

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Cédérom Pages Pro

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-2002-ALE-007>

Gestion du document

Référence	CERTA-2002-ALE-007
Titre	Cédérom Pages Pro
Date de la première version	4 septembre 2002
Date de la dernière version	–
Source(s)	Alerte de sécurité de la société Le Mamousse : «Logiciel « les Pages Pro » sur CDROM »
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Perte de confidentialité et d'intégrité de tout fichier présent sur la machine accueillant le cédérom ;
- prise de contrôle à distance de la machine ;
- déni de service.

2 Systèmes affectés

Cédérom « les Pages Pro » version novembre 2001 | 2002 distribué par les Pages Jaunes.

3 Résumé

Par une URL habilement constituée, un individu mal intentionné peut accéder à distance et modifier n'importe quel fichier du poste de travail sur lequel est démarrée l'application vulnérable.

4 Description

« Les Pages Pro » est un logiciel distribué par les Pages Jaunes (filiale du groupe France Telecom).

Ce logiciel permet d'accéder à la base d'annuaire Pages Pro sur cédérom via un serveur HTTP intégré à l'application.

La conjonction des trois points suivants :

1. une vulnérabilité présente dans le serveur HTTP permet d'accéder à tout fichier d'un disque dur, même si celui-ci n'appartient pas à l'arborescence du serveur HTTP (c'est une vulnérabilité de type `directory traversal`);
2. l'interface de navigation HTTP du logiciel permet de lancer certaines applications ;
3. par défaut, l'accès au serveur HTTP n'est pas restreint à la seule machine qui accueille le cédérom (adresse 127.0.0.1).

permet à un individu distant mal intentionné, par le biais d'une URL habilement constituée :

- d'accéder et de modifier n'importe quel fichier,
- de lancer certains applicatifs.

Il peut en résulter une perte de confidentialité, d'intégrité et la possibilité d'effectuer un déni de service.

5 Contournement provisoire

Une commande permet de déterminer si la version du logiciel fournie sur le cédérom est vulnérable ou non :

```
c:> netstat -an
Proto  Adresse locale  Adresse distant Etat
TCP    0.0.0.0:8100    0.0.0.0          Listening
```

"0.0.0.0:8100" indique que la vulnérabilité est présente.

Afin d'interdire tout accès non local aux données de l'ordinateur, il est recommandé lors de l'utilisation du cédérom les Pages Pro de :

- débrancher (physiquement) le câble qui relie le poste de travail accueillant le cédérom au réseau ;
- ou interdire au niveau du firewall tout accès entrant sur le port 8100/tcp (ce qui empêche toute exploitation de cette vulnérabilité depuis l'Internet, mais ne protège pas contre les attaques depuis l'intranet).

6 Solution

La version du cédérom les Pages Pro de novembre 2002 corrige cette vulnérabilité.

7 Documentation

Note d'information de la société les Pages Jaunes :

- <http://www.pagespro.com>
- <http://www.bienvenue.pagesjaunes.fr>

Gestion détaillée du document

4 septembre 2002 version initiale.