des droits.

On remarque que les données arbitraires sont souvent écrites en javascript, en html ou en vbscript. La personne malveillante introduit ainsi du code dans le serveur vulnérable qui héberge le site. Ce serveur est rarement affecté par ce code (porteur sain). Les visiteurs du site, potentiellement victimes, consultent la page contenant le code injecté. L'exécution du code ne se fait pas au niveau du serveur, mais par le client de navigation de l'utilisateur. La notation XSS a été introduite pour remplacer CSS, acronyme déjà utilisé pour signifier Cascading Style Sheet.

Les risques engendrés par cette vulnérabilité sont liés au langage de script utilisé pour réaliser l'attaque par « Cross Site Scripting ». Si, par exemple, le langage javascript est utilisé, il est alors possible :

– d'afficher une fenêtre demandant à l'utilisateur de rentrer son login et son mot de passe puis de valider, après quoi le résultat sera alors envoyé par mél à l'attaquant ;
– de récupérer les cookies de la machine victime ;
– d'exécuter des commandes système...

Les risques liés à cette vulnérabilité sont donc nombreux : déni de service de la machine victime, utilisation de la machine victime à des fins malveillantes, récupération de données personnelles, vol d'identification de connexion.

Pour se protéger, les utilisateurs doivent, dans la mesure du possible, suivre les recommandations, souvent énoncées par le CERTA :

– éviter de cliquer de façon inconsidérée sur les différents liens insérés dans les messages électroniques ;
– naviguer sur des sites de confiance : cela signifie, dans ce contexte, sur des sites sur lesquels il n'y aurait pas, *a priori*, de liens malveillants ;
– désactiver le javascript sur leur navigateur.

Pour limiter les risques, les concepteurs ou administrateurs de sites web doivent impérativement prévoir un contrôle sur le contenu des différents champs d'un formulaire, ou, de manière plus générale, sur toute donnée que le site est susceptible de récupérer suite à la navigation d'un utilisateur. Ces contrôles peuvent par exemple porter sur la longueur du contenu, sur la présence d'une redirection, sur la présence de caractères spéciaux (comme '>' et '<'), etc ; sans oublier pour autant l'application des correctifs.

Références:

– Terminologie d'usage au CERTA :
http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
– Vulnérabilité de type « Cross Site Scripting » :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/

2 Récapitulatif des différentes mises à jour Mozilla

Le CERTA a mentionné des produits Mozilla dans plusieurs documents ces dernières semaines. Parmi ceux-ci, il faut noter :

– *CERTA-2006-AVI-227* : cet avis a été mis à jour, suite aux modifications apportées par certaines distributions Linux pour corriger les vulnérabilités détaillées dans le bulletin de sécurité Mozilla du 01 juin 2006. Ce dernier nécessite le changement de version des produits Firefox et Thunderbird qui évoluent en 1.5.0.4.
– *CERTA-2006-AVI-312* : cet avis du CERTA fait suite au bulletin de sécurité Mozilla du 27 juillet 2006, et implique le changement de version des produits Firefox et Thunderbird en 1.5.0.5. Plusieurs vulnérabilités (14 références citées) sont corrigées, celles-ci permettant à un utilisateur malveillant de provoquer un déni de service, de réaliser une attaque de type *cross site scripting* ou d'exécuter du code arbitraire à distance. Une majorité de ces vulnérabilités sont issues du module Javascript.

Le 02 août 2006, Mozilla a mis à disposition sur son site une nouvelle version de Firefox et Thunderbird : 1.5.0.6. Cette version n'est pas une mise à jour de sécurité, mais corrige un problème de compatibilité avec des fichiers Windows Media.

3 Serveur Web et modules associés

Le CERTA a publié cette semaine un avis concernant une vulnérabilité présente dans un module d'`Apache httpd` (CERTA-2006-AVI-315). Elle concerne une erreur dans le module *Rewrite* (`mod_rewrite`) généralement inclus dans Apache, mais pas systématiquement chargé par défaut. Ce module permet la ré-écriture à la volée d'URLs et s'utilise parfois pour les besoins internes du serveur httpd dans certaines distributions GNU/Linux. Il est donc recommandé d'effectuer les mises à jour.

De manière générale, il est important de passer en revue les différents modules activés dans la configuration d'`Apache httpd` et, le cas échéant, de les désactiver s' ils ne sont d'aucune utilité. Le plus souvent, ceux-ci sont visibles dans le fichier `httpd.conf`. Les modules utilisés se manifestent par une ligne débutant par `LoadModule` et `AddModule`. Ceux commentés ont été inclus pendant la compilation mais ne sont pas chargés par défaut. Toute modification de ce fichier ne prend effet qu'après arrêt et redémarrage du service Apache httpd.

