

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Cahier de Texte

---

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-2006-AVI-543>

---

### Gestion du document

Référence	CERTA-2006-AVI-543
Titre	Vulnérabilités dans Cahier de Texte
Date de la première version	12 décembre 2006
Date de la dernière version	–
Source(s)	Page des correctifs de Cahier de Texte
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- vol d'identifiants.

## 2 Systèmes affectés

*Cahier de Texte* versions 2.2 (avant le correctif du 08 décembre 2006) et antérieures.

## 3 Description

Deux vulnérabilités ont été découvertes dans *Cahier de Texte*.

La première concerne le fichier `administration/telecharger.php` qui ne contrôle pas correctement les paramètres.

La seconde vulnérabilité concerne le fichier `administration/dump.sql` qui peut être téléchargé.

L'exploitation de ces vulnérabilités permet la récupération des sauvegardes dans lesquelles se trouve, entre autres, le mot de passe de l'administrateur en clair.

## 4 Solution

Suivre les indications sur la page des correctifs de l'éditeur pour la mise à jour de la version 2.2 (voir Documentation).

## 5 Documentation

- Page des correctifs de Cahier de Texte :  
[http://www.etab.ac-caen.fr/bsauveur/cahier\\_de\\_texte/correctifs.html](http://www.etab.ac-caen.fr/bsauveur/cahier_de_texte/correctifs.html)
- Référence CVE CVE-2006-6253 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6253>
- Référence CVE CVE-2006-6254 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6254>

## Gestion détaillée du document

12 décembre 2006 version initiale.