Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 7 février 2003
N° CERTA-2003-AVI-001-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur xpdf

Gestion du document

Référence	CERTA-2003-AVI-001-002
Titre	Vulnérabilité sur pdftops
Date de la première version	3 janvier 2003
Date de la dernière version	7 février 2003
Source(s)	Avis de sécurité iDefense CVE : CAN-2002-1384
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 commande arbitraire.

2 Systèmes affectés

La fonction `pdftops` incluse des logiciels comme `xpdf` et `cups`.

3 Résumé

Une vulnérabilité présente sur `pdftops` permet à un utilisateur mal intentionné de réaliser un débordement de mémoire.

4 Description

Le logiciel utilisé pour afficher des documents au format pdf `xpdf` et le gestionnaire d'impression `cups` utilisent le filtre `pdftops`.

Ce filtre contient un risque de débordement de mémoire permettant à un utilisateur mal intentionné d'exécuter du code arbitraire ou de réaliser un déni de service à l'aide d'un document au format `pdf` malicieusement construit.

5 Solution

Appliquer les mises à jour de vos logiciels (cf section documentation)

6 Documentation

- Avis de sécurité iDefense :
  http://www.idefense.com/advisory/12.23.02.txt
- Correctif de xpdf :
  ftp://ftp.foolabs.com/pub/xpdf/
- Bulletin de sécurité MDKSA-2003:002 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:002
- Bulletin de sécurité DSA-222 de Debian :
  http://www.debian.org/security/2003/dsa-222
- Bulletin de sécurité DSA-226 de Debian :
  http://www.debian.org/security/2003/dsa-226
- Bulletin de sécurité RHSA-2003:037 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-037.html

Gestion détaillée du document

03 janvier 2003 version initiale.
22 janvier 2003 ajout références aux bulletins de Mandrake et Debian.
07 février 2003 ajout référence au bulletin de Red Hat.