

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°2005-06

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-006>

Gestion du document

Référence	CERTA-2005-ACT-006
Titre	Bulletin d'actualité N°2005-06
Date de la première version	11 février 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 trois dispositifs de filtrage, entre le 27 janvier et le 03 février 2005.

Un de nos correspondants nous a signalés qu'au moins une machine de son réseau a tenté de télécharger un fichier exécutable à maintes reprises. L'utilisation d'un antivirus à jour sur le poste concerné a permis de mettre en évidence un cheval de Troie de type downloader (code malicieux effectuant de multiples téléchargements de fichiers).

2 Correctifs de Microsoft

Microsoft a publié cette semaine douze correctifs. Beaucoup d'entre eux concernent des failles applicatives sur le poste client (CERTA-2005-AVI-050, 052, 053, 054, 056, 058, 059, 060). La plupart des vulnérabilités indiquées dans ces avis peuvent être exploitées en incitant l'utilisateur à visualiser un site web en cliquant sur un lien.

Une des vulnérabilités concerne le traitement des images au format PNG (Portable Network Graphics). L'outil de messagerie instantanée MSN messenger est affecté par cette vulnérabilité. Un petit programme permettant de façonner un fichier PNG mal formé dans le but d'exploiter la vulnérabilité sous MSN messenger a été rendu public.

Il est extrêmement important d'appliquer ces correctifs dans les plus brefs délais, notamment parce que le pare-feu ne protégera pas les utilisateurs dans le cas des failles applicatives (le flux est légitime).

Le tableau 2 a été mis à jour pour prendre en compte l'avis CERTA-2005-AVI-051. Pour la vulnérabilité décrite dans cet avis, les tentatives d'exploitation sont visibles au niveau du pare-feu (accès non sollicité au port 445/tcp de la machine).

3 Propagation d'un faux message du MRAP

Le CERTA a été informé de la propagation d'un faux message du MRAP à caractère diffamatoire. Nous vous rappelons qu'avant de prendre toute mesure concernant ce type de messages (en bloquant l'adresse de messagerie de l'expéditeur par exemple), nous vous invitons à vérifier dans l'en-tête complet l'adresse IP qui a réellement émis le message, et à prendre contact avec le CERTA.

4 Rappel des avis et des mises à jour émis

Durant la période du 31 janvier au 04 février 2005, le CERTA a émis l'avis suivant :

- CERTA-2005-AVI-037 : Vulnérabilité de Evolution
- CERTA-2005-AVI-038 : Multiples vulnérabilités dans SquirrelMail
- CERTA-2005-AVI-039 : Vulnérabilité dans BlackBerry Enterprise Server
- CERTA-2005-AVI-040 : Vulnérabilité de ncpfs
- CERTA-2005-AVI-041 : Vulnérabilité de mailman
- CERTA-2005-AVI-042 : Multiples vulnérabilités dans Squid
- CERTA-2005-AVI-043 : Vulnérabilité sur Juniper
- CERTA-2005-AVI-044 : Vulnérabilité de ClamAV
- CERTA-2005-AVI-045 : Vulnérabilité de Eudora
- CERTA-2005-AVI-046 : Vulnérabilité de Perl
- CERTA-2005-AVI-047 : Vulnérabilité des équipements IP/VC de Cisco
- CERTA-2005-AVI-048 : Vulnérabilité dans UW-Imapd

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

- CERTA-2005-AVI-033-001 : Vulnérabilité des serveurs DNS BIND
(ajout de la référence CVE et des références aux bulletins de sécurité Mandrake et NetBSD)
- CERTA-2005-AVI-020-002 : Vulnérabilité de ImageMagick
(ajout de la référence au second bulletin de sécurité Gentoo et au bulletin de sécurité NetBSD)
- CERTA-2005-AVI-014-002 : Multiples vulnérabilités dans Exim
(ajout des références à un second bulletin Debian, aux bulletins de sécurité OpenBSD, FreeBSD et NetBSD, et de la note de vulnérabilité de l'US-CERT)
- CERTA-2005-AVI-019-003 : Vulnérabilité dans Xpdf
(ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2005-AVI-038-001 : Multiples vulnérabilités dans SquirrelMail
(ajout de la référence au bulletin de sécurité Debian DSA-662 et de la référence CVE CAN-2005-0152)
- CERTA-2005-AVI-019-004 : Vulnérabilité dans Xpdf
(ajout des références aux bulletins de sécurité RedHat RHSA-2005:049, Debian DSA-645 et Debian DSA-648)
- CERTA-2005-AVI-038-002 : Multiples vulnérabilités dans SquirrelMail
(ajout de la référence au bulletin de sécurité Gentoo GLSA 200501-39)
- CERTA-2005-AVI-040-001 : Vulnérabilité de ncpfs
(ajout de la référence au bulletin de sécurité Mandrake MDKSA-2005:028)
- CERTA-2005-AVI-022-002 : Vulnérabilité de Ethernal
(ajout de la référence au bulletin de sécurité RedHat RHSA-2005:011)
- CERTA-2005-AVI-042-001 : Multiples vulnérabilités dans Squid
(mise à jour des vulnérabilités, ajout des références aux bulletins de sécurité OpenBSD, NetBSD, Gentoo et des références CVE CAN-2005-096, 097, 0173, 0174, 0175)
- CERTA-2004-AVI-402-007 : Vulnérabilité de Samba
(ajout références aux bulletins de sécurité HP HPSBUX01115 et Sun #57730)
- CERTA-2005-AVI-040-002 : Vulnérabilité de ncpfs
(ajout de la référence au bulletin de sécurité Debian DSA-665)

5 Actions suggérées

5.1 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.

5.2 Concevoir une architecture robuste

À 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 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.

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.

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.

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.

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	53,15
135/tcp	14,31
139/tcp	6,89
137/udp	3,63
1026/udp	2,93
15118/tcp	2,79
1027/udp	2,58
2745/tcp	2,17
4899/tcp	2,14
1433/tcp	1,26
80/tcp	1,07
9898/tcp	0,80
1434/udp	0,75
5554/tcp	0,70
11768/tcp	0,61
6129/tcp	0,60
1080/tcp	0,55
22/tcp	0,55
443/tcp	0,50
3306/tcp	0,37
1023/tcp	0,37
42/tcp	0,27
5000/tcp	0,24
3127/tcp	0,21
6101/tcp	0,15
21/tcp	0,14
23/tcp	0,11
3128/tcp	0,06
111/tcp	0,04
6112/tcp	0,04
3389/tcp	0,01

TAB. 3 – *Paquets rejetés*

Liste des tableaux

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

Gestion détaillée du document

11 février 2005 version initiale.