Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 août 2007
N° CERTA-2007-ACT-031

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-31

Gestion du document

Référence	CERTA-2007-ACT-031
Titre	Bulletin d'actualité 2007-31
Date de la première version	03 août 2007
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-2007-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-2007-ACT-031/

1 Les référencements douteux

Cette semaine, le CERTA a rencontré le cas d'un portail web offrant à ses visiteurs des liens relatifs à des sites officiels : administrations, commerciaux, bancaires, ... Les sites demandés sont affichés à l'intérieur du portail par le biais de cadres. Les problèmes soulevés par ce genre de portail sont :

- la sécurité des visiteurs ne peut pas être assurée. Du code malveillant peut être exécuté au moment de l'affichage du site légitime ;
- l'authenticité des sites affichés ne peut être vérifiée. En effet, le gestionnaire du portail peut à tout moment rediriger ses visiteurs vers des sites frauduleux ou de filoutage (*phishing*) ;
- ils tentent d'utiliser la notorité de sites existant à leur profit. De la publicité est généralement ajoutée lors de l'affichage du site légitime ;
- L'image de marque des sites officiels ciblés peut être mise à mal car listée au milieu de sites pour adultes.

Le CERTA rappelle que ce genre de comportement est contraire à la *Netiquette* qui indique les règles de bonne conduite sur l'Internet, comme avoir l'accord du propriétaire d'un site avant de le référencer. Le CERTA rappelle également que pour des raisons de sécurité il est préférable de saisir à la main dans le navigateur l'adresse réticulaire (*URL*) du site désiré. Il est également recommandé aux gestionnaires de site de vérifier régulièrement

les sites les référençant sur l'Internet. Ceci peut être fait en consultant régulièrement les journaux de votre serveur web dans lesquels se trouve le champs Referer.

2 Vulnérabilités sur les produits Mozilla

Un article du bulletin d'actualité CERTA-2007-ACT-030 décrivait une nouvelle vulnérabilité affectant Mozilla Firefox installé sur une machine avec Microsoft Windows XP SP2 avec Internet Explorer 7.

Dans la première publication, la mauvaise gestion d'URI commançant par la chaîne %00 dans FireFox était soupçonnée d'être la cause de la faille. Après quelques jours il s'est avéré que la cause était plus large et non limitée à ce type de chaîne ; le système d'exploitation Microsoft Windows 2003 SP2 a également été cité comme vulnérable. Compte tenu de la criticité de la vulnérabilité, l'équipe de développement de Mozilla Firefox a publié rapidement un correctif. En effet, celui-ci était présent dans la mise à jour vers la version 2.0.0.6 dès le 30 juillet 2007.

Après plusieurs tests, le CERTA a également pu mettre en évidence que le client de messagerie Mozilla Thunderbird était vulnérable via une technique d'attaque similaire à celle utilisée dans Firefox. La fondation Mozilla a d'ailleurs fourni un correctif pour ce logiciel le 01 août 2007 par l'intermédiaire de la mise à jour vers la version 2.0.0.6.

3 Safari pour Windows

Il y a quelques semaines Apple annonçait la disponibilité de son navigateur Safari sous Microsoft Windows. Ce navigateur est basé sur un moteur de rendu différent de Gecko (utilisé par Firefox et SeaMonkey) ou de celui de Internet Explorer. En effet Safari se base sur le moteur KHTML initialement fourni par le projet KDE, un environnement graphique sous GNU/Linux.

Ce fait est plutôt intéressant car le CERTA propose souvent dans ses alertes l'utilisation d'un navigateur dit *« Alternatif »* comme contournement provisoir. L'alerte rappelle souvent qu'il faut bien utiliser un navigateur dont le moteur de rendu varie par rapport à celui affecté par la vulnérabilité. Ainsi, si Firefox est vulnérable, on préférera, par exemple, Opera ou Internet Explorer. A l'inverse, si c'est Internet Explorer, on privilégiera alors plutôt l'un des deux autres.

En ce sens, l'arrivée d'un nouveau navigateur basé sur une autre technologie d'affichage est plutôt positive. Cependant, le CERTA attire votre attention sur le fait qu'à la date de la rédaction de ce bulletin, Safari n'est disponible qu'en version dite « Beta » donc non finalisée. D'ailleurs peu de temps après sa sortie cette version « Beta » faisait déjà l'objet d'un avis du CERTA (CERTA-2007-AVI-265). Plusieurs vulnérabilités importantes ont donc été corrigées, dont quatre au cours de cette semaine (CERTA-2007-AVI-343). Celles-ci permettaient potentiellement l'exécution de code arbitraire.

Recommandation :

Par définition, une version « Beta », « Alpha » ou même « Release Candidate » fait qu'elle est encore en cours de stabilisation ou de fiabilisation. Il est donc déconseillé de l'utiliser dans un environnement de production. Elle peut en revanche faire l'objet de tests ponctuels afin de suivre l'évolution du projet pour un déploiement futur. Ceci est d'ailleurs vrai pour tout logiciel mis en production : il conviendra toujours de préférer les versions stables faisant l'objet de correctifs et de suivis d'erreurs plutôt que des logiciels en cours de développement faisant l'objet de modifications quotidiennes (parfois avec des effets désastreux).

