

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans libxml2

---

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-2008-AVI-465>

---

### Gestion du document

Référence	CERTA-2008-AVI-465-001
Titre	Vulnérabilité dans libxml2
Date de la première version	16 septembre 2008
Date de la dernière version	16 octobre 2008
Source(s)	Bulletin de sécurité Red Hat RHSA-2008-0884 du 11 septembre 2008 Bulletin de sécurité Red Hat RHSA-2008-0886 du 11 septembre 2008
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

libxml2 2.6.x.

## 3 Résumé

Une vulnérabilité dans libxml2 permet à une personne malintentionnée distante d'effectuer un déni de service voire d'exécuter du code arbitraire.

## 4 Description

Une vulnérabilité de type débordement de mémoire a été identifiée dans la fonction `xmlParseAttValueComplex` dans libxml2. Elle permet à une personne malintentionnée distante d'effectuer un déni de service voire d'exécuter du code arbitraire.

## 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-2008:0884 du 11 septembre 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0884.html>
- Bulletin de sécurité RedHat RHSA-2008:0886 du 11 septembre 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0886.html>
- Bulletin de sécurité Ubuntu USN-644-1 du 11 septembre 2008 :  
<http://www.ubuntu.com/usn/usn-644-1>
- Bulletin de sécurité Debian DSA-1654 du 14 octobre 2008 :  
<http://www.debian.org/security/2008/dsa-1654>
- Référence CVE CVE-2008-3529 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3529>

## Gestion détaillée du document

**16 septembre 2008** version initiale ;

**16 octobre 2008** ajout de la référence au bulletin Debian.