



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 juillet 2000
N° CERTA-2000-AVI-020

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous Adobe Acrobat

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-2000-AVI-020>

Gestion du document

Référence	CERTA-2000-AVI-020
Titre	Vulnérabilité sous Adobe Acrobat
Date de la première version	27 juillet 2000
Date de la dernière version	–
Source(s)	Adobe Security Focus Bugtraq
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

- Déni de service ;
- Exécution de code arbitraire.

2 Systèmes affectés

- Adobe Acrobat 4.05 pour Windows ;
- Adobe Acrobat Reader 4.05 pour Windows ;
- Adobe Acrobat Business Tools 4.05 ;
- Acrobat Fill In ;
- Plugin Acrobat pour navigateur Web (Netscape, Internet Explorer).

3 Résumé

Tous les produits Acrobat sous Windows sont vulnérables lors de la lecture d'un fichier PDF malformé. Au mieux l'application s'arrête, au pire du code arbitraire est exécuté sur la machine.

4 Description

Le format PDF est un format de lecture de document très répandu. Les logiciels de la famille Acrobat permettent de manipuler les documents PDF. Acrobat est vulnérable à un débordement de pile. Dès lors un utilisateur malveillant peut construire un document PDF qui, lors de sa visualisation, stoppe l'application ou exécute du code.

5 Solution

Correctif pour Acrobat 4.05, Acrobat Reader 4.05, Acrobat Business Tools 4.05 et Acrobat Fill In :
<ftp://ftp.adobe.com/pub/adobe/win/4.x/ac405up2.exe>

En cas de consultation d'un site internet proposant un fichier PDF, enregistrer le fichier concerné afin de l'ouvrir avec la version corrigée d'Acrobat.

6 Documentation

Site Adobe
<http://www.adobe.com/misc/pdfsecurity.html>

Gestion détaillée du document

27 juillet 2000 version initiale.