Références

Alerte CERTA-2007-ALE-013 du 27 juillet 2007, mise à jour le 31 juillet 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-013/index.html

4 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 02 août 2007.

5 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
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/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
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB :
  http://www.certa.ssi.gouv.f r/site/CERTA-2000-INF-006/
- Note d'information du CERTA CERTA-2006-INF-009 sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/
- Note d'information du CERTA CERTA-2007-INF-001 sur la gestion des noms de domaine :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/
- Note d'information sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002

6 Rappel des avis émis

Durant la période du 27 juillet au 02 août 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-335 : Multiples vulnérabilités dans certains produits sans-fil Cisco
- CERTA-2007-AVI-336 : Vulnérabilité dans Novell Client
- CERTA-2007-AVI-337 : Multiples vulnérabilités dans des produits Mozilla
- CERTA-2007-AVI-338 : Vulnérabilité dans HP-UX ARPA
- CERTA-2007-AVI-339 : Multiples vulnérabilités dans Apache
- CERTA-2007-AVI-340 : Multiples vulnérabilités dans Apple Mac OS X
- CERTA-2007-AVI-341 : Vulnérabilité dans gpdf
- CERTA-2007-AVI-342 : Vulnérabilité dans IBM Lotus Sametime
- CERTA-2007-AVI-343 : Vulnérabilité dans Apple Safari pour Windows

Pendant la même période, l'avis suivant a été mis à jour :

- CERTA-2007-AVI-138-004 : Vulnérabilité dans file (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2007-AVI-284-001 : Vulnérabilités dans MIT Kerberos 5 (ajout des références aux bulletins de sécurité Gentoo, Debian et SuSE)
- CERTA-2007-AVI-290-001 : Vulnérabilités dans GIMP (ajout des références aux bulletins de sécurité Gentoo, Debian et Ubuntu)
- CERTA-2007-AVI-306-001 : Vulnérabilité de ClamAV (ajout de la référence CVE et des références aux bulletins de sécurité Mandriva et Debian)
- CERTA-2007-AVI-323-002 : Vulnérabilité dans Tcpdump (ajout des références aux bulletins de sécurité Gentoo et Ubuntu)
- CERTA-2007-AVI-327-003 : Vulnérabilité dans BIND (ajout des références aux bulletins de sécurité SuSE et FreeBSD)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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

8 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.

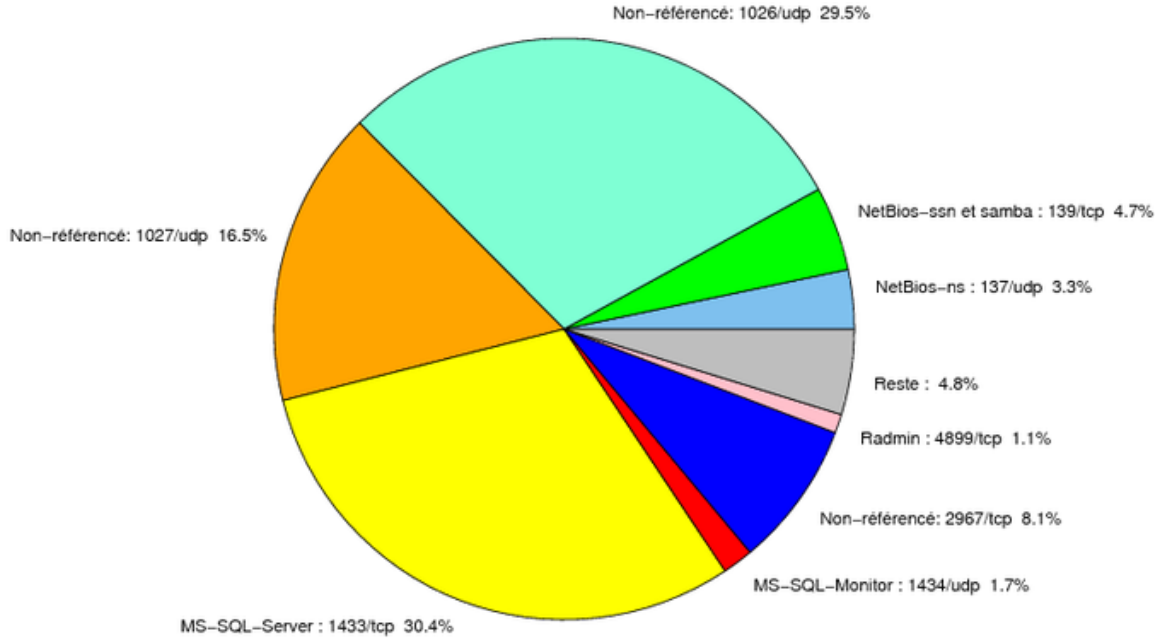

FIG. 1: Répartition relative des ports pour la semaine du 26.07.2007 au 02.08.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE

2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1433/tcp	30.41
1026/udp	29.47
1027/udp	16.49
2967/tcp	8.11
139/tcp	4.69
137/udp	3.29
1434/udp	1.71
4899/tcp	1.05
22/tcp	0.87
1080/tcp	0.62
3306/tcp	0.58
80/tcp	0.42
3128/tcp	0.38
3389/tcp	0.15
23/tcp	0.09
15118/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 7
3 Paquets rejetés 8

Gestion détaillée du document

03 août 2007 version initiale.