Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 décembre 2005
N° CERTA-2005-ACT-052

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-52

Gestion du document

Référence	CERTA-2005-ACT-052
Titre	Bulletin d'actualité n° 2005-52
Date de la première version	30 décembre 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 Incident traité

Cette semaine le CERTA a traité un incident concernant un *reverse-proxy* en protection d'un serveur *HTTP*. Un problème de configuration a fait, qu'au lieu d'être *proxy* vers ce seul serveur *HTTP*, **le relais était ouvert vers les serveurs web du monde entier**. Beaucoup d'individus sur la toile sont friands de ce type de relais (recherche d'anonymisation, « spam »,...) et il y a des balayages permanents à la recherche de serveurs ouverts. Le *proxy* s'est retrouvé saturé, incapable d'honorer les requêtes légitimes et le site protégé s'en est trouvé inaccessible. Parmi les clients indésirables a même été identifiée une société commercialisant un balayeur de *proxies* ouverts et des listes de serveurs identifiés. En tout état de cause, le *proxy* a très bien pu être utilisé pour réaliser des actions répréhensibles. Il est alors souhaitable, dans un tel cas de figure, d'envisager un dépôt de plainte et au moins de procéder à la sauvegarde et à l'archivage des journaux du *proxy*.

1.2 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 22 et le 29 décembre 2005.

2 Vulnérabilité de Microsoft Windows

Celle-ci affecte le moteur de rendu graphique de Windows. Il s'agit d'un défaut de sécurité dans le composant qui permet de voir des images et des télécopies. Cela peut être par exemple le cas de la visualisation d'images au format wmf insérées dans un message. Il apparaît que cette vulnérabilité n'est pas limitée aux seules applications Microsoft (comme `Internet Explorer` ou `Outlook`) mais concerne l'ensemble des applications qui utilisent le moteur de rendu graphique de Windows. On peut citer par exemple « Google Desktop » ou "Lotus Notes". Il existe déjà de nombreux sites web hébergeant le code malveillant. Le CERTA a émis une alerte à ce sujet : `http://www.certa.ssi.gouv.fr/site/CERTA-2005-ALE-019.pdf`. Le CERTA estime que les risques d'utilisation massive de cette vulnérabilité sont élevés compte tenu de la facilité de mise en œuvre de l'attaque et préconise dans l'alerte du 29 décembre un moyen de contournement en attendant la diffusion d'un correctif par l'éditeur.

3 Vulnérabilité dans IIS 5.1 de Microsoft

Une vulnérabilité, non corrigée, présente sur `Internet Information Services 5.1` de Microsoft peut être exploitée afin de causer un déni de service à distance. Cette vulnérabilité est due à une erreur dans le traitement de certaines adresses réticulaires (url) malicieusement construites. Des codes d'exploitations sont d'ores et déjà disponibles sur l'Internet. La version 5.1 d'`IIS` est livrée uniquement avec les versions de `Microsoft Windows XP Professional`. L'installation par défaut du système d'exploitation n'inclut pas le serveur web `IIS`. Dans l'attente d'une mise à jour de sécurité, voici quelques contournements provisoires :

- Filtrer les requêtes *HTTP* contenant à la fin le caractère '~' (tilde) suivis d'un chiffre ;
- modifier les droits d'exécutions de tous répertoires (sauf si indispensable) de manière à ce que les scripts ne soient pas exécutables ;

`exemple : http://[site ciblé]/[répertoire 'scripts&exécutables']/*\~8`

Remarque : les deux caractères avant le tilde peuvent être arbitrairement choisis.

