Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 février 2006
N° CERTA-2006-AVI-087

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Xpdf et ses dérivés

Gestion du document

Référence	CERTA-2006-AVI-087
Titre	Vulnérabilité de Xpdf et ses dérivés
Date de la première version	22 février 2006
Date de la dernière version	–
Source(s)	Bulletin d'erreurs du site Novell
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 à distance.

2 Systèmes affectés

Toutes les versions `xpdf`, ainsi que ses dérivés, comme `poppler`, `kdegraphics`, `gpdf` ou `pdfkit.framework`.

3 Description

Un dépassement de tampon dans le fichier `Splash.cc` peut laisser un utilisateur malveillant exécuter du code arbitraire. Il lui suffit de créer un document pdf contenant une image splash de taille anormalement grande.

4 Solution

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

5 Documentation

- Bulletin de sécurité Debian DSA 971 du 14 février 2006 :
  http://www.debian.org/security/2006/dsa-971
- Bulletin de sécurité Debian DSA 972 du 15 février 2006 :
  http://www.debian.org/security/2006/dsa-972
- Bulletin de sécurité Debian DSA 974 du 15 février 2006 :
  http://www.debian.org/security/2006/dsa-974
- Bulletin de sécurité Gentoo GLSA-200602-04 du 12 février 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200602-04.xml
- Bulletin de sécurité Gentoo GLSA-200602-05 du 12 février 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200602-05.xml
- Bulletin de sécurité Mandriva MDKSA-2006:030 du 2 février 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:030
- Bulletin de sécurité Mandriva MDKSA-2006:031 du 2 février 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:031
- Bulletin de sécurité Mandriva MDKSA-2006:032 du 2 février 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:032
- Bulletin de sécurité RedHat RHSA-2006:0201 du 13 février 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0201.html
- Bulletin de sécurité RedHat RHSA-2006:0206 du 13 février 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0206.html
- Bulletin de sécurité Ubuntu USN-249-1 du 14 février 2006 :
  http://www.ubuntulinux.org/usn/usn-249-1
- Référence CVE CVE-2006-0301 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0301

Gestion détaillée du document

22 février 2006 version initiale.