

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°23

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-2004-ACT-023>

Gestion du document

| | |
|-----------------------------|---------------------------|
| Référence | CERTA-2004-ACT-023 |
| Titre | Bulletin d'actualité N°23 |
| Date de la première version | 21 octobre 2004 |
| 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 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.

2 Activité en cours

Durant la semaine du 07 au 14 octobre 2004, les rejets constatés concernaient essentiellement les ports 445/tcp et 135/tcp. Suite à la vulnérabilité du service NNTP (port 119/tcp) sous IIS (voir avis CERTA-2004-AVI-340), nous avons ajouté le port 119/tcp à la liste des ports sous surveillance. Pour le moment, nous ne constatons pas de recherche de ce port, mais on peut s'attendre à ce que la situation évolue dans les semaines à venir.

| port | pourcentage |
|----------|-------------|
| 445/tcp | 26,50 |
| 135/tcp | 23,16 |
| 137/udp | 11,92 |
| 139/tcp | 9,68 |
| 2745/tcp | 5,86 |
| 1433/tcp | 3,46 |
| 80/tcp | 2,55 |
| 9898/tcp | 2,29 |
| 5554/tcp | 2,11 |
| 1026/udp | 2,00 |
| 1023/tcp | 1,97 |
| 1027/udp | 1,45 |
| 1080/tcp | 1,31 |
| 1434/udp | 1,31 |
| 3127/tcp | 0,92 |
| 6129/tcp | 0,63 |
| 22/tcp | 0,58 |
| 4899/tcp | 0,57 |
| 21/tcp | 0,51 |
| 443/tcp | 0,38 |
| 3128/tcp | 0,28 |
| 23/tcp | 0,23 |
| 111/tcp | 0,16 |
| 5000/tcp | 0,14 |
| 3389/tcp | 0,02 |

TAB. 2 – *Paquets rejetés*

3 Actions suggérées

3.1 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.

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 3 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 immédiat. Unpare-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.

| 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-179 CERTA-2003-AVI-131 |
| 80 | TCP | HTTP | – | CERTA-2004-AVI-050 CERTA-2004-AVI-195 CERTA-2004-AVI-210 CERTA-2004-AVI-239 CERTA-2004-AVI-313 CERTA-2004-AVI-315 |
| 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 | – | CERTA-2003-AVI-168 CERTA-2003-AVI-144 CERTA-2004-AVI-126 |
| 389 | TCP | LDAP | – | CERTA-2004-AVI-045 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-095 CERTA-2004-AVI-126 CERTA-2004-AVI-178 CERTA-2004-AVI-247 CERTA-2004-AVI-301 CERTA-2004-AVI-313 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 |
| 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 | – |
| 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 | – |

3
TAB. 3 – Correctifs correspondant aux ports destination des paquets rejetés

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.

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 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.

4 Rappel des avis et des mises à jour émis

Durant la semaine du 11 au 15 octobre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-333 : Vulnérabilité de la bibliothèque RPC sous Windows NT 4.0
- CERTA-2004-AVI-334 : Vulnérabilité dans WebDAV
- CERTA-2004-AVI-335 : Vulnérabilité du service Microsoft NetDDE
- CERTA-2004-AVI-336 : Multiples vulnérabilités dans Microsoft Windows
- CERTA-2004-AVI-337 : Vulnérabilité dans Microsoft Excel
- CERTA-2004-AVI-338 : Vulnérabilité des répertoires compressés sous Windows
- CERTA-2004-AVI-339 : Vulnérabilité dans le composant SMTP de Windows Server 2003
- CERTA-2004-AVI-340 : Failles dans le service NNTP de Microsoft IIS
- CERTA-2004-AVI-341 : Multiples vulnérabilités dans l'interpréteur de commandes Windows
- CERTA-2004-AVI-342 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2004-AVI-343 : Vulnérabilité du module mod_ssl du serveur HTTP Apache
- CERTA-2004-AVI-344 : Multiples vulnérabilités dans PHP
- CERTA-2004-AVI-345 : Multiples Vulnérabilités de Libtiff
- CERTA-2004-AVI-346 : Mauvaise gestion de l'authentification Radius sous OpenBSD
- CERTA-2004-AVI-347 : Vulnérabilités dans MySQL

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

- CERTA-2004-AVI-325-003 : Vulnérabilités de XFree86, libXpm et LessTif (ajout référence au bulletin de sécurité Gentoo GLSA 200410-09 relatif à LessTif)
- CERTA-2004-AVI-317-002 : Vulnérabilité de CUPS (ajout référence au bulletin de sécurité de Sun)
- CERTA-2004-AVI-322-001 : Vulnérabilité du filtre d'impression foomatic-rip (ajout référence au bulletin de Sun)
- CERTA-2004-AVI-324-001 : Vulnérabilité dans Sudo (Modification sur les versions vulnérables)
- CERTA-2004-AVI-325-004 : Vulnérabilités de XFree86, libXpm et LessTif (ajout référence au bulletin de sécurité Debian (DSA-561) et Sun)
- CERTA-2004-AVI-332-001 : Vulnérabilité de Samba (ajout référence au bulletin de sécurité RedHat (RHSA-2004-498) et au bulletin de sécurité de Fedora (FLSA:2102))
- CERTA-2004-AVI-257-004 : Vulnérabilité de SoX (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2004-AVI-304-004 : Vulnérabilité de mpg123 (ajout de la référence au bulletin de sécurité Debian)
- CERTA-2004-AVI-325-005 : Vulnérabilités de XFree86, libXpm et LessTif (ajout référence au bulletin de sécurité OpenBSD)
- CERTA-2004-AVI-323-001 : Vulnérabilités sous FreeRadius (Ajout de la note FreeBSD et des avis de Secunia et de l'US-CERT)

Liste des tableaux

| | | |
|---|--|---|
| 1 | Gestion du document | 1 |
| 2 | Paquets rejetés | 2 |
| 3 | Correctifs correspondant aux ports destination des paquets rejetés | 3 |

Gestion détaillée du document

21 octobre 2004 version initiale.