



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 11 mars 2004  
N° CERTA-2004-AVI-065-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité d'Adobe Acrobat Reader

---

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-AVI-065>

---

### Gestion du document

Référence	CERTA-2004-AVI-065-001
Titre	Vulnérabilité d'Adobe Acrobat Reader
Date de la première version	04 mars 2004
Date de la dernière version	11 mars 2004
Source(s)	Avis de sécurité de NGSSoftware
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 Acrobat Reader version 5.1 pour les systèmes Microsoft Windows.

## 3 Résumé

Une vulnérabilité du produit Adobe Acrobat Reader permet à un utilisateur mal intentionné d'exécuter du code arbitraire par le biais d'un fichier *.xpdf*.

## 4 Description

Le lecteur Adobe Acrobat Reader peut être utilisé pour visualiser des documents au format PDF. Il peut être également utilisé avec les documents au format XFDF (XML Forms Data Format).

Lorsqu'un document au format XFDF est traité par Acrobat Reader, la fonction *sprintf()* est appelée de manière non sûre, et présente une vulnérabilité de type débordement de mémoire.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité à l'aide d'un document au format XFDF malicieusement construit pour exécuter du code arbitraire sur la machine victime.

## **5 Solution**

La version 6.0 d'Adobe Acrobat Reader corrige cette vulnérabilité.

## **6 Documentation**

Avis de sécurité de NGSSoftware :  
<http://www.nextgenss.com/advisories/adobexfdf.txt>

Site d'Adobe :  
<http://www.adobe.com>

## **Gestion détaillée du document**

**04 mars 2004** version initiale.

**11 mars 2004** première révision : seuls les systèmes Windows sont vulnérables.