



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 07 avril 2010  
N° CERTA-2009-AVI-448-003

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Xpdf et 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-2009-AVI-448>

---

### Gestion du document

Référence	CERTA-2009-AVI-448-003
Titre	Vulnérabilités dans Xpdf et dérivés
Date de la première version	16 octobre 2009
Date de la dernière version	07 avril 2010
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

## 2 Systèmes affectés

Compte tenu de la réutilisation de fragments de code source, la liste suivante n'est pas exhaustive.

- Xpdf 3.x ;
- gpdf (GNOME 2.x) ;
- KPDF (KDE 3.x) ;
- CUPS 1.x ;
- Poppler 0.x.

## 3 Résumé

Plusieurs vulnérabilités dans Xpdf et dans des applications qui en reprennent le code source permettent à un utilisateur malveillant de réaliser un déni de service, voire d'exécuter du code arbitraire, à distance.

## 4 Description

Plusieurs débordements d'entier dans Xpdf permettent à un utilisateur malveillant de provoquer un débordement du tas (*heap*). L'exploitation de cette vulnérabilité permet de provoquer un arrêt inopiné du logiciel ou d'exécuter du code arbitraire en incitant un utilisateur à ouvrir ou à imprimer un fichier au format PDF spécialement conçu.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Debian DSA-1941 du 25 novembre 2009 :  
<http://www.debian.org/security/2009/dsa-1941>
- Bulletin de sécurité Debian DSA-2028 du 05 avril 2010 :  
<http://www.debian.org/security/2010/dsa-2028>
- Bulletins de sécurité RedHat RHSA-2009:1500 et suivants du 15 octobre 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-1500.html>  
<http://rhn.redhat.com/errata/RHSA-2009-1501.html>  
<http://rhn.redhat.com/errata/RHSA-2009-1502.html>  
<http://rhn.redhat.com/errata/RHSA-2009-1503.html>  
<http://rhn.redhat.com/errata/RHSA-2009-1504.html>  
<http://rhn.redhat.com/errata/RHSA-2009-1512.html>  
<http://rhn.redhat.com/errata/RHSA-2009-1513.html>
- Bulletins de sécurité RedHat RHSA-2009:1083 du 03 juin 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-1083.html>
- Bulletins de sécurité RedHat RHSA-2009:0480 du 13 mai 2009 :  
<http://rhn.redhat.com/errata/RHSA-2009-0480.html>
- Bulletins de sécurité Ubuntu USN-759-1 du 16 avril 2009 :  
<http://www.ubuntu.com/usn/usn-759-1>
- Bulletins de sécurité SuSE SUSE-SR:2009:018 du 10 novembre 2009 :  
<http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00004.html>
- Bulletins de sécurité SuSE SUSE-SR:2009:012 du 03 juillet 2009 :  
<http://lists.opensuse.org/opensuse-security-announce/2009-07/msg00002.html>
- Bulletin Oracle Solaris #6904352 du 25 février 2010 :  
<http://sunsolve.sun.com/search/assetkey=1-66-274030-1>
- Référence CVE CVE-2009-0755 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0755>
- Référence CVE CVE-2009-0791 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0791>
- Référence CVE CVE-2009-1188 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1188>
- Référence CVE CVE-2009-3603 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3603>
- Référence CVE CVE-2009-3604 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3604>
- Référence CVE CVE-2009-3606 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3606>
- Référence CVE CVE-2009-3607 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3607>
- Référence CVE CVE-2009-3608 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3608>

- Référence CVE CVE-2009-3609 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3609>
- Référence CVE CVE-2009-3938 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3938>

## **Gestion détaillée du document**

**16 octobre 2009** version initiale.

**27 novembre 2009** ajout des références CVE et des bulletins de sécurité Red Hat, SuSE, Ubuntu et Debian.

**01 mars 2010** ajout du bulletin de sécurité Oracle Solaris.

**07 avril 2010** ajout du bulletin de sécurité Debian pour Xpdf.