

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de OpenSSL sous Debian

---

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-392>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2009-AVI-392  |
| Titre                       | Vulnérabilité de OpenSSL sous Debian                      |
| Date de la première version | 18 septembre 2009   |
| Date de la dernière version | –   |
| Source(s)                   | Bulletin de sécurité Debian DSA-1888 du 15 septembre 2009 |
| 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- Debian 4.0 ;
- Debian 5.0.

## 3 Résumé

Une vulnérabilité dans OpenSSL sous Debian permet à un utilisateur distant d'usurper un certificat arbitraire.

## 4 Description

La version d'OpenSSL mise en œuvre sous Debian autorise l'utilisation de certificats signés au moyen de condensats MD2. Or, l'algorithme MD2 est considéré comme non-sûr d'un point de vue cryptographique. De ce fait, il est possible à un utilisateur malintentionné d'usurper un certificat arbitraire qu'il aura signé en utilisant un condensat de ce type.

## **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 1888 du 15 septembre 2009 :  
<http://www.debian.org/security/2009/dsa-1888>
- Référence CVE CVE-2009-2409 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2409>

## **Gestion détaillée du document**

**18 septembre 2009** version initiale.