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 août 2007
N° CERTA-2007-AVI-341-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans gpdf

Gestion du document

Référence	CERTA-2007-AVI-341-002
Titre	Vulnérabilité dans gpdf et dérivés
Date de la première version	01 août 2007
Date de la dernière version	22 août 2007
Source(s)	CVE-2007-3387
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

- *gpdf* versions antérieures à 2.8.2 ;
- applications dérivées ou utilisatrices, telles *CUPS*, *kdegraphics*, *Xpdf*, *poppler*.

Cette liste d'applications n'est pas limitative.

3 Résumé

Un utilisateur malveillant pourrait, par le biais d'un document au format PDF spécialement conçu, exécuter du code arbitraire à distance.

4 Description

Dans la fonction `StreamPredictor::StreamPredictor` de *gpdf*, il est possible de provoquer un débordement d'entier. Ce problème permettrait à un utilisateur malveillant, par le biais d'un document au format PDF spécialement conçu, d'exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Mandriva MDKSA-2007:165 du 15 août 2007 : http://www.mandriva.com/security/advisories?name=MDKSA-2007:165
- Bulletin de sécurité Mandriva MDKSA-2007:164 du 14 août 2007 : http://www.mandriva.com/security/advisories?name=MDKSA-2007:164
- Bulletin de sécurité Mandriva MDKSA-2007:163 du 14 août 2007 : http://www.mandriva.com/security/advisories?name=MDKSA-2007:163
- Bulletin de sécurité Mandriva MDKSA-2007:162 du 14 août 2007 : http://www.mandriva.com/security/advisories?name=MDKSA-2007:162
- Bulletin de sécurité Mandriva MDKSA-2007:161 du 13 août 2007 : http://www.mandriva.com/security/advisories?name=MDKSA-2007:161
- Bulletin de sécurité Mandriva MDKSA-2007:160 du 13 août 2007 : http://www.mandriva.com/security/advisories?name=MDKSA-2007:160
- Bulletin de sécurité Mandriva MDKSA-2007:158 du 13 août 2007 : http://www.mandriva.com/security/advisories?name=MDKSA-2007:158
- Bulletin de sécurité RedHatKDE du 30 juillet 2007 : http://www.kde.org/info/security/advisory-20070730-1.txt
- Bulletin de sécurité RedHat RHSA-2007:0720 du 30 juillet 2007 : http://rhn.redhat.com/errata/RHSA-2007-0720.html
- Bulletin de sécurité RedHat RHSA-2007:0729 du 30 juillet 2007 : http://rhn.redhat.com/errata/RHSA-2007-0729.html
- Bulletin de sécurité RedHat RHSA-2007:0730 du 30 juillet 2007 : http://rhn.redhat.com/errata/RHSA-2007-0730.html
- Bulletin de sécurité RedHat RHSA-2007:0731 du 01 août 2007 : http://rhn.redhat.com/errata/RHSA-2007-0731.html
- Bulletin de sécurité RedHat RHSA-2007:0732 du 30 juillet 2007 : http://rhn.redhat.com/errata/RHSA-2007-0732.html
- Bulletin de sécurité RedHat RHSA-2007:0735 du 30 juillet 2007 : http://rhn.redhat.com/errata/RHSA-2007-0732.html
- Bulletin de sécurité Debian DSA-1357 du 19 août 2007 : http://www.debian.org/security/2007/dsa-1357
- Bulletin de sécurité Debian DSA-1355 du 13 août 2007 : http://www.debian.org/security/2007/dsa-1355
- Bulletin de sécurité Debian DSA-1354 du 13 août 2007 : http://www.debian.org/security/2007/dsa-1354
- Bulletin de sécurité Debian DSA-1352 du 07 août 2007 : http://www.debian.org/security/2007/dsa-1352
- Bulletin de sécurité Debian DSA-1350 du 06 août 2007 : http://www.debian.org/security/2007/dsa-1350
- Bulletin de sécurité Debian DSA-1349 du 04 août 2007 : http://www.debian.org/security/2007/dsa-1349

- Bulletin de sécurité Debian DSA-1348 du 04 août 2007 :
  http://www.debian.org/security/2007/dsa-1348
- Bulletin de sécurité Debian DSA-1347 du 04 août 2007 :
  http://www.debian.org/security/2007/dsa-1347
- Bulletin de sécurité Ubuntu USN-496-2 du 07 août 2007 :
  http://www.ubuntu.com/usn/usn-496-2
- Bulletin de sécurité Ubuntu USN-496-1 du 07 août 2007 :
  http://www.ubuntu.com/usn/usn-496-1
- Bulletin de sécurité SuSE SUSE-SR:2007:016 du 10 août 2007 :
  http://www.novell.com/linux/security/advisories/2007_16_sr.html
- Bulletin de sécurité SuSE SUSE-SR:2007:015 du 03 août 2007 :
  http://lists.opensuse.org/opensuse-security-announce/2007-08/msg00003.html
- Référence CVE CVE-2007-3387 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3387

Gestion détaillée du document

01 août 2007 version initiale.
16 août 2007 ajout des références aux bulletins de sécurité Mandriva, Debian, SuSE, Red Hat.
22 août 2007 ajout de la référence au bulletin de sécurité Debian.