

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Adobe PageMaker

---

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-2008-AVI-535>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2008-AVI-535                                      |
| Titre                       | Vulnérabilités dans Adobe PageMaker                     |
| Date de la première version | 30 octobre 2008   |
| Date de la dernière version | –   |
| Source(s)                   | Bulletin de sécurité Adobe APSA08-10 du 29 octobre 2008 |
| 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

Exécution de code arbitraire.

## 2 Systèmes affectés

Adobe PageMaker versions 7.0.1 et 7.0.2.

## 3 Résumé

Des vulnérabilités dans Adobe PageMaker permettent d'exécuter du code arbitraire.

## 4 Description

Deux vulnérabilités ont été découvertes dans Adobe PageMaker (CVE-2008-5394 et CVE-2008-6432). L'exploitation de ces vulnérabilités permet l'exécution de code arbitraire. L'éditeur a publié un correctif de sécurité pour ces deux failles mais admet l'existence d'une troisième vulnérabilité (CVE-2008-6021) non corrigée.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Adobe apsa08-10 du 29 octobre 2008 :  
<http://www.adobe.com/support/security/bulletins/apsa08-10.html>
- Référence CVE CVE-2008-5394 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5394>
- Référence CVE CVE-2008-6021 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-6021>
- Référence CVE CVE-2008-6432 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-6432>

## Gestion détaillée du document

**30 octobre 2008** version initiale.