Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 février 2006
N° CERTA-2005-AVI-483-009

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées

Gestion du document

Référence	CERTA-2005-AVI-483-009
Titre	Multiples vulnérabilités dans Xpdf et les bibliothèques dérivées
Date de la première version	08 décembre 2005
Date de la dernière version	1er février 2006
Source(s)	Bulletins de sécurité iDefense du 05 décembre 2005 Bulletin de sécurité CESA-2005-003 du 06 janvier 2006
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, potentiellement à distance ;
- déni de service.

2 Systèmes affectés

Tout système (Unix, Microsoft DOS/Windows) utilisant `Xpdf`, jusqu'à la version 3.01, (ou `kpdf`, `gpdf`) comme lecteur de document `PDF` (voire une liste plus étendue dans la section description).

Par ailleurs le service d'impression Unix `CUPS` est également touché via son convertisseur `PDF` vers `Postscript`.

3 Résumé

Un utilisateur mal intentionné peut transmettre à sa victime un document `PDF` volontairement mal formé dans le but de provoquer une erreur fatale dans le code du lecteur utilisé voire d'exécuter du code arbitraire.

Le problème peut être étendu à l'impression d'un document `PDF` par le service d'impression `CUPS`.

4 Description

Quatre vulnérabilités ont été identifiées par IDefense dans le code source de `Xpdf`. Elles permettent de générer des allocations mémoires trop petites par rapport aux données qui y sont placées. Cela provoque généralement un arrêt brutal du programme voire l'exécution de code.

Par ailleurs, cinq nouvelles vulnérabilités proches (problèmes sur le décodage du format) ont été publiées début janvier 2006.

Parmi les applications affectées on peut identifier :

- Les lecteurs `gpdf` et `kpdf`,
- la distribution LaTeX `teTeX`,
- le convertisseur `pdftohmtl` et celui du traitement de texte `KWord`,
- la bibliothèque `poppler`,
- le service d'impression `CUPS`.

5 Solution

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

6 Documentation

- Site internet du lecteur `Xpdf` :
  http://www.foolabs.com/xpdf/
- Correctif pour les sources du lecteur `Xpdf` (ne corrige que les 4 failles identifiées par iDefense) :
  ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.01pl1.patch
- Mise à jour de sécurité Fedora Core 3 FEDORA-2005-1121 du 06 décembre 2005 pour `Xpdf` :
  http://www.redhat.com/archives/fedora-announce-list/2005-December/msg00010.html
- Mise à jour de sécurité Fedora Core 3 FEDORA-2005-1125 du 07 décembre 2005 pour `gpdf` :
  http://www.redhat.com/archives/fedora-announce-list/2005-December/msg00014.html
- Mise à jour de sécurité Fedora Core 3 FEDORA-2005-1127 du 07 décembre 2005 pour `tetex` :
  http://www.redhat.com/archives/fedora-announce-list/2005-December/msg00016.html
- Mise à jour de sécurité Fedora Core 4 FEDORA-2005-1126 du 07 décembre 2005 pour `tetex` :
  http://www.redhat.com/archives/fedora-announce-list/2005-December/msg00015.html
- Mise à jour de sécurité Fedora Core 3 FEDORA-2005-000 du 05 janvier 2006 pour `cups` :
  http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00011.html
- Mise à jour de sécurité Fedora Core 4 FEDORA-2005-000 du 05 janvier 2006 pour `cups` :
  http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00010.html
- Mise à jour de sécurité Fedora Core 4 FEDORA-2005-026 du 10 janvier 2006 pour `poppler` :
  http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00031.html
- Mise à jour de sécurité Fedora Core 4 FEDORA-2005-027 du 11 janvier 2006 pour `xpdf` :
  http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00033.html
- Mise à jour de sécurité Fedora Core 4 FEDORA-2005-028 du 12 janvier 2006 pour `tetex` :
  http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00035.html
- Mise à jour de sécurité Fedora Core 3 FEDORA-2005-029 du 12 janvier 2006 pour `tetex` :
  http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00036.html
- Mise à jour de sécurité Fedora Core 4 FEDORA-2005-037 du 16 janvier 2006 pour `kdegraphics` :
  http://www.redhat.com/archives/fedora-announce-list/2006-January/msg00043.html
- Bulletin de sécurité Debian DSA-931 du 09 janvier 2006 pour `xpdf` :
  http://www.debian.org/security/2006/DSA-931
- Bulletin de sécurité Debian DSA-932 du 09 janvier 2006 pour `kdegraphics` :
  http://www.debian.org/security/2006/DSA-932
- Bulletin de sécurité Debian DSA-936 du 09 janvier 2006 pour `libextractor` :
  http://www.debian.org/security/2006/DSA-936

