



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 novembre 2007
N° CERTA-2007-AVI-484-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans gpdf et produits dérivés

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-2007-AVI-484>

Gestion du document

Référence	CERTA-2007-AVI-484-001
Titre	Multiples vulnérabilités dans gpdf et produits dérivés
Date de la première version	08 novembre 2007
Date de la dernière version	09 novembre 2007
Source(s)	Bulletin de sécurité Secunia 27260 du 07 novembre 2007
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.

2 Systèmes affectés

- Gnome gpdf ;
- Poppler ;
- CUPS ;
- KDE, au moins les versions 3.2.0 à 3.5.8;
- KOffice 1.x ;
- Xpdf version 3.02.

3 Résumé

De multiples vulnérabilités dans Xpdf permettent à un individu malveillant l'exécution de code arbitraire en local.

Ces vulnérabilités affectent les produits utilisant la même souche logicielle.

4 Description

De multiples vulnérabilités dans le script *Stream.cc* de *Xpdf* permettent à un individu malveillant l'exécution de code arbitraire en local via un fichier pdf spécialement conçu.

Ces vulnérabilités affectent les produits utilisant la même souche logicielle.

5 Solution

Se référer aux sites des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin KDE du 07 novembre 2007 :
<http://www.kde.org/info/security/advisory-20071107-1.txt>
- Bulletin de sécurité Redhat 1021-3 du 07 novembre 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-1021.html>
- Bulletin de sécurité Redhat 1022-2 du 07 novembre 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-1022.html>
- Bulletin de sécurité Redhat 1025-5 du 07 novembre 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-1025.html>
- Bulletin de sécurité Redhat 1026-3 du 07 novembre 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-1026.html>
- Bulletin de sécurité Secunia numéro 27260 du 07 novembre 2007 :
<http://secunia.com/advisories/27260/>
- Rustine Xpdf :
<ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.02pl2.patch>
- Référence CVE CVE-2007-4352 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4352>
- Référence CVE CVE-2007-5392 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5392>
- Référence CVE CVE-2007-5393 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5393>

Gestion détaillée du document

08 novembre 2007 version initiale.

09 novembre 2007 ajouts des produits associés.