Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 février 2005
N° CERTA-2005-AVI-019-007

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Xpdf

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-2005-AVI-019

Gestion du document

Référence	CERTA-2005-AVI-019-007
Titre	Vulnérabilité dans Xpdf
Date de la première version	20 janvier 2005
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité iDefense du 18 janvier 2005
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

Lecteur de documents au format PDF (`Portable Document Format`) `Xpdf` version 3.00.

D'autres applications utilisant le code de `Xpdf` peuvent également être affectées (`cups`, `gpdf`, `pdftohtml`, `kpdf`, `KOffice`, ...).

3 Résumé

Une vulnérabilité du lecteur `Xpdf` permet l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire a été découverte dans la fonction `Decrypt::makeFileKey2`.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité par le biais d'un document au format PDF habilement construit. Il est alors possible d'exécuter du code arbitraire à distance avec les privilèges de l'utilisateur ayant lancé le lecteur `Xpdf`.

5 Solution

Mettre à jour le lecteur `Xpdf` (cf. section Documentation).

6 Documentation

- Site Internet du lecteur `Xpdf` :
  http://www.foolabs.com/xpdf/
- Correctif pour le lecteur `Xpdf` :
  ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch
- Bulletin de sécurité de iDefense du 18 janvier 2005 :
  http://www.idefense.com/application/poi/display?id=186&type=vulnerabilities
- Correctifs de sécurité pour Fedora Core 2 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
- Correctifs de sécurité pour Fedora Core 3 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/
- Bulletin de sécurité Debian DSA-645 du 19 janvier 2005 :
  http://www.debian.org/security/2005/dsa-645
- Bulletin de sécurité Debian DSA-648 du 19 janvier 2005 :
  http://www.debian.org/security/2005/dsa-648
- Bulletin de sécurité KDE pour kpdf du 19 janvier 2005 :
  http://www.kde.org/info/security/advisory-20050119-1.txt
- Bulletin de sécurité KDE pour KOffice du 20 janvier 2005 :
  http://www.kde.org/info/security/advisory-20050120-1.txt
- Bulletin de sécurité Mandrake MDKSA-2005:016 du 25 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:016
- Bulletin de sécurité Mandrake MDKSA-2005:017 du 25 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:017
- Bulletin de sécurité Mandrake MDKSA-2005:018 du 25 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:018
- Bulletin de sécurité Mandrake MDKSA-2005:019 du 25 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:019
- Bulletin de sécurité Mandrake MDKSA-2005:020 du 25 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:020
- Bulletin de sécurité Mandrake MDKSA-2005:021 du 25 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:021
- Bulletin de sécurité RedHat RHSA-2005:059 du 26 janvier 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-059.html
- Bulletin de sécurité RedHat RHSA-2005:049 du 01 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-049.html
- Bulletin de sécurité RedHat RHSA-2005:034 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-034.html
- Bulletin de sécurité RedHat RHSA-2005:053 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-053.html
- Bulletin de sécurité RedHat RHSA-2005:057 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-057.html
- Bulletin de sécurité RedHat RHSA-2005:066 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-066.html

- Bulletin de sécurité Gentoo GLSA 200501-28 du 21 janvier 2005 : http://www.gentoo.org/security/en/glsa/glsa-200501-28.xml
- Bulletin de sécurité Gentoo GLSA 200502-10 du 09 février 2005 : http://www.gentoo.org/security/en/glsa/glsa-200502-10.xml
- Bulletin de sécurité SGI 20050201-01-U du 02 février 2005 : ftp://patches.sgi.com/support/free/security/advisories/20050201-01-U.asc
- Bulletin de sécurité SGI 20050202-01-U du 09 février 2005 : ftp://patches.sgi.com/support/free/security/advisories/20050202-01-U.asc
- Référence CVE CAN-2005-0064 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0064

Gestion détaillée du document

20 janvier 2005 version initiale.

24 janvier 2005 ajout des autres applications vulnérables et des références aux bulletins de sécurité Fedora et KDE.

27 janvier 2005 ajout des références aux bulletins de sécurité Mandrake.

01 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:059.

02 février 2005 ajout des références aux bulletins de sécurité RedHat RHSA-2005:049, Debian DSA-645 et Debian DSA-648.

10 février 2005 ajout des références aux bulletins de sécurité Gentoo GLSA 200501-28 et GLSA 200502-10.

14 février 2005 ajout des références aux bulletins de sécurité SGI 20050201-01-U et 20050202-01-U.

17 février 2005 ajout des références aux bulletins de sécurité RedHat.