

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°2005-11

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-2005-ACT-011>

Gestion du document

Référence	CERTA-2005-ACT-011
Titre	Bulletin d'actualité N°2005-11
Date de la première version	18 mars 2005
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.

1 Activité en cours

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 03 et le 10 mars 2005.

Un cas de défiguration d'un site web a été traité par le CERTA. D'autre part, l'analyse d'une défiguration annoncée dans le bulletin d'actualité CERTA-2005-ACT-010 a révélé que la faille exploitée était relative au programme `fck_editor`. Ce dernier était configuré de telle manière que n'importe qui pouvait ajouter des images sur le site.

Nous avons par ailleurs constaté l'apparition de rejets sur les ports 12022/tcp et 31511/tcp. Nous n'avons pas, à ce jour, d'explication à propos de cette activité.

2 Problèmes avec phpBB et application des correctifs

Un ingénieur sécurité d'un hébergeur de sites web a informé le CERTA qu'il avait reçu un message provenant du site `phpBB-fr.com` (communauté francophone d'utilisateurs de phpBB). Ce message contenait une information concernant le piratage de leur propre site, ainsi que des éléments au sujet d'une faille de phpBB 2.0.13. A la fin du message, un correctif non-officiel, réalisé par le découvreur de la vulnérabilité, était proposé. Les conséquences liées à l'exploitation de cette vulnérabilité ne sont pas connues.

Après vérification sur le site officiel de phpBB (`www.phpbb.com`), il apparaît que les auteurs de ce produit ne font pas mention de ce correctif.

Le CERTA rappelle que l'acquisition des correctifs doit toujours se faire auprès des éditeurs. Il ne faut jamais appliquer un correctif envoyé par messagerie, d'autant plus que l'expéditeur d'un message peut être trivialement falsifiée. Nous vous conseillons par ailleurs la lecture de la note d'information CERTA-2001-INF-004 intitulée « Acquisition des correctifs » traitant de ces aspects.

Nous vous recommandons donc de ne pas appliquer ce correctif. Outre le fait qu'il n'y a aucune garantie quant à l'efficacité de la modification proposée, elle pourrait ne pas être prise en compte lors de l'application ultérieure de correctifs officiels.

Dans l'attente de la publication de correctifs de l'éditeur, il peut être préférable de fermer les forums phpBB, et de veiller à ce que vos éventuels hébergeurs n'appliquent pas la modification proposée par phpBB-fr.com.

3 Rappel des avis et des mises à jour émis

Durant la période du 07 au 11 mars 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-101 : Vulnérabilité de KDE
- CERTA-2005-AVI-102 : Multiples vulnérabilités dans GAIM
- CERTA-2005-AVI-103 : Vulnérabilité dans Ethereal
- CERTA-2005-AVI-104 : Vulnérabilité de libXpm
- CERTA-2005-AVI-105 : Vulnérabilité de libexif
- CERTA-2005-AVI-106 : Multiples vulnérabilités de grsecurity
- CERTA-2005-AVI-107 : Vulnérabilité de xv

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

- CERTA-2005-AVI-082-003 : Vulnérabilité de gFTP
(ajout de la référence au bulletin de sécurité Mandrake)
- CERTA-2005-AVI-093-001 : Vulnérabilités dans cURL/libcURL
(ajout de la référence au bulletin de sécurité Mandrake)
- CERTA-2005-AVI-098-001 : Vulnérabilité de kppp
(ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-081-001 : Vulnérabilité de Midnight Commander
(ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-087-001 : Multiples Vulnérabilités dans Cyrus IMAP
(ajout des références CVE et du bulletin de sécurité Mandrake)
- CERTA-2005-AVI-095-001 : Multiples vulnérabilités dans Mozilla
(ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-003-006 : Multiples vulnérabilités de libtiff
(ajout référence au bulletin de sécurité Mandrake MDKSA-2005:052)
- CERTA-2005-AVI-095-002 : Multiples vulnérabilités dans Mozilla
(ajout des références aux bulletins de sécurité RedHat et Gentoo)
- CERTA-2005-AVI-095-003 : Multiples vulnérabilités dans Mozilla
(ajout des références aux bulletins de sécurité NetBSD)
- CERTA-2005-AVI-098-002 : Vulnérabilité de kppp
(ajout des références aux bulletins de sécurité Debian et NetBSD)
- CERTA-2005-AVI-099-002 : Vulnérabilités dans RealOne Player
(ajout de la référence CVE CAN-2005-0611 et des bulletins de sécurité iDEFENSE et SUSE SUSE-SA:2005:014)
- CERTA-2005-AVI-102-001 : Multiples vulnérabilités dans GAIM
(ajout des références aux bulletins de sécurité RedHat et NetBSD)

4 Actions suggérées

4.1 Respecter la politique de sécurité

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.

4.2 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.

4.3 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.

4.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiat. 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.

4.5 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.

4.6 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 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.

Liste des tableaux

1	Gestion du document	1
2	Correctifs correspondant aux ports destination des paquets rejetés	4
3	Paquets rejetés	5

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
42	TCP	WINS	–	CERTA-2004-AVI-384
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239
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
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
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
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	–
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

port	pourcentage
445/tcp	82,02
139/tcp	7,15
137/udp	2,36
1433/tcp	1,59
1026/udp	1,53
4899/tcp	1,30
1027/udp	0,84
15118/tcp	0,83
12022/tcp	0,42
2745/tcp	0,27
80/tcp	0,26
1080/tcp	0,21
1434/udp	0,17
6129/tcp	0,13
22/tcp	0,13
23/tcp	0,11
31511/tcp	0,10
6101/tcp	0,09
5554/tcp	0,08
11768/tcp	0,07
3127/tcp	0,05
1023/tcp	0,05
21/tcp	0,05
3306/tcp	0,04
9898/tcp	0,04
42/tcp	0,03
443/tcp	0,03
5000/tcp	0,03
3128/tcp	0,01

TAB. 3 – Paquets rejetés

Gestion détaillée du document

18 mars 2005 version initiale.