

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité N°26

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-026>

Gestion du document

| | |
|-----------------------------|---------------------------|
| Référence | CERTA-2004-ACT-026 |
| Titre | Bulletin d'actualité N°26 |
| Date de la première version | 26 novembre 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 Activité en cours

L'activité remarquée sur deux pare-feux entre le 11 et le 18 novembre 2004 (voir Tab. 3) n'est pas différente de celle constatée les semaines précédentes. L'analyse des journaux a toutefois permis de détecter plusieurs machines compromises (dont un serveur mutualisé chez un hébergeur) qui effectuaient des recherches sur le port 22/tcp.

Les incidents qui nous ont été signalés concernaient essentiellement des activités virales, qui se traduisaient par la réception massive de messages infectés. Pour l'un de ces incidents, le volume de messages reçus était tel (plusieurs milliers par jour) qu'il saturait le serveur de messagerie.

2 Non, ce correspondant ne vous envoie pas de virus !

Nous recevons parfois des signalements de réception de virus. On entend souvent « j'ai reçu un virus d'une personne que je ne connais pas ! », ou encore « untel m'a envoyé un virus ! ».

Le fonctionnement des vers de messagerie (c'est-à-dire qui se propagent par la messagerie) repose sur l'utilisation des carnets d'adresses. En effet, pour se propager, le ver construit un message, dont il remplit les champs « expéditeur » et « destinataire » en puisant des adresses de messagerie dans le carnet d'adresses (il faut préciser que sous Outlook Express, le carnet d'adresses se remplit automatiquement par défaut avec les adresses des expéditeurs). Ces attaques ne sont donc pas ciblées, et l'émetteur figurant dans le message n'est pas le véritable expéditeur du message. Il est donc recommandé de configurer les passerelles antivirales pour qu'elles n'envoient pas de notification de détection d'un virus à l'adresse apparaissant dans le champ « expéditeur » du message.

Mais alors, est-il possible de retrouver la machine ayant réellement émis le message infecté? La réponse est oui. Il faut, pour ce faire, afficher l'en-tête complet du message (par exemple, sous Outlook Express, utiliser le bouton droit de la souris, puis afficher les propriétés du message). Voici un exemple d'en-tête :

```
From untel@nom_de_domaine_quelconque Tue Nov 23 11:25:47 2004
Return-Path: <untel@nom_de_domaine_quelconque>
Delivered-To: certa-svp@certa.ssi.gouv.fr
Received: from serveur_messagerie (serveur_messagerie [10.65.123.2])
    by mail.certa.ssi.gouv.fr (Postfix) with ESMTTP
Received: from ofivsfojr (ozrovj [192.168.92.87])
    by serveur_messagerie.quelquepart
    id BC9323A847; Tue, 23 Nov 2004 11:25:40 0100 (CET)+
Subject: My Photos !
Date: Tue, 23 Nov 2004 11:25:33 0100+
```

Dans cet en-tête, le chemin suivi par le message apparaît : il part de la machine 192.168.92.87 (seules les informations entre les crochets sont pertinentes), puis atteint le serveur 10.65.123.2 avant d'être reçu par le serveur mail.certa.ssi.gouv.fr. L'émetteur réel de ce message est donc la machine qui possédait l'adresse IP 192.168.92.87 le 23 novembre 2004 à 11h25.

Cependant, de fausses informations peuvent être ajoutées volontairement dans les en-têtes (par exemple par un virus). Une certaine expertise ou habitude est alors nécessaire pour trouver l'origine de proche en proche.

Lorsque vous signalez un virus, ou tout problème relatif à un message électronique, il est extrêmement important de fournir l'en-tête complet, afin de pouvoir en extraire l'adresse IP émettrice ainsi que les date et heure de l'envoi.

3 Rappel des avis et des mises à jour émis

Durant la période du 08 novembre au 19 novembre 2004, le CERTA a émis les avis suivants :

- CERTA-2004-AVI-363 : Faille dans le gestionnaire de volumes Linux LVM
- CERTA-2004-AVI-364 : Vulnérabilité de gzip
- CERTA-2004-AVI-365 : Vulnérabilité dans ISA Server / Proxy Server
- CERTA-2004-AVI-366 : Vulnérabilité sur Cisco IOS
- CERTA-2004-AVI-367 : Vulnérabilité dans Cisco Security Agent (CSA)
- CERTA-2004-AVI-368 : Multiples vulnérabilités de Samba
- CERTA-2004-AVI-369 : Vulnérabilité d'ImageMagick
- CERTA-2004-AVI-370 : Vulnérabilités du serveur HTTP Apache
- CERTA-2004-AVI-371 : Vulnérabilité dans l'utilitaire sudo
- CERTA-2004-AVI-372 : Vulnérabilité des noyaux Linux 2.4 et 2.6

Pendant cette même période, le CERTA a publié les mises à jour suivantes :

- CERTA-2004-AVI-360-001 : Vulnérabilité de la bibliothèque gd (ajout références aux bulletins de sécurité de Debian)
- CERTA-2004-AVI-361-002 : Multiples vulnérabilités de libxml2 (ajout référence au bulletin de sécurité RHSA-2004:615 de Red Hat)
- CERTA-2004-AVI-325-008 : Vulnérabilités de XFree86, libXpm, LessTif, Motif et OpenMotif (ajout référence au bulletin de sécurité SSRT4831 pour HP Tru64)
- CERTA-2004-AVI-360-002 : Vulnérabilité de la bibliothèque gd (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.

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-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 CERTA-2004-AVI-348 |
| 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 | – |

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

| port | pourcentage |
|-------------|--------------------|
| 135/tcp | 33,01 |
| 445/tcp | 25,49 |
| 139/tcp | 7,67 |
| 137/udp | 6,24 |
| 80/tcp | 4,69 |
| 1433/tcp | 4,19 |
| 1026/udp | 3,58 |
| 1027/udp | 2,82 |
| 9898/tcp | 1,86 |
| 5554/tcp | 1,84 |
| 1023/tcp | 1,60 |
| 2745/tcp | 1,30 |
| 4899/tcp | 0,81 |
| 3127/tcp | 0,77 |
| 1080/tcp | 0,76 |
| 21/tcp | 0,73 |
| 6129/tcp | 0,62 |
| 1434/udp | 0,58 |
| 22/tcp | 0,49 |
| 23/tcp | 0,32 |
| 443/tcp | 0,25 |
| 5000/tcp | 0,13 |
| 3389/tcp | 0,13 |
| 111/tcp | 0,09 |
| 3128/tcp | 0,01 |

TAB. 3 – *Paquets rejetés*

Gestion détaillée du document

26 novembre 2004 version initiale.