



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 30 juin 2009  
N° CERTA-2009-AVI-192-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités 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-2009-AVI-192>

---

### Gestion du document

Référence	CERTA-2009-AVI-192-001
Titre	Vulnérabilités dans OpenSSL
Date de la première version	19 mai 2009
Date de la dernière version	30 juin 2009
Source(s)	Bulletins de sécurité OpenSSL #1838, #1923, #1930 et #1931
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 0.9.x.

## 3 Résumé

Deux vulnérabilités découvertes dans OpenSSL permettent à un utilisateur distant malintentionné de provoquer un déni de service.

## 4 Description

Deux vulnérabilités causées par un manque de contrôle dans le traitement des enregistrements et messages de type DTLS (*Datagram Transport Layer Security*), peuvent être exploitées pour réaliser un déni de service par consommation de mémoire excessive.

## 5 Solution

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

## 6 Documentation

- Site Internet de l'éditeur OpenSSL :  
<http://www.openssl.org/>
- Bulletins de sécurité OpenSSL #1838, #1923, #1930 et #1931 :  
<http://rt.openssl.org/Ticket/Display.html?id=1838>  
<http://rt.openssl.org/Ticket/Display.html?id=1923>  
<http://rt.openssl.org/Ticket/Display.html?id=1930>  
<http://rt.openssl.org/Ticket/Display.html?id=1931>
- Référence CVE CVE-2009-1377 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1377>
- Référence CVE CVE-2009-1378 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1378>
- Référence CVE CVE-2009-1379 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1379>
- Référence CVE CVE-2009-1386 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1386>
- Référence CVE CVE-2009-1387 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1387>
- Bulletin de sécurité IBM du 29 juin 2009 :  
[http://aix.software.ibm.com/aix/efixes/security/ssl\\_advisory.asc](http://aix.software.ibm.com/aix/efixes/security/ssl_advisory.asc)
- Bulletin de sécurité Ubuntu USN-792-1 du 25 juin 2009 :  
<https://lists.ubuntu.com/archives/ubuntu-security-announce/2009-June/000923.html>

## Gestion détaillée du document

**19 mai 2009** version initiale.

**30 juin 2009** ajout des références aux bulletins de sécurités OpenSSL, IBM, Ubuntu et aux CVE.