

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°2005-12

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-012>

Gestion du document

Référence	CERTA-2005-ACT-012
Titre	Bulletin d'actualité N°2005-12
Date de la première version	25 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

1.1 Ports observés

Le tableau 3 montre les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 10 et le 17 mars 2005.

Les rejets constatés la semaine précédente sur les ports 12022/tcp et 31511/tcp ont complètement disparu.

Nous remarquons une augmentation des rejets sur le port 42/tcp qui est associé au service WINS (résolution de noms Netbios), ce service faisant l'objet d'une vulnérabilité critique permettant d'obtenir les droits administrateur à distance (avis CERTA-2004-AVI-384).

1.2 Quelques attaques traitées

5 cas de défiguration de site web ont été traités :

- un était relatif à l'exploitation d'une faille du forum phpBB (voir alerte CERTA-2004-ALE-014) ;
- un lié à l'utilisation de droits en écriture laissés par l'administrateur (commande PUT).

Nous n'avons pas d'information quant à la faille exploitée pour les trois autres cas.

Par ailleurs, nous avons été informés de la compromission d'un serveur web sous Linux qui a été utilisé à des fins de « phishing ». Ce serveur a été compromis par l'exploitation d'une faille de phpBB. Cet incident montre bien que les failles des serveurs web ne sont pas utilisées uniquement pour des défigurations.

2 Corruption des caches DNS

Ces dernières semaines, des attaques par corruption de cache DNS (Domain Name System) ont été observées.

Le DNS est le protocole qui permet de faire la correspondance entre le nom d'un domaine ou d'une machine et une adresse IP. Un client DNS va ainsi effectuer une requête auprès d'un serveur DNS. Le protocole de transport utilisé par le protocole DNS est UDP sur le port 53 (et dans certains cas TCP).

Du côté serveur on pourra citer les serveurs DNS `bind`, `djbdns` ainsi que le serveur de Microsoft Windows.

Du côté client, des utilitaires d'interrogation de serveurs DNS sont disponibles nativement sur tous les systèmes d'exploitation. Par exemple, sous Microsoft Windows, l'utilitaire `nslookup` permet d'interroger un serveur DNS afin d'effectuer des résolutions de noms. Sous les UNIX (GNU/Linux, BSD etc), citons par exemple les outils `nslookup`, `host` ou `dig`.

Lorsqu'un client ou un serveur cache DNS adresse une requête à un serveur, il va mémoriser le résultat dans un cache (service `Dnscache` sous Windows par exemple). Ce mécanisme améliore les performances du protocole.

Les attaques par corruption de cache DNS consistent à ajouter ou modifier une ou plusieurs entrées de ce cache.

Lorsqu'un utilisateur demandera l'adresse IP associée à un nom de domaine (par exemple `google.fr`) au serveur DNS victime, l'adresse IP renvoyée sera inexacte (`IP_du_serveur_Pirate` au lieu de `216.239.59.104` par exemple).

Le principe général de la corruption de cache DNS est l'envoi de données complémentaires malicieuses par un serveur DNS sous contrôle d'un pirate à un serveur DNS victime. Le serveur DNS victime va mettre à jour son cache de manière aveugle, en fonction des données envoyées. Lors de la prochaine requête DNS par un utilisateur interrogeant le cache DNS corrompu, l'adresse IP renvoyée sera non pas celle légitime mais celle d'un serveur sous contrôle du pirate.

Une fois la victime redirigée vers le site pirate, plusieurs actions pourront être intentées comme du vol d'information (site à l'allure identique à un site bancaire par exemple), l'installation de code malveillant en exploitant une faille connue du navigateur, etc.

Comme tout applicatif, il est important d'effectuer les mises à jour dès la découverte d'une vulnérabilité et la mise à disposition du correctif.

Tous les serveurs DNS ne sont pas vulnérable à ces attaques.

Dans le cas des serveurs DNS sous Microsoft Windows NT ou Microsoft Windows 2000 on pourra se référer à l'article 241352 de la base de connaissance Microsoft :

<http://support.microsoft.com/kb/q241352/>

3 Rappel des avis et des mises à jour émis

Durant la période du 14 au 18 mars 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-108 : Vulnérabilité de Microsoft Exchange Server 2003
- CERTA-2005-AVI-109 : Multiples vulnérabilités dans Novell iChain FTP Server
- CERTA-2005-AVI-110 : Vulnérabilités dans Mysql
- CERTA-2005-AVI-111 : Vulnérabilité de Trillian Basic
- CERTA-2005-AVI-112 : Déni de service sous HP Tru64 Unix
- CERTA-2005-AVI-113 : Vulnérabilité dans les produits Avaya
- CERTA-2005-AVI-114 : Multiples vulnérabilités de xli
- CERTA-2005-AVI-115 : Vulnérabilité dans OpenVMS
- CERTA-2005-AVI-116 : Vulnérabilité dans OpenBSD
- CERTA-2005-AVI-117 : Vulnérabilités dans OpenSLP

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

- CERTA-2005-AVI-093-002 : Vulnérabilités dans `cURL/libcURL`
(ajout de la référence au bulletin de sécurité Gentoo)
- CERTA-2005-AVI-104-001 : Vulnérabilité de `libXpm`
(ajout référence au bulletin de sécurité Gentoo GLSA 200503-15)
- CERTA-2005-AVI-105-001 : Vulnérabilité de `libexif`
(ajout référence au bulletin de sécurité de Gentoo)
- CERTA-2005-AVI-117-001 : Vulnérabilités dans OpenSLP
(ajout référence au bulletin de sécurité de 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.

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	70,92
139/tcp	11,03
137/udp	4,90
1433/tcp	3,36
4899/tcp	2,68
1080/tcp	1,45
1026/udp	1,13
15118/tcp	0,97
1027/udp	0,68
80/tcp	0,38
6129/tcp	0,35
1434/udp	0,28
6101/tcp	0,24
23/tcp	0,20
22/tcp	0,20
2745/tcp	0,17
5554/tcp	0,15
9898/tcp	0,15
42/tcp	0,15
443/tcp	0,12
3306/tcp	0,09
3127/tcp	0,08
3128/tcp	0,08
21/tcp	0,07
11768/tcp	0,07
1023/tcp	0,06
135/tcp	0,02
5000/tcp	0,02
10080/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

25 mars 2005 version initiale.