4 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
  http://www.auscert.org.au/render.html?it=1935

5 Rappel des avis et mises à jour émis

Durant la période du 28 juillet au 03 août 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-315 : Vulnérabilité dans Apache httpd
- CERTA-2006-AVI-316 : Multiples vulnérabilités des pilotes Microsoft pour Intel Centrino PRO/Wireless
- CERTA-2006-AVI-317 : Multiples vulnérabilités dans Mac OS X
- CERTA-2006-AVI-318 : Vulnérabilité dans les produits McAfee
- CERTA-2006-AVI-319 : Vulnérabilité dans la librairie libgd
- CERTA-2006-AVI-320 : Vulnérabilités Symantec
- CERTA-2006-AVI-321 : Vulnérabilité dans la bibliothèque libwmf
- CERTA-2006-AVI-322 : Multiples vulnérabilités dans Ruby
- CERTA-2006-AVI-323 : Vulnérabilité dans PowerArchiver
- CERTA-2006-AVI-324 : Vulnérabilité dans Dokeos
- CERTA-2006-AVI-325 : Vulnérabilité dans la pile IP de Sun Solaris
- CERTA-2006-AVI-326 : Vulnérabilité dans TCP de Sun Solaris

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2005-AVI-190-003 : Vulnérabilité de divers outils gérant le format ELF
  (ajout de la référence au bulletin de sécurité SGI)
- CERTA-2006-AVI-067-005 : Vulnérabilité sur OpenSSH
  (ajout de la référence au bulletin de sécurité SGI)
- CERTA-2006-AVI-229-002 : Vulnérabilité dans SquirrelMail
  (ajout de la référence au bulletin de sécurité SGI)
- CERTA-2006-AVI-294-002 : Vulnérabilité dans Samba
  (ajout des références aux bulletins de sécurité Gentoo, RedHat, Suse, Debian et SGI)
- CERTA-2006-AVI-301-001 : Multiples vulnérabilités dans Ethereal/ Wireshark
  (ajout des références aux bulletins de sécurité Debian, Gentoo et Mandriva)
- CERTA-2006-AVI-312-001 : Multiples vulnérabilités dans les produits Mozilla
  (ajout des références aux bulletins de sécurité Redhat, Ubuntu et SGI)

6 Actions suggérées

6.1 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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

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

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

6.2 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 œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

6.3 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.

6.4 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.

6.5 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.

6.6 Réagir aux incidents de sécurité

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

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

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

6.7 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

7 Les bulletins d'actualité

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

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

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

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

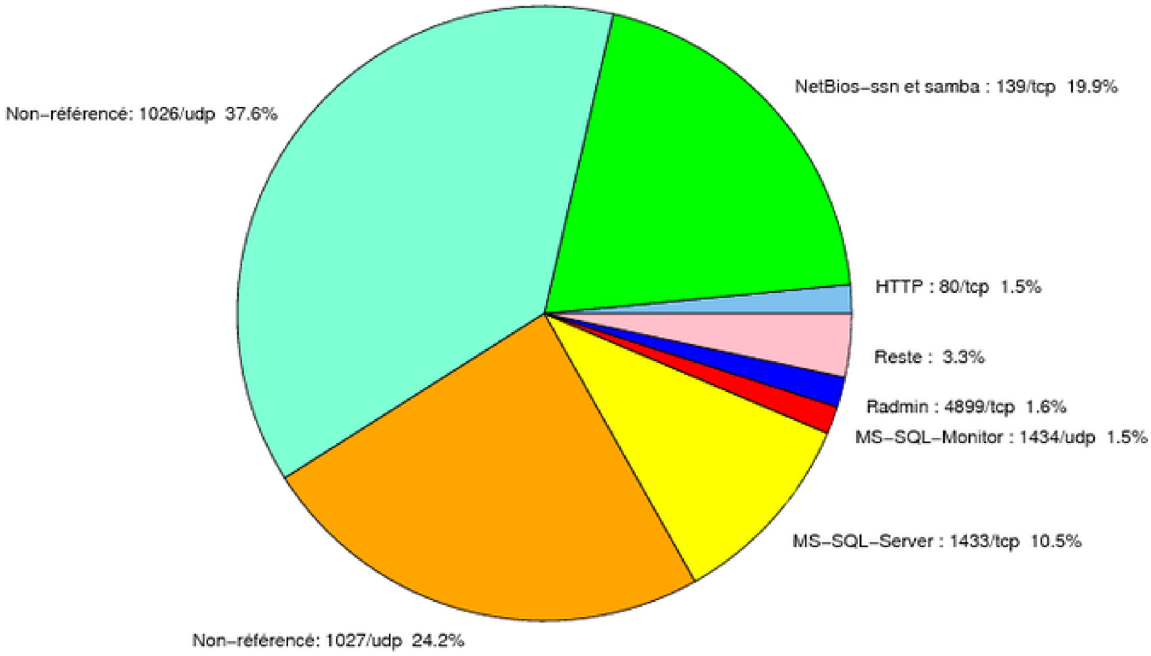

FIG. 1: Répartition relative des ports pour la semaine du 27.07.2006 au 03.08.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERT
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERT
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERT
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERT
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERT
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERT
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERT
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERT
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERT
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–

5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER
6070 6101	TCP TCP	BrightStor ARCserve/Enterprise Backup Veritas Backup Exec	– –	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
15118	TCP	–	Netdepix	–

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

port	**pourcentage**
1026/udp	37.59
1027/udp	24.16
139/tcp	19.89
1433/tcp	10.47
4899/tcp	1.58
80/tcp	1.5
1434/udp	1.45
137/udp	0.65
1080/tcp	0.64
22/tcp	0.53
25/tcp	0.46
3128/tcp	0.18
443/tcp	0.17
3306/tcp	0.13
15118/tcp	0.09
2100/tcp	0.06
9898/tcp	0.05
42/tcp	0.04
6129/tcp	0.03
143/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

04 août 2006 version initiale.