



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 31 janvier 2012  
N° CERTA-2012-AVI-028-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans OpenSSL

---

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-2012-AVI-028>

---

### Gestion du document

Référence	CERTA-2012-AVI-028-001
Titre	Vulnérabilité dans OpenSSL
Date de la première version	20 janvier 2012
Date de la dernière version	31 janvier 2012
Source(s)	Bulletin de sécurité OpenSSL du 18 janvier 2012
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.

## 2 Systèmes affectés

- OpenSSL 1.0.0f;
- OpenSSL 0.9.8s.

## 3 Résumé

Une vulnérabilité a été corrigée dans OpenSSL et permet à un utilisateur malintentionné de provoquer un déni de service à distance.

## 4 Description

Une vulnérabilité a été corrigée dans OpenSSL. Elle permet à un utilisateur malintentionné de provoquer un déni de service à distance. Seules les applications utilisant le protocole *DTLS* sont affectées.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité OpenSSL du 18 janvier 2012 :  
[http://www.openssl.org/news/secadv\\_20120118.txt](http://www.openssl.org/news/secadv_20120118.txt)
- Bulletin de sécurité Debian du 23 janvier 2012 :  
<http://www.debian.org/security/2012/dsa-2392>
- Référence CVE CVE-2012-0050 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0050>

## Gestion détaillée du document

**20 janvier 2012** version initiale.

**31 janvier 2012** ajout du bulletin de sécurité Debian.