

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-28

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-2006-ACT-028>

Gestion du document

Référence	CERTA-2006-ACT-028
Titre	Bulletin d'actualité 2006-28
Date de la première version	13 juillet 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-028.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-028/>

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 07 et le 13 juillet 2006.

2 Problèmes liés à extCalendar

Plusieurs déformations ont été relevées cette semaine, certaines impliquant des sites institutionnels ou académiques. Le traitement de ces incidents, en collaboration avec le CERT Renater, a permis d'identifier dans les journaux la cause de celles-ci. Il s'agit d'une vulnérabilité affectant le produit extCalendar. Ce composant permet de faire apparaître un calendrier. Il s'interface avec les produits Mambo et Joomla!, très souvent utilisés pour développer des sites Internet. L'attaque permet d'acquies les droits du serveur web et de modifier toute page du serveur. La prise de contrôle de la machine est possible et a été constatée dans les incidents traités. La vulnérabilité n'étant pas corrigée, le CERTA a émis une alerte (CERTA-2006-ALE-008) en indiquant un contournement provisoire. Le CERTA appelle l'attention des responsables sécurité et des administrateurs sur les risques d'attaques via

cette vulnérabilité compte tenu du déploiement massif de ce composant. Il est par ailleurs vivement conseillé de n'installer que les modules applicatifs nécessaires au bon fonctionnement du site.

3 Site Web et redirection d'URL

Le traitement d'un incident cette semaine conduit le CERTA a rappelé quelques principes concernant les redirections d'URL (ou adresses réticulaires).

Au niveau applicatif :

Quand une adresse appelle un script qui permet d'insérer un objet référencé sous forme d'une seconde adresse, il est important de vérifier le format de celle-ci. Par exemple, considérons l'adresse de la forme :

```
http://www.A.B/index.php?AfficheObjet insert=http://adresse_Objct.C.D/etc..
```

Il est important de vérifier que le domaine C.D est bien celui de la redirection voulue. Dans le cas contraire, le site peut fonctionner comme un outil de redirection vers d'autres sites. Rien n'empêche alors une personne malveillante d'envoyer un courriel contenant la nouvelle adresse, pour rediriger le lecteur vers un site compromis via le site légitime.

Au niveau du pare-feu :

Le serveur Web n'a souvent aucune raison d'initier des connexions HTTP ou FTP vers des machines extérieures, ou alors il s'agit de sites clairement identifiés. Ces connexions doivent donc être correctement bloquées au niveau du pare-feu séparant le site web du monde extérieur. Cette opération protège également du problème de redirection mentionné ci-dessus.

4 Recommandations pour l'été

Le CERTA souhaite aux lecteurs du bulletin d'actualité d'excellentes vacances d'été. Nous rappelons à cet égard qu'il est important d'identifier au sein de l'administration des systèmes d'information une personne suppléante qui pourra s'occuper des problèmes de sécurité pendant l'été.

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>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1935>

6 Rappel des avis et mises à jour émis

Durant la période du 07 au 12 juillet 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-275 : Vulnérabilité dans phpMyAdmin
- CERTA-2006-AVI-276 : Multiples vulnérabilités dans ATutor
- CERTA-2006-AVI-277 : Vulnérabilité d'OpenOffice.org et StarOffice
- CERTA-2006-AVI-278 : Vulnérabilités dans WebEx

- CERTA-2006-AVI-279 : Vulnérabilité de Shadow
- CERTA-2006-AVI-280 : Vulnérabilité de Qbik WiNGate
- CERTA-2006-AVI-281 : Vulnérabilité de Microsoft .NET Framework
- CERTA-2006-AVI-282 : Vulnérabilité de Microsoft IIS utilisant ASP
- CERTA-2006-AVI-283 : Multiples vulnérabilités du service Serveur de Microsoft Windows
- CERTA-2006-AVI-284 : Vulnérabilités de certains filtres de Microsoft Office
- CERTA-2006-AVI-285 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2006-AVI-286 : Plusieurs vulnérabilités dans les logiciels Microsoft
- CERTA-2006-AVI-287 : Vulnérabilité du client DHCP de Microsoft Windows
- CERTA-2006-AVI-288 : Vulnérabilité d'Adobe Acrobat
- CERTA-2006-AVI-289 : Vulnérabilité IPv6 dans JunOS de Juniper

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'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.

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 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.