4 Liens utiles

- Note d'information pour sur les systèmes obsolètes ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information pour limiter l'impact du SPAM ;
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/index.html
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien)
  http://www.auscert.org.au/render.html?it=1935

5 Rappel des avis et mises à jour émis

Durant la période du 22 au 29 décembre 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-505 : Multiples vulnérabilités dans HP-UX
- CERTA-2005-AVI-506 : Multiples vulnérabilités dans Cisco IOS
- CERTA-2005-AVI-507 : Vulnérabilité sur Bugzilla
- CERTA-2005-AVI-508 : Vulnérabilité sur Sun Solaris Netlink
- CERTA-2005-AVI-509 : Vulnérabilité dans udev
- CERTA-2005-AVI-510 : Multiples vulnérabilités dans MailEnable

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

- CERTA-2005-AVI-400-003 : Faiblesse dans OpenSSL 0.9.x
  (ajout de la référence à l'avis de sécurité Cisco)
- CERTA-2005-AVI-487-002 : Vulnérabilité de Ethereal
  (ajout de la référence au bulletin de sécurité Ethereal)
- CERTA-2005-AVI-497-001 : Mise à jour des noyaux des distributions Linux
  (ajout de la référence CVE CAN-2005-3660)

6 Actions suggérées

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 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

7 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.

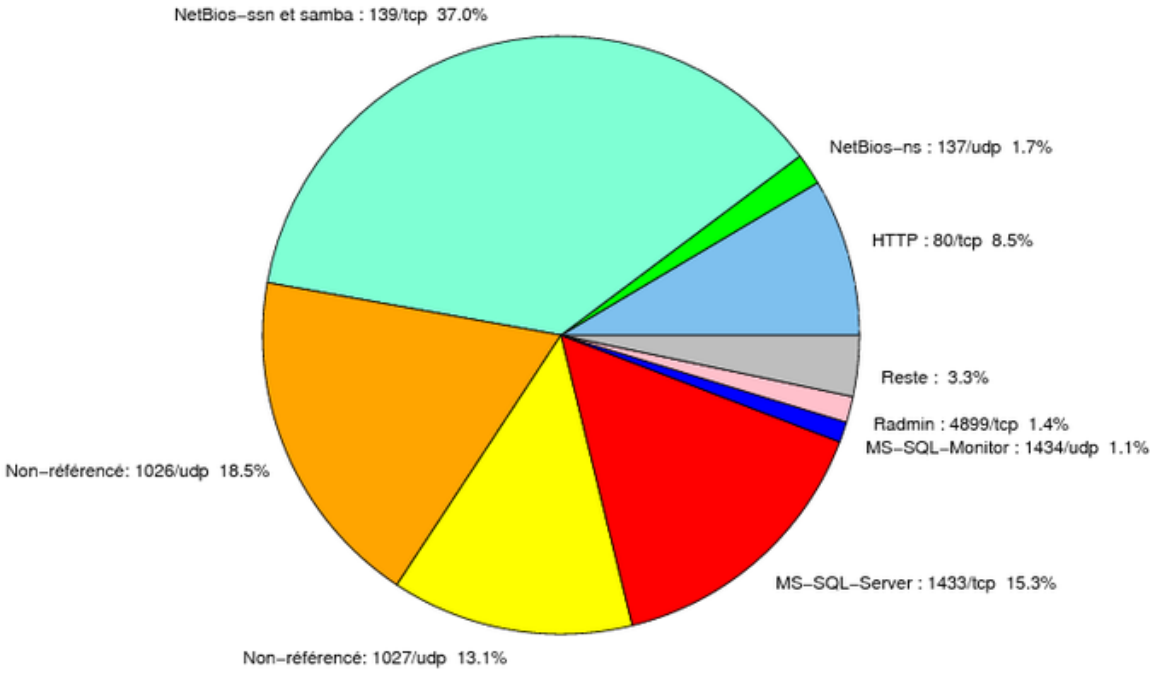

FIG. 1: Répartition relative des ports pour la semaine du 22.12.2005 au 29.12.2005

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/CERT http://www.certa.ssi.gouv.fr/site/CERT
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT

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/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

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

port	pourcentage
139/tcp	36.96
1026/udp	18.54
1433/tcp	15.34
1027/udp	13.11
80/tcp	8.51
137/udp	1.7
4899/tcp	1.4
1434/udp	1.1
1080/tcp	0.86
22/tcp	0.37
15118/tcp	0.27
9898/tcp	0.26
3127/tcp	0.14
3128/tcp	0.13
6129/tcp	0.12
143/tcp	0.11
3306/tcp	0.1
1023/tcp	0.08
111/tcp	0.07
23/tcp	0.05
10000/tcp	0.04
3389/tcp	0.02
11768/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

30 décembre 2005 version initiale.