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-2004-AVI-357-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du lecteur PDF xpdf et de ses dérivés et du service d'impression CUPS

Gestion du document

Référence	CERTA-2004-AVI-357-003
Titre	Vulnérabilités du lecteur PDF xpdf et de ses dérivés et du service d'impression CUPS
Date de la première version	22 octobre 2004
Date de la dernière version	17 février 2005
Source(s)	–
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 à distance.

2 Systèmes affectés

- Tout système (Unix, Microsoft DOS/Windows) utilisant *xpdf* versions 2 jusqu'à 3.0 (ou des versions dérivées telles Gnome *gpdf* ou KDE *kpdf*) comme lecteur de documents PDF ;
- tout système Unix utilisant le service d'impression CUPS (pour les sources jusqu'à la version 1.1.22rc2).

3 Résumé

Plusieurs failles ont été identifiées dans *xpdf*. Elles permettent à un individu mal intentionné, via un document PDF habilement construit, d'exécuter du code arbitraire avec les privilèges de l'utilisateur.

Ces failles affectent les produits qui reprennent du code de *xpdf*, en particulier les lecteurs *gdf*, *kpdf* et le service d'impression CUPS ("Common Unix Printing System").

4 Description

Les lecteurs *xpdf* depuis la version 2.0 jusqu'à la version 3.0 comportent plusieurs débordements d'entiers (références CVE CAN-2004-0888 et CAN-2004-0889). Ils peuvent alors être utilisés pour exécuter du code arbitraire avec les privilèges de l'utilisateur consultant un document PDF volontairement mal construit.

CUPS est un service d'impression disponible sur de nombreux systèmes Unix. Il est souvent accessible par le réseau à l'aide du protocole IPP ("Internet Printing Protocol") sur le port 631/tcp. Un utilisateur distant mal intentionné peut alors lui soumettre un document PDF habilement construit qui provoquera l'exécution de code avec les privilèges du service (généralement l'utilisateur *lp*).

5 Solution

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

6 Documentation

- Site Internet de xpdf :
  http://www.foolabs.com/xpdf/
- Site Internet de CUPS :
  http://www.cups.org
- Bulletin de sécurité Debian :
  - CUPS, DSA-573 du 21 octobre 2004 :
    http://www.debian.org/security/2004/dsa-573
- Bulletins de sécurité Mandrake :
  - *xpdf*, MDKSA-2004:113 du 21 octobre 2004 :
    http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:113
  - *gpdf*, MDKSA-2004:114 du 21 octobre 2004 :
    http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:114
  - *kdegraphics* (*kpdf*), MDKSA-2004:115 du 21 octobre 2004 :
    http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:115
  - CUPS, MDKSA-2004:116 du 21 octobre 2004 :
    http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:116
- Bulletin de sécurité Gentoo GLSA 200410-20 du 21 octobre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200410-20.xml
- Bulletin de sécurité RedHat RHSA-2004:543 du 22 octobre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-543.html
- Bulletin de sécurité RedHat RHSA-2004:592 du 27 octobre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-592.html
- Bulletin de sécurité RedHat RHSA-2005:066 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-066.html
- Bulletin de sécurité SUSE SUSE-SA:2004:039 du 26 octobre 2004 :
  http://www.suse.com/de/security/2004_39_pdftools_cups.html
- Bulletin de sécurité FreeBSD pour xpdf du 25 octobre 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité OpenBSD pour xpdf du 23 octobre 2004 :
  http://www.vuxml.org/openbsd/
- Mise à jour de sécurité du paquetage NetBSD xpdf :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/print/xpdf/README.html
- Bulletin de sécurité Debian DSA-599 du 25 novembre 2004 :
  http://www.debian.org/security/2004/dsa-599
- Référence CVE CAN-2004-0888 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0888
- Référence CVE CAN-2004-0889 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0889

Gestion détaillée du document

22 octobre 2004 version initiale.

25 novembre 2004 ajout des références aux bulletins de sécurité Gentoo, RedHat, SUSE, FreeBSD, OpenBSD et NetBSD.

26 novembre 2004 ajout de la référence au bulletin de sécurité Debian.

17 février 2004 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:066.