

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-38

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-038>

Gestion du document

Référence	CERTA-2006-ACT-038
Titre	Bulletin d'actualité 2006-38
Date de la première version	22 septembre 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-038.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-038/>

1 Activité en cours

1.1 Incidents traités

1.1.1 Défigurations

Le CERTA a traité trois cas de défiguration cette semaine. Pour l'un de ces incidents, il s'agit de l'exploitation d'une faille de la version 2.0.10 de *phpBB*. Les deux autres incidents font l'objet d'investigations complémentaires afin de déterminer quelles ont été les vulnérabilités exploitées.

1.1.2 Propagation d'un ver

Un de nos correspondants nous a informés de l'infection de cinq machines sous Windows par un code malveillant de la famille Gaobot/Sdbot/Rbot. Le scénario de propagation a été le suivant : un poste nomade a été reconnecté sur un sous-réseau interne (après plusieurs semaines en dehors de ce réseau) alors qu'il avait déjà été infecté. Le code malveillant s'est ensuite propagé par les partages réseau.

Cet incident illustre bien la problématique posée par les postes nomades : il s'agit souvent de machines amenées à être exposées en étant directement connectées à l'Internet (sans aucune protection), qui sont par la suite introduites dans des sous-réseaux. Le code malveillant peut donc ainsi profiter des faiblesses liées au fonctionnement du sous-réseau : partages réseau, exploitation de vulnérabilités car les machines que l'on pense protégées ne sont pas mises à jour, etc.

1.2 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 14 et le 21 septembre 2006.

2 Nouvelle vulnérabilité sous Windows - vgx.dll

Le CERTA a mis à jour l'alerte CERTA-2006-ALE-011 pour intégrer une vulnérabilité affectant la bibliothèque `vgx.dll`. Cette bibliothèque est utilisée pour prendre en compte le format VML (Vector Markup Language). Ce format, basé sur le langage XML, est utilisé pour éditer certaines images.

Deux vecteurs d'attaque pour cette vulnérabilité : l'un consiste à utiliser des pages HTML spécifiquement conçues pour exploiter la faille par l'intermédiaire d'*Internet Explorer*, l'autre repose sur des messages électroniques qui seraient lus à l'aide des clients de la famille d'*Outlook* avec prise en compte du langage HTML.

Microsoft, qui a admis l'existence de cette vulnérabilité, propose, dans l'attente d'un correctif, un contournement provisoire. Il s'agit de modifier le registre afin de ne plus prendre en compte la bibliothèque `vgx.dll`. Cela peut se faire à l'aide de la commande :

```
regsvr32.exe "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll" -u
```

Il est possible que cette action entrave le bon fonctionnement de certaines applications.

Documentation :

- Alerte CERTA-2006-ALE-011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-011>
- Bulletin de sécurité 925568 de Microsoft du 21 septembre 2006 :
<http://www.microsoft.com/technet/security/advisory/925568.msp>
- Bulletin de sécurité VU#416092 de l'US-CERT du 21 septembre 2006 :
<http://www.kb.cert.org/vuls/id/416092>

3 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>

4 Rappel des avis et mises à jour émis

Durant la période du 15 au 21 septembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-399 : Vulnérabilités dans Claroline
- CERTA-2006-AVI-400 : Vulnérabilité dans Adobe ColdFusion
- CERTA-2006-AVI-401 : Vulnérabilité dans Dokeos
- CERTA-2006-AVI-402 : Vulnérabilités dans Drupal
- CERTA-2006-AVI-403 : Vulnérabilité CISCO IOS
- CERTA-2006-AVI-404 : Vulnérabilité CISCO
- CERTA-2006-AVI-405 : Vulnérabilités dans CISCO IDS et CISCO IPS

Pendant cette même période, l'alerte suivante a été mise à jour :

- CERTA-2006-ALE-011-002 : Multiples vulnérabilités de produits Microsoft (Rappels sur les ActiveX)
- CERTA-2006-ALE-011-003 : Multiples vulnérabilités de produits Microsoft (Ajouts références Microsoft et CVE)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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>

6 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.

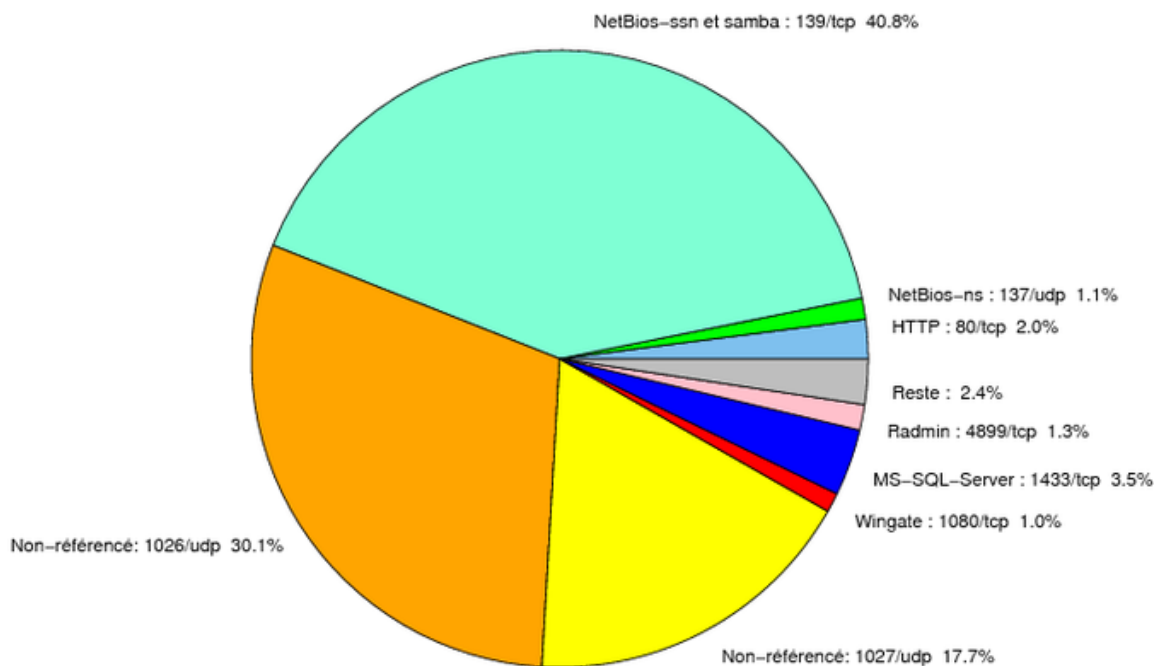


FIG. 1: Répartition relative des ports pour la semaine du 14.09.2006 au 21.09.2006

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
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
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
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	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 re-jetés

port	pourcentage
139/tcp	40.84
1026/udp	30.07
1027/udp	17.69
1433/tcp	3.49
80/tcp	2.04
4899/tcp	1.33
137/udp	1.11
1080/tcp	1.01
1434/udp	0.89
22/tcp	0.32
3128/tcp	0.3
25/tcp	0.23
15118/tcp	0.16
21/tcp	0.06
9898/tcp	0.05
143/tcp	0.03
5000/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

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

Gestion détaillée du document

22 septembre 2006 version initiale.