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.

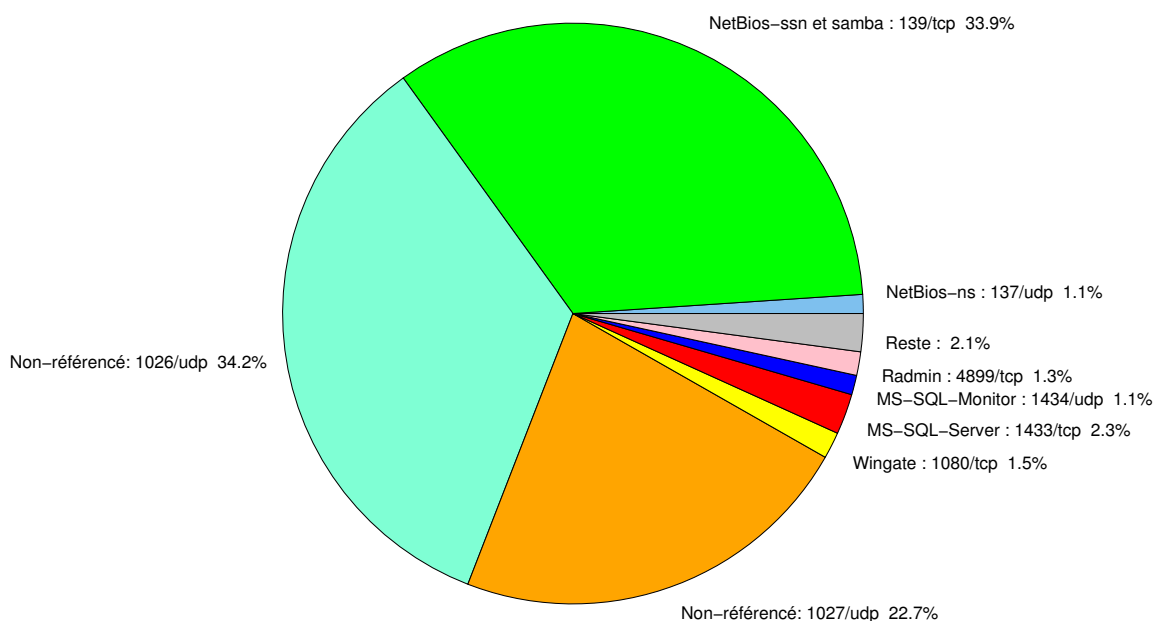


FIG. 1: Répartition relative des ports pour la semaine du 07.07.2006 au 13.07.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	CERTA-2004-AVI-066 CERTA-2004-AVI-064 CERTA-2003-AVI-132
22	TCP	SSH	-	CERTA-2003-AVI-152
23	TCP	Telnet	-	CERTA-2003-AVI-209 CERTA-2003-AVI-131
25	TCP	SMTP	-	CERTA-2006-AVI-124
42	TCP	WINS	-	CERTA-2004-AVI-384
80	TCP	HTTP	-	CERTA-2004-AVI-195 CERTA-2004-AVI-239
106	TCP	MailSite Email Server	-	-
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
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
443	TCP	HTTPS	-	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
445	TCP	Microsoft-smb	-	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302
1023	TCP	-	Serveur ftp de Sasser.E	-
1080	TCP	Wingate	MyDoom.F	-
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
2745	TCP	-	Bagle	-
3127	TCP	-	MyDoom	-
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	-	-
3389	TCP	Microsoft RDP	-	CERTA-2002-AVI-213
4899	TCP	Radmin	-	-
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	-

5900	TCP	VNC	–	CERTA-2006-AVI-198
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
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	–
11768	TCP	–	Netdepix	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
15118	TCP	–	Netdepix	–

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

port	pourcentage
1026/udp	34.16
139/tcp	33.88
1027/udp	22.65
1433/tcp	2.25
1080/tcp	1.48
4899/tcp	1.31
1434/udp	1.08
137/udp	1.05
80/tcp	0.55
22/tcp	0.54
25/tcp	0.26
3306/tcp	0.21
3128/tcp	0.14
443/tcp	0.09
6129/tcp	0.08
143/tcp	0.06

TAB. 3: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Correctifs associés aux ports destination des paquets rejetés	6
3	Paquets rejetés	7

Gestion détaillée du document

13 juillet 2006 version initiale.