

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Xpdf

---

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-2010-AVI-479>

---

### Gestion du document

Référence	CERTA-2010-AVI-479-003
Titre	Vulnérabilités dans Xpdf
Date de la première version	08 octobre 2010
Date de la dernière version	20 octobre 2010
Source(s)	Avis de sécurité Red Hat RHSA-2010-0751 du 07 octobre 2010
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 à distance ;
- exécution de code arbitraire à distance .

## 2 Systèmes affectés

Xpdf dans différentes distributions Linux (cf. section Documentation).

## 3 Résumé

Deux vulnérabilités permettant à une personne distante malintentionnée de provoquer un déni de service ou d'exécuter du code arbitraire à distance ont été découvertes dans Xpdf et Poppler.

## 4 Description

Des vulnérabilités de type utilisation de pointeur non initialisé et de type débordement de mémoire ont été identifiées dans Xpdf. L'exploitation de ces vulnérabilités peut conduire à un déni de service à distance ou de l'exécution de code arbitraire à distance par le biais d'un fichier pdf spécialement construit.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité RedHat RHSA-2010:0749 du 07 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0749.html>
- Bulletin de sécurité RedHat RHSA-2010:0750 du 07 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0750.html>
- Bulletin de sécurité RedHat RHSA-2010:0751 du 07 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0751.html>
- Bulletin de sécurité RedHat RHSA-2010:0752 du 07 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0752.html>
- Bulletin de sécurité RedHat RHSA-2010:0753 du 07 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0753.html>
- Bulletin de sécurité RedHat RHSA-2010:0754 du 07 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0754.html>
- Bulletin de sécurité RedHat RHSA-2010:0755 du 07 octobre 2010 :  
<http://rhn.redhat.com/errata/RHSA-2010-0755.html>
- Avis de sécurité Debian DSA-2119-1 du 12 octobre 2010 :  
<http://debian.org/security/2010/dsa-2119>
- Avis de sécurité Ubuntu USN-1005-1 :  
<http://www.ubuntu.com/usn/usn-1005-1>
- Référence CVE CVE-2010-3702 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3702>
- Référence CVE CVE-2010-3704 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3704>

## Gestion détaillée du document

**08 octobre 2010** version initiale.

**13 octobre 2010** ajout des références aux bulletins de sécurité Red Hat.

**18 octobre 2010** ajout de la référence au bulletin de sécurité Debian.

**20 octobre 2010** ajout de la référence au bulletin de sécurité Ubuntu.