

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°2005-05

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-005>

Gestion du document

Référence	CERTA-2005-ACT-005
Titre	Bulletin d'actualité N°2005-05
Date de la première version	04 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 que nous avons constatés sur trois dispositifs de filtrage, entre le 20 et le 27 janvier 2005. Le ver exploitant les mots de passe faibles sous MySQL (port 3306/tcp) n'a pas engendré énormément de trafic réseau. Il est le deuxième à exploiter des comptes mal protégés, et il est possible que d'autres vers de ce type s'attaquent à d'autres services, comme telnet (port 23/tcp), pop3 (port 110/tcp), etc. Il est donc important de s'assurer que des mots de passe sont utilisés pour les services réseau nécessitant une authentification.

Le 27 janvier 2005, le CERTA a publié un bulletin de sécurité concernant une faille dans l'outil awstats. Awstats est un outil d'analyse de fichiers journaux et de génération de statistiques pour les serveurs web, FTP ou mail. La tentative d'exploitation de cette vulnérabilité par les pirates a été observée. C'est pourquoi le CERTA vous demande dans un premier temps d'appliquer le correctif de sécurité le plus rapidement possible et dans un second temps de remonter au CERTA toute tentative observée. La commande suivante appliquée aux fichiers de journalisation Apache permet d'extraire les lignes relatives aux tentatives d'attaques :

```
cat access_log |grep -i "configdir=|"
```

2 Rappel sur les canulars par messagerie (Hoax)

Le nombre de hoax circulant encore sur la messagerie aujourd'hui a poussé le CERTA à faire un rappel sur les canulars de messagerie et les menaces que cela peut entraîner pour le système d'information.

Un hoax est un message électronique contenant une rumeur ou une fausse information destinée à faire exécuter une ou plusieurs actions à l'utilisateur dont l'action de renvoyer le message à un plus grand nombre de personnes

possibles. Dans certains cas l'information propagée peut entraîner un déni de service du système de l'utilisateur en l'incitant à effectuer des actions destructrices sur son propre système et dans tous les cas un hoax aura pour effet de surcharger votre réseau voire même de réaliser un déni de service sur votre messagerie.

Même s'il existe des sites d'information destinés à repérer ces hoaxes, le CERTA recommande aux utilisateurs de la messagerie électronique de ne pas retransmettre les messages sans une certaine objectivité. Pour plus d'information sur les canaux de messageries il est conseillé de lire la note d'information CERTA-2000-INF-005 diffusée en 2000 et toujours d'actualité disponible à l'adresse suivante :

<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005>

3 Rappel des avis et des mises à jour émis

Durant la période du 24 au 28 janvier 2005, le CERTA a émis l'avis suivant :

- CERTA-2005-AVI-022 : Vulnérabilité de Ethereal
- CERTA-2005-AVI-023 : Multiples vulnérabilités du noyau Linux
- CERTA-2005-AVI-024 : Vulnérabilité de Veritas Backup Exec
- CERTA-2005-AVI-025 : Correctif de sécurité cumulatif pour les produits Oracle
- CERTA-2005-AVI-026 : Vulnérabilité des points d'accès 3Com OfficeConnect Wireless 11g
- CERTA-2005-AVI-027 : Vulnérabilité de Konversation
- CERTA-2005-AVI-028 : Failles dans les greffons Java de Sun
- CERTA-2005-AVI-029 : Vulnérabilité du système d'exploitation Cisco IOS
- CERTA-2005-AVI-030 : Vulnérabilités dans le traitement des paquets BGP par Cisco IOS
- CERTA-2005-AVI-031 : Vulnérabilité les routeurs Cisco supportant MPLS
- CERTA-2005-AVI-032 : Vulnérabilité IPv6 dans Cisco IOS
- CERTA-2005-AVI-033 : Vulnérabilité des serveurs DNS BIND
- CERTA-2005-AVI-034 : Multiples vulnérabilités dans Mac OS X
- CERTA-2005-AVI-035 : Vulnérabilité de AWStats
- CERTA-2005-AVI-036 : Vulnérabilité dans WinAMP

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

- CERTA-2004-AVI-405-003 : Multiples vulnérabilités de PHP
(ajout référence au bulletin de sécurité Red Hat)
- CERTA-2004-AVI-411-003 : Vulnérabilité de MIT Kerberos 5
(ajout référence au bulletin de sécurité RedHat RHSA-2005-012)
- CERTA-2005-AVI-019-019 : Vulnérabilité dans Xpdf
(ajout des autres applications vulnérables et des références aux bulletins de sécurité Fedora et KDE)
- CERTA-2004-AVI-373-002 : Vulnérabilité de unarj
(ajout de la référence au bulletin de sécurité Debian)
- CERTA-2005-AVI-004-002 : Vulnérabilité dans Xine
(ajout référence au bulletin de sécurité Mandrake MDKSA-2005:011)
- CERTA-2005-AVI-022-001 : Vulnérabilité de Ethereal
(ajout des références aux bulletins de sécurité Mandrake et NetBSD)
- CERTA-2005-AVI-027-001 : Vulnérabilité de Konversation
(ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2005-AVI-017-001 : CUPS : vulnérabilité dans l'impression de certains documents PDF
(ajout de la référence au bulletin de sécurité Mandrakelinux)
- CERTA-2005-AVI-019-002 : Vulnérabilité dans Xpdf
(ajout des références aux bulletins de sécurité Mandrake)

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-2003-AVI-144 CERTA-2004-AVI-126
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-2003-AVI-038 CERTA-2004-AVI-126
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	68,95
135/tcp	11,30
139/tcp	4,37
15118/tcp	2,10
137/udp	1,88
1026/udp	1,84
1027/udp	1,47
4899/tcp	1,27
1433/tcp	1,21
6129/tcp	0,64
5554/tcp	0,56
9898/tcp	0,55
80/tcp	0,46
2745/tcp	0,44
11768/tcp	0,44
5000/tcp	0,40
1434/udp	0,33
1023/tcp	0,29
1080/tcp	0,26
3306/tcp	0,19
22/tcp	0,19
42/tcp	0,17
6101/tcp	0,16
21/tcp	0,13
3127/tcp	0,12
443/tcp	0,05
111/tcp	0,05
23/tcp	0,05
3389/tcp	0,04
3128/tcp	0,03
389/tcp	0,01
119/tcp	0,01

TAB. 3: Paquets rejetés

Gestion détaillée du document

04 février 2005 version initiale.