- Bulletin de sécurité Debian DSA-937 du 12 janvier 2006 pour `tetex-bin` :
  http://www.debian.org/security/2006/DSA-937
- Bulletin de sécurité Debian DSA-938 du 12 janvier 2006 pour `koffice` :
  http://www.debian.org/security/2006/DSA-938
- Bulletin de sécurité Debian DSA-940 du 13 janvier 2006 pour `gpdf` :
  http://www.debian.org/security/2006/DSA-940
- Bulletin de sécurité Debian DSA-950 du 23 janvier 2006 pour `cupsys` :
  http://www.debian.org/security/2006/DSA-950
- Bulletin de sécurité Debian DSA-961 du 01 février 2006 pour `pdfkit.framework` :
  http://www.debian.org/security/2006/DSA-961
- Bulletin de sécurité Debian DSA-962 du 01 février 2006 pour `pdftohtml` :
  http://www.debian.org/security/2006/DSA-962
- Bulletin de sécurité Mandriva MDKSA-2006:003 du 05 janvier 2006 pour `poppler` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:003
- Bulletin de sécurité Mandriva MDKSA-2006:004 du 05 janvier 2006 pour `pdftohtml` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:004
- Bulletin de sécurité Mandriva MDKSA-2006:005 du 05 janvier 2006 pour `xpdf` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:005
- Bulletin de sécurité Mandriva MDKSA-2006:006 du 05 janvier 2006 pour `gpdf` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:006
- Bulletin de sécurité Mandriva MDKSA-2006:008 du 05 janvier 2006 pour `koffice` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:008
- Bulletin de sécurité Mandriva MDKSA-2006:010 du 10 janvier 2006 pour `cups` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:010
- Bulletin de sécurité Mandriva MDKSA-2006:011 du 10 janvier 2006 pour `tetex` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:011
- Bulletin de sécurité Mandriva MDKSA-2006:012 du 12 janvier 2006 pour `kdegraphics` :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:012
- Bulletin de sécurité RedHat RHSA-2005:840 du 06 décembre 2005 pour `xpdf` :
  http://rhn.redhat.com/errata/RHSA-2005-840.html
- Bulletin de sécurité RedHat RHSA-2005:868 du 20 décembre 2005 pour `kdegraphics` :
  http://rhn.redhat.com/errata/RHSA-2005-868.html
- Bulletin de sécurité RedHat RHSA-2006:0160 du 19 janvier 2006 pour `tetex` :
  http://rhn.redhat.com/errata/RHSA-2006-0160.html
- Bulletin de sécurité RedHat RHSA-2006:0163 du 11 janvier 2006 pour `CUPS` :
  http://rhn.redhat.com/errata/RHSA-2006-0163.html
- Bulletin de sécurité RedHat RHSA-2006:0177 du 11 janvier 2006 pour `gpdf` :
  http://rhn.redhat.com/errata/RHSA-2006-0177.html
- Bulletin de sécurité Gentoo GLSA 200512-08 du 16 décembre 2006 pour `cups` :
  http://www.gentoo.org/security/en/glsa/glsa-200512-08.xml
- Bulletin de sécurité Gentoo GLSA 200601-02 du 04 janvier 2006 pour `kdegraphics`, `kpdf`, `koffice` et `kword` :
  http://www.gentoo.org/security/en/glsa/glsa-200601-02.xml
- Bulletin de sécurité Gentoo GLSA 200601-17 du 30 janvier 2006 pour `xpdf`, `gpdf`, `poppler`, `libextractor`, `pdftohtml` :
  http://www.gentoo.org/security/en/glsa/glsa-200601-17.xml
- Bulletin de sécurité Ubuntu USN-236-1 du 05 janvier 2006 pour `cupsys`, `xpdf`, `poppler` et `tetex-bin` :
  http://ubuntu.com/usn/usn-236-1
- Bulletin de sécurité Ubuntu USN-236-2 du 09 janvier 2006 pour `koffice` et `kdegraphics` :
  http://ubuntu.com/usn/usn-236-2
- Bulletin de sécurité SUSE SUSE-SA:2006:001 du 11 janvier 2006 pour `xpdf`, `gpdf`, `kpdf` et `kword` :
  http://lists.suse.com/archive/suse-security-announce/2006-Jan/0001.html

- Bulletin de sécurité iDefense du 05 décembre 2005 : http://www.idefense.com/application/poi/display?id=342
- Bulletin de sécurité iDefense du 05 décembre 2005 : http://www.idefense.com/application/poi/display?id=343
- Bulletin de sécurité iDefense du 05 décembre 2005 : http://www.idefense.com/application/poi/display?id=344
- Bulletin de sécurité iDefense du 05 décembre 2005 : http://www.idefense.com/application/poi/display?id=345
- Bulletin de sécurité cd Chris Evans du 06 janvier 2006 : http://scary.beasts.org/security/CESA-2005-003.txt
- Référence CVE CAN-2005-3191 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3191
- Référence CVE CAN-2005-3192 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3192
- Référence CVE CAN-2005-3193 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3193
- Référence CVE CAN-2005-3624 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3624
- Référence CVE CAN-2005-3625 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3625
- Référence CVE CAN-2005-3626 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3626
- Référence CVE CAN-2005-3627 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3627
- Référence CVE CAN-2005-3628 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3628

Gestion détaillée du document

08 décembre 2005 version initiale.

21 décembre 2005 ajout des références aux bulletins de sécurité Gentoo GLSA 200512-08, RedHat RHSA-2005:867, RedHat RHSA-2005:868 et RedHat RHSA-2005:878.

05 janvier 2006 ajout de la référence au bulletin de sécurité Gentoo GLSA 200601-02.

09 janvier 2006 ajout des références aux bulletins de sécurité Mandriva.

10 janvier 2006 ajout des références aux bulletins de sécurité Debian.

12 janvier 2006 remplacement de l'avis Fedora FEDORA-2005-1122 par l'avis FEDORA-2005-027 du 11 janvier 2006, remplacement des avis RedHat RHSA-2005-867 et RHSA-2005-878 par respectivement les avis RHSA-2006-0163 et RHSA-2006-0177 du 11 janvier 2006 ; ajout des avis Ubuntu USN-236-1 et USN-236-2, SuSE SUSE-SA:2006:001, Mandriva MDKSA-2006:010 et MDKSA-2006:011, Debian DSA-936 et DSA-937, des références CVE CAN-2005-3624 à CAN-2005-3628 et du bulletin sécurité de Chris Evans.

13 janvier 2006 ajout des références aux bulletins de sécurité Debian DSA-938, DSA-940 et Mandriva MDKSA-2006:012.

20 janvier 2006 ajout de la référence au bulletin de sécurité RedHat RHSA-2006:0160.

23 janvier 2006 ajout de la référence au bulletin de sécurité Debian DSA-950.

1er févier 2006 remplacement partiel de l'avis GLSA 200512-08 par l'avis GLSA 200601-17, ajout des références aux avis Debian DSA-961 et DSA-962 et des avis Fedora FEDORA-2005-028, FEDORA-2005-029 et FEDORA-2005-037.