



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 20 novembre 2008  
N° CERTA-2008-AVI-562

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités de 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-562>

---

### Gestion du document

Référence	CERTA-2008-AVI-562
Titre	Vulnérabilités de Libxml2
Date de la première version	20 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité RedHat RHSA-2008:0988 du 17 novembre 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

- Déni de service à distance ;
- exécution de code à distance.

## 2 Systèmes affectés

Libxml2 2.x.

## 3 Résumé

Deux vulnérabilités de Libxml2 permettent à un utilisateur malveillant la réalisation d'un déni de service à distance ou d'exécuter du code arbitraire à distance.

## 4 Description

Une première vulnérabilité provient d'un débordement d'entier dans la fonction `xmlSAX2Characters()`. Elle est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance.

Une deuxième vulnérabilité, dans la fonction `xmlBufferResize()`, peut être exploitée pour provoquer une boucle infinie.

## 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-1666-1 du 17 novembre 2008 :  
<http://www.debian.org/security/2008/dsa-1666>
- Bulletin de sécurité sécurité Fedora 8 FEDORA-2008-9729 du 19 novembre 2008 :  
<https://www.redhat.com/archives/fedora-package-announce/2008-November/msg00472.html>
- Bulletin de sécurité sécurité Fedora 9 FEDORA-2008-9773 du 19 novembre 2008 :  
<https://www.redhat.com/archives/fedora-package-announce/2008-November/msg00513.html>
- Bulletin de sécurité RedHat RHSA-2008:0988 du 17 novembre 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0988.html>
- Bulletin de sécurité Ubuntu USN-673-1 du 19 novembre 2008 :  
<http://www.ubuntulinux.org/usn/usn-673-1>
- Référence CVE CVE-2008-4225 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4225>
- Référence CVE CVE-2008-4226 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4226>

## Gestion détaillée du document

**20 novembre 2008** version